The Purple Book on Cyber Security

For
Sales, Pre-sales, & Delivery
BEGINNERS

Sudhansu M Nayak & OpenAI

Table of Contents

Preface

This book is intended to simplify cyber security as much as possible and help beginners, semi-technical, and non-technical practitioners with leading questions to field. To explain certain concepts, ideas have been stretched to normal real-life scenarios. Please do send in your thoughts and questions for us to make this more engaging.

The attempt to flatten the learning curve and build consensus among buyers, technology owners, and service providers guided us to structure the book into technology chapters. Each chapter has basics explained, a la what is the technology and how it helps, sales cue, pre-sales cue, and delivery cue.

Sales cue deals with what questions sales leaders can ask prospective clients to develop needs and use cases. Similarly, in this section, we have also dealt with what possible questions may a prospective client ask of the sales leader while exploring the use cases. And between the sales leaders and the prospective clients, what parameters can they agree on while finalising the terms and conditions of the sales transaction.

Pre-sales cue deals with what could be possible sizing guidelines or benchmarks for the technology, to which other systems can the solution connect with, steps of implementation of the solution, services levels parameters they can agree to, and where things can go wrong.

Delivery cue deals with daily, weekly, monthly operations activities, which level of capability (L1, L2, L3) can manage what activities, typical set of reports for the solution, and what factors can be looked at for a holistic governance of the solution.

This compilation is by no means the most exhaustive, but it aims to build enough thrust for beginners-to-cyber-security sales, pre-sales, and delivery personnel to move to the next level of expertise. With your continued support, we can augment this book easier to comprehend, manage the simplicity, and still address frequently asked questions in the market

OpenAI has been used to generate answers to frequently asked questions and where necessary, answers have been augmented by practical suggestions. Since OpenAI has been used, we have decided to make this book open and free to use.

While reading the book, if you see a text-portion in saffron italics (for example: *malware signatures*), it means the term has been explained in the next sub-section. If there are terms you want more explanation on, please do give us the feedback and we shall try and add them to the sections. Italic also shows new terms and some sample programs.

Hope you enjoy reading or referring to it more than we enjoyed compiling it.

1. Cybersecurity, Information Security- simple introductions

"A ship is safe in harbor, but that's not what ships are built for."

—John A. Shedd

Cyber refers to the digital world and all things related to technology and the internet. This includes online communication, computers, networks, and the security of these systems from unauthorized access and harm. In short, cyber refers to the virtual world and ensuring its safety.

So, cybersecurity is the practice of protecting computer systems, networks, and internet-connected devices from digital attacks, theft, and damage. This involves implementing various technologies, processes, and practices to secure sensitive information and prevent unauthorized access, hacking, and other cyber threats. The goal of cybersecurity is to keep the internet and connected devices safe and secure for individuals, businesses, and governments.

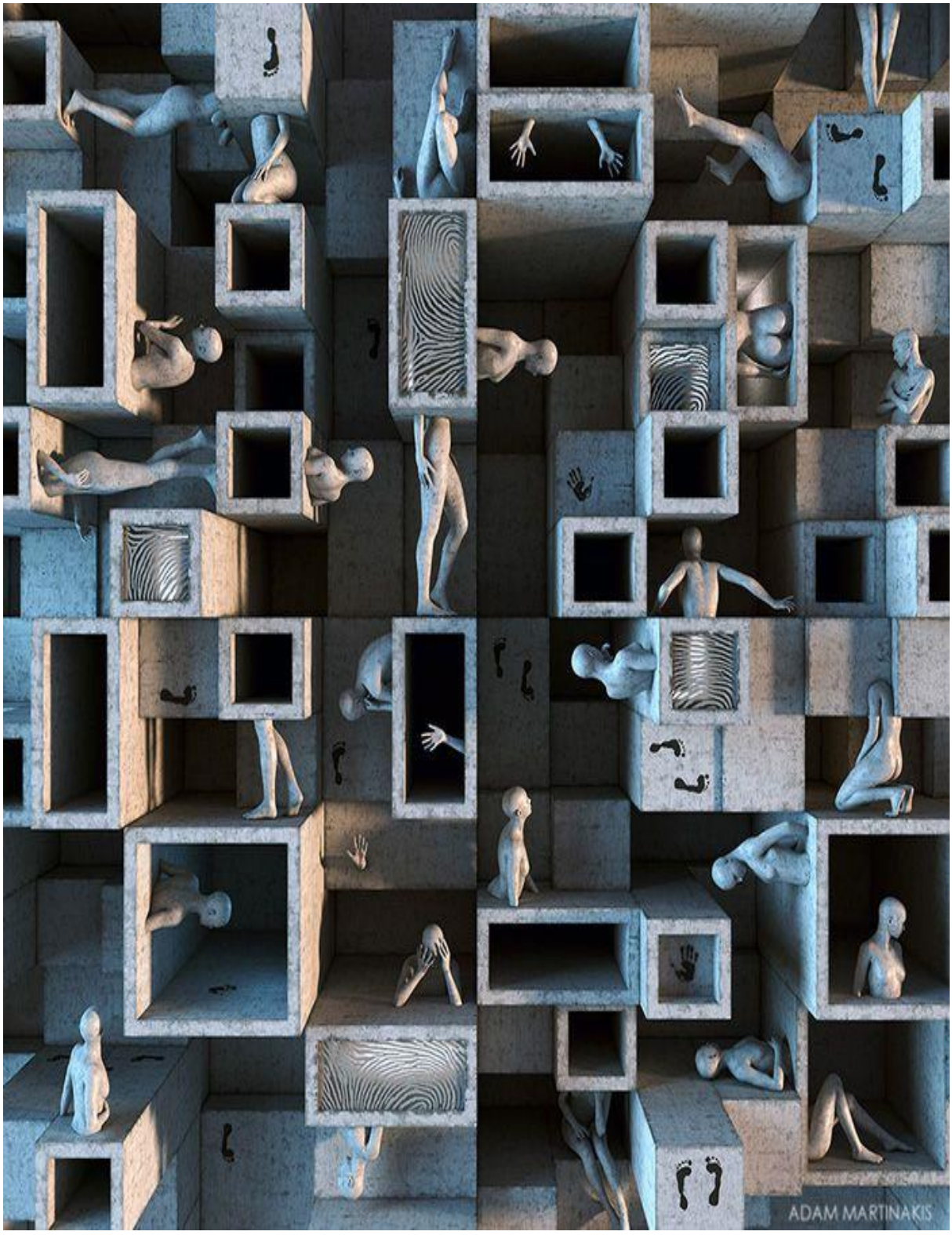
Information security and cybersecurity are closely related but slightly different concepts. Information security refers to the protection of information and data from unauthorized access, use, disclosure, disruption, modification, or destruction. This encompasses a wide range of practices and technologies, including access control, encryption, firewalls, and backup and recovery systems.

Information Security= Cyber + Physical

In short, information security is a broad term that encompasses all aspects of protecting information, while cybersecurity specifically focuses on the protection of digital systems and networks.

To make information security solutions precisely effective, clients focus on use cases. In the context of cybersecurity, a use case is a specific scenario or situation that describes how a security event or incident should be detected, investigated, and/or responded to by an organization's security operations team. A use case typically includes a set of rules, criteria, or thresholds that define what constitutes an abnormal or suspicious activity that requires further investigation or response.

Purple is commonly used in information security- purple from mixing red for offense and blue for defense. Purple Teaming is a collaborative process that combines the expertise and knowledge of both the "blue team" (defenders) and the "red team" (attackers) to improve an organization's cybersecurity defenses. The objective of Purple Teaming is to identify and close gaps in an organization's security posture, as well as to improve the effectiveness and efficiency of the overall security strategy. In a Purple Team engagement, the blue team provides the red team with access to its systems, tools, and processes, and then actively works with them to identify vulnerabilities, test defenses, and develop mitigation strategies. Through this collaboration, the blue team gains a better understanding of the organization's vulnerabilities, and the red team learns how to improve its attack methodologies. The Purple Teaming approach helps organizations to better prepare for real-world attacks and to continuously improve their security posture over time.



This brilliant creation is from Adam Martinakis. https://www.martinakis.com/

2. Endpoint Security- Antivirus Solution

Endpoint security is a branch of cybersecurity that focuses on protecting individual devices that connect to a network, such as

- computers,
- smartphones,
- tablets, and
- internet of things (IoT) devices.

The endpoint is the last line of defense against cyber threats, and the goal of endpoint security is to prevent these devices from becoming compromised and used to access sensitive information or launch attacks on the network.

Endpoint security typically involves a combination of hardware and software solutions, including antivirus software, firewalls, and encryption technologies. The objective of endpoint security is to protect the network by securing each endpoint and preventing the spread of malware and other cyber threats.

2.1 What is an Anti-virus solution?

An anti-virus (AV) solution is a type of software that is designed to prevent, detect, and remove malicious software, also known as malware, from a computer or network. Malware can include *viruses, trojans, worms, spyware*, and other types of malicious software that can cause harm to a computer or steal sensitive information.

An anti-virus solution typically works by continuously scanning a computer's files and incoming emails and network traffic for known *malware signatures*.

If malware is detected, the anti-virus software will either remove it or quarantine it to prevent it from spreading to other parts of the computer or network. Some anti-virus solutions also include additional security features, such as firewalls, intrusion detection and prevention systems, and real-time threat intelligence updates.

In short, an anti-virus solution is an essential tool in maintaining the security of a computer or network and protecting against the spread of malware.

2.1.1 What are viruses, trojans, worms, spyware?

A **virus** is a type of malware that infects a computer by attaching itself to other legitimate software. Once installed, a virus can spread to other parts of the computer and cause damage, such as corrupting files or slowing down the system.

A **trojan** is a type of malware that disguises itself as legitimate software and is used to gain unauthorized access to a computer. Trojans are often used by hackers to steal sensitive information, such as passwords and credit card numbers.

A **worm** is a type of malware that is designed to spread itself from one computer to another, often over a network. Unlike a virus, a worm does not need to attach itself to other software and can spread on its own.

Spyware is a type of malware that is used to collect information about a computer and its user, without their knowledge. Spyware can be used to track a user's internet activity, steal passwords, and gather other sensitive information.

2.1.2 What is a malware signature?

Malware signatures are a set of unique patterns or characteristics that are used to identify a specific type of malware. These signatures can include file names, code patterns, or other unique identifiers that are unique to each type of malware.

Anti-virus (AV) software uses malware signatures to detect and remove malware from a computer or network. When an AV software scans a computer or network, it compares the files and incoming data to its database of known malware signatures. If a match is found, the AV software can identify the type of malware and take the appropriate action, such as removing the malware or quarantining it.

Malware signatures are constantly updated by anti-virus vendors to keep up with new and evolving malware threats. This allows anti-virus software to stay current and effectively protect against the latest cyber threats.

In short, malware signatures are a key component of anti-virus software, allowing it to accurately identify and remove malware from a computer or network.

2.1.3 Anti-virus types

There are several types of anti-virus (AV) solutions, including:

1. **Traditional Anti-Virus:** This is the most basic type of anti-virus software and uses a database of malware signatures to detect and remove malware from a computer or network.
2. **Real-Time Anti-Virus:** This type of anti-virus software provides continuous protection by scanning incoming data and files in real-time, as well as regularly scanning the computer or network.
3. **Behaviour-Based Anti-Virus:** This type of anti-virus software looks for unusual behaviour on a computer or network, such as a file executing itself without the user's knowledge, to detect and remove malware.
4. **Cloud-Based Anti-Virus:** This type of anti-virus software uses the cloud to detect and remove malware, which allows for faster and more effective protection against cyber threats.
5. **Endpoint Anti-Virus:** This type of anti-virus software is designed specifically to protect individual devices that connect to a network, such as laptops, smartphones, and IoT devices.

In short, there are several different types of anti-virus solutions available, each with its own strengths and weaknesses. The type of anti-virus solution that is best for a particular organization will depend on its specific needs and requirements.

2.2 Sales cue- Questions to ask and answers to give

2.2.1 Questions to ask prospective client

To gain a better understanding of the prospective client's current security situation and identify potential areas where an anti-virus solution could provide additional protection, ask the following questions. These can help you determine if the prospective client has a genuine need for an anti-virus solution and how your solution can meet their specific requirements.

1. What types of devices does your organization use, and how are they connected to the internet and each other?
2. What types of data and information does your organization handle, and how is it stored and protected?
3. How often do your employees access sensitive information or use the internet while on the job?
4. What security measures are currently in place to protect against cyber threats, such as malware and hacking?
5. Have you experienced any security breaches or incidents in the past, and how were they handled?
6. What are your organization's regulations and compliance requirements regarding data security?

2.2.2 Questions prospective clients will ask of sales

Clients looking for an anti-virus solution may ask a variety of questions to determine if a particular solution will meet their needs. Some common questions include:

1. What types of threats does the solution protect against?
2. How does the solution detect and prevent malware?
3. What is the false positive rate of the solution?
4. How often are the virus definitions updated? Does the solution have a proven track record of protecting against the types of threats faced by the client's industry or organization?
5. Does the solution integrate with other security technologies, such as firewalls or intrusion detection systems?
6. How does the solution handle outbreak and rapidly evolving threats?
7. What kind of support and maintenance is included with the solution?
8. Does the solution require any special hardware or software to run?
9. How does the solution impact performance and system resources?
10. What is the cost of the solution and what payment options are available?

These are just a few examples of the types of questions that clients may ask when evaluating an anti-virus solution. The specific questions that are asked will depend on the client's needs, concerns, and requirements.

2.2.3 Payment terms to agree with the clients

All antivirus technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays antivirus technology owners via distributors) payment options with clients always keeps the cash-registers green and healthy.

For further reference, the payment terms for antivirus solutions can vary depending on the specific solution being offered. Some common payment options include:

1. Subscription-based: Many antivirus solutions are offered on a subscription basis, where clients pay a monthly or annual fee to access the solution and receive ongoing updates and support.
2. Per-device: Some antivirus solutions charge clients based on the number of devices that the solution is installed on. This can be a useful option for organizations that need to protect a large number of devices.
3. Per-user: Some antivirus solutions charge clients based on the number of users that the solution is protecting, rather than the number of devices.
4. One-time fee: Some antivirus solutions are sold as a one-time fee, with no ongoing subscription or maintenance costs.
5. Volume pricing: Some antivirus vendors offer volume pricing for clients that purchase large numbers of licenses, as an incentive to increase sales.

These are just a few examples of the types of payment options that are available for antivirus solutions. The specific payment terms will depend on the solution being offered. It's always recommended to carefully review the terms and conditions of an antivirus solution before making a purchase.

2.3 Pre-sales cue: Solution building complexities

2.3.1 Sizing the anti-virus solution

Sizing for an anti-virus solution involves determining the necessary resources and capacities required to effectively protect a computer or network from malware and other security threats. To do this, you will need to consider the following factors:

1. **Environment size**: The size of the environment, including the number of endpoints and servers, will impact the size and capacity requirements of the anti-virus solution.
2. **Threat landscape**: The threat landscape will impact the number of malware detections and the frequency of malware updates required, which will impact the processing power, storage, and network bandwidth required.

3. **Performance requirements:** The performance requirements of the environment, including the response time and processing power required, will impact the size and capacity of the anti-virus solution.
4. **Resource constraints:** The available resources, including processing power, storage, and network bandwidth, will impact the size and capacity of the anti-virus solution.
5. **Scalability:** The scalability of the environment, including the ability to add or remove endpoints or servers as needed, will impact the size and capacity of the anti-virus solution.
6. **Security requirements:** The security requirements of the environment, including the need for real-time threat protection, will impact the size and capacity of the anti-virus solution.
7. **Encryption:** Check for existing encryption and whether encryption keys are available with client or not.
8. **Make in India Clauses:** Check for Make in India clauses in the compliance. Sometime data residency and sovereignty compliance guidelines may build complications.

Once you ascertain these, then choose the type of anti-virus solution and the work on the sizing using the technology and practice teams. In general, it is important to ensure the solution is appropriately sized for the specific environment and security requirements. This can help to minimize the risk of performance issues and ensure that the solution is effective in protecting against malware and other security threats.

2.3.2 To what will Antivirus solution connect to?

An antivirus solution can potentially connect to a variety of other organizational systems, depending on the specific needs and requirements of the organization. Some common systems that antivirus solutions can connect to include:

1. **Endpoint devices:** Antivirus solutions can be installed on individual endpoint devices, such as laptops, desktop computers, and mobile devices, to protect against malware and other threats on those devices.
2. **Network infrastructure:** Antivirus solutions can integrate with network infrastructure components, such as routers, switches, and firewalls, to provide a comprehensive view of network traffic and identify potential threats.
3. **Servers:** Antivirus solutions can be installed on servers, including file servers, web servers, and database servers, to protect against malware and other threats that target those systems.
4. **Cloud systems:** Antivirus solutions can be integrated with cloud systems, such as cloud storage services, to protect against malware and other threats in the cloud environment.
5. **Management systems:** Antivirus solutions can integrate with management systems, such as security information and event management (SIEM) systems, to provide centralized management and reporting of antivirus activity.

These are just a few examples of the types of systems that antivirus solutions can connect to. The specific systems that an antivirus solution will connect to will depend on the needs and requirements of the organization.

2.3.3 Implementation steps of Anti-virus solution

The implementation steps of an antivirus solution typically involve the following:

1. Assessment: Before implementing an antivirus solution, it's important to assess the current security environment and identify the specific needs and requirements of the organization. This step can involve a threat analysis, security gap assessment, and review of current security infrastructure.
    a. Some clients ask for installing desk-side licenses on mobiles devices and tablets. Note that the iOS, MacOS, Android, Windows, Unix, Linux environments react differently and may need different type of licenses.
    b. Some systems may have old hardware, software, firmware and may not support latest version or next 2-3 years of updates on the technology. Do a detailed diligence of the existing end-of-life or approaching-end-of-life devices and query on status of warranty and annual maintenance contracts on all endpoints.
    c. Some organisations will have field personnel with devices without internet connectivity (due to physical or compliance requirements (air-gapped systems)) and organisation information security management policy may prohibit USB/ Bluetooth access. These are tricky scenarios. Cross-check with clients on these aspects and agree on the workable solution.
2. Planning: Based on the results of the assessment, a plan for implementing the antivirus solution should be developed. This may involve determining the scope of the project, identifying the systems and devices that need protection, and determining the budget and timeline for the project.
3. Selection: Based on the results of the assessment and planning steps, a specific antivirus solution can be selected. This may involve evaluating different solutions, requesting demos, and comparing the features and costs of each solution.
4. Installation: Once a solution has been selected, it can be installed on the systems and devices that need protection. This may involve downloading software, configuring settings, and integrating the solution with other security technologies. The installation steps of an antivirus solution typically involve the following:
    a. Prepare the environment: Before installing the antivirus solution, it's important to prepare the environment by checking the system requirements, backing up important data, and disabling any conflicting software or security technologies. Check for encryption. You will need to decrypt systems to prevent conflicts. During the data backup process, sometimes endpoint devices or storage devices misbehave and may crash. Discuss in detail what could be the possible data recovery options with these lapses and who will bear the cost of these data recovery charges. Sometimes, external data recovery specialists may be needed to recover data and it has potential to exceed project budget.

b. Download the software: The antivirus software can be downloaded from the vendor's website or obtained through other means, such as a CD or USB drive. Check whether organisation allows using CDs or USB drives or large online data drives.

c. Install the software: The installation process will vary depending on the solution being used, but typically involves following the instructions provided by the vendor. This may involve accepting a license agreement, choosing an installation location, and configuring basic settings.

d. Configure the software: After the software has been installed, it will need to be configured to meet the specific needs and requirements of the organization. This may involve setting policies, defining security settings, and configuring alert and reporting settings.

e. Update virus definitions: The antivirus software will need to be updated with the latest virus definitions to ensure that it can effectively protect against known threats. This can typically be done automatically or manually through the software's interface.

f. Scan the system: Once the antivirus software has been installed and configured, it's important to run a scan of the system to ensure that there are no existing threats. The scan can be performed using the software's default settings or using custom settings if desired.

g. Verify the installation: After the scan has been completed, it's important to verify that the antivirus software is working as expected. This may involve checking the accuracy of alerts, reviewing logs and reports, and ensuring that the software is running without any errors or issues.

h. These are the general steps involved in installing an antivirus solution. The specific steps will depend on the solution being used and the environment in which it is being installed. It's always recommended to follow the vendor's instructions and best practices when installing an antivirus solution.

5. Configuration: After installation, the antivirus solution will need to be configured to meet the specific needs and requirements of the organization. This may involve setting policies, defining security settings, and configuring alert and reporting settings. Sometimes, in complex environments, configuration, fine-tuning, and stabilisation takes 6-9 months of regular trial and error. This has potential for cost over-runs. Agree with client on what the expectations are and if over-runs take place, how will they be handled.

6. Testing: Before going live with the antivirus solution, it's important to test the solution to ensure that it is working as expected. This may involve running tests, verifying the accuracy of alerts, and checking the effectiveness of the solution against known threats. Test Environments normally need extra

    a. sandboxes,

    b. hardware or virtual machines

    c. operating systems and licenses,

d. database systems and licenses, and sometimes,

e. client access licenses

Clients normally agree to provide these environments. If not, these need to be costed in the solution and provided as price to clients.

7. Deployment: After the solution has been tested and validated, it can be deployed in the production environment. This may involve installing the solution on all devices, updating virus definitions, and ensuring that the solution is integrated with other security technologies.
8. Maintenance: After the antivirus solution has been deployed, ongoing maintenance will be required to ensure that the solution remains effective and up to date. This may involve updating virus definitions, applying software patches, and monitoring the solution for performance and security issues.

These are the general steps involved in implementing an antivirus solution. The specific steps will depend on the needs and requirements of the organization, as well as the solution being used.

2.3.4 What can go wrong in antivirus solution

There are several things that can go wrong when implementing an antivirus solution, including:

1. **Compatibility issues**: The antivirus solution may not be compatible with the systems and devices that it is intended to protect, leading to performance issues or even system crashes.
2. **Configuration errors:** The antivirus solution may be configured incorrectly, leading to false positives or false negatives, or causing the solution to miss threats.
3. **Updates not installed:** If antivirus definition updates are not installed regularly, the solution may be unable to protect against new threats.
4. **Human error:** The antivirus solution can only be as effective as the people using it. User error, such as clicking on malicious links or disabling the antivirus solution, can expose the system to risk.
5. **Lack of integration:** If the antivirus solution is not integrated with other security technologies, such as firewalls or intrusion detection systems, it may not provide adequate protection.
6. **Performance impact:** The antivirus solution may have a significant impact on system performance, especially on older systems or systems with limited resources.
7. **False alarms:** The antivirus solution may generate false alarms, leading to user frustration and potentially wasting time and resources.
8. **Vulnerability exploitation:** In some cases, the antivirus solution itself may contain vulnerabilities that can be exploited by attackers.

These are just some of the potential issues that can arise when implementing an antivirus solution. It's important to carefully consider these risks and take steps to mitigate them, such

as properly configuring the solution, regularly updating virus definitions, and providing user education and training.

2.3.5 What Service Levels can be committed/ expected?

Service Level Agreements (SLAs) in antivirus services can vary depending on the specific needs of an organization and the level of service offered by the provider. However, some common SLAs that can be committed in antivirus services include:

1. **Availability:** The percentage of time that antivirus software and related systems are available and functioning as intended.
2. **Response time:** The amount of time it takes for the antivirus support team to respond to and resolve a reported issue.
3. **Update frequency:** The frequency at which the antivirus software is updated to protect against new threats.
4. **Threat detection rate:** The percentage of malware incidents detected by the antivirus software.
5. **False positive rate:** The percentage of benign files that are incorrectly flagged as malware by the antivirus software.
6. **Incident resolution time:** The amount of time it takes to resolve a malware incident, from the time it is reported to the time it is fully resolved.
7. **Data privacy:** The measures taken by the antivirus service provider to protect sensitive data, such as client information, during the course of providing antivirus services.

These are just a few examples of the types of SLAs that can be committed in antivirus services. The specific SLAs that are included in a contract will depend on the needs and requirements of the organization. But, please keep in mind, it is not always possible to accurately provide a resolution time commitment and hence, take penalty conditions in contracts.

2.3.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.
2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.

4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

2.4 Delivery cue- Anti-virus operations

2.4.1 Daily Anti-virus operations activities

Daily anti-virus operation activities typically include the following tasks:

1. Running regular scans: Regularly scanning all devices, systems, and networks for malware to detect and remove any potential threats.
2. Updating malware definitions: Keeping the anti-virus software up to date with the latest malware definitions to ensure that it can detect and remove the latest threats.
3. Monitoring event logs: Reviewing event logs for any suspicious activity, such as repeated failed login attempts, to detect and respond to potential threats.
4. Managing quarantined files: Regularly reviewing and managing quarantined files to ensure that no legitimate files are mistakenly quarantined and to determine the appropriate action for any malware detected.
5. Maintaining backups: Regularly backing up important data to ensure that it can be restored in the event of a malware attack or other security breach.
6. Evaluating security reports: Reviewing security reports to identify any potential security weaknesses or areas where the anti-virus solution can be improved.
7. Responding to incidents: Responding quickly to any security incidents, such as a malware attack, to contain the damage and prevent further spread of the malware.

In short, daily anti-virus operation activities are essential to ensuring the effective protection of a computer or network against malware and other cyber threats. By performing these tasks regularly, organizations can keep their anti-virus software up-to-date and effectively respond to any potential threats.

2.4.2 Weekly Anti-virus operations activities

Weekly anti-virus operation activities typically include the following tasks:

1. Updating anti-virus software: Regularly updating the anti-virus software to ensure that it has the latest security patches and features.
2. Reviewing scan results: Reviewing the results of regular anti-virus scans to ensure that all devices, systems, and networks are free from malware and other threats.
3. Performing vulnerability assessments: Conducting regular vulnerability assessments to identify any potential security weaknesses in the system and to determine what steps need to be taken to address them.

4. Conducting security audits: Conducting security audits to ensure that all devices and systems are properly configured and that all security measures are in place and working as intended.
5. Testing disaster recovery procedures: Regularly testing disaster recovery procedures to ensure that they will work as intended in the event of a malware attack or other security breach.
6. Training employees: Providing regular training to employees on how to identify and respond to cyber threats, as well as best practices for security awareness and safe computing.
7. Reviewing security policies: Reviewing and updating security policies as needed to ensure that they are current and relevant to the organization's changing security needs.

In short, weekly anti-virus operation activities are essential to ensuring the ongoing effectiveness of a computer or network's anti-virus solution. By performing these tasks regularly, organizations can identify potential security weaknesses and take the necessary steps to address them, as well as keep their employees informed and trained on how to respond to cyber threats.

2.4.3 Monthly Anti-virus operations activities

Monthly anti-virus operation activities typically include the following tasks:

1. Reviewing security incidents: Reviewing and analysing security incidents from the past month to determine if any trends or patterns exist, and to identify areas for improvement in the anti-virus solution.
2. Evaluating security software: Evaluating the performance of the anti-virus software and determining if it needs to be updated or replaced with a more effective solution.
3. Updating security plans: Updating the organization's security plans and procedures as needed, to ensure that they are current and relevant to the organization's changing security needs.
4. Conducting risk assessments: Conducting regular risk assessments to identify any potential security risks and to determine what steps need to be taken to mitigate them.
5. Reviewing user access: Reviewing user access logs to ensure that users are only accessing the systems and data that they need to do their job, and to identify any potential security threats.
6. Managing software licenses: Reviewing and managing software licenses to ensure that all software used by the organization is properly licensed and up to date.
7. Monitoring network activity: Monitoring network activity for any unusual activity or potential security threats.

In short, monthly anti-virus operation activities are important for maintaining the overall security of a computer or network. By performing these tasks regularly, organizations can identify potential security risks and take the necessary steps to mitigate them, as well as keep their anti-virus software and security plans up-to-date and effective.

2.4.4 What does an L1 Antivirus/ EDR Engineer do?

An L1 (Level 1) Antivirus/EDR (Endpoint Detection and Response) Engineer is responsible for the initial triage and response to alerts generated by the antivirus and EDR system. Some of the common activities performed by an L1 Antivirus/EDR Engineer include:

1. Monitoring and triaging alerts: The L1 engineer monitors the alerts generated by the antivirus and EDR system, assesses their severity, and takes appropriate actions to investigate and contain the threat.
2. Conducting basic analysis: The L1 engineer performs basic analysis of the alerts to determine the nature of the threat and identify any affected systems. They may also search for additional indicators of compromise and communicate their findings to the L2 or L3 team.
3. Responding to incidents: The L1 engineer responds to security incidents, such as malware infections or suspicious activity, by initiating remediation steps, such as isolating or quarantining affected systems.
4. Escalating incidents: If the L1 engineer is unable to contain or remediate a security incident, they escalate the issue to the L2 or L3 team for further investigation and response.
5. Maintaining documentation: The L1 engineer maintains detailed documentation of the alerts, incidents, and their responses, including any remediation steps taken, for future reference and reporting purposes.
6. Conducting basic maintenance: The L1 engineer may perform basic maintenance activities on the antivirus and EDR system, such as updating virus definitions or running scans, to ensure its ongoing effectiveness.

Overall, the L1 Antivirus/EDR Engineer plays a critical role in the initial response to security incidents and in ensuring the overall effectiveness of the antivirus and EDR system. They work closely with the L2 and L3 teams to provide support, escalate issues, and drive the ongoing development and improvement of the system.

2.4.5 What does an L2 Antivirus/ EDR Engineer do?

An L2 (Level 2) Antivirus/EDR (Endpoint Detection and Response) Engineer is responsible for investigating and responding to security incidents that have been escalated by the L1 team. Some of the common activities performed by an L2 Antivirus/EDR Engineer include:

1. Incident investigation: The L2 engineer investigates security incidents escalated by the L1 team and performs in-depth analysis to identify the root cause of the incident, the extent of the impact, and any affected systems.
2. Malware analysis: The L2 engineer conducts malware analysis to determine the behaviour of the malware, the systems it has infected, and any potential vulnerabilities or attack vectors that may have been exploited.

3. Threat hunting: The L2 engineer performs threat hunting activities, such as proactively searching for indicators of compromise and conducting analysis to detect any suspicious or anomalous activity on the network or endpoints.
4. Response coordination: The L2 engineer coordinates incident response activities, including isolating infected systems, containing the incident, and remediating the threat.
5. Documentation and reporting: The L2 engineer maintains detailed documentation of the incident investigation and response, including any remediation steps taken, for future reference and reporting purposes.
6. Technology management: The L2 engineer is responsible for managing the antivirus and EDR technology, ensuring that it is up to date, properly configured, and effectively integrated into the overall security architecture.

Overall, the L2 Antivirus/EDR Engineer plays a critical role in incident investigation and response, as well as in ensuring the ongoing effectiveness of the antivirus and EDR system. They work closely with the L1 and L3 teams to provide support, drive the development of new security controls and processes, and continuously improve the overall security posture of the organization.

2.4.6 What does an L3 Antivirus/ EDR Engineer do?

An L3 (Level 3) Antivirus/EDR (Endpoint Detection and Response) Engineer is responsible for the overall management of the antivirus and EDR system, including designing, implementing, and maintaining the solution. Some of the common activities performed by an L3 Antivirus/EDR Engineer include:

1. Design and architecture: The L3 engineer is responsible for designing and architecting the antivirus and EDR system, ensuring that it meets the organization's security requirements, is scalable, and integrates effectively with other security technologies.
2. Technical leadership: The L3 engineer provides technical leadership to the L1 and L2 teams, serving as a subject matter expert and providing guidance and direction on incident investigation and response, system management, and technology implementation.
3. Performance and capacity management: The L3 engineer monitors the performance and capacity of the antivirus and EDR system, identifying and addressing any performance or scalability issues, and proactively planning for future growth.
4. Risk management: The L3 engineer is responsible for managing the risk associated with the antivirus and EDR system, identifying and mitigating any vulnerabilities or weaknesses in the system.
5. Vendor management: The L3 engineer works closely with vendors to ensure that the antivirus and EDR solution is up to date, properly configured, and effectively integrated with other security technologies.

6. Technology innovation: The L3 engineer drives technology innovation within the antivirus and EDR domain, researching new technologies and approaches to improve the overall effectiveness of the system.

Overall, the L3 Antivirus/EDR Engineer plays a critical role in the ongoing management and optimization of the antivirus and EDR system. They work closely with other security teams to ensure that the system is integrated effectively with other security technologies, and they are responsible for ensuring that the system is designed, implemented, and maintained to the highest standards.

2.4.7 Reports

Anti-virus operation reports typically include the following:

1. Anti-virus scan results report: A report that shows the results of regular anti-virus scans, including any malware detections and the actions taken to remediate them.
2. Security incident report: A report that details any security incidents that occurred during the reporting period, including the type of incident, the cause, and the steps taken to mitigate the risk.
3. Vulnerability assessment report: A report that details the results of regular vulnerability assessments, including any potential security weaknesses and the steps taken to address them.
4. Security audit report: A report that details the results of regular security audits, including any findings or recommendations for improvement.
5. User access report: A report that provides a detailed view of user access to systems and data, including which users have accessed what resources and when.
6. License management report: A report that provides an overview of software licenses and usage, including the number of licenses in use and any licenses that are due to expire.
7. Network activity report: A report that provides a detailed view of network activity, including any unusual or potentially malicious traffic.

In short, anti-virus operation reports provide valuable insights into the security of a computer or network and are essential for understanding the effectiveness of the anti-virus solution and for identifying areas for improvement.

2.4.8 Governance of Antivirus solution

The governance of an antivirus solution refers to the policies, processes, and practices that are put in place to manage, monitor, and maintain the solution over time. The goal of antivirus governance is to ensure that the solution is effective, efficient, and aligned with the needs and goals of the organization. Some key aspects of antivirus governance include:

1. Policy development: Developing clear policies that outline the scope, purpose, and use of the antivirus solution, as well as the responsibilities of users and administrators.
2. Deployment planning: Carefully planning and executing the deployment of the antivirus solution, including considerations such as testing, training, and support.

3. Configuration management: Ensuring that the antivirus solution is configured and maintained in accordance with established policies and best practices, including updating virus definitions and making any necessary changes to settings.
4. Monitoring and reporting: Regularly monitoring the performance and effectiveness of the antivirus solution, and providing regular reports on its status, health, and usage.
5. Incident response: Establishing clear processes and procedures for responding to security incidents and potential threats, including the involvement of internal teams and external partners as needed.
6. Compliance: Ensuring that the antivirus solution follows relevant regulations, standards, and best practices, such as data privacy laws, industry standards, and security guidelines.
7. User education and training: Providing users with the knowledge and skills needed to use the antivirus solution effectively and safely, including regular training on security awareness and best practices.

These are just some of the key aspects of antivirus governance. The specific policies and procedures will depend on the needs and goals of the organization, as well as the scope and complexity of the antivirus solution. It's important to regularly review and update the governance framework as needed to ensure that the antivirus solution remains effective and relevant over time. Work with client teams to baseline, benchmark, and build+ implement these governance steps.

3. Endpoint Security- Mobile Security

Mobile security refers to the measures taken to protect mobile devices such as smartphones and tablets from cyber threats, data theft, and unauthorized access. This includes using secure passwords and lock screens, avoiding public Wi-Fi, installing anti-virus software, keeping the operating system and apps up to date, and being cautious of suspicious links or emails. Additionally, using encrypted messaging and storage apps and regularly backing up important data can also help enhance mobile security.

3.1 What is a mobile threat defence solution?

A mobile threat defense (MTD) solution is a type of software designed to protect mobile devices against various security threats such as malware, malicious apps, phishing attacks, and unauthorized access. MTD solutions typically use a combination of technologies such as endpoint protection, mobile device management (MDM), mobile application management (MAM), and threat intelligence to secure devices and protect sensitive data. Some MTD solutions also provide features such as real-time monitoring, device management, and reporting to help organizations manage and mitigate mobile security risks. The goal of MTD is to prevent data breaches and protect sensitive information on mobile devices, both for personal and business use.

3.1.1 EMM, MDM, MTD: What are these?

Enterprise Mobility Management (EMM), Mobile Device Management (MDM), and Mobile Threat Defense (MTD) are related to securing mobile devices but serve different purposes.

EMM is a broader concept that encompasses MDM and provides additional functions beyond just device management. EMM solutions provide a comprehensive approach to managing and securing mobile devices, applications, and data across an organization. EMM solutions typically include MDM capabilities, but also provide additional features such as mobile application management (MAM), security and access control, and the ability to manage both corporate and personal devices.

MDM refers to the process of managing and securing mobile devices such as smartphones and tablets that are used for both personal and business purposes. MDM solutions provide centralized control over devices, allowing IT administrators to manage device configurations, enforce security policies, and remotely wipe devices in case of theft or loss.

MTD, on the other hand, is a type of software that focuses on protecting mobile devices from specific security threats such as malware, phishing attacks, and unauthorized access. MTD solutions typically use threat intelligence and endpoint protection to provide real-time monitoring and protection against security threats.

A 20- point difference is as per the table below:

Sl No	Category	Elements	EMM	MDM	MTD
1	Device Management	Remote Lock or wipe	Yes	Yes	
2	Device Management	Apply enterprise policies on mobiles	Yes	Yes	
3	Device Management	Enforce mobile device encryption	Yes	Yes	
4	Device Management	Enforce business data encryption on mobiles	Yes		
5	Device Management	Enforce device password	Yes	Yes	
6	Device Management	Enforce VPN	Yes	Yes	
7	Device Management	Advanced jailbreak/root detection, Risky device configurations			Yes
8	Device Management	On- device App-based threat protection- Malware, spyware, rootkits, ransomware			Yes
9	Device Management	On-device phishing protection			Yes
10	Device Management	Remote observability of high risk and malicious events			Yes
11	Device Management	Network-based threat protection- Man in the Middle, SSL			Yes
12	Device Apps Management	Malicious App Detection and Analysis			Yes
13	Device Apps Management	Enterprise software/ app mobile vulnerability detection			Yes
14	Device Apps Management	Block apps on mobiles	Yes	Yes	Yes
15	Device Apps Management	Block URLs- Web & Content-based threat protection	Yes	Yes	Yes
16	Device Apps Management	Remote app deployment and updates	Yes		
17	Device Apps Management	Control Access to apps and data as per enterprise policy	Yes		
18	Device Apps Management	Containerise personal and enterprise business data	Yes		
19	Device Features compatibility	iOS, Android, and ChromeOS compatibility	Partial	Partial	Partial
20	Device Features compatibility	Device Battery hogger	Partial	Partial	Partial

In summary, while EMM provides a more comprehensive solution for managing and securing the entire mobile ecosystem within an organization, MDM provides a broader set of management and control functions, and MTD focuses specifically on security and protecting devices against specific security threats. In many cases, to provide a comprehensive mobile device security solution, organizations use both EMM/ MDM and MTD solutions.

3.1.2 EMM, MDM, MTD types

There are several types of Enterprise Mobility Management (EMM), Mobile Device Management (MDM), and Mobile Threat Defense (MTD) solutions available on the market:

EMM:

1. Full-fledged EMM: Provides a comprehensive solution for managing and securing mobile devices, applications, and data across an organization.
2. Standalone EMM: Focuses on a specific aspect of EMM, such as mobile application management (MAM) or security.

MDM:

1. On-premises MDM: Software installed on an organization's internal servers to manage and secure mobile devices.
2. Cloud-based MDM: Manages and secures mobile devices through a cloud-based solution.

MTD:

1. Real-time MTD: Provides real-time monitoring and protection against security threats.
2. On-demand MTD: Scans devices for threats on-demand, such as when prompted by the user.

It is important to note that some EMM solutions also include MTD capabilities, while some MTD solutions may also include some MDM features. Organizations can choose a solution based on their specific needs and requirements.

3.2 Sales cue- Questions to ask and answers to give

3.2.1 Questions to ask prospective client

When evaluating Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solutions, it is important to ask the right questions to ensure that the solution meets your prospective client's specific needs and requirements. Here are some questions you may want to ask your prospective client:

EMM:

1. What type of devices does the EMM solution need to support?
2. Does the EMM solution need to support both corporate and personal devices?
3. What security and access control features need to be included in the EMM solution?
4. How does the EMM solution need to handle mobile application management (MAM)?
5. What is the deployment model for the EMM solution (cloud-based or on-premises)?

MDM:

1. What type of devices does the MDM solution need to support?
2. How does the MDM solution need to enforce security policies on mobile devices?
3. What remote management features are needed to be included in the MDM solution?
4. How does the MDM solution need to handle device enrolment and configuration?
5. What is the deployment model for the MDM solution (cloud-based or on-premises)?

MTD:

1. Does the MTD solution need to provide real-time monitoring and protection against security threats?
2. How does the MTD solution need to detect and prevent malware and phishing attacks?
3. What types of security threats does the MTD solution need to protect against?
4. How does the MTD solution need to integrate with other security solutions (e.g., firewalls, intrusion detection systems)?
5. What is the deployment model for the MTD solution (cloud-based or on-premises)?

It is recommended to ask problem areas and use-cases from the prospective client to understand the solution's real-world effectiveness and benefits for organizations similar to your own.

3.2.2 Questions prospective client will ask of sales

Clients evaluating Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solutions may have a variety of questions based on their specific needs and requirements. Here are some common questions that clients ask:

EMM:

1. Can the EMM solution manage and secure both corporate and personal devices?
2. How does the EMM solution handle mobile application management (MAM)?
3. What security and access control features are included in the EMM solution?
4. How easy is it to deploy and manage the EMM solution?
5. How does the EMM solution handle data protection and privacy?

MDM:

1. What type of devices does the MDM solution support?
2. How does the MDM solution enforce security policies on mobile devices?
3. Can IT administrators manage and secure devices remotely?
4. How easy is it to enrol and configure devices in the MDM solution?
5. What types of reporting and analytics are available in the MDM solution?

MTD:

1. Does the MTD solution provide real-time monitoring and protection against security threats?
2. How does the MTD solution detect and prevent malware and phishing attacks?
3. What types of security threats does the MTD solution protect against?
4. How does the MTD solution integrate with other security solutions (e.g., firewalls, intrusion detection systems)?
5. What is the impact on device performance when the MTD solution is installed?

It is recommended to provide clear and concise answers to these questions, and to demonstrate how the solution addresses the client's specific requirements and concerns. Additionally, it may be helpful to provide relevant case studies or client references to show how the solution has benefited similar organizations.

3.2.3 Payment terms to agree with the clients

All EMM, MDM, MTD technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays EMM, MDM, MTD technology owners

via distributors) payment options with clients always keeps the cash-registers green and healthy.

The payment terms for Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solutions can vary depending on the specific solution. Here are some common payment terms that clients may agree with clients and EMM, MDM, MTD technology owners:

1. Subscription-based: Clients pay a recurring fee (e.g., monthly, or annually) for access to the EMM, MDM, or MTD solution. This model is commonly used for cloud-based solutions.
2. Per-device pricing: Clients pay a fee for each device that is enrolled in the EMM, MDM, or MTD solution. This model is commonly used for on-premises solutions.
3. Volume pricing: Clients receive discounts based on the number of devices enrolled in the EMM, MDM, or MTD solution.
4. Licensing: Clients pay a one-time fee for a license to use the EMM, MDM, or MTD solution. This model is commonly used for on-premises solutions.

It is important to carefully review and understand the payment terms before entering into an agreement. It is also recommended to discuss and negotiate any potential discounts or incentives that may be available, based on the number of devices enrolled or the length of the agreement. The specific payment terms will depend on the solution being offered. It's always recommended to carefully review the terms and conditions of an antivirus solution before making a purchase.

3.3 Pre-sales cue: Solution building complexities

3.3.1 Sizing the solution

Sizing an Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solution involves determining the appropriate resources and capacities required to effectively manage and secure mobile devices in your organization. Here are some factors to consider when sizing an EMM, MDM, or MTD solution:

1. Number of devices: The number of mobile devices in your organization is a key factor in determining the appropriate resources and capacities required for the EMM, MDM, or MTD solution.
2. Types of devices: The types of devices used in your organization (e.g., smartphones, tablets, laptops) can impact the resources and capacities required for the EMM, MDM, or MTD solution.
3. Security requirements: The level of security required for your organization's mobile devices will impact the resources and capacities required for the EMM, MDM, or MTD solution.
4. User requirements: The specific requirements of your users (e.g., device management, application management, data protection) can impact the resources and capacities required for the EMM, MDM, or MTD solution.

5. Deployment model: The deployment model for the EMM, MDM, or MTD solution (e.g., cloud-based, on-premises) can impact the resources and capacities required for the solution.

It is important to work closely with the technology owner and client to ensure that the EMM, MDM, or MTD solution is appropriately sized for organization's specific requirements. The technology owner and client should be able to provide guidance and recommendations based on organization's specific needs and requirements.

3.3.2 To what will EMM, MDM, MTD solution connect to?

Enterprise Mobility Management (EMM), Mobile Device Management (MDM), and Mobile Threat Defense (MTD) solutions can integrate with a variety of other systems to enhance their functionality and capabilities. Some common systems that may connect to an EMM, MDM, or MTD solution include:

1. Active Directory (AD): Integration with AD allows for seamless user authentication and authorization within the EMM, MDM, or MTD solution.
2. Identity and Access Management (IAM) systems: Integration with IAM systems can enhance the security of the EMM, MDM, or MTD solution by providing additional layers of authentication and authorization.
3. Mobile Application Management (MAM) solutions: Integration with MAM solutions can enhance the application management capabilities of the EMM, MDM, or MTD solution.
4. Mobile content management systems: Integration with mobile content management systems can enhance the data protection and privacy capabilities of the EMM, MDM, or MTD solution.
5. Email systems: Integration with email systems can enhance the email management capabilities of the EMM, MDM, or MTD solution.
6. Network security solutions: Integration with network security solutions (e.g., firewalls, intrusion detection systems) can enhance the security of the EMM, MDM, or MTD solution by providing additional layers of protection.

It is important to carefully evaluate the integration requirements of organization's systems and to work with the System Integrator to ensure that the EMM, MDM, or MTD solution integrates with the necessary systems. The System Integrator should be able to provide guidance and recommendations on the most appropriate integration approach.

3.3.3 Implementation steps of EMM, MDM, MTD solution

The implementation of an Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solution typically involves the following steps:

1. Requirements gathering: This involves identifying the specific requirements of organization for mobile device management, security, and data protection.

2. Solution selection: This involves selecting the appropriate EMM, MDM, or MTD solution for organization based on the requirements gathered in the first step.
3. Installation: The installation of an Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solution typically involves the following steps:
    a. Prepare the environment: This involves verifying that the necessary hardware, software, and network infrastructure is in place to support the EMM, MDM, or MTD solution.
    b. Download the software: This involves downloading the EMM, MDM, or MTD software from the vendor's website or through a distribution channel.
    c. Install the software: This involves installing the EMM, MDM, or MTD software on the necessary servers, devices, or gateways.
    d. Configure the solution: This involves configuring the EMM, MDM, or MTD solution to meet the specific requirements of organization. This may include setting up device policies, configuring security settings, and integrating with other systems as needed.
    e. Deploy the solution: This involves deploying the EMM, MDM, or MTD solution to organization's users. This may involve installing software on devices, enrolling devices in the solution, and configuring devices to meet the organization's requirements.
    f. Test the solution: This involves testing the EMM, MDM, or MTD solution to ensure that it is functioning as expected.
4. Solution configuration: This involves configuring the EMM, MDM, or MTD solution to meet the specific requirements of organization. This may include setting up device policies, configuring security settings, and integrating with other systems as needed.
5. User training: This involves providing training to organization's users on how to use the EMM, MDM, or MTD solution. This may include training on how to enrol devices, manage device policies, and access data and applications securely.
6. Deployment: This involves deploying the EMM, MDM, or MTD solution to organization's users. This may involve installing software on devices, enrolling devices in the solution, and configuring devices to meet the organization's requirements.
7. Monitoring and maintenance: These involve monitoring the EMM, MDM, or MTD solution to ensure that it is functioning as expected, and performing maintenance and updates as needed to keep the solution up-to-date and secure.

These are the general steps involved in implementing an EMM, MDM or MTD solution. The specific steps will depend on the needs and requirements of the organization, as well as the solution being used.

3.3.4 What can go wrong in EMM, MDM, MTD solution

There are several things that can go wrong when implementing an Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solution, including:

1. Complexity: The implementation and use of an EMM, MDM, or MTD solution can be complex and require a significant investment of time and resources.
2. Integration challenges: Integrating the EMM, MDM, or MTD solution with other systems, such as email, file storage, and security systems, can be challenging and may require significant effort and expertise.
3. User adoption: Getting users to adopt the EMM, MDM, or MTD solution can be a challenge, particularly if the solution is perceived as cumbersome or difficult to use.
4. Performance issues: The EMM, MDM, or MTD solution can impact the performance of devices, leading to slow response times, battery drain, and other issues.
5. Data security: Ensuring that sensitive data is protected and remains secure can be a challenge with an EMM, MDM, or MTD solution.
6. Compliance challenges: Ensuring that the EMM, MDM, or MTD solution is compliant with various regulations and standards can be a complex and time-consuming process.
7. Vendor support: Ensuring that the vendor provides adequate support, and that the solution is up-to-date and secure can be a challenge.

These are just some of the potential issues that can arise when implementing an EMM, MDM, MTD solution. It's important to carefully consider these risks and take steps to mitigate them, such as properly configuring the solution, regularly updating virus definitions, and providing user education and training.

3.3.5 What Service Levels can be committed/ expected?

Service Level Agreements (SLAs) in EMM MDM MTD services can vary depending on the specific needs of an organization and the level of service offered by the provider. However, some common SLAs that can be committed in EMM MDM MTD solution include:

1. Availability: The percentage of time that the EMM, MDM, or MTD solution is available and accessible to users.
2. Response time: The amount of time it takes for the vendor to respond to support requests or incidents.
3. Resolution time: The amount of time it takes for the technology owner to resolve support requests or incidents.
4. Upgrades: The frequency and timing of software upgrades and patches provided by the vendor.
5. Data protection: The level of protection provided for sensitive data stored or processed by the EMM, MDM, or MTD solution.
6. Compliance: The level of compliance with various regulations and standards required by the organization.
7. Training: The level of training provided to users and administrators on the use of the EMM, MDM, or MTD solution.

These are just a few examples of the types of SLAs that can be committed in EMM, MDM, or MTD services. The specific SLAs that are included in a contract will depend on the needs and requirements of the organization. But, please keep in mind, it is not always possible to

accurately provide a resolution time commitment and hence, take penalty conditions in contracts.

3.3.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.
2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

3.4 Delivery cue- EMM MDM MTD operations

3.4.1 Daily Activities

Daily EMM MDM MTD operation activities typically include the following tasks:

1. Monitoring: Regularly monitoring the EMM, MDM, or MTD solution to ensure that it is functioning properly and to identify any issues or potential threats.
2. Device management: Managing and updating the configurations of mobile devices, including enrolling new devices, managing device profiles, and securing devices.
3. User management: Managing and updating user accounts, including creating new accounts, revoking access, and managing user permissions.
4. Security management: Implementing and monitoring security policies, such as device encryption, password policies, and access control.
5. Software updates: Installing software updates and patches to ensure that the EMM, MDM, or MTD solution is up-to-date and secure.

6. Reporting: Generating and reviewing reports to monitor the use of mobile devices, security threats, and other relevant metrics.
7. Compliance: Ensuring that the EMM, MDM, or MTD solution complies with various regulations and standards required by the organization.
8. Training: Providing training and support to users and administrators on the use of the EMM, MDM, or MTD solution.

It is important to establish a routine and regularly perform these activities to ensure that the EMM, MDM, or MTD solution is functioning properly and providing the necessary protection and support for mobile devices.

In short, daily EMM, MDM, or MTD solution operation activities are essential to ensuring the effective protection of a computer or network against malware and other cyber threats. By performing these tasks regularly, organizations can keep their anti-virus software up-to-date and effectively respond to any potential threats.

3.4.2 Weekly Activities

Weekly EMM, MDM, or MTD operation activities typically include the following tasks:

1. Device inventory management: Updating the inventory of mobile devices, including adding new devices, retiring old devices, and updating device information.
2. Policy management: Reviewing and updating security policies to ensure that they remain effective and relevant.
3. Incident management: Reviewing and responding to security incidents, such as malware infections, lost or stolen devices, or unauthorized access attempts.
4. Compliance reporting: Generating and reviewing reports to ensure that the EMM, MDM, or MTD solution follows various regulations and standards required by the organization.
5. User training: Providing training and support to users and administrators on the use of the EMM, MDM, or MTD solution.
6. System updates: Installing software updates and patches to ensure that the EMM, MDM, or MTD solution is up-to-date and secure.
7. Performance monitoring: Monitoring the performance of the EMM, MDM, or MTD solution and identifying any potential issues.

It is important to establish a routine and regularly perform these activities to ensure that the EMM, MDM, or MTD solution is functioning properly and providing the necessary protection and support for mobile devices. Additionally, these weekly activities can help identify areas for improvement and ensure that the EMM, MDM, or MTD solution continues to meet the evolving needs of the organization.

3.4.3 Monthly Activities

Monthly EMM, MDM, or MTD operation activities typically include the following tasks:

1. Device audit: Auditing the inventory of mobile devices to ensure accuracy and to identify any discrepancies or missing devices.
2. Security assessment: Conducting a security assessment to identify potential threats and vulnerabilities, and to assess the effectiveness of existing security policies.
3. Compliance review: Reviewing the compliance status of the EMM, MDM, or MTD solution with various regulations and standards required by the organization.
4. User feedback: Gathering feedback from users and administrators on the use of the EMM, MDM, or MTD solution, and incorporating this feedback into future updates and improvements.
5. System optimization: Optimizing the performance of the EMM, MDM, or MTD solution, including tuning settings and configurations, and optimizing resource utilization.
6. Budget review: Reviewing the budget and resources dedicated to the EMM, MDM, or MTD solution, and making recommendations for future investments.
7. Reporting: Generating and reviewing reports to provide a comprehensive overview of the status of the EMM, MDM, or MTD solution, including usage statistics, security incidents, and other relevant metrics.

It is important to establish a routine and regularly perform these monthly activities to ensure that the EMM, MDM, or MTD solution is functioning properly and providing the necessary protection and support for mobile devices. Additionally, these monthly activities can help identify areas for improvement and ensure that the EMM, MDM, or MTD solution continues to meet the evolving needs of the organization.

3.4.4 What does an L1 EMM, MDM, or MTD Engineer do?

An L1 EMM, MDM, or MTD Engineer is responsible for providing first-level technical support and resolving simple issues. This may include tasks such as password resets, device enrolment, and basic troubleshooting. L1 (Level 1) EMM (Enterprise Mobility Management), MDM (Mobile Device Management), or MTD (Mobile Threat Defense) Engineer activities typically involve the following:

1. Providing first-level technical support: The L1 engineer is responsible for handling the initial support requests and troubleshooting issues related to EMM, MDM, or MTD systems. They should have a good understanding of the system and be able to resolve basic issues or escalate them to the appropriate level.
2. Monitoring system alerts: The L1 engineer is responsible for monitoring system alerts and notifications and taking appropriate action when necessary. This can include investigating system failures or errors, resolving issues related to user access, or escalating issues to higher levels when necessary.
3. Performing system maintenance: The L1 engineer is responsible for performing regular maintenance tasks, such as system updates and patches, to ensure that the EMM, MDM, or MTD system is functioning properly.

4. Documenting and reporting issues: The L1 engineer is responsible for documenting and reporting any issues or problems related to the EMM, MDM, or MTD system. They should keep detailed records of support requests, troubleshooting steps, and resolutions.
5. Providing end-user training: The L1 engineer may be responsible for providing basic training and support to end-users on how to use the EMM, MDM, or MTD system. This can include providing guidance on how to access and use applications, or how to configure devices to meet organizational security requirements.
6. Performing security tasks: The L1 engineer may be responsible for performing basic security tasks, such as reviewing logs, conducting security scans, or configuring security policies, to help ensure that the EMM, MDM, or MTD system is secure.

Overall, the L1 EMM, MDM, or MTD engineer plays a critical role in ensuring the smooth functioning of the system, providing basic support and troubleshooting, and escalating issues when necessary.

3.4.5 What does an L2 EMM, MDM, or MTD Engineer do?

L2 (Level 2) EMM (Enterprise Mobility Management), MDM (Mobile Device Management), or MTD (Mobile Threat Defense) Engineer activities involve more advanced technical support and troubleshooting tasks, such as:

1. Providing technical support: The L2 engineer provides more advanced technical support, troubleshooting issues that could not be resolved by the L1 engineer. This may involve more in-depth analysis and investigation of the root cause of the problem.
2. Performing system upgrades and migrations: The L2 engineer may be responsible for performing system upgrades and migrations, such as moving the EMM, MDM, or MTD system to a new platform or version.
3. Developing and implementing system integrations: The L2 engineer may be responsible for developing and implementing system integrations, such as integrating the EMM, MDM, or MTD system with other systems in the organization.
4. Developing and implementing automation scripts: The L2 engineer may develop and implement automation scripts to help streamline the management of the EMM, MDM, or MTD system.
5. Conducting system testing: The L2 engineer may be responsible for conducting system testing, such as testing new features, patches, or updates to ensure that they function properly and do not cause issues.
6. Providing training and mentoring: The L2 engineer may be responsible for providing training and mentoring to L1 engineers, or to end-users who need more advanced technical training on the EMM, MDM, or MTD system.

Overall, the L2 EMM, MDM, or MTD engineer provides more advanced technical support and takes on more complex tasks related to the management of the system. They work closely with L1 engineers and other technical staff to ensure the smooth functioning of the system and to provide support to end-users as needed.

3.4.6 What does an L3 EMM, MDM, or MTD Engineer do?

L3 (Level 3) EMM (Enterprise Mobility Management), MDM (Mobile Device Management), or MTD (Mobile Threat Defense) Engineer activities involve highly specialized technical support and problem-solving tasks, such as:

1. Providing advanced technical support: The L3 engineer provides advanced technical support, resolving complex technical issues that could not be resolved by L1 or L2 engineers.
2. Conducting root cause analysis: The L3 engineer is responsible for conducting root cause analysis of complex technical issues, identifying underlying problems and developing solutions to prevent their recurrence.
3. Designing and implementing system architecture: The L3 engineer may be responsible for designing and implementing the system architecture, including the hardware, software, and network infrastructure required to support the EMM, MDM, or MTD system.
4. Developing and implementing custom solutions: The L3 engineer may be responsible for developing and implementing custom solutions, such as scripts or plugins, to address specific technical challenges or business requirements.
5. Evaluating new technologies and solutions: The L3 engineer may be responsible for evaluating new technologies and solutions, such as new mobile devices or operating systems, and developing strategies for incorporating them into the EMM, MDM, or MTD system.
6. Providing training and mentoring: The L3 engineer may be responsible for providing training and mentoring to L1 and L2 engineers, as well as to other technical staff and end-users.

Overall, the L3 EMM, MDM, or MTD engineer is a highly specialized technical expert, responsible for resolving complex technical issues and ensuring the smooth functioning of the system. They work closely with other technical staff, management, and end-users to provide support, solve problems, and drive the ongoing development and improvement of the system.

3.4.7 Reports

EMM, MDM, or MTD operation reports typically include the following:

1. Device inventory report: A report that provides an inventory of all mobile devices enrolled in the EMM, MDM, or MTD solution. This report can include information such as device type, operating system, and ownership.
2. Security report: A report that provides information about the security status of mobile devices, including the number of security incidents, the types of incidents, and the devices affected.

3. Compliance report: A report that provides information about the compliance status of mobile devices with security policies, regulations, and standards required by the organization.
4. User report: A report that provides information about the usage of mobile devices, including the number of devices in use, the number of applications installed, and the amount of data transmitted.
5. Resource utilization report: A report that provides information about the resource utilization of the EMM, MDM, or MTD solution, including the amount of storage used, the number of processors used, and the amount of network bandwidth used.
6. Incident response report: A report that provides information about incidents that have been reported and the steps taken to resolve them. This report can be used to track the status of incidents and to ensure that they are being resolved in a timely manner.

In short, EMM, MDM, or MTD operation reports provide valuable insights into the security of a mobile or network and are essential for understanding the effectiveness of the EMM, MDM, or MTD solution and for identifying areas for improvement. It is important to regularly review and analyse these reports to ensure that the EMM, MDM, or MTD solution is functioning properly and providing the necessary protection and support for mobile devices.

3.4.8 Governance of EMM, MDM, or MTD solution

Governance refers to the processes and policies that ensure the effective and efficient management of an Enterprise Mobility Management (EMM), Mobile Device Management (MDM), or Mobile Threat Defense (MTD) solution. Effective governance of these solutions is crucial to ensure that they provide the necessary protection and support for mobile devices, while also balancing the needs of the organization and its employees. The following are some key elements of governance for an EMM, MDM, or MTD solution:

1. Policies and procedures: Policies and procedures are the foundation of effective governance for an EMM, MDM, or MTD solution. They provide guidelines and standards for how the solution should be used and maintained and help ensure that it is used in a consistent and effective manner.
2. Security controls: Effective governance of an EMM, MDM, or MTD solution requires the implementation of robust security controls to protect against threats and prevent data breaches. These controls can include encryption, access control, and security monitoring and reporting.
3. Compliance management: Compliance with regulations and standards is an important aspect of governance for an EMM, MDM, or MTD solution. Organizations must ensure that their solution is compliant with relevant regulations and standards, such as HIPAA, PCI DSS, and ISO 27001.
4. User management: Effective governance of an EMM, MDM, or MTD solution requires the proper management of users and their access to the solution. This includes the management of user roles, permissions, and authentication.
5. Risk management: Risk management is a crucial component of governance for an EMM, MDM, or MTD solution. Organizations must assess the risks associated with their solution and implement controls to mitigate these risks.

6. Incident management: Effective governance of an EMM, MDM, or MTD solution requires the proper management of incidents, such as security breaches and system failures. This includes the development of incident response plans and procedures, as well as the implementation of monitoring and reporting capabilities.

Effective governance of an EMM, MDM, or MTD solution is essential to ensure that it provides the necessary protection and support for mobile devices while balancing the needs of the organization and its employees. Regularly reviewing and updating governance policies and procedures can help ensure that the solution remains effective and efficient over time.

4. Network Security- Next Generation Firewall (NGFW)

Network security refers to the protection of a computer network from unauthorized access, misuse, modification, or denial of service. It encompasses a set of technologies, processes, and practices designed to secure data and resources on a network. Network security measures can include firewalls, intrusion detection and prevention systems, encryption, secure protocols, access control, and *network segmentation*. The goal of network security is to ensure the confidentiality, integrity, and availability of information and resources on a network, while also protecting against threats such as malware, hacking, and data theft. Effective network security requires a comprehensive approach that addresses both technical and non-technical factors and involves regularly reviewing and updating security measures to adapt to evolving threats.

A firewall is a network security system that monitors, and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a private internal network and the public Internet, allowing only authorized traffic to pass through. Firewalls are commonly used to protect against unauthorized access, malware, and other cyber threats. They can be hardware-based, software-based, or a combination of both. Firewalls can be configured to filter traffic based on source and destination addresses, port numbers, and application protocols, among other factors. The goal of a firewall is to enhance security by controlling access to and from a network and protecting against malicious activity.

4.1 What is Network Segmentation, Micro-segmentation, ZTNA?

Network segmentation is the process of dividing a computer network into smaller sub-networks, called segments, to improve network security, manageability, and performance. Network segmentation creates isolated parts of a network, which reduces the attack surface and limits the potential damage that a security breach can cause.

Each segment can be assigned a different level of security, allowing different parts of the network to be secured differently. For example, sensitive data can be stored in a segment with stricter security measures, while less sensitive data can be stored in a segment with more relaxed security measures. This approach helps organizations to balance the need for security with the need for accessibility and performance.

For example: HR functions dealing sensitive employee salaries can be segmented separately from differently sensitive and patent-researching Research and Development functions which can be different from finance functions.

Network segmentation can be achieved through various methods, including virtual LANs (VLANs), virtual private networks (VPNs), and firewalls. The choice of method depends on the specific requirements of the organization and the network architecture. In general, network segmentation is considered a best practice for enhancing network security and is widely used by organizations of all sizes.

Micro-segmentation, on the other hand, takes network segmentation to a more granular level. It creates small, isolated security domains for individual applications or workloads within a network. Micro-segmentation provides a higher level of security, as it helps to limit the spread of threats and reduces the attack surface by creating smaller, well-defined security domains.

Zero Trust Network Access (ZTNA) is a security model that assumes that all users, devices, and network traffic are untrusted, and thus requires verification of identity and device security before granting access to applications and resources. Unlike traditional network access models, which rely on a network perimeter for security, ZTNA uses a "never trust, always verify" approach that enforces access policies on a per-user and per-device basis.

ZTNA uses a variety of security technologies to enforce access policies, including multi-factor authentication, device profiling, network segmentation, and encryption. These technologies work together to ensure that only authorized users and devices can access specific applications and resources, and that sensitive data is protected against unauthorized access.

ZTNA is increasingly popular in modern cloud and hybrid environments, where traditional network perimeters are often not sufficient to provide effective security. By using a ZTNA approach, organizations can provide secure access to applications and resources from any location or device, without compromising security.

4.2 What is a Next Generation Firewall solution?

A Next Generation Firewall (NGFW) is a type of firewall that provides advanced security features beyond traditional firewalls. NGFW solutions typically incorporate features such as *deep packet inspection*, *application control*, *user identity management*, and *intrusion prevention*. The goal of NGFW is to provide a comprehensive security solution that can detect and prevent threats, while also allowing organizations to enforce security policies and manage network traffic. NGFW solutions are designed to meet the needs of modern organizations that rely on complex and diverse network environments and require a more sophisticated level of security to protect against advanced cyber threats.

Cloud Next-Generation Firewall (NGFW) refers to a type of firewall that provides network security in a cloud computing environment. A cloud NGFW solution is deployed and managed in a cloud environment, such as Amazon Web Services (AWS) or Microsoft Azure or Google Cloud, rather than on-premises hardware. Cloud NGFW solutions offer several advantages over traditional on-premises NGFW solutions, including:

1. Scalability: Cloud NGFW solutions can be easily scaled up or down to accommodate changing network needs, without the need for physical hardware upgrades.
2. Flexibility: Cloud NGFW solutions can be accessed from anywhere, allowing organizations to secure remote and mobile workers and branch offices.
3. Cost-effectiveness: Cloud NGFW solutions can reduce the costs associated with purchasing and maintaining on-premises hardware and software.
4. Improved security: Cloud NGFW solutions can provide improved security compared to traditional on-premises solutions, as they are managed and maintained by experienced security experts.

When choosing a cloud NGFW solution, it is important to consider the specific security requirements of the network, the size and complexity of the network, and the technical capabilities of the cloud provider. It is also important to ensure that the solution integrates well with other security solutions and tools already in use within the organization.

4.2.1 What is Deep Packet Inspection?

A data packet is a unit of data transmitted over a network. It is the basic building block of data transmission in computer networks. A packet typically contains a header and a payload, where the header contains information such as the source and destination addresses, and the payload contains the actual data being transmitted. In a network, data is divided into smaller packets for transmission, and each packet is sent individually through the network. At the destination, the packets are reassembled into the original data. This approach is called packet-switched networking, and it allows for efficient use of network resources, as multiple packets from different sources can be transmitted over the network simultaneously. Packet inspection and analysis is a common technique used in network security to monitor and protect against malicious activity. By examining the contents of each packet, security devices can identify and prevent malicious traffic from entering the network or identify and isolate infected devices within the network.

Deep packet Inspection (DPI) is a method used by network security devices to inspect data packets in real-time as they pass through a network. DPI enables the device to examine not only the header of a packet, but also its payload, allowing for a more thorough analysis of the data being transmitted.

DPI is often used in firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to identify and prevent malicious network activity. It can also be used to monitor network traffic and enforce policies such as quality of service (QoS) and bandwidth management.

DPI works by examining each packet in detail, looking for specific patterns and attributes that match known security threats or violate network policies. This information can then be used to block malicious traffic, or to enforce security policies and optimize network performance. DPI is considered an important component of advanced security solutions, as it enables organizations to protect against evolving threats and maintain secure networks. However, it can also introduce privacy concerns, as it allows organizations to inspect and potentially store sensitive data.

4.2.2 What is Application Control?

Application control is a security feature used to monitor and manage the use of applications on a network. The goal of application control is to prevent unauthorized or malicious applications from running on the network, while allowing authorized applications to function normally.

Application control typically works by examining the characteristics of network traffic, such as the source and destination addresses, port numbers (think of similarity to actual physical ports through which ships transfer goods from one place to another), and application protocols (like real life similarity of how must one person talk to another, applications also follow communication protocols), and then using that information to identify and control the applications generating the traffic. The information is used to create policies that define which applications are allowed to run on the network and which are not.

Application control can be implemented through various means, including firewalls, intrusion prevention systems (IPS), and unified threat management (UTM) devices. Application control is considered an important component of advanced security solutions, as it helps

organizations to prevent the spread of malware and other threats, and to enforce policies for the use of applications on the network. However, it can also introduce some level of complexity and management overhead, as organizations need to create and maintain policies for each application that is used on the network.

4.2.3 What is User Identity Management?

User identity management (UIM) is the process of identifying, authenticating, and authorizing individuals or systems to access resources within an organization's network. The goal of UIM is to ensure that only authorized users have access to sensitive data and systems, while at the same time making it easy for users to access the resources they need.

UIM typically involves the use of user accounts, passwords, and other forms of authentication, such as smart cards, biometric devices, and single sign-on (SSO) systems. The authentication information is then used to grant or deny access to specific resources, based on the user's role and privileges within the organization.

UIM is a critical component of any organization's security strategy, as it helps to prevent unauthorized access to sensitive data and systems, and helps to maintain the confidentiality, integrity, and availability of information.

There are several challenges associated with UIM, including the need to manage large numbers of users and their associated authentication information, the need to support multiple authentication methods and protocols, and the need to integrate with other security systems and technologies. Effective UIM requires a well-designed strategy, robust security systems, and ongoing monitoring and management to ensure that users are properly authenticated and authorized to access resources.

4.2.4 What is Intrusion Prevention and unified threat management?

Intrusion Prevention Systems (IPS): An IPS is a security solution that uses deep packet inspection (DPI) and other techniques to monitor and prevent security threats in real-time. IPS works by examining the contents of network packets in real-time and comparing that information to a database of known security threats. If a threat is detected, the IPS will take action to prevent the traffic from entering the network.

Unified Threat Management (UTM) Devices: A UTM device is a security solution that combines multiple security technologies into a single device or platform. UTMs typically include firewalls, IPS, anti-virus, anti-spam, and other security technologies. The goal of a UTM is to provide a comprehensive security solution for small to medium-sized organizations, by combining multiple security technologies into a single device or platform.

In summary, firewalls, IPS, and UTM devices are all important components of a comprehensive security solution. However, each of these technologies has a different focus and approach to network security, and the choice of technology depends on the specific depth and requirements of the organization and the network architecture.

4.2.5 NGFW types

Next-Generation Firewalls (NGFWs) are advanced firewall solutions that provide enhanced security features compared to traditional firewalls. There are several types of NGFWs, including:

1. **Stateful Firewall NGFW:** This type of NGFW provides the same basic firewall functionality as traditional firewalls, but with improved performance and scalability. A stateful firewall keeps track of the state of each connection, allowing it to manage network traffic and enforce security policies more effectively.

   The state of a connection refers to the current status or condition of a communication between two devices in a network. In a stateful firewall, the state of each connection is tracked and maintained by the firewall, allowing it to manage network traffic and enforce security policies more effectively. For example, when a connection is established between a client and a server, the stateful firewall records information about the connection, such as the source and destination IP addresses (like address of physical locations used in context of internet), the ports being used, and the current status of the connection (e.g., established, closed, etc.). This information is used to allow or block subsequent network traffic related to that connection, based on the security policies defined in the firewall.

   By tracking the state of each connection, a stateful firewall can provide a higher level of security compared to traditional firewalls, which only examine the source and destination addresses of each packet and cannot distinguish between different types of network traffic related to a single connection. In summary, the state of each connection is an important concept in stateful firewall technology, as it allows the firewall to effectively manage network traffic and enforce security policies based on the status and context of each connection.

2. **Application-Aware NGFW:** This type of NGFW is designed to inspect and control application traffic. It uses deep packet inspection (DPI) and other techniques to identify and control specific applications, such as web-based applications, email, and instant messaging. This allows organizations to enforce security policies and control the use of specific applications on their networks.

3. **Threat Prevention NGFW**: This type of NGFW is designed to prevent security threats, such as malware, from entering the network. It uses intrusion prevention systems (IPS) and other security technologies to inspect network traffic in real-time and block or quarantine traffic that is suspected of being malicious.

4. **Identity-Aware NGFW:** This type of NGFW is designed to enforce security policies based on user identity. It integrates with user identity management systems to provide context-aware security, allowing organizations to control access to specific resources based on the user's role and privileges.

5. **SSL/TLS Inspection NGFW**: This type of NGFW is designed to inspect encrypted network traffic, such as that generated by SSL/TLS-encrypted applications. It allows organizations to inspect the contents of encrypted network traffic and enforce security policies, even when the traffic is encrypted.

   Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide secure communication over the internet. They are commonly used to encrypt sensitive information, such as financial transactions, login credentials, and other confidential data. When a client and a server communicate over the internet using SSL/TLS, they establish an encrypted connection. All data transmitted between the client and the server is encrypted and can only be decrypted by the intended

recipient. This protects the confidentiality and integrity of the data being transmitted, even if it is intercepted by an attacker.

SSL/TLS inspection refers to the process of examining the contents of encrypted network traffic to ensure that it complies with security policies. This is typically performed by a firewall or other security device that is designed to inspect SSL/TLS traffic. By inspecting SSL/TLS traffic, organizations can detect and prevent security threats that might otherwise be hidden within encrypted network traffic. For example, an SSL/TLS inspection firewall can detect and block malware that is transmitted over encrypted connections or enforce policies that control the use of specific encrypted applications. In summary, SSL/TLS inspection is an important security feature for organizations that need to secure their network traffic, as it allows them to inspect and control encrypted network traffic, even if it is encrypted with SSL/TLS.

In summary, there are several types of NGFWs, each designed to provide specific security features and functionalities. The choice of NGFW depends on the specific security requirements and needs of the organization.

4.3 Sales cue- Questions to ask and answers to give

4.3.1 Questions to ask prospective client

When evaluating NGFW solutions, it is important to ask the right questions to ensure that the solution meets your prospective clients' specific needs and requirements. Here are some questions you may want to ask your prospective client:

1. Can you describe your current security posture and any recent security incidents or breaches?
2. What are your top security concerns and priorities?
3. What is the current size of your network and how is it expected to grow in the near future?
4. Can you describe your network architecture and the type of devices you use?
5. How do you handle the management and deployment of security updates and patches?
6. What is your current budget for network security solutions?
7. How do you manage and control network access for your employees and external partners?
8. What is your current firewall setup and how well does it meet your security needs?
9. What applications and services are critical to your business operations and where are they- on premises, in cloud, partially in both creating a hybrid scenario?
10. How do you handle the increasing amount of network traffic and applications?
11. Who manages daily, weekly, monthly operations of your network and how?

These questions can understand NGFW opportunity by understanding the size and complexity of the prospective client's network and determining their readiness and budget for implementing a solution.

4.3.2 Questions prospective clients will ask of sales

When evaluating a Next-Generation Firewall (NGFW) solution, prospective clients tend to ask specific questions to ensure that the solution meets their organization's requirements and expectations. Some key questions are as follows:

1. What security features does the NGFW provide? They are looking for features such as deep packet inspection (DPI), intrusion prevention systems (IPS), application control, and user identity management.
2. How does the NGFW manage network traffic? They are looking for capabilities such as stateful firewall, traffic prioritization, and quality of service (QoS) management.
3. What is the NGFW's performance and scalability? They are checking for NGFW's maximum throughput, number of concurrent connections, and how it can be scaled to meet the needs of their organization.
4. What types of network protocols and applications does the NGFW support? They are trying to ensure the NGFW supports the protocols and applications used by their organization.
5. How does the NGFW integrate with other security solutions? They will ask about the NGFW's integration with other security technologies, such as user identity management systems, intrusion detection systems (IDS), and security information and event management (SIEM) systems.
6. What is the NGFW's management and reporting capability? They will check about the NGFW's management interface, reporting capabilities, and how it can be used to monitor and manage the firewall.
7. What is the NGFW's support and maintenance policy? They will explore about the technology owner’s and System-Integrator-cum-Managed-Security-Services provider support and maintenance policy, including the availability of firmware updates and bug fixes.
8. What is the total cost of ownership (TCO) of the NGFW solution? This is important and they will definitely ask about the initial cost of the NGFW, as well as ongoing costs for support, maintenance, and upgrades.

4.3.3 Payment terms to agree with the clients

All NGFW technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays NG-FW technology owners via distributors) payment options with clients always keeps the cash-registers green and healthy.

The payment terms for NGFW solutions can vary depending on the specific solution. Here are some common payment terms that clients may agree with clients and NGFW technology owners:

1. Upfront payment: The client pays for the entire NGFW solution before it is deployed.

2. Subscription-based payment: The client pays for the NGFW solution on a recurring basis, such as monthly or annually.
3. Financing: The client pays for the NGFW solution over a specified period of time, such as 36 or 60 months.
4. Usage-based payment: The client pays for the NGFW solution based on usage, such as the number of devices protected, or the amount of network traffic processed.

It is important to carefully review and understand the support backlining for firmware upgrades and sometime free upgrades along with other payment terms before entering into an agreement. It is also recommended to discuss and negotiate any potential discounts or incentives that may be available, based on the number of devices enrolled or the length of the agreement. The specific payment terms will depend on the solution being offered. It's always recommended to carefully review the terms and conditions of an NGFW solution.

4.4 Pre-sales cue: Solution building complexities

4.4.1 Sizing the solution

Sizing an NGFW solution involves determining the appropriate resources and capacities required to effectively manage and secure mobile devices in your organization. Here are some factors to consider when sizing:

1. Network size and complexity: The size and complexity of the network, including the number of devices, locations, and types of devices, will impact the size of the NGFW solution required.
2. Traffic volume and throughput: The amount of network traffic and the rate at which it needs to be processed will impact the size and capacity of the NGFW solution required.
3. Applications and services: The specific applications and services being used in the network will impact the size of the NGFW solution required, as different applications may have different security requirements.
4. Security requirements: The level of security required for the network, such as the need for intrusion prevention, advanced threat protection, or data loss prevention, will impact the size of the NGFW solution required.
5. Cloud provider capabilities: The capabilities of the cloud provider, including the available security features and the capacity of their infrastructure, will impact the size of the cloud NGFW solution required. Be extremely clear of what the cloud service providers call as “Shared Responsibility matrix”. This is a potential black hole of cost over-runs. Additionally, it is important to consider the resources and capabilities available through the cloud provider, such as virtual machine size, storage capacity, and network throughput. This will ensure that the cloud NGFW solution is optimized for performance and security and is able to meet the needs of the network.
6. Passive components: Passive components refer to hardware components that do not require a power source to function. For this, you may need to work with a different 3rd party vendor. In the context of a Next-Generation Firewall (NGFW) implementation, the following passive components may be required:

a. Cables: Network cables, such as Ethernet cables, may be required to connect the NGFW to other network components, such as routers, switches, and servers.

b. Rack Mounting Brackets: If the NGFW is a physical appliance, it may require rack mounting brackets to be installed in a server rack.

c. SFP Modules: Small Form-Factor Pluggable (SFP) modules may be required to provide fibre connectivity to the NGFW.

d. Patch Panels: Patch panels may be used to terminate cables and provide a central location for cable management.

e. Cable Management: Cable management systems, such as cable trays or raceways, may be required to organize and secure cables within a server rack or data centre.

7. Monitoring and Management The monitoring and management of an NGFW solution involves several tasks to ensure that the solution is functioning properly and effectively protecting the network. Some common tasks include:

    a. Traffic analysis: Regularly monitoring network traffic to identify any unusual activity or security threats.

    b. Log management: Collecting and analysing logs from the NGFW solution to detect and respond to security incidents.

    c. Configuration management: Regularly reviewing and updating the configuration of the NGFW solution to ensure that it is optimized for performance and security.

    d. Software updates and patches: Keeping the NGFW software up to date with the latest security updates and patches. Check and implement backlining with technology owner. This hidden cost gets missed the most and causes project and cost over-runs later.

    e. Performance monitoring: Regularly monitoring the performance of the NGFW solution to ensure that it is functioning as expected and meeting the needs of the network.

    f. The frequency and detail of monitoring and management tasks will depend on the size and complexity of the network and the security requirements of the organization. It is important to have a plan in place for monitoring and managing the NGFW solution to ensure its effectiveness and to minimize the risk of security incidents.

To size a comprehensive NGFW solution, it is recommended to work with a technology owner, system integrator, and managed security services partner who has experience with NGFW implementations and can assist in determining the right solution based on the specific requirements of the network.

4.4.2 To what will NGFW solution connect to?

A Next-Generation Firewall (NGFW) solution will typically connect to the network at the perimeter to provide protection for the internal network and its connected devices. The

NGFW will typically be placed between the Internet and the internal network to act as the first line of defense against external security threats. The NGFW solution will typically be connected to the following network components:

1. Router: The NGFW solution will connect to the router to control incoming and outgoing network traffic.
2. Switch: The NGFW solution will connect to the switch to monitor and control traffic within the internal network.
3. Servers and endpoints: The NGFW solution will connect to servers and endpoints within the network to provide protection for these devices and the data they contain.
4. Wireless access points: If the network includes wireless access points, the NGFW solution may connect to these devices to provide security for wireless traffic.
5. Management systems: NGFW solutions can integrate with management systems, such as security information and event management (SIEM) systems, to provide centralized management and reporting of antivirus activity.

The specific components that the NGFW solution will connect to will depend on the size and complexity of the network and the security requirements of the organization. It is important to work with a vendor or solution provider who has experience with NGFW implementations to ensure that the solution is connected to the right components and configured correctly. The System Integrator should be able to provide guidance and recommendations on the most appropriate integration approach.

4.4.3 Implementation steps of NGFW solution

The implementation of a Next-Generation Firewall (NGFW) solution typically involves the following steps

1. Planning and Assessment: Conduct a thorough assessment of the network to determine the specific security requirements and identify any potential implementation challenges. This step should also include the development of a project plan, including a timeline and budget.
2. Architecture Design: Design the NGFW architecture,
    a. determining the types of traffic that need to be monitored and protected, traffic flow including the source and destination of the traffic, and the types of applications and protocols that are being used, and security requirements including access control policies, traffic filtering policies, and intrusion prevention policies,
    b. any specific compliance requirements that must be met taking into consideration the network topology,
    c. location of the firewall, the type of firewall (physical, virtual, or cloud-based), and the connection points to the rest of the network,
    d. selection of appropriate hardware and software components, including firewall appliances, virtual firewalls, and cloud-based firewalls as well as any necessary passive components, such as cables and rack mounting brackets,

e. plan for the scalability and high availability of the NGFW solution, taking into consideration the expected growth of the network, and the need for reliable, continuous protection. This may involve the deployment of multiple firewalls, or the use of high availability features, such as failover or load balancing, and

f. validate the design of the NGFW architecture to ensure that it meets the specific security requirements of the network, and that it is aligned with the overall security strategy of the organization. This step may involve conducting a risk assessment or working with a third-party security consultant to review the design.

3. Deployment:

   a. Before starting the installation, it is important to plan the deployment, including determining the appropriate placement of the firewall within the network, and ensuring that the necessary hardware and software components are available.

   b. Prepare the network for the installation of the NGFW, including configuring any necessary switches, routers, or access points to support the firewall.

   c. Install and configure the NGFW hardware and software components, including connecting the firewall to the network and configuring the firewall policies. This step may also involve the deployment of any necessary passive components, such as cables and rack mounting brackets.

   d. Configure the firewall, including setting up the network interfaces, configuring the firewall policies, and setting up any necessary VPN connections.

   e. Test the NGFW solution to ensure that it is functioning as expected and that security policies are properly enforced. This step should also involve validating the performance and scalability of the solution to ensure that it can handle the expected network traffic. This may involve conducting a series of security tests or working with a third-party security consultant to validate the firewall configuration.

   f. Integrate the NGFW with any existing security tools, such as intrusion detection systems, log management systems, or threat intelligence feeds, to ensure that the firewall is able to provide the desired level of protection.

4. Configuration and Management: Configure and manage the NGFW solution to ensure that it is functioning optimally and that security policies are properly enforced. This step may also involve the integration of the NGFW solution with other security tools, such as intrusion detection systems and threat intelligence platforms.

5. Ongoing Maintenance: Regularly monitor and maintain the NGFW solution to ensure that it is functioning optimally and that security policies are properly enforced. This step may also involve the regular update of the NGFW solution to address any vulnerabilities or performance issues.

It is important to work with a system integrator who has experience with NGFW implementations to ensure that the solution is properly deployed, configured, and maintained. Additionally, it is important to ensure that the implementation is aligned with the

overall security strategy of the organization, and that appropriate training is provided for network administrators and security personnel.

4.4.4 What can go wrong in NGFW solution

There are several things that can go wrong when implementing an NGFW solution, including:

1. Configuration errors: Configuration errors, such as incorrect firewall policies, incorrect network interface configurations, or incorrect VPN configurations, can result in security vulnerabilities or reduced performance.
2. Performance issues: Performance issues, such as slow network performance or high resource utilization, can impact the overall effectiveness of the NGFW solution, and can result in delays in processing traffic or reduced reliability.
3. Integration issues: Integration issues, such as compatibility problems with existing security tools, or difficulties integrating the NGFW with existing network infrastructure, can impact the overall effectiveness of the NGFW solution, and can result in security gaps or reduced visibility into network activity.
4. Security incidents: Security incidents, such as unauthorized access to network resources, data breaches, or malware infections, can occur if the NGFW is not properly configured or maintained, or if attackers are able to bypass the firewall.
5. Resource constraints: Resource constraints, such as insufficient memory or processing power, can impact the performance of the NGFW solution, and can result in reduced reliability or reduced capacity to process traffic.
6. Technical problems: Technical problems, such as software bugs, hardware failures, or network outages, can impact the functionality of the NGFW solution, and can result in reduced reliability or reduced capacity to process traffic.

To minimize the risk of these potential issues, it is important to follow best practices for configuring, deploying, and maintaining NGFW solutions, including regular software updates, routine security audits, and ongoing security training for network administrators and security personnel. Additionally, it is important to work with experienced security professionals to ensure that the NGFW solution is properly integrated with existing security tools and infrastructure, and that any potential issues are quickly identified and addressed.

4.4.5 What Service Levels can be committed/ expected?

Service Level Agreements (SLAs) in NGFW solutions can vary depending on the specific needs of an organization and the level of service offered by the provider. However, some common SLAs that can be committed in NGFW solution include:

1. Availability: The guaranteed percentage of time that the NGFW will be available for use, measured in uptime, and defined as the amount of time that the firewall is operational and accessible, excluding planned maintenance or upgrades.
2. Performance: The minimum performance standards for the NGFW, including network throughput, latency, and other performance metrics, such as the number of concurrent connections that can be supported.

3. Support: The level of support that will be provided by the vendor, including the hours of support availability, response times, and the types of support services that are included, such as troubleshooting and maintenance.
4. Security: The level of security that will be provided by the NGFW, including the types of threats that the firewall is designed to protect against, and the level of protection that is provided against those threats.
5. Reporting: The level of reporting that will be provided by the vendor, including the types of reports that will be generated, the frequency of reporting, and the level of detail that is included in each report.
6. Updates and upgrades: The frequency of software updates and upgrades that will be provided by the vendor, and the process for deploying those updates and upgrades.
7. Compliance: The level of compliance with relevant security and privacy regulations and standards, such as PCI DSS, HIPAA, or GDPR.

It is important to negotiate service levels that are appropriate for the specific NGFW solution and the client's needs, and to agree on a service level agreement (SLA) that is clearly defined and measurable. Additionally, it is important to regularly review the service levels to ensure that they remain relevant and effective, and to take appropriate steps to resolve any issues or challenges that arise during the deployment and use of the NGFW solution.

4.4.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.
2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

4.5 Delivery cue- NGFW operations

4.5.1 Daily Activities

Daily NGFW operation activities typically include the following tasks:

1. Monitoring: Monitoring the firewall's performance and logs to detect any potential security incidents, performance issues, or configuration errors, and taking appropriate action to address those issues.
2. Reporting: Generating regular reports on firewall performance, network activity, and security incidents, and reviewing those reports to identify trends and potential security risks.
3. Updating: Applying regular software updates and patches to the firewall to maintain the latest security and performance capabilities, and to resolve any known issues or vulnerabilities.
4. Maintenance: Performing routine maintenance tasks, such as backing up firewall configurations, testing disaster recovery procedures, or performing other system health checks.
5. Configuration: Modifying firewall configurations to meet changing network requirements, or to address any performance or security issues that have been identified.
6. Troubleshooting: Troubleshooting any issues that arise with the firewall, including performance problems, connectivity issues, or security incidents, and taking appropriate action to resolve those issues.
7. Incident response: Responding to any security incidents that occur, including investigating the cause of the incident, containing the impact, and taking appropriate action to restore normal operations.

It is important to have well-defined processes and procedures in place to manage the daily operations of the NGFW solution, and to ensure that all operations activities are performed in a consistent and effective manner. Additionally, it is important to regularly review and update those processes and procedures to ensure that they remain relevant and effective, and to ensure that the NGFW solution continues to meet the evolving needs and security requirements of the network.

4.5.2 Weekly Activities

Weekly NGFW operation activities typically include the following tasks:

1. Reviewing firewall logs: Reviewing the firewall's logs to identify any security incidents or performance issues that have occurred over the previous week, and taking appropriate action to address those issues.
2. Updating policies: Reviewing and updating firewall policies to ensure that they remain appropriate for the organization's security and compliance requirements.

3. Testing disaster recovery procedures: Performing regular testing of disaster recovery procedures to ensure that the NGFW solution can be quickly restored in the event of an unexpected outage.
4. Performing backups: Regularly backing up firewall configurations to ensure that the firewall can be quickly restored in the event of a hardware failure or other issue.
5. Reviewing performance: Reviewing the firewall's performance over the previous week to identify any trends or potential performance issues and taking appropriate action to address those issues.
6. Reviewing security incidents: Reviewing any security incidents that have occurred over the previous week, including investigating the cause of the incidents, determining the impact, and taking appropriate action to prevent similar incidents from occurring in the future.
7. Meeting with stakeholders: Holding regular meetings with stakeholders to review the current state of the firewall, discuss any issues or challenges that have arisen, and make any necessary changes to the firewall's configuration or operations.

It is important to have well-defined processes and procedures in place for managing the weekly operations of the NGFW solution, and to ensure that all operations activities are performed in a consistent and effective manner. Additionally, it is important to regularly review and update those processes and procedures to ensure that they remain relevant and effective, and to ensure that the NGFW solution continues to meet the evolving needs and security requirements of the network.

4.5.3 Monthly Activities

Monthly NGFW operation activities typically include the following tasks:

1. Monitoring: Regular monitoring of the firewall logs to detect and respond to any security threats or suspicious activities.
2. Security policy review: Reviewing and updating the firewall security policies to ensure that they are aligned with the organization's current security needs and standards.
3. Software updates: Installing the latest software and firmware updates to ensure that the firewall is running on the latest version and has the latest security features and bug fixes.
4. Traffic analysis: Analysing network traffic to identify any unusual patterns or activities that may indicate a security threat.
5. Vulnerability assessments: Conducting regular vulnerability assessments to identify any vulnerabilities in the firewall configuration and to ensure that they are addressed promptly.
6. Backup and disaster recovery planning: Regularly backing up the firewall configuration and preparing a disaster recovery plan to ensure that the firewall can be quickly restored in case of a failure.

7. Reporting: Generating regular reports on the firewall's performance and security posture, to provide visibility into the effectiveness of the firewall's security measures.

It is important to establish a routine and regularly perform these monthly activities to ensure that the NGFW solution is functioning properly and providing the necessary protection and support. Additionally, these monthly activities can help identify areas for improvement and ensure that the NGFW solution continues to meet the evolving needs of the organization.

4.5.4 What does an L1, L2, L3 NGFW Engineer do?

The roles and responsibilities of an L1, L2, and L3 NGFW Engineer vary based on the level of support they provide. However, in general, the following are the responsibilities of each level:

L1 NGFW Engineer:

1. Provide first-level technical support to resolve basic firewall-related issues
2. Troubleshoot simple firewall problems and perform routine maintenance tasks
3. Escalate complex issues to higher-level engineers for resolution
4. Help Desk Support: Responding to client inquiries and resolving basic firewall-related issues through a help desk or ticketing system.
5. Routine Maintenance: Performing routine maintenance tasks such as checking firewall logs, monitoring traffic patterns, and verifying firewall performance.
6. Basic Configuration Changes: Making basic configuration changes to the firewall such as modifying firewall rules, adding new users, and updating security policies.
7. Problem Escalation: Escalating complex or technical issues to higher-level engineers for resolution.
8. Documentation: Keeping detailed documentation of all firewall-related issues and their resolutions.
9. User Training: Providing basic training to users on the use of the firewall and its features.
10. Technical Assistance: Providing technical assistance to lower-level engineers on basic firewall-related issues.
11. Compliance Monitoring: Monitoring firewall configuration and performance to ensure compliance with company policies and industry standards.

L2 NGFW Engineer:

1. Provide second-level technical support to resolve intermediate firewall-related issues
2. Troubleshoot complex firewall problems and perform advanced maintenance tasks
3. Escalate critical issues to higher-level engineers for resolution
4. Intermediate Troubleshooting: Troubleshooting intermediate-level firewall-related issues and resolving them in a timely manner.
5. Advanced Maintenance: Performing advanced maintenance tasks such as firmware upgrades, backups, and disaster recovery planning.

6. Complex Configuration Changes: Making complex configuration changes to the firewall such as creating new firewall policies, implementing VPNs, and integrating the firewall with other security systems.
7. Incident Response: Responding to security incidents and performing root cause analysis to determine the source of the issue.
8. Problem Escalation: Escalating critical issues to higher-level engineers for resolution.
9. Knowledge Management: Staying up to date with the latest firewall technologies and security trends and sharing knowledge with the rest of the team.
10. Performance Monitoring: Monitoring firewall performance and capacity utilization and making recommendations for optimization.
11. Technical Assistance: Providing technical assistance to lower-level engineers on intermediate firewall-related issues.
12. Compliance Monitoring: Monitoring firewall configuration and performance to ensure compliance with company policies and industry standards.

L3 NGFW Engineer:

1. Provide third-level technical support to resolve advanced firewall-related issues
2. Troubleshoot complex firewall problems and perform advanced maintenance tasks
3. Manage and resolve critical firewall-related incidents
4. Perform root cause analysis and implement preventive measures
5. Act as a subject matter expert and provide guidance to lower-level engineers
6. Advanced Troubleshooting: Troubleshooting complex firewall-related issues and resolving them in a timely manner.
7. Expert Maintenance: Performing expert-level maintenance tasks such as performance tuning, system upgrades, and complex configuration changes.
8. Incident Management: Leading incident response efforts, performing root cause analysis, and implementing preventive measures.
9. Design and Architecture: Designing and architecting firewall solutions to meet the organization's security requirements.
10. Technical Leadership: Acting as a technical leader and subject matter expert, providing guidance and mentorship to lower-level engineers.
11. Knowledge Management: Staying up to date with the latest firewall technologies and security trends and sharing knowledge with the rest of the team.
12. Performance Monitoring: Monitoring firewall performance and capacity utilization and making recommendations for optimization.
13. Compliance Monitoring: Monitoring firewall configuration and performance to ensure compliance with company policies and industry standards.
14. Vendor Management: Managing relationships with firewall vendors and ensuring that the organization is receiving the best possible support and services.

15. Strategic Planning: Participating in strategic planning efforts and providing input on the organization's long-term firewall needs and objectives.

The roles and responsibilities of an NGFW Engineer may vary depending on the organization and the specific job requirements. These are general responsibilities that are commonly associated with each level of support.

4.5.5 Reports

NGFW operation reports provide valuable information about the performance and security of a network's firewall system. Some common types of reports that are generated by NGFW operations include:

1. Firewall Traffic Report: Provides information on the volume of traffic that is passing through the firewall, including the number of bytes transmitted and received, the number of packets, and the number of sessions.
2. Firewall Threat Report: Provides information on the number of security threats that have been detected and blocked by the firewall, including the type of threat, the source of the threat, and the time it was detected.
3. Firewall Configuration Report: Provides information on the configuration of the firewall, including the firewall rules, the security policies, and the user accounts.
4. Firewall Performance Report: Provides information on the performance of the firewall, including the processing time for packets, the response time for sessions, and the utilization of firewall resources.
5. Firewall Compliance Report: Provides information on the compliance of the firewall with company policies and industry standards, including any deviations from the standard configuration and any security incidents that have been detected.
6. Firewall Audit Report: Provides information on the firewall's compliance with regulatory requirements, including the results of security audits and penetration testing.

These reports can help NGFW engineers identify trends, assess the effectiveness of the firewall, and make informed decisions about firewall maintenance and security. They can also be used to demonstrate the value of the firewall to the organization and to secure funding for future firewall projects.

4.5.6 Governance of NGFW solution

The governance of an NGFW solution is a critical aspect of its implementation and management, as it ensures that the firewall is being used effectively and securely. The following are some of the key elements of NGFW governance:

1. Policy Development: Developing and maintaining clear and concise policies that define the organization's security requirements and expectations for the NGFW solution.
2. Risk Assessment: Assessing the security risks associated with the NGFW solution and implementing appropriate controls to mitigate these risks.

3. Change Management: Implementing a robust change management process to ensure that all changes to the NGFW solution are well-planned, tested, and approved before they are implemented in production.
4. Compliance Monitoring: Monitoring the configuration and performance of the NGFW solution to ensure that it follows company policies and industry standards.
5. Incident Management: Implementing a comprehensive incident management process to ensure that security incidents are detected, investigated, and resolved in a timely and effective manner.
6. Auditing and Monitoring: Performing regular audits and monitoring of the NGFW solution to identify any security vulnerabilities and to ensure that it is being used as intended.
7. User Management: Implementing robust user management policies to ensure that only authorized users have access to the firewall and its features.
8. Technical Support: Providing timely and effective technical support for the NGFW solution, including training and guidance for users.
9. Vendor Management: Managing relationships with firewall vendors and ensuring that the organization is receiving the best possible support and services.

By implementing these elements of NGFW governance, organizations can ensure that their firewall solution is secure, effective, and meeting their security needs. Regularly reviewing and updating governance policies and procedures can help ensure that the solution remains effective and efficient over time.

5. Web Security- Web Application Firewall

A Web Application Firewall (WAF) is a security solution that protects web applications from various types of cyber-attacks, such as *SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF)*.

WAFs operate by inspecting incoming HTTP traffic and blocking malicious requests before they reach the web application. They use a set of predefined security rules or a machine learning algorithm to identify and block malicious requests based on the characteristics of the request, such as the URL, HTTP headers, and request parameters.

5.1 SQL injection, Cross-site Scripting (XSS), Cross-site request forgery (CSRF)

SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) are common types of cyber-attacks that target web applications.

SQL Injection: SQL injection is a type of attack that allows *an attacker to execute malicious SQL code on a web application's database*. This can result in sensitive data being compromised, such as login credentials, financial information, and other sensitive information stored in the database.

Cross-Site Scripting (XSS): XSS is a type of attack that allows an attacker to inject malicious scripts into a web page that is viewed by other users. This can be done through various techniques, such as *URL parameters*, form fields, and comments in a blog or forum. An attacker can inject malicious scripts into a web page through several methods, including:

1. Persistent XSS: This type of XSS attack involves injecting a malicious script into a web page that is stored on the server and served to all users who view the page.
2. Reflected XSS: This type of XSS attack involves injecting a malicious script into a web page that is executed immediately when the page is loaded. The malicious script is sent to the server as part of a request and reflected back to the user in the response.
3. DOM-based XSS: This type of XSS attack occurs in the client-side JavaScript code and involves manipulating the Document Object Model (DOM) of a web page to inject a malicious script.

Once the malicious script is injected into the web page, it can be used to steal sensitive information, such as login credentials, or to execute malicious actions on behalf of the user, such as posting spam or making unauthorized purchases. It is important for organizations to implement security measures, such as input validation, to prevent XSS attacks and protect their web applications from this type of vulnerability.

Cross-Site Request Forgery (CSRF): CSRF is a type of attack that tricks a user into performing actions on a web application, such as changing their password or making a purchase, without their knowledge. The attacker exploits the trust that the web application has in the user's browser to execute actions on the user's behalf.

In a CSRF attack, the attacker creates a malicious webpage or email that contains a hidden form or link that submits a request to a vulnerable web application on behalf of the victim. The victim is tricked into visiting the malicious webpage or email, and their browser automatically submits the malicious request without their knowledge or consent.

For example, consider a web application that allows users to change their password. The change password form might be vulnerable to CSRF if it does not include proper protection, such as a unique token that is verified on the server. An attacker could create a malicious webpage that contains a hidden form that submits a request to change the victim's password, like this:

```
<html>
 <body>
  <form action="https://www.example.com/change-password" method="POST">
   <input type="hidden" name="password" value="new_password">
   <input type="hidden" name="confirm_password" value="new_password">
   <input type="submit" style="display: none;">
  </form>
  <script>
   document.forms[0].submit();
  </script>
 </body>
</html>
```

When the victim visits the malicious webpage, their browser will automatically submit the form and change their password without their knowledge or consent. To protect against CSRF attacks, web applications should implement proper CSRF protection, such as including a unique token in all form submissions that is verified on the server, or by using the SameSite attribute in cookies. Additionally, users should be cautious when clicking on links or visiting web pages that they are not familiar with.

These types of attacks can result in significant damage to an organization, including loss of sensitive data, financial loss, and harm to reputation. It is important for organizations to implement security measures, such as using web application firewalls and input validation, to prevent these types of attacks and protect their web applications.

5.2 How does an attacker execute malicious SQL code on a web application's database?

An attacker can execute malicious SQL code on a web application's database by exploiting vulnerabilities in the web application's code. This type of attack is called a SQL Injection attack.

SQL injection attacks occur when a web application takes user-supplied data and uses it to build a SQL query that is executed against the database. If the user-supplied data is not properly validated and sanitized, an attacker can craft malicious input that causes the query to behave in unexpected ways.

For example, consider a web application that allows users to search for products in a database. The search query is constructed from user-supplied data as follows:

```
SELECT * FROM products WHERE name = '$search_term'
```

Where $search_term is the user-supplied data. If an attacker crafts the following search term:

*SELECT * FROM products WHERE name = '' OR '1'='1'*

This query would return all rows in the products table, regardless of the product name, because the condition '1'='1' is always true. In a more malicious scenario, an attacker could craft a search term that includes arbitrary SQL code, like this:

'; DROP TABLE products; --

The resulting query would become:

*SELECT * FROM products WHERE name = ''; DROP TABLE products; --'*

This query would cause the products table to be dropped, effectively deleting all of its data.

To protect against SQL injection attacks, it is important for web applications to properly validate and sanitize user-supplied data before using it to build SQL queries. This can be done by using prepared statements with placeholders or by escaping special characters in the user-supplied data.

5.3 What are URL parameters?

URL parameters are the data that is passed from a client to a server as part of a URL. They are used to pass information to a web application and are typically used for dynamic web pages, such as search results pages or product detail pages.

For example, consider a URL for a search results page on an e-commerce website:

https://www.example.com/search?q=shoes

In this example, the URL parameter "q=shoes" is passed to the server and used to retrieve search results for the term "shoes".

URL parameters can be vulnerable to attack if they are not properly validated and sanitized on the server. An attacker could manipulate the parameters to inject malicious code or to modify the behaviour of the web application. For example, an attacker could modify the URL parameter to inject a cross-site scripting (XSS) payload, like this:

https://www.example.com/search?q=<script>alert('XSS Attack')</script>

If the web application is vulnerable to XSS, the attacker's payload will be executed when the search results page is loaded, potentially compromising the security of the web application and its users. To protect against these types of attacks, it is important for web applications to properly validate and sanitize URL parameters on the server to ensure that they are safe and do not contain malicious code.

5.4 What are key benefits of using WAF?

Some key benefits of using a WAF include:

1. Protection against cyber-attacks: WAFs provide protection against a wide range of cyber-attacks that target web applications, including SQL injection, XSS, and CSRF.
2. Compliance: WAFs can help organizations meet security and privacy regulations, such as the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR).

3. Improved performance: By blocking malicious requests, WAFs can reduce the load on web applications and improve performance.
4. Easier management: WAFs provide a centralized location for managing web application security, making it easier for administrators to monitor and manage security.
5. Customization: Many WAFs allow administrators to customize the security rules to meet the specific needs of their organization.

WAFs are an important component of an overall web application security strategy and can help organizations protect their web applications from cyber-attacks and meet security and privacy regulations.

5.5 Web Application Firewall types

There are two main types of Web Application Firewalls (WAFs):

1. Network-based WAF: Network-based WAFs are installed on the network perimeter and operate at the network layer (layer 7 of the OSI model). They inspect incoming traffic to the web application and block malicious requests based on rules and signature-based detection.
2. Application-based WAF: Application-based WAFs are integrated into the web application itself and operate at the application layer (layer 7 of the OSI model). They have a deeper understanding of the application and its behaviour, allowing for more precise and effective security protection.

Both types of WAFs can provide protection against a range of web application threats, including SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). Some WAFs also include additional security features, such as rate limiting, IP reputation analysis, and bot detection.

Rate limiting: Rate limiting is a security mechanism that restricts the rate at which incoming requests to a web application can be made. The purpose of rate limiting is to prevent malicious actors from overwhelming a web application with a large number of requests, a technique known as a "denial of service" (DoS) attack. By setting a limit on the number of requests that can be made in a certain time period, rate limiting can help ensure that the web application remains available and responsive to legitimate users.

IP reputation analysis: IP reputation analysis is a security feature that helps identify and block traffic from known malicious IP addresses. The reputation of an IP address can be determined based on a variety of factors, such as the number of prior attacks that have originated from that IP, the type of attacks that have been performed, and the geographical location of the IP. IP reputation analysis can help reduce the risk of attacks that are initiated by automated tools and botnets.

Bot detection: Bot detection is a security feature that helps identify and block traffic from automated tools, known as "bots." Bots can be used for a variety of malicious purposes, such as scraping data from a web application, launching DoS attacks, or performing brute-force attacks on login forms. By detecting and blocking bots, a web application can reduce the risk of these types of attacks and ensure that the web application is only accessible to legitimate users.

Rate limiting, IP reputation analysis, and bot detection are all important security features that can help protect web applications from a range of threats. These features can be incorporated into a Web Application Firewall (WAF) or other security solution to provide comprehensive protection for a web application.

The choice between a network-based and application-based WAF depends on the specific security requirements and architecture of a web application. In general, network-based WAFs are a good option for web applications that are deployed in a traditional data centre environment, while application-based WAFs are a good option for cloud-based web applications or for organizations that want to have more control over the security of their applications.

5.6 Sales cue- Questions to ask and answers to give

5.6.1 Questions to ask prospective client on WAF opportunity

When exploring if a prospective client needs Web Application Firewall, some questions you may want to ask:

1. What type of web applications do you have? Understanding the types of web applications that need to be protected can help determine the level of security required.
2. How sensitive is the information processed by the web application? If the web application processes sensitive information, such as credit card numbers, personal information, or medical records, a WAF may be necessary to protect this information from theft or unauthorized access.
3. Has the web application been the target of a security breach in the past? If a web application has been the target of a successful attack in the past, it may be necessary to implement a WAF to prevent similar attacks from happening again.
4. How critical is the web application to your business operations? If a web application is critical to the business operations, a WAF can help ensure that the web application remains available and responsive even in the event of an attack.
5. What is the current security infrastructure of the web application? If the web application is currently protected by firewalls, intrusion detection/prevention systems, or other security solutions, a WAF may still be necessary to provide additional security.
6. What is the budget for web application security? Implementing a WAF can be a significant investment, so it is important to determine the budget for web application security and determine if a WAF is affordable.

By asking these questions, you can get a better understanding of the security needs of the web application and whether a WAF is necessary to protect it from threats.

5.6.2 Questions prospective clients will ask of sales

Clients evaluating Web Application Firewall solutions may have a variety of questions based on their specific needs and requirements. Here are some common questions that clients ask:

1. What security features does the WAF offer? Does the WAF have features such as rate limiting, IP reputation analysis, bot detection, SQL injection protection, cross-site scripting (XSS) protection, and cross-site request forgery (CSRF) protection?
2. How does the WAF integrate with your existing security infrastructure? Can the WAF integrate with your existing firewalls, intrusion detection/prevention systems, or other security solutions?
3. What is the deployment process like? Is the WAF easy to deploy and manage?
4. How does the WAF handle false positive and false negative security alerts? What is the process for resolving false positive and false negative alerts?
5. Does the WAF provide detailed reporting and analytics? Does the WAF provide the ability to view detailed logs and reports to help identify and respond to security threats?
6. What is the pricing structure of the WAF? Is the WAF offered as a standalone solution or as part of a suite of security solutions? What is the cost of the WAF, and what is included in the cost?
7. What type of support does the vendor offer for the WAF? Does the vendor provide 24/7 support, and what is the process for getting support?
8. What is the reputation of the vendor and the WAF? Have other organizations used the WAF successfully? What are the reviews and ratings of the WAF?
9. How are you planning to monitor and manage the WAF solution?

By asking these questions, clients can get a better understanding of the WAF and its capabilities and make an informed decision about whether it is the right solution for their organization's security needs.

5.6.3 Payment terms to agree with the clients

All WAF technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays WAF technology owners via distributors) payment options with clients always keeps the cash-registers green and healthy.

The payment terms for WAF solutions can vary depending on the specific solution. Here are some common payment terms' considerations that clients may agree with clients and WAF technology owners:

1. Payment Frequency: Will the client be paying monthly, quarterly, or annually?
2. Payment Method: Will the client be paying by credit card, wire transfer, or check?
3. Invoicing: Will invoices be sent electronically or via regular mail?
4. Payment Due Date: When is payment due, and what is the process for late payments?
5. Pricing Structure: Is the pricing based on a fixed rate, a usage-based model, or a combination of both?

6. Renewal Terms: How will renewals be handled, and what is the process for renewing the WAF service?
7. Refund Policy: What is the policy for refunds, and what is the process for requesting a refund?
8. Termination Policy: What is the process for terminating the WAF service, and what is the policy for any outstanding payments in the event of termination?
9. Late Payment Fees: Are late payment fees applicable, and if so, what is the amount of the fee?
10. Operations Costs: How will a services provider deliver the services and at what cost?

It is important to carefully review and understand the payment terms before entering into an agreement. The specific payment terms will depend on the solution being offered. It's always recommended to carefully review the terms and conditions of an WAF solution before making a purchase.

5.7 Pre-sales cue: Solution building complexities

5.7.1 Sizing the WAF solution

Sizing a Web Application Firewall solution involves several factors to consider, including:

1. Traffic Volume: The amount of traffic that the WAF will need to process is an important factor in sizing the WAF solution. This includes both incoming and outgoing traffic and the volume of requests per second.
2. Bandwidth Requirements: The amount of bandwidth required by the WAF will depend on the traffic volume and the size of the requests.
3. Number of Applications: The number of applications that will be protected by the WAF will also impact the sizing of the solution.
4. Application Complexity: The complexity of the applications being protected by the WAF, such as the number of database connections and dynamic content, will also impact the sizing of the solution.
5. Compliance Requirements: Any compliance requirements, such as PCI DSS, that the WAF needs to meet will also impact the sizing of the solution.
6. Customization Requirements: The level of customization required for the WAF, such as custom rule sets, will also impact the sizing of the solution.

It is important to work with a WAF technology owner or consult with system integrators and managed services providers to properly size the WAF solution to ensure that it can handle the expected traffic volume and meet the specific needs of the organization. Over-sizing the solution may result in excessive costs, while under-sizing the solution may result in inadequate security.

5.7.2 To what will WAF solution connect to?

WAF solutions can integrate with a variety of other systems to enhance their functionality and capabilities. Some common systems that may connect to WAF solution include:

1. Web Server: The WAF solution is typically deployed in front of the web server to protect the applications hosted on the server.
2. Load Balancer: If the organization is using a load balancer, the WAF solution may connect to the load balancer to balance the incoming traffic across multiple web servers.
3. Database Server: If the web application accesses a database, the WAF solution may also connect to the database server to protect against database-related attacks.
4. Network Devices: The WAF solution may connect to network devices, such as routers and switches, to monitor and control network traffic.
5. Monitoring and Logging Systems: The WAF solution may also connect to monitoring and logging systems, such as log management and SIEM platforms, to provide detailed information on security events and incidents.
6. Authentication and Authorization Systems: The WAF solution may connect to authentication and authorization systems, such as LDAP or AD, to provide user and role-based access control.

The specific connection points and configurations will vary depending on the specific requirements and architecture of the organization's infrastructure. The System Integrator should be able to provide guidance and recommendations on the most appropriate integration approach.

5.7.3 Implementation steps of WAF solution

The implementation of a Web Application Firewall solution typically involves the following steps:

1. Assessment: Assess the current web application security posture and identify the specific security requirements for the organization. This step may include conducting a penetration test or security assessment to identify any vulnerabilities or potential attack vectors.
2. Planning: Plan the implementation of the WAF solution, including determining the deployment architecture, the specific components required, and the integration with existing security and network infrastructure.
3. Deployment: Deploy the WAF solution in accordance with the planned architecture, including configuring the firewall policies and rules, and connecting it to the web server, database server, and other components as required.
4. Testing: Test the WAF solution to ensure that it is properly configured and working as expected. This may include conducting penetration testing and other security testing to validate the effectiveness of the WAF in blocking known attack vectors and mitigating security risks.

5. Ongoing Management: Manage and maintain the WAF solution on an ongoing basis, including updating the firewall policies and rules, monitoring security events, and conducting regular security assessments to ensure the continued effectiveness of the solution.

It is important to involve security experts and work with a trusted vendor to ensure a smooth and successful implementation of the WAF solution. The specific implementation steps may vary based on the specific requirements and architecture of the organization.

5.7.4 What can go wrong in WAF solution

There are several things that can go wrong when implementing a WAF solution, including:

1. Configuration errors: The WAF solution may be improperly configured, which can result in false positives (incorrectly blocking legitimate traffic) or false negatives (failing to detect and block malicious traffic).
2. Compatibility issues: The WAF solution may not be compatible with other components in the organization's infrastructure, such as web servers, database servers, or network devices, which can result in performance or functionality issues.
3. Overhead and Latency: The WAF solution may introduce latency or overhead, slowing down the performance of the web application and affecting the user experience.
4. False sense of security: Organizations may have a false sense of security if they rely solely on a WAF solution to secure their web applications, without implementing additional security controls or following best practices for web application security.
5. Lack of Expertise: Organizations may not have the necessary expertise to properly implement, manage, and maintain the WAF solution, which can result in security vulnerabilities or ineffective protection against attacks.
6. Maintenance and Updates: Regular maintenance and updates are required to keep the WAF solution current and effective, including updating firewall policies and rules, and addressing vulnerabilities as they are discovered.
7. Blind spots: The WAF solution may not protect against all types of attacks and may have blind spots that can be exploited by attackers.

It is important to work with security experts, system integrators and trusted managed security services providers, and to follow best practices for web application security, to minimize the risk of these issues and ensure the effectiveness of the WAF solution.

5.7.5 What Service Levels can be committed/ expected?

Service Level Agreements (SLAs) in WAF services can vary depending on the specific needs of an organization and the level of service offered by the provider. However, some common SLAs that can be committed in WAF solution include:

1. Uptime: The guaranteed availability of the WAF solution, expressed as a percentage of time over a specified period. For example, an uptime service level of 99.99% means that the WAF solution will be available for all but 0.01% of the time over a given year.

2. Performance: The guaranteed performance of the WAF solution, expressed in terms of latency, throughput, and other metrics. For example, a performance service level of 100 ms latency and 1 Gbps throughput means that the WAF solution will process requests within 100 milliseconds and handle up to 1 Gbps of traffic.
3. Support: The level of technical support and assistance provided by the vendor, including response times, availability of support personnel, and resolution times. For example, a support service level of 24/7 availability and 1-hour response time means that support will be available 24 hours a day, 7 days a week, and that a response to a support request will be provided within one hour.
4. Maintenance: The level of maintenance and updates provided by the vendor, including the frequency of updates, the scope of updates, and the impact of updates on the availability and performance of the WAF solution.
5. Compliance: The level of compliance with industry standards and regulations, such as PCI DSS, HIPAA, and others, as relevant to the organization.
6. Reporting: The level of reporting and visibility provided by the WAF solution, including access to logs, alerts, and other security-related data.

These service levels should be clearly defined in the agreement between the organization and the system integrator, technology owner, and managed security services provider, and should be regularly reviewed and updated as needed to ensure that the WAF solution continues to meet the evolving needs of the organization.

5.7.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.
2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible,

while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

5.8 Delivery cue- WAF operations

5.8.1 Daily WAF Activities

Daily WAFoperation activities typically include the following tasks:

1. Monitoring: Monitoring the WAF solution to ensure that it is functioning as expected and that there are no issues or failures. This may involve reviewing logs, alerts, and dashboards for any suspicious activity or potential threats.
2. Configuration: Updating and modifying the configuration of the WAF solution as needed to accommodate changes in the environment or to improve its performance and security.
3. Maintenance: Performing regular maintenance tasks, such as applying updates and patches, to ensure that the WAF solution is up to date and secure.
4. Threat intelligence: Staying up to date with the latest threat intelligence and security trends and incorporating that information into the WAF solution to better protect the organization.
5. Policy management: Managing the security policies that govern the behaviour of the WAF solution, including creating, modifying, and enforcing policies as needed.
6. Incident response: Responding to security incidents or alerts generated by the WAF solution, including conducting investigations, identifying the root cause of incidents, and taking appropriate remediation steps.
7. Reporting: Generating and reviewing reports on the performance and security of the WAF solution, including traffic patterns, attack trends, and security incidents.
8. Collaboration: Collaborating with other teams, such as network security, application development, and incident response, to ensure that the WAF solution is integrated with the organization's overall security posture and that security incidents are handled effectively.

These daily activities help to ensure that the WAF solution is functioning effectively, and that the organization is protected from potential threats and attacks.

5.8.2 Weekly WAF Activities

Weekly WAF operation activities typically include the following tasks:

1. Review: Reviewing logs, alerts, and dashboards from the previous week to identify any trends or patterns in security incidents or traffic.
2. Reporting: Generating weekly reports on the performance and security of the WAF solution, including traffic patterns, attack trends, and security incidents.

3. Policy management: Reviewing and updating security policies to ensure that they are current and relevant, and that the WAF solution is effectively protecting the organization.
4. Maintenance: Scheduling any necessary maintenance tasks, such as applying updates and patches, to ensure that the WAF solution is up to date and secure.
5. Threat intelligence: Reviewing and incorporating new threat intelligence and security trends into the WAF solution to improve its protection.
6. Collaboration: Collaborating with other teams, such as network security, application development, and incident response, to ensure that the WAF solution is integrated with the organization's overall security posture and that security incidents are handled effectively.
7. Planning: Planning for any upcoming changes or projects related to the WAF solution, such as updates to the environment or new security requirements.

These weekly activities help to ensure that the WAF solution is functioning effectively, that the organization is protected from potential threats and attacks, and that the solution is regularly reviewed and updated as needed.

5.8.3 Monthly WAF Activities

Monthly WAF operation activities typically include the following tasks:

1. Compliance review: Reviewing the WAF solution to ensure that it follows any relevant security standards, such as PCI DSS, and making any necessary updates to meet those standards.
2. Performance analysis: Analysing the performance of the WAF solution, including its throughput, response times, and resource utilization, to ensure that it is meeting the organization's needs.
3. Capacity planning: Planning for future capacity needs of the WAF solution, such as adding additional resources or updating the solution, to ensure that it continues to meet the organization's needs.
4. Licensing and maintenance: Reviewing and renewing any necessary licenses and maintenance agreements for the WAF solution to ensure that it continues to function effectively.
5. Integration: Integrating the WAF solution with other security systems, such as intrusion detection and prevention systems, to ensure that the organization has a comprehensive security posture.
6. Auditing: Auditing the WAF solution to ensure that it is functioning as intended and that security policies are being enforced.
7. Backup and recovery: Performing regular backups of the WAF solution and testing the recovery process to ensure that the organization can recover quickly and effectively in the event of an outage.

These monthly activities help to ensure that the WAF solution is functioning effectively, that the organization is protected from potential threats and attacks, and that the solution is regularly reviewed and updated as needed.

5.8.4 What does an L1 WAF Security Engineer do?

A Level 1 (L1) WAF Engineer is responsible for the basic level of support and maintenance of a WAF solution. The primary responsibilities of an L1 WAF Engineer typically include:

1. Monitoring: Monitoring the WAF solution for any security incidents or threats and responding to alerts and alarms in a timely manner.
2. Troubleshooting: Troubleshooting any technical issues that arise with the WAF solution and working with other members of the security team to resolve them.
3. Configuration: Configuring the WAF solution to meet the needs of the organization, including setting up security policies, rules, and alerts.
4. Maintenance: Performing routine maintenance and updates on the WAF solution to ensure that it continues to function effectively.
5. Documentation: Keeping documentation of the WAF solution up to date, including its configuration, maintenance activities, and security incidents.
6. Reporting: Generating reports on the performance and usage of the WAF solution, including security incidents and the effectiveness of security policies.
7. Communication: Communicating with other members of the security team and stakeholders within the organization to ensure that the WAF solution is functioning effectively and meeting the organization's needs.

L1 WAF Security Engineers play a crucial role in ensuring that the WAF solution is functioning effectively, and that the organization is protected from potential threats and attacks. They are responsible for providing the first line of support for the solution and ensuring that security incidents are responded to quickly and effectively.

5.8.5 What does an L2 WAF Security Engineer do?

A Level 2 (L2) WAF Engineer is responsible for a higher level of support and maintenance of a WAF solution. The primary responsibilities of an L2 WAF Engineer typically include:

1. Monitoring: Monitoring the WAF solution for any security incidents or threats and responding to alerts and alarms in a timely manner.
2. Troubleshooting: Troubleshooting complex technical issues that arise with the WAF solution, working with other members of the security team, and coordinating with vendors if necessary.
3. Configuration: Configuring the WAF solution to meet the needs of the organization, including setting up security policies, rules, and alerts, and ensuring that the WAF solution is configured optimally to meet the organization's needs.

4. Maintenance: Performing routine maintenance and updates on the WAF solution to ensure that it continues to function effectively and troubleshooting any issues that arise during maintenance activities.
5. Documentation: Keeping documentation of the WAF solution up to date, including its configuration, maintenance activities, and security incidents, and working with the L1 WAF Security Engineer to ensure that documentation is accurate and complete.
6. Reporting: Generating reports on the performance and usage of the WAF solution, including security incidents and the effectiveness of security policies, and analysing this data to identify areas for improvement.
7. Communication: Communicating with other members of the security team and stakeholders within the organization to ensure that the WAF solution is functioning effectively and meeting the organization's needs and working with the L1 WAF Security Engineer to ensure that communication is clear and effective.

L2 WAF Security Engineers play a critical role in ensuring that the WAF solution is functioning effectively, and that the organization is protected from potential threats and attacks. They are responsible for providing advanced support for the solution and working with other members of the security team to ensure that security incidents are responded to quickly and effectively. They also play a key role in ensuring that the WAF solution is configured optimally to meet the organization's needs and that its performance and usage are analyzed and reported on regularly.

5.8.6 What does an L3 WAF Security Engineer do?

The role of a Level 3 (L3) Web Application Firewall (WAF) Security Engineer is to provide expert-level support for the WAF solution in an organization. The responsibilities of an L3 WAF Security Engineer can include:

1. Design and Architecture: Designing and implementing the WAF solution to meet the needs of the organization, including defining security policies, rules, and alerts, and ensuring that the WAF solution is configured optimally to meet the organization's needs.
2. Problem Resolution: Resolving complex technical problems that arise with the WAF solution, working with other members of the security team, vendors, and other stakeholders, and coordinating the resolution of security incidents.
3. Performance Optimization: Optimizing the performance of the WAF solution, including analysing performance data and tuning the configuration to ensure that the solution is functioning optimally.
4. Research and Development: Conducting research and development activities to improve the functionality and security of the WAF solution, including identifying and testing new security technologies and features.
5. Knowledge Management: Maintaining a repository of knowledge about the WAF solution, including documentation, best practices, and lessons learned, and working with other members of the security team to ensure that this knowledge is shared and leveraged effectively.

6. Leadership: Providing leadership and mentorship to other members of the security team, including the L1 and L2 WAF Security Engineers, and ensuring that the WAF solution is managed and operated effectively.

L3 WAF Security Engineers play a critical role in ensuring that the WAF solution is functioning effectively and that the organization is protected from potential threats and attacks. They are responsible for providing expert-level support for the solution and working with other members of the security team to ensure that security incidents are responded to quickly and effectively. They also play a key role in ensuring that the WAF solution is designed, configured, and optimized to meet the organization's needs and that its performance and functionality are continually improved. As leaders within the security team, L3 WAF Security Engineers also play an important role in mentoring and developing other members of the team.

5.8.7 WAF Reports

The types of Web Application Firewall (WAF) operation reports can vary depending on the specific WAF solution being used and the needs of the organization. However, here are some common types of WAF operation reports:

1. Security Incidents: A report that provides details on security incidents that have been detected and responded to by the WAF solution, including the type of incident, the time and date of the incident, and the action taken to resolve the incident.
2. Rule and Policy Violations: A report that provides details on the violations of WAF security policies and rules, including the type of violation, the number of violations, and the time and date of the violations.
3. Traffic and Performance: A report that provides information on the traffic and performance of the WAF solution, including the volume of traffic, the number of requests, and the response time.
4. Threat Intelligence: A report that provides information on the latest threats and attack patterns detected by the WAF solution, including information on the type of threat, the source of the threat, and the response taken to mitigate the threat.
5. Compliance and Audit: A report that provides information on the compliance of the WAF solution with relevant regulations and standards, including information on the types of regulations and standards being met, and any gaps or non-compliance issues that need to be addressed.
6. Capacity Planning: A report that provides information on the current and future capacity requirements of the WAF solution, including information on the volume of traffic, the number of requests, and the response time, and projections for future growth.

These types of reports can provide valuable information for WAF administrators and security teams, helping them to monitor the performance and security of the WAF solution, respond to security incidents effectively, and make informed decisions about the design, configuration, and operation of the solution.

5.8.8 Governance of WAF solution

Governance of a Web Application Firewall (WAF) solution involves the creation and implementation of policies, procedures, and processes to ensure the effective and secure operation of the WAF solution. This includes the following key areas:

1. Ownership: Designating an individual or team responsible for the overall governance of the WAF solution, including the development and enforcement of policies, procedures, and processes.
2. Policy Development: Developing and documenting policies for the use, operation, and maintenance of the WAF solution, including security policies, change management policies, and incident response policies.
3. Risk Management: Conducting regular risk assessments to identify potential security risks and vulnerabilities associated with the WAF solution and implementing appropriate controls to mitigate these risks.
4. Monitoring and Reporting: Establishing and maintaining a system for monitoring and reporting on the performance and security of the WAF solution, including the generation of regular reports and alerts for security incidents, policy violations, and performance issues.
5. Incident Response: Developing and implementing an incident response plan for responding to security incidents and breaches, including the identification of the incident response team, the processes for responding to incidents, and the procedures for reporting incidents to relevant authorities.
6. Training and Awareness: Providing regular training and awareness activities for WAF administrators and security personnel, including training on the use, operation, and maintenance of the WAF solution, and awareness on the latest security threats and best practices.
7. Auditing and Compliance: Conducting regular audits to ensure the WAF solution follows relevant regulations and standards, including security, privacy, and data protection regulations, and addressing any gaps or non-compliance issues that are identified.

Implementing effective governance for a WAF solution is critical for ensuring the security and reliability of the solution, protecting against security incidents and breaches, and ensuring compliance with relevant regulations and standards.

6. Network Security- DNS Security

DNS (Domain Name System) security is an important aspect of cybersecurity, as DNS is the infrastructure that translates human-readable domain names into IP addresses and enables communication between systems on the Internet. The Domain Name System (DNS) is a hierarchical and decentralized naming system used to translate human-readable domain names into IP addresses and vice versa. The DNS is a critical component of the Internet, as it enables users to access websites, email, and other online resources using domain names instead of IP addresses.

In a DNS system, domain names are organized into a hierarchical structure, with the top-level domains (TLDs) such as .com, .org, .net, and others forming the top level of the hierarchy. Each domain name is associated with an IP address, which is used by network devices to route traffic to the correct destination. When a user enters a domain name into their web browser, the DNS system resolves the name into an IP address and returns the address to the user's browser. The browser then uses the IP address to initiate a connection to the server hosting the website or resource. The DNS is maintained by a network of servers, which work together to ensure that domain names are properly translated into IP addresses. These servers are organized into a hierarchical system, with root servers at the top and authoritative servers responsible for specific domains at the bottom. Overall, the DNS plays a critical role in enabling users to access online resources and ensuring that the Internet operates smoothly and efficiently.

6.1 What are key elements of DNS (Domain Name System) security?

The following are some of the key elements of DNS security:

1. DNSSEC (DNS Security Extensions): Implementing DNSSEC, which is a set of security extensions for DNS, to secure the authenticity and integrity of DNS data. DNS data refers to the information stored in the Domain Name System (DNS), which is a hierarchical and decentralized naming system used to translate human-readable domain names into IP addresses and vice versa. DNS data includes information such as:
    a. Domain Names: The domain names that are used to identify websites, email servers, and other online resources.
    b. IP Addresses: The IP addresses that correspond to each domain name, which are used by network devices to route traffic to the correct destination.
    c. DNS Records: The records that define the relationship between domain names and IP addresses, including A records, MX records, and others.
    d. DNS Zones: The portion of the DNS hierarchy that is managed by a specific organization or domain administrator.
    e. DNS Caches: The temporary storage locations used by DNS servers to store frequently accessed DNS data, which speeds up the resolution of domain names into IP addresses.
    f. DNSSEC Data: Information related to the security extensions for DNS (DNSSEC), including public and private keys, signatures, and other data used to secure the authenticity and integrity of DNS data.

Overall, DNS data is critical to the functioning of the Internet, as it enables users to access websites, email, and other online resources using domain names instead of IP addresses. Ensuring the accuracy and security of DNS data is a critical aspect of DNS security, as malicious changes to DNS data can lead to security incidents and compromise the integrity of the Internet.

2. DNS Firewall: Implementing a DNS firewall to block malicious or unwanted DNS traffic, such as malware and phishing attempts.
3. DNS Filtering: DNS filtering is the process of controlling access to specific domains or IP addresses based on predefined policies and criteria. This can be done to block access to malicious or unwanted domains, including those associated with malware, phishing, and other cyber threats. DNS filtering can be implemented using various methods, including the following:
    a. DNS Firewalls: A DNS firewall is a network security device that is specifically designed to control access to domains based on predefined policies. A DNS firewall can be used to block access to specific domains, redirect traffic to alternative domains, or allow access to specific domains only.
    b. Router or Gateway Configuration: Routers and gateways can be configured to block access to specific domains or IP addresses, effectively implementing DNS filtering at the network edge.
    c. Software Solutions: Software-based solutions, such as DNS security solutions or web filtering solutions, can be used to implement DNS filtering. These solutions typically use databases of known malicious domains, as well as real-time analysis and threat intelligence, to block access to malicious domains.
    d. Public DNS Services: Some public DNS services, such as OpenDNS, offer built-in DNS filtering capabilities that can be used to block access to specific domains.

    Overall, DNS filtering is a critical aspect of cybersecurity, as it can help to prevent access to malicious domains and protect users and systems from cyber threats. However, DNS filtering can also impact the availability and performance of legitimate domains, so it's important to balance the need for security with the need for availability and performance.
4. Recursive DNS: Implementing a secure recursive DNS server to protect against DNS spoofing and cache poisoning attacks. Recursive DNS (Domain Name System) refers to a type of DNS server that is responsible for resolving domain names into IP addresses. In a recursive DNS system, a client makes a query to a recursive DNS server, which then searches for the answer to the query by querying other DNS servers on behalf of the client. The recursive DNS server will continue this process of querying other servers until it has obtained the answer to the client's query or has determined that the answer cannot be found. A recursive DNS server provides a crucial service to clients on a network, as it enables clients to access websites and other online resources using domain names instead of IP addresses. The recursive DNS server acts as an intermediary between clients and other DNS servers, caching frequently accessed DNS data to speed up the resolution of domain names into IP addresses.

There are two main types of recursive DNS servers: open recursive DNS servers and closed recursive DNS servers. An open recursive DNS server will resolve domain names for any client, while a closed recursive DNS server will only resolve domain names for clients that are specifically authorized.

Overall, recursive DNS is a critical component of the Internet, as it enables clients to access websites, email, and other online resources using domain names instead of IP addresses. Ensuring the availability and performance of recursive DNS servers is a critical aspect of network security and availability, as failures in the recursive DNS system can impact the availability of online resources and the performance of networked applications.

5. Encrypted DNS: Implementing encrypted DNS protocols, such as DNS over HTTPS (DoH) and DNS over TLS (DoT), to protect DNS data in transit and prevent eavesdropping.
6. Monitoring and Logging: Monitoring DNS traffic and logs to detect and respond to potential security incidents.
7. Regular Software Updates: Keeping the DNS software and infrastructure up to date to ensure that any security vulnerabilities are addressed in a timely manner.

By implementing these security measures, organizations can ensure that their DNS infrastructure is secure and that their systems are protected against cyber threats that could originate from malicious DNS traffic.

6.2 Why is DNS (Domain Name System) important to internet access?

DNS (Domain Name System) is one of the most critical components of the Internet, as it enables the resolution of human-readable domain names into IP addresses, which are used to route traffic over the Internet. DNS is essential to the functioning of the Internet because it provides a way to translate the domain names used by users into the IP addresses used by network devices, making it possible to access websites, email servers, and other online resources using domain names instead of IP addresses. The importance of DNS to the Internet can be summarized as follows:

1. Enables User Access: DNS makes it possible for users to access websites and other online resources using domain names instead of IP addresses, which are difficult to remember and use.
2. Improves Network Efficiency: DNS reduces the amount of traffic on the Internet by caching frequently accessed DNS data, which speeds up the resolution of domain names into IP addresses.
3. Enhances Network Security: DNS security features, such as DNSSEC, can be used to secure the authenticity and integrity of DNS data, protecting against malicious changes to DNS data that can lead to security incidents.
4. Facilitates Website and Email Delivery: DNS enables the delivery of websites and email, as it provides the necessary information for network devices to route traffic to the correct destination.

5. Supports Scalability: The hierarchical and decentralized design of DNS supports scalability, enabling the Internet to grow and expand to accommodate new domains, IP addresses, and online resources.

Overall, DNS is a critical component of the Internet, as it enables users to access websites and other online resources using domain names instead of IP addresses, while also improving network efficiency, security, and scalability. Ensuring the availability and performance of DNS is a critical aspect of network management, as failures in the DNS system can impact the availability of online resources and the performance of networked applications.

6.3 Is DNS important to dark web?

The dark web, also known as the darknet, is a portion of the Internet that is only accessible through specialized software or configurations, and it is often used for illegal or illicit activities such as illegal trade, the distribution of harmful content, and cyberattacks. DNS is important to the dark web because it provides a means of resolving domain names into IP addresses, allowing users to access hidden services and websites on the dark web.

However, the use of DNS in the dark web also poses risks and challenges, as it can be used to carry out malicious activities such as cyberattacks and the distribution of harmful content. In addition, the use of DNS in the dark web can also make it difficult for law enforcement and cybersecurity professionals to track and monitor criminal activities and threats.

To address these risks and challenges, organizations may implement security measures such as DNS filtering, which blocks access to known malicious domains and IP addresses, and DNS logging, which provides visibility into DNS queries and responses, enabling organizations to detect and respond to security incidents.

In summary, DNS is important to the dark web because it provides a means of accessing hidden services and websites, but it also poses risks and challenges that must be addressed through appropriate security measures.

6.4 Sales cue- Questions to ask and answers to give

6.4.1 Questions to ask prospective client

When evaluating a DNS security opportunity, it is important to ask questions that will help you understand prospective client's approach to security and data privacy. Some questions to consider asking are as follows:

1. What measures do you have in place to prevent unauthorized access to your DNS servers and data?
2. How do you detect and respond to security threats, such as DDoS attacks or data breaches?
3. Do you have any security certifications or compliance requirements (e.g., SOC 2, PCI DSS, etc.)?
4. Can you provide details about your incident response plan and procedures for handling security incidents?

5. How do you keep your systems and software up to date with the latest security patches and updates?
6. What measures do you have in place to secure and protect client data, such as data encryption and backup/recovery processes?
7. Do you have a vulnerability management program in place for identifying and mitigating potential security risks?
8. Have you undergone any independent security audits or penetration testing to validate the security of your systems?
9. How do you educate and train your employees on security best practices and processes?
10. Can you provide references or case studies demonstrating your ability to effectively handle security incidents or threats?

These questions can help you understand the client's commitment to security and their ability to protect DNS data and systems. It is recommended to ask problem areas and use-cases from the prospective client to understand the solution's real-world effectiveness and benefits for organizations.

6.4.2 Questions prospective clients will ask of sales

When evaluating a DNS security solution, clients would like to understand how it will meet their organization's specific needs and requirements. Here are some questions they will ask:

1. What types of threats does the solution protect against (e.g., DDoS attacks, data breaches, malware, etc.)?
2. How does the solution integrate with existing security systems and processes?
3. Can you provide details about the solution's performance and scalability, including its ability to handle high traffic volumes and large numbers of queries?
4. What level of technical support and client service can I expect to receive?
5. How does the solution ensure the availability and reliability of DNS infrastructure?
6. How does the solution protect against data breaches or unauthorized access to DNS data?
7. Can you provide details about the solution's pricing and licensing options, including any recurring fees or charges?
8. How does the solution handle updates and changes to DNS configuration?
9. What is the solution's implementation timeline and process, and what resources will I need to allocate?
10. Can you provide references or case studies demonstrating the effectiveness of the solution in real-world scenarios?

These questions can help you better understand the capabilities of the DNS security solution and determine whether it is a good fit for organization's needs.

6.4.3 Payment terms to agree with the clients

All DNS Security technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays DNs Security technology owners via distributors) payment options with clients always keeps the cash-registers green and healthy.

When negotiating payment terms for a DNS security solution, there are several key considerations to keep in mind:

1. Billing Frequency: Determine how often you will invoice your client, such as monthly, quarterly, or annually.
2. Payment Due Date: Specify when payments are due, such as immediately upon receipt of invoice, net 30 days, or some other specific date.
3. Payment Methods: Consider which payment methods you will accept, such as credit card, electronic funds transfer (EFT), or check.
4. Late Payment Fees: Establish a policy for late payment fees and specify the fee amount and when it will be applied.
5. Payment Terms for Contracts: Determine the payment terms for long-term contracts, such as upfront payment, instalment payments, or a combination of both.
6. Payment for Upgrades and Additional Services: Clearly define the payment terms for upgrades and additional services that may be requested by the client.
7. Automatic Renewals: Specify the terms for automatic renewals, including payment amounts and dates, and the process for cancelling the automatic renewal.
8. Currency: Specify the currency in which payments will be made.
9. Invoicing: Specify the method for invoicing, such as email, snail mail, or an online portal.

It is important to carefully review and understand the payment terms before entering into an agreement. It is also recommended to discuss and negotiate any potential discounts or incentives that may be available. The specific payment terms will depend on the solution being offered. It is important to be clear and transparent about payment terms with your clients to ensure a smooth and mutually beneficial business relationship. Make sure to document all agreed upon payment terms in a written contract or agreement.

6.5 Pre-sales cue: Solution building complexities

6.5.1 Sizing the solution

Sizing a DNS security solution involves determining the appropriate number of resources required to effectively protect your DNS infrastructure. There are several factors that should be considered when sizing a DNS security solution, including:

1. Traffic Volume: The amount of DNS traffic being received now or in future will impact the amount of processing power, storage, and network capacity required. Be

specifically careful if the client is an e-commerce player or does massive business using online portals and/ or via websites.

2. Number of Domains: The number of domains client manages will impact the amount of storage and processing power required for your DNS security solution.
3. Threat Level: The level of security threats client is facing, such as DDoS attacks or malware, will impact the amount of processing power and network capacity required to effectively detect and respond to these threats.
4. Integration with Existing Security Systems: Consider the amount of integration required with your existing security systems, such as firewalls, intrusion detection systems, and data loss prevention tools, when sizing your DNS security solution.
5. Business Requirements: Specific business requirements, such as compliance requirements and performance SLAs, should be considered when sizing your DNS security solution.
6. Disaster Recovery and Business Continuity: Consider the need for disaster recovery and business continuity capabilities when sizing your DNS security solution, as these may require additional resources or components.
7. Scalability: Consider the potential for future growth and the ability to scale your DNS security solution as your business needs change.

By considering these factors, you can ensure that you have the appropriate resources in place to effectively protect client's DNS infrastructure and meet specific business requirements. It is important to work closely with the technology owner and client to ensure that the DNS Security solution is appropriately sized for organization's specific requirements. The technology owner and client should be able to provide guidance and recommendations based on organization's specific needs and requirements.

6.5.2 To what will DNS Security solution connect to?

A DNS security solution can connect to a variety of other systems and devices to provide a comprehensive and integrated security solution. Some of the systems and devices that a DNS security solution may connect to include:

1. DNS Servers: The DNS security solution will connect to your organization's DNS servers to monitor and protect your DNS traffic.
2. Firewalls: The DNS security solution can integrate with your organization's firewalls to provide additional security and control over network traffic.
3. Intrusion Detection and Prevention Systems (IDS/IPS): The DNS security solution can integrate with IDS/IPS systems to provide real-time threat detection and response capabilities.
4. Web Application Firewalls (WAF): The DNS security solution can integrate with WAFs to provide protection against web-based threats and attacks.
5. Data Loss Prevention (DLP) Systems: The DNS security solution can integrate with DLP systems to provide protection against unauthorized access to sensitive data.

6. Security Information and Event Management (SIEM) Systems: The DNS security solution can integrate with SIEM systems to provide centralized event logging, reporting, and analysis capabilities.
7. Network Monitoring and Management Tools: The DNS security solution can integrate with network monitoring and management tools to provide visibility into network performance and behaviour.

By connecting to these other systems and devices, a DNS security solution can provide a comprehensive and integrated security solution for your organization. It is important to carefully evaluate the integration requirements of organization's systems and to work with the System Integrator to ensure that the DNS Security solution integrates with the necessary systems. The System Integrator should be able to provide guidance and recommendations on the most appropriate integration approach.

6.5.3 Implementation steps of DNS Security solution

The implementation of a DNS security solution involves several steps to ensure a smooth and successful deployment. Here is a high-level overview of the implementation steps:

1. Planning and Preparation: This stage involves identifying the specific security needs of the organization, reviewing existing systems and infrastructure, and developing a deployment plan.
2. Assessment and Design: This stage involves conducting a thorough assessment of DNS infrastructure to determine the optimal configuration and design of DNS security solution.
3. Configuration and Installation: This stage involves configuring the DNS security solution and installing it on your network. Following steps provide greater detail:
    a. Prepare the Environment: Before installing the DNS security solution, you need to prepare the environment by verifying the hardware and software requirements, creating backup copies of your existing DNS configurations, and determining the optimal placement of the solution within your network.
    b. Download and install the DNS Security Solution: The next step is to download the DNS security solution from the vendor's website or obtain it from a distribution channel. Follow the vendor's installation instructions to install the solution on your network.
    c. Configure the DNS Security Solution: After installation, you will need to configure the solution to meet your specific requirements, including setting up network interfaces, specifying security policies, and integrating the solution with other security systems.
    d. Test the DNS Security Solution: Before deploying the solution to production, it is important to test it to ensure that it is functioning properly. This may involve testing the solution's performance, configuration, and integration with other systems.

e. Deploy the DNS Security Solution: Once you have tested the solution and validated that it is functioning properly, you can deploy it to production. This may involve updating DNS configurations and migrating existing data to the new solution.

f. Monitor and maintain the DNS Security Solution: After deployment, it is important to monitor the solution to ensure that it is functioning as expected. This may involve reviewing log files, responding to alerts, and performing regular software upgrades.

4. Integration with Other Security Systems: This stage involves integrating the DNS security solution with other security systems and devices, such as firewalls, intrusion detection systems, and data loss prevention tools.
5. Testing and Validation: This stage involves testing the DNS security solution to validate that it is functioning as expected and meets your organization's security requirements.
6. Deployment: This stage involves deploying the DNS security solution into your production environment, monitoring its performance, and responding to any issues that may arise.
7. Maintenance and Upgrades: This stage involves ongoing maintenance and upgrades to the DNS security solution to ensure its continued functionality and performance.

By following these steps, you can ensure a smooth and successful deployment of a DNS security solution that meets client organization's specific security needs and requirements.

6.5.4 What can go wrong in DNS Security solution

There are several potential issues that can arise when implementing a DNS security solution, including:

1. Configuration Errors: Incorrect configuration of the DNS security solution can result in security vulnerabilities or reduced performance.
2. Integration Issues: Integrating the DNS security solution with other security systems and devices can be challenging, and failure to properly integrate can result in security gaps or reduced performance.
3. Performance Issues: The DNS security solution can place a significant load on the network, and performance issues can arise if the solution is not properly sized or configured.
4. False Positives: The DNS security solution may generate false positive alerts, indicating a security threat when there is none. This can result in increased administrative overhead and reduced trust in the solution.
5. False Negatives: The DNS security solution may miss real security threats, resulting in a reduced level of protection for your network and data.
6. Upgrades and Maintenance: The DNS security solution requires regular software upgrades and maintenance to ensure that it remains effective in protecting your network. Failing to perform these tasks can result in reduced performance or security vulnerabilities.

7. Lack of Expertise: Implementing a DNS security solution requires a high level of technical expertise, and lack of expertise can result in configuration errors, performance issues, or other problems.

By being aware of these potential issues, you can take steps to minimize the risk of problems arising and ensure the successful deployment and operation of your DNS security solution. It is important to work with an experienced security provider or vendor to ensure that the solution is deployed and maintained properly.

6.5.5 What Service Levels can be committed/ expected?

Service Level Agreements (SLAs) in DNs Security services can vary depending on the specific needs of an organization and the level of service offered by the provider. However, some common SLAs that can be committed in DNs Security solution include:

1. Availability: The DNS provider can commit to a specific level of availability for the DNS security solution, such as 99.9% uptime. Check for overlapping SLAs on resolution. This is tricky.
2. Response Time: The technology owner or provider can commit to a specific response time for support requests, such as a four-hour response time during business hours.
3. Security Updates: The technology owner or provider can commit to providing regular security updates to the DNS security solution to ensure that it remains effective in protecting your network.
4. Performance Guarantees: The technology owner or provider can commit to specific performance guarantees for the DNS security solution, such as a specific level of throughput or low latency.
5. Maintenance: The technology owner or provider can commit to providing regular maintenance and software upgrades to the DNS security solution to ensure that it remains effective in protecting your network.
6. Disaster Recovery: The technology owner or provider can commit to providing disaster recovery services in the event of a failure of the DNS security solution, including restoring service and data.

By agreeing to these service levels, you can ensure that your DNS security solution is properly maintained and supported, and that you have a clear understanding of the level of protection that you can provide. It is important to work with a technology provider/ owner that can commit to the service levels that are appropriate for client organization's specific needs.

6.5.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

5. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.

6. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
7. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
8. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

6.6 Delivery cue- DNS Security operations

6.6.1 Daily Activities

Daily activities that are typically involved in maintaining and managing a DNS security solution:

1. Monitoring: Regular monitoring of the DNS security solution is necessary to ensure that it is functioning properly and providing the desired level of protection. This can include monitoring of security events, performance metrics, and system logs.
2. Maintenance: Regular maintenance of the DNS security solution is necessary to ensure that it remains effective in protecting your network. This can include applying software upgrades, updating configurations, and performing backups.
3. Incident Response: In the event of a security incident, it is necessary to respond promptly to ensure that the incident is contained, and the network is protected. This can include investigating the incident, isolating affected systems, and restoring normal operation.
4. Policy Updates: Regular review and updates to security policies are necessary to ensure that the DNS security solution remains aligned with the changing security needs of your organization.
5. User Management: Regular management of user accounts and permissions is necessary to ensure that the DNS security solution is used appropriately and that the network is protected.
6. Reporting: Regular reporting on the status and performance of the DNS security solution is necessary to ensure that stakeholders have the information they need to make informed decisions about the security of the network.

7. Compliance: Regular review and assessment of compliance with security policies and regulations is necessary to ensure that the DNS security solution is being used appropriately and that the network is protected.

By performing these daily activities, you can ensure that your DNS security solution remains effective in protecting network and that the security of network is maintained. It is important to have well-defined security operations plan in place that outlines the steps to be taken in the event of a security incident, and to have the necessary resources in place to perform the required daily activities.

6.6.2 Weekly Activities

Weekly activities that are typically involved in maintaining and managing a DNS security solution:

1. Patch Management: Regularly applying software patches and upgrades to the DNS security solution is necessary to ensure that it remains secure and effective in protecting your network.
2. Threat Intelligence: Regular review of threat intelligence sources and incorporation of new information into the security strategy is necessary to ensure that the DNS security solution is up-to-date and aligned with the latest threats.
3. Vulnerability Management: Regular review and assessment of system and network vulnerabilities is necessary to ensure that the DNS security solution is able to effectively protect against threats.
4. Performance Monitoring: Regular review and analysis of performance metrics is necessary to ensure that the DNS security solution is functioning optimally and providing the desired level of protection.
5. Configuration Management: Regular review and update of configuration settings is necessary to ensure that the DNS security solution is properly configured and providing the desired level of protection.
6. Incident Response Review: Regular review and analysis of past incidents is necessary to identify areas for improvement and to ensure that incident response processes are effective.
7. Security Awareness Training: Regular security awareness training for employees is necessary to ensure that all stakeholders are aware of the importance of security and the steps that can be taken to maintain the security of the network.

By performing these weekly activities, you can ensure that your DNS security solution remains effective in protecting network and that the security of network is maintained. It is important to have well-defined security operations plan in place that outlines the steps to be taken in the event of a security incident, and to have the necessary resources in place to perform the required weekly activities.

6.6.3 Monthly Activities

Monthly activities that are typically involved in maintaining and managing a DNS security solution:

1. Risk Assessment: Regular review and assessment of the risk to the network is necessary to ensure that the DNS security solution is aligned with the current security needs of the organization.
2. Compliance Review: Regular review and assessment of compliance with security policies and regulations is necessary to ensure that the DNS security solution is being used appropriately and that the network is protected.
3. Performance Review: Regular review and analysis of performance metrics is necessary to ensure that the DNS security solution is functioning optimally and providing the desired level of protection.
4. Capacity Planning: Regular review and assessment of resource utilization is necessary to ensure that the DNS security solution has the capacity to handle current and future demand.
5. Incident Response Review: Regular review and analysis of past incidents is necessary to identify areas for improvement and to ensure that incident response processes are effective.
6. Security Audit: Regular security audit is necessary to ensure that the DNS security solution is being used appropriately and that the network is protected.

By performing these monthly activities, you can ensure that your DNS security solution remains effective in protecting network and that the security of network is maintained. It is important to have well-defined security operations plan in place that outlines the steps to be taken in the event of a security incident, and to have the necessary resources in place to perform the required monthly activities.

6.6.4 What does an L1 DNS Security Engineer do?

A Level 1 (L1) DNS Security Engineer is responsible for the basic level of support and maintenance of a DNS security solution. The primary responsibilities of an L1 DNS Security Engineer typically include:

1. Monitoring: Monitoring the DNS security solution to ensure that it is functioning optimally and providing the desired level of protection.
2. Troubleshooting: Resolving basic technical issues related to the DNS security solution, such as connectivity issues or performance problems.
3. Incident Response: Responding to basic security incidents, such as attempted network intrusions, and reporting incidents to the appropriate personnel.
4. Maintenance: Performing basic maintenance tasks, such as software upgrades or patches, to ensure that the DNS security solution remains secure and effective.
5. Documentation: Maintaining documentation related to the DNS security solution, including configuration information and incident reports.

6. Client Support: Providing basic client support, such as answering questions or resolving basic technical issues, related to the DNS security solution.

An L1 DNS Security Engineer typically works as part of a larger security operations team and may report to a more senior security engineer or manager. The role requires a basic understanding of network security concepts and technologies, as well as the ability to troubleshoot technical issues and provide basic client support. Strong communication and documentation skills are also important in this role.

6.6.5 What does an L2 DNS Security Engineer do?

A Level 2 (L2) DNS Security Engineer is responsible for a higher level of support and maintenance of a DNS security solution. The primary responsibilities of an L2 DNS Security Engineer typically include:

1. Monitoring: Monitoring the DNS security solution to ensure that it is functioning optimally and providing the desired level of protection.
2. Troubleshooting: Resolving more complex technical issues related to the DNS security solution, such as configuration issues or performance problems.
3. Incident Response: Responding to more complex security incidents, such as attempted network intrusions, and coordinating incident response efforts with other members of the security operations team.
4. Maintenance: Performing more complex maintenance tasks, such as software upgrades or patches, to ensure that the DNS security solution remains secure and effective.
5. Documentation: Maintaining and updating documentation related to the DNS security solution, including configuration information and incident reports.
6. Client Support: Providing higher-level client support, such as answering more complex technical questions or resolving more complex technical issues, related to the DNS security solution.

An L2 DNS Security Engineer typically works as part of a larger security operations team and may report to a more senior security engineer or manager. The role requires a strong understanding of network security concepts and technologies, as well as the ability to troubleshoot complex technical issues and provide high-level client support. Strong communication, documentation, and leadership skills are also important in this role.

6.6.6 What does an L3 DNS Security Engineer do?

An L3 (Level 3) DNS Security Engineer is responsible for the design, implementation, and maintenance of secure Domain Name System (DNS) infrastructure. The role requires a deep understanding of DNS and its security-related aspects, as well as experience with related technologies such as *BIND, DHCP, and IPAM*. Some specific responsibilities of an L3 DNS Security Engineer may include:

1. Designing and implementing secure DNS infrastructure to meet the needs of the organization

2. Monitoring and analysing DNS traffic for potential security threats
3. Implementing security measures such as DNSSEC, DDoS mitigation techniques, and firewalls to protect the DNS infrastructure
4. Ensuring the availability and reliability of the DNS infrastructure
5. Collaborating with other security teams to investigate and resolve security incidents related to the DNS infrastructure
6. Staying up to date with emerging security threats and new technologies related to DNS security

Overall, the goal of an L3 DNS Security Engineer is to ensure the secure and efficient operation of the organization's DNS infrastructure, while also proactively identifying and mitigating potential security threats.

6.6.7 What are BIND, DHCP, and IPAM?

BIND, DHCP, and IPAM are three commonly used network protocols and services:

BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. BIND allows you to map domain names to IP addresses, making it easier for users to locate resources on the Internet.

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses to devices on a network. DHCP eliminates the need for manual IP address configuration and ensures that IP addresses are unique and avoid conflicts on the network.

IPAM (IP Address Management) is a software-based solution for managing and organizing IP addresses within an organization's network. IPAM helps administrators keep track of IP addresses, manage subnets, and monitor network usage. IPAM also provides a centralized location for IP address management, which simplifies the administration of large networks.

In summary, these protocols and services play important roles in network management and are essential for ensuring the smooth operation of a network.

6.6.8 DNS Security Reports

DNS Security operation reports typically include the following:

1. DNS Traffic Report: Provides a detailed view of the volume and types of DNS traffic passing through the network, including the source and destination IP addresses and the type of DNS query (e.g., A record, MX record).
2. DNS Query Report: Shows the frequency of DNS queries and the domains being queried, providing insights into the types of services and resources being accessed on the network.
3. DNSSEC Validation Report: Reports on the validation of DNSSEC-signed DNS records and the number of successful or failed validations.
4. DNS Threat Report: Provides a summary of potential security threats related to the DNS infrastructure, such as DNS spoofing, cache poisoning, and DDoS attacks.
5. DNS Performance Report: Monitors the performance of the DNS infrastructure and reports on factors such as response time, query time, and resource utilization.

6. IP Address Utilization Report: Provides a view of the IP addresses used in the network, including their utilization and availability.
7. DHCP Lease Report: Shows the number of DHCP leases granted and the IP addresses assigned to devices on the network.
8. DNS Zone Transfer Report: Reports on the number of zone transfers initiated by the DNS server and provides information on the source and destination of the transfers.

These reports provide valuable information for DNS security operations, helping administrators monitor the health and security of the DNS infrastructure, identify potential issues, and make informed decisions about how to optimize the network.

6.6.9 Governance of DNS Security solution

Governance of a DNS security solution is the process of establishing policies, procedures, and controls to ensure the effective and secure operation of the DNS infrastructure. The following are some key elements of a DNS security governance program:

1. Policies and Standards: Define policies and standards for the design, implementation, and management of the DNS infrastructure. This should include guidelines for security, performance, and availability.
2. Risk Management: Implement a risk management program to identify and assess potential security threats to the DNS infrastructure and develop mitigation strategies to minimize risk.
3. Incident Response: Establish an incident response plan to ensure that security incidents related to the DNS infrastructure are quickly detected, analysed, and resolved.
4. Change Management: Implement a change management process to ensure that changes to the DNS infrastructure are made in a controlled and secure manner. This should include change approval procedures and documentation of changes.
5. Compliance: Ensure that the DNS security solution is compliant with relevant security and privacy regulations, such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).
6. Monitoring and Reporting: Implement continuous monitoring and reporting of the DNS infrastructure to ensure that it is functioning correctly and securely.
7. Training and Awareness: Provide training and awareness programs for administrators and users to ensure that they understand the importance of DNS security and how to use the DNS security solution effectively.

By establishing a comprehensive DNS security governance program, organizations can ensure that their DNS infrastructure is secure, reliable, and in compliance with relevant regulations and standards.

7. Cloud Access Security Broker (CASB)

A Cloud Access Security Broker (CASB) is a type of security software that provides visibility and control over cloud application usage and data. CASBs are deployed as a proxy between users and cloud applications, providing security and compliance controls for cloud-based services. The primary objectives of a CASB are to:

1. Ensure security: CASBs enforce security policies, including encryption, data loss prevention, and *multi-factor authentication*, to protect data and maintain the security of cloud applications.
2. Ensure compliance: CASBs ensure compliance with regulations and standards, such as *HIPAA, GDPR, and PCI*, by monitoring and reporting on cloud application usage and data access.
3. Improve visibility: CASBs provide visibility into cloud application usage and data access, including who is accessing what data, when, and from where, to help organizations gain better control and insight into their cloud environments.
4. Enforce data governance: CASBs enforce data governance policies, such as retention and deletion policies, to help organizations maintain control over their data and prevent data breaches.

CASBs are becoming increasingly important as organizations continue to adopt cloud applications and services, as they help organizations address the security and compliance challenges associated with cloud computing and ensure that cloud applications and data are being used in a secure and compliant manner.

7.1 What is a multi-factor authentication?

Multi-factor authentication (MFA) is a security process that requires multiple methods of authentication from independent categories of authentication methods. The goal of MFA is to reduce the risk of unauthorized access to a system, network, or application.

MFA typically involves a combination of two or more of the following authentication methods: something you know: could be a password, PIN, or secret question and answer, something you have: could be a security token, smart card, or mobile phone or something you are: could be a fingerprint, face recognition, or other biometric information.

By requiring multiple methods of authentication, MFA provides a higher level of security than a single-factor authentication system, as it makes it more difficult for attackers to gain access to a system. MFA is commonly used for sensitive systems and applications, such as online banking, email, and cloud-based applications, where the security of sensitive information and data is a top priority.

7.2 HIPAA, GDPR, and PCI: What are these?

HIPAA, GDPR, and PCI are three major regulatory standards that organizations must comply with to ensure the privacy and security of sensitive information.

HIPAA (Health Insurance Portability and Accountability Act): HIPAA is a US federal law that sets standards for protecting the privacy and security of individuals' health information, known as "protected health information" (PHI). HIPAA applies to covered entities, such as

healthcare providers, health plans, and healthcare clearinghouses, and imposes strict requirements for the handling and protection of PHI.

GDPR (General Data Protection Regulation): GDPR is a European Union (EU) regulation that sets standards for the protection of personal data of EU residents. The regulation applies to organizations that process personal data of EU residents, regardless of where the organization is located. GDPR imposes strict requirements for the collection, storage, and processing of personal data, including the right of individuals to control their personal data and the right to be forgotten.

PCI (Payment Card Industry Data Security Standard): PCI is a set of security standards that organizations must comply with to ensure the secure handling of payment card information. The standard applies to merchants, service providers, and financial institutions that handle payment card information. PCI requires organizations to implement strict security controls for the handling and protection of payment card information, including encryption, firewalls, and regular security assessments.

Compliance with these regulations is mandatory for organizations in the respective industries, and failure to comply can result in significant fines and reputational damage. These regulations help ensure that sensitive information is protected, and that individuals' privacy rights are respected.

7.3 CASB types

There are several types of CASBs, including:

1. API-based CASB: These CASBs use *APIs* to connect to cloud services and provide security controls.
2. Agent-based CASB: These CASBs require the installation of an agent on the endpoint device, which provides real-time protection and monitoring.
3. Hybrid CASB: These CASBs combine the capabilities of API-based and agent-based CASBs to provide a comprehensive security solution.
4. Cloud-native CASB: These CASBs are built specifically for cloud environments and provide native integration with cloud services.
5. Network-based CASB: These CASBs are deployed in the network and provide security controls by intercepting and inspecting traffic between the cloud and the endpoint device.

Each type of CASB has its own strengths and weaknesses, and the choice of CASB will depend on the specific security needs of an organization.

7.4 What are APIs?

API stands for Application Programming Interface. It is a set of rules and protocols that enables two software applications to communicate with each other. APIs provide a way for different software systems to exchange data and functionality. For example, a software company may offer an API that allows other developers to access some of its services, such as retrieving data

or triggering certain actions. This way, developers can build new applications that leverage the services offered by the company, without having to build all the functionality from scratch.

APIs are typically accessed over the Internet and use the HTTP protocol to exchange data. They often include specifications for making requests to the API, as well as the format in which data will be returned. There are many examples of APIs, here are a few of the most common ones:

1. Social Media APIs: For example, the Twitter API allows developers to access Twitter data, such as tweets, user information, and media, and to post tweets on behalf of a user.
2. Maps and Location APIs: For example, the Google Maps API enables developers to embed Google Maps into their own web pages and to perform location-based searches.
3. Payment APIs: For example, the Stripe API provides a way for developers to securely accept payments and manage client data in their own applications.
4. Weather APIs: For example, the OpenWeatherMap API allows developers to access current weather data, as well as historical data, for locations around the world.
5. E-commerce APIs: For example, the Amazon Product Advertising API enables developers to retrieve information about products for sale on Amazon and to display this information in their own applications.
6. Music and Audio APIs: For example, the Spotify Web API enables developers to access Spotify's music data and to control a user's Spotify playback from their own applications.

APIs have become a key enabler of the digital economy, allowing companies to integrate with a variety of services and system quickly and easily.

7.5 Sales cue- Questions to ask and answers to give

7.5.1 Questions to ask prospective client

Here are some questions you could ask to discover if someone wants to buy a Cloud Access Security Broker (CASB):

1. Can you tell me about your current cloud environment and usage? This question can help you understand the extent to which the organization is already using cloud services and what types of services they are using.
2. Have you experienced any security incidents or data breaches in the cloud? If so, what were the consequences and how did you respond? This question can help you understand the organization's concerns around cloud security and their need for a CASB.
3. How do you currently secure and manage access to your cloud services? This question can help you understand the organization's current security posture and what gaps a CASB may be able to fill.

4. Have you considered the regulatory requirements for your data in the cloud, such as data privacy and data residency? This question can help you understand the organization's requirements around data protection and their need for a CASB.
5. Are there any specific security features or capabilities you are looking for in a CASB solution? This question can help you understand the organization's specific needs and requirements for a CASB.
6. Do you have any concerns about the performance or latency of a CASB solution? This question can help you understand any potential limitations or trade-offs that the organization may be willing to accept in exchange for improved security.

These questions can help you gather information about an organization's cloud environment, security posture, and specific needs and requirements for a CASB solution. This information can then be used to determine whether a CASB is the right solution for the organization and to guide the selection of a specific CASB solution.

7.5.2 Questions prospective clients will ask of sales

Before buying a Cloud Access Security Broker (CASB), it's important to understand organization's needs and requirements and to evaluate the different CASB solutions available. Here are some questions clients can ask to help make an informed decision:

1. Can you describe the features and capabilities of CASB solution, and how it addresses the security needs of cloud environments? This question can help them understand the scope of the solution and how it can meet their security requirements.
2. How does CASB solution integrate with other security tools and systems in their environment, such as firewalls, identity and access management systems, and data loss prevention solutions? This question can help them determine whether the CASB solution can integrate with their existing security tools and systems and provide a comprehensive security posture.
3. How does CASB solution enforce security policies and control access to cloud services? This question can help them understand how the solution enforces security policies and manages access to cloud services.
4. Can you provide any references or case studies of organizations that have successfully implemented CASB solution? This question can help them understand the experiences and outcomes of other organizations that have implemented the solution and make a more informed decision. Normally, the late adopters of technologies ask these questions.
5. Can you describe support and maintenance model for the CASB solution? This question can help them understand the level of support and maintenance one can expect from the system integrator and managed security services provider and ensure that the resources needed to effectively manage the solution are available.
6. What is the cost of CASB solution, and what is included in the price? This question can help them understand the total cost of ownership of the solution and whether it fits within their budget.

7. Can you provide a demonstration or trial of CASB solution, so we can see it in action and evaluate its functionality and performance? This question can help them see the solution in action and make a more informed decision about whether it is a good fit for their organization.

By asking these questions and getting clear answers, clients can make an informed decision and select the best CASB solution for their organization.

7.5.3 Payment terms to agree with the clients

All CASB technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays CASB technology owners via distributors) payment options with clients always keeps the cash-registers green and healthy.

The payment terms that you agree with your Cloud Access Security Broker (CASB) clients will depend on several factors, including the size and complexity of the solution, the length of the contract, and the services provided. Here are some common payment terms that you may consider:

1. Upfront payment: You may require clients to make an upfront payment for the entire cost of the solution. This payment model can provide a guaranteed revenue stream and ensure that the client is committed to the solution.
2. Instalment payments: You may structure the payment as instalment payments over the course of the contract, which can make the solution more affordable for the client and spread out the costs over time.
3. Monthly or annual subscription: You may offer a monthly or annual subscription model, where the client pays a recurring fee for access to the solution. This payment model can provide a predictable and recurring revenue stream and ensure that the client is committed to the solution for the long term.
4. Pay-per-use: You may offer a pay-per-use model, where the client pays based on their actual usage of the solution. This payment model can be attractive to clients who may only need to use the solution occasionally and want to avoid paying for unused capacity.
5. Volume-based pricing: You may offer volume-based pricing, where the client pays a lower rate for larger quantities of usage or services. This payment model can be attractive to clients who anticipate high usage of the solution and want to reduce their costs.
6. Maintenance and support fees: You may charge clients a separate fee for maintenance and support services, which can provide a recurring revenue stream and ensure that clients have access to the resources they need to effectively manage the solution.

It's important to agree on payment terms that are fair and reasonable for both you and your clients, and to clearly communicate the terms and conditions in the contract. This can help ensure that the relationship is transparent and predictable and can help you build trust and long-term relationships with your clients.

7.6 Pre-sales cue: Solution building complexities

7.6.1 Sizing the solution

Sizing a Cloud Access Security Broker (CASB) solution involves determining the amount of computing resources, storage, and other resources that are required to support the solution. This process can help you ensure that the solution is appropriately scaled to meet the needs of your organization and provides adequate performance and reliability. When sizing a CASB solution, you should consider the following factors:

1. Number of users: The number of users who will access the cloud services through the CASB solution is a key factor in determining the size of the solution. You should consider the number of concurrent users and the number of users who will access the solution on a daily, weekly, or monthly basis.
2. Cloud services used: The types and number of cloud services that will be used through the CASB solution is another key factor in determining the size of the solution. Different cloud services may have different resource requirements, and you should consider the specific requirements of each service to ensure that the solution is appropriately sized.
3. Data volume: The volume of data that will be processed by the CASB solution is another important factor to consider when sizing the solution. You should consider the size of the data sets, the frequency of data transfers, and the bandwidth required to process the data.
4. Security policies: The complexity of the security policies that will be enforced by the CASB solution is another factor to consider when sizing the solution. More complex security policies may require more resources to enforce, and you should consider the specific requirements of your security policies when sizing the solution.
5. Deployment model: The deployment model for the CASB solution is another important factor to consider when sizing the solution. Different deployment models may have different resource requirements, and you should consider the specific requirements of your deployment model to ensure that the solution is appropriately sized.

It's important to size the CASB solution appropriately to ensure that it provides adequate performance and reliability, and to ensure that the solution is cost-effective. You may need to perform performance testing and tuning to ensure that the solution meets your performance requirements, and you may need to adjust the size of the solution as your needs change over time.

7.6.2 To what will CASB solution connect to?

A Cloud Access Security Broker (CASB) solution is designed to connect to cloud services and secure access to these services. The specific cloud services that a CASB solution connects to will depend on the needs of the organization. Typically, a CASB solution will connect to the following types of cloud services:

1. SaaS applications: CASB solutions can secure access to Software-as-a-Service (SaaS) applications such as productivity applications, client relationship management (CRM) systems, and collaboration platforms.
2. Infrastructure-as-a-Service (IaaS): CASB solutions can also secure access to infrastructure-as-a-service (IaaS) platforms such as Amazon Web Services (AWS) and Microsoft Azure.
3. Platform-as-a-Service (PaaS): CASB solutions can also secure access to platform-as-a-service (PaaS) platforms such as Google App Engine and Heroku.
4. File storage and sharing: CASB solutions can secure access to file storage and sharing services such as Box, Dropbox, and Google Drive.
5. Social media: CASB solutions can secure access to social media platforms such as Twitter, Facebook, and LinkedIn.

It's important to understand the cloud services that are used in your organization and the specific requirements for securing access to these services. This can help you determine the specific cloud services that a CASB solution should connect to and ensure that the solution is configured to meet your specific needs.

7.6.3 Implementation steps of CASB solution

Implementing a Cloud Access Security Broker (CASB) solution involves several steps, including planning, deployment, configuration, and testing. Here is a general outline of the steps involved in implementing a CASB solution:

1. Plan: The first step in implementing a CASB solution is to plan the deployment. This includes identifying the specific cloud services that need to be secured, determining the security policies that will be enforced, and assessing the resources required to deploy the solution.
2. Deployment: The next step is to deploy the CASB solution. This may involve deploying the solution in a virtual environment or as a physical appliance, depending on the solution and the requirements of your organization.
3. Configuration: Once the CASB solution is deployed, the next step is to configure the solution. This includes defining security policies, setting up user authentication and authorization, and configuring the solution to integrate with your existing security infrastructure.
4. Test: After the solution is configured, the next step is to test the solution to ensure that it meets your requirements and that it provides the expected level of security. This may involve testing the solution in a test environment, performing security scans and vulnerability assessments, and testing the solution with a subset of users.
5. Deployment and rollout: After testing is complete, the next step is to deploy the CASB solution to your production environment and begin rolling it out to your users. This may involve configuring access controls, monitoring the solution for security events, and providing training and support to users.

6. Ongoing management: The final step is to manage and maintain the CASB solution on an ongoing basis. This includes monitoring the solution for security events, updating security policies as needed, and performing regular maintenance and upgrades to the solution.

Implementing a CASB solution can be a complex process, and it's important to have a clear plan and a well-defined implementation strategy to ensure success. You may also need to work with CASB technology owner and client to implement the solution, and you should consider the specific requirements of client's organization.

7.6.4 What can go wrong in CASB solution

Like any technology solution, a Cloud Access Security Broker (CASB) can have its own set of challenges and potential problems. Here are some of the most common issues that can arise when implementing a CASB solution:

1. Integration with existing infrastructure: CASB solutions can be complex to integrate with existing security infrastructure, and there may be compatibility issues with existing systems and tools.
2. Performance: CASB solutions can have an impact on performance and response times, especially when there is a high volume of traffic or a large number of users accessing cloud services.
3. Configuration errors: CASB solutions can be complex to configure, and configuration errors can result in reduced security or the failure of the solution to work as intended.
4. False positive alerts: CASB solutions can generate a large number of alerts, many of which may be false positive alerts that don't represent real security threats.
5. Policy management: CASB solutions require regular updates and management to ensure that security policies are up-to-date, and that the solution is providing the expected level of security.
6. User adoption: CASB solutions can be disruptive to user workflows, and user adoption may be limited if the solution is perceived as being too difficult to use or too restrictive.
7. Cost: CASB solutions can be expensive, and the cost of deploying and maintaining the solution can be a significant burden for organizations.

It's important to be aware of these potential issues and to plan for them when implementing a CASB solution. This may involve working with CASB technology vendor and client to implement the solution, and it may also require regular monitoring and maintenance to ensure that the solution is working as intended.

7.6.5 What Service Levels can be committed/ expected?

Service level commitments for a Cloud Access Security Broker (CASB) solution can vary depending on the CASB technology owner and the solution, but they typically include commitments related to availability, performance, security, and support.

1. Availability: This refers to the percentage of time that the CASB solution will be available and accessible to users. This can be expressed as an uptime percentage, such as 99.9% uptime.
2. Performance: This refers to the response time and speed of the CASB solution. Performance commitments may include measures such as the average response time for user requests or the maximum processing time for security events.
3. Security: This refers to the level of security provided by the CASB solution, including commitments related to data protection, access controls, and security event reporting.
4. Support: This refers to the level of support provided by the vendor or provider, including the availability of technical support, the response time for support requests, and the availability of training and documentation.

It's important to understand the service level commitments provided by your CASB solution technology owner and to ensure that these commitments align with client organization's needs and expectations. You should also include and review the service level commitments regularly to ensure that they remain relevant.

.

7.6.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.
2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

7.7 Delivery cue- CASB operations

7.7.1 Daily CASB Activities

Daily CASB operation activities typically include the following tasks:

1. Monitoring and analysing security events: Monitoring and analysing security events generated by the CASB solution is an important part of ensuring the solution is working as intended. This may involve reviewing logs, alerts, and reports to identify any security incidents or anomalies.
2. Updating policies: CASB solutions require regular updates to policies and security rules to ensure that they remain relevant and effective. This may involve reviewing and modifying policies related to data protection, access controls, and user activity monitoring.
3. Managing users and permissions: CASB solutions may require the management of user accounts and permissions, including the creation and removal of users and the assignment of access controls.
4. Maintaining the solution: Regular maintenance and updates are necessary to keep the CASB solution functioning effectively and to address any issues or bugs that arise. This may involve applying software patches, updating firmware, and performing system backups.
5. Troubleshooting: Troubleshooting issues that arise with the CASB solution can be an important part of daily activities. This may involve working with vendors or third-party providers to resolve technical issues or addressing user complaints related to the solution's performance or functionality.
6. Training and education: Training and educating users on the use of the CASB solution can help to increase user adoption and ensure that the solution is being used effectively. This may involve providing training sessions, creating user guides and documentation, or providing online resources and support.

By performing these tasks on a regular basis, you can help to ensure that CASB solution is providing the expected level of security and that the solution is functioning effectively.

7.7.2 Weekly CASB Activities

Weekly CASB operation activities typically include the following tasks:

1. Reviewing security reports: Reviewing security reports generated by the CASB solution can help to identify any security incidents or trends, and to ensure that the solution is providing the expected level of security.
2. Updating policies: Regularly updating security policies and rules to ensure that they remain relevant and effective is an important part of managing a CASB solution. This may involve reviewing and modifying policies related to data protection, access controls, and user activity monitoring.
3. Managing users and permissions: CASB solutions may require the management of user accounts and permissions, including the creation and removal of users and the assignment of access controls.

4. Monitoring system performance: Monitoring the performance of the CASB solution, including response time and processing speed, can help to identify any issues that may impact the solution's effectiveness.
5. Performing system backups: Regularly backing up the CASB solution can help to ensure that data and configuration settings are protected in the event of a system failure or other issue.
6. Evaluating security trends: Evaluating security trends and new threat vectors can help to identify areas where the CASB solution can be improved or where new policies and security rules should be added.
7. Staying current with industry developments: Staying current with industry developments, including new security threats and new technologies, can help to ensure that the CASB solution remains relevant and effective.

By performing these tasks on a regular basis, you can help to ensure that CASB solution is providing the expected level of security and that the solution is functioning effectively.

7.7.3 Monthly CASB Activities

Monthly CASB operation activities typically include the following tasks:

1. Reviewing security reports: Reviewing security reports generated by the CASB solution on a monthly basis can help to identify any security incidents or trends, and to ensure that the solution is providing the expected level of security.
2. Performing system backups: Regularly backing up the CASB solution, on a monthly basis or more frequently, can help to ensure that data and configuration settings are protected in the event of a system failure or other issue.
3. Evaluating security trends: Evaluating security trends and new threat vectors can help to identify areas where the CASB solution can be improved or where new policies and security rules should be added.
4. Staying current with industry developments: Staying current with industry developments, including new security threats and new technologies, can help to ensure that the CASB solution remains relevant and effective.
5. Performing system audits: Performing regular system audits, such as security and compliance audits, can help to identify any issues or areas for improvement in the CASB solution.
6. Reviewing vendor performance: Reviewing the performance of the CASB solution vendor on a monthly basis can help to ensure that the vendor is providing the expected level of service and support.
7. Planning future upgrades: Planning future upgrades and improvements to the CASB solution can help to ensure that the solution remains relevant and effective in the face of evolving security threats and changing business needs.

By performing these tasks on a regular basis, you can ensure that CASB solution is providing the expected level of security and that the solution is functioning effectively.

7.7.4 What does an L1 CASB Engineer do?

A Level 1 (L1) CASB Engineer is responsible for the basic level of support and maintenance of a CASB solution. The primary responsibilities typically include:

1. Monitoring and troubleshooting: Monitoring the performance of the CASB solution and troubleshooting any issues that arise, such as system errors or security incidents.
2. User account management: Creating and managing user accounts and permissions and ensuring that access controls are properly configured.
3. Policy enforcement: Ensuring that security policies and rules are properly enforced by the CASB solution, and updating policies as needed.
4. Incident response: Responding to security incidents and performing necessary investigations, such as data breaches or unauthorized access attempts.
5. Reporting: Generating security reports and other documentation and sharing these reports with relevant stakeholders.
6. System maintenance: Performing routine maintenance tasks, such as software upgrades and system backups, to ensure the CASB solution is functioning properly.
7. Training: Providing training and support to users of the CASB solution, and assisting with any questions or concerns

The L1 CASB Engineer plays a critical role in ensuring the proper functioning of the CASB solution and ensuring that the solution is providing the expected level of security. The L1 CASB Engineer may also be responsible for working with senior-level security personnel and vendors to resolve complex technical issues and to plan for future upgrades and improvements.

7.7.5 What does an L2 CASB Engineer do?

A Level 2 (L2) CASB Engineer is responsible for a higher level of support and maintenance of a CASB solution. The primary responsibilities typically include:

1. Monitoring and troubleshooting: Monitoring the performance of the CASB solution and troubleshooting any complex issues that arise, such as system errors or security incidents.
2. User account management: Creating and managing user accounts and permissions and ensuring that access controls are properly configured.
3. Policy enforcement: Ensuring that security policies and rules are properly enforced by the CASB solution, and updating policies as needed.
4. Incident response: Responding to complex security incidents and performing necessary investigations, such as data breaches or unauthorized access attempts.
5. Reporting: Generating security reports and other documentation and sharing these reports with relevant stakeholders.
6. System maintenance: Performing routine maintenance tasks, such as software upgrades and system backups, to ensure the CASB solution is functioning properly.

7. Training: Providing training and support to users of the CASB solution and assisting with any questions or concerns.
8. Optimization: Identifying areas for improvement in the CASB solution and working with senior-level security personnel and vendors to plan and implement upgrades and improvements.
9. Escalation: Escalating complex technical issues to senior-level security personnel or vendors for resolution.

The L2 CASB Engineer plays a critical role in ensuring the proper functioning of the CASB solution, optimizing the solution for performance and security, and providing expert-level support and assistance to users of the solution. The L2 CASB Engineer may also be responsible for working with senior-level security personnel to develop and implement security policies and procedures that align with the organization's overall security strategy.

7.7.6 What does an L3 CASB Engineer do?

A Level 3 (L3) Cloud Access Security Broker (CASB) Engineer is a senior-level position responsible for the design, implementation, and management of an organization's CASB solution. The specific responsibilities of an L3 CASB Engineer may vary depending on the size of the organization and the complexity of the CASB solution, but some common tasks include:

1. Design and implementation: Designing and implementing the CASB solution, including defining policies, configuring access controls, and setting up system integrations.
2. Monitoring and troubleshooting: Monitoring the performance of the CASB solution and troubleshooting complex issues that arise, such as system errors or security incidents.
3. User account management: Creating and managing user accounts and permissions and ensuring that access controls are properly configured.
4. Policy enforcement: Ensuring that security policies and rules are properly enforced by the CASB solution, and updating policies as needed.
5. Incident response: Responding to complex security incidents and performing necessary investigations, such as data breaches or unauthorized access attempts.
6. Reporting: Generating security reports and other documentation and sharing these reports with relevant stakeholders.
7. System maintenance: Performing routine maintenance tasks, such as software upgrades and system backups, to ensure the CASB solution is functioning properly.
8. Training: Providing training and support to users of the CASB solution and assisting with any questions or concerns.
9. Optimization: Identifying areas for improvement in the CASB solution and working with senior-level security personnel and vendors to plan and implement upgrades and improvements.
10. Escalation: Escalating complex technical issues to senior-level security personnel or vendors for resolution.

11. Management: Managing the day-to-day operations of the CASB solution, including managing resources, prioritizing tasks, and ensuring the solution is aligned with the organization's overall security strategy.

The L3 CASB Engineer plays a critical role in leading the design, implementation, and management of the CASB solution, ensuring that the solution is providing the expected level of security, and providing expert-level support and assistance to users of the solution. The L3 CASB Engineer may also be responsible for working with senior-level security personnel to develop and implement security policies and procedures that align with the organization's overall security strategy.

7.7.7 CASB Reports

CASB operation reports typically include the following:

1. Threat intelligence reports: Provide information about the latest security threats, such as malware, phishing attacks, and data breaches, and how these threats are impacting organizations.
2. User activity reports: Provide detailed information about user activity in the cloud, including which users are accessing which cloud services and when.
3. Data loss prevention (DLP) reports: Provide information about sensitive data that is being stored, shared, or transmitted in the cloud, and any potential risks associated with this data.
4. Shadow IT reports: Provide information about the use of unauthorized cloud services within an organization, including which services are being used, how they are being used, and who is using them.
5. Compliance reports: Provide information about an organization's compliance with various security and privacy regulations, such as the General Data Protection Regulation (GDPR) or the Payment Card Industry Data Security Standard (PCI DSS).
6. Security incident reports: Provide information about security incidents that have been detected, including the type of incident, the severity of the incident, and the steps taken to resolve the incident.
7. Threat mitigation reports: Provide information about the steps taken to mitigate security threats, including the effectiveness of security controls and the impact of security incidents.
8. Real-time alerts: Provide real-time notifications of security incidents and other security-related events, such as a user attempting to access a restricted cloud service.

These reports can be customized and filtered to meet the specific needs of an organization and can be used to inform security decision-making and to track the effectiveness of the CASB solution over time. The frequency and level of detail of these reports can also be adjusted to meet the needs of different stakeholders within an organization, such as security teams, compliance teams, and business leaders.

7.7.8 Governance of CASB solution

The governance of a Cloud Access Security Broker (CASB) solution is the process of setting and enforcing policies, standards, and procedures for the use and management of the solution. The goal of CASB governance is to ensure that the solution is being used effectively and efficiently, and that it aligns with the overall security and compliance objectives of the organization. Here are some key components of CASB solution governance:

1. Policy development: Developing and maintaining clear policies for the use of cloud services and the CASB solution, including which services are approved for use, how sensitive data is to be protected, and how security incidents are to be reported and addressed.
2. Role-based access control: Defining roles and responsibilities for managing and using the CASB solution and granting access to the solution based on those roles. This can help ensure that the solution is being used by the right people, with the right level of access.
3. Monitoring and reporting: Regularly monitoring the use of cloud services and the CASB solution and generating reports on usage and security incidents. These reports can be used to identify trends and areas for improvement, and to track the overall effectiveness of the solution.
4. Incident response: Establishing a clear and effective incident response process, including who is responsible for responding to security incidents, what steps should be taken to contain and resolve incidents, and how incidents will be communicated to stakeholders.
5. Risk management: Regularly assessing the risks associated with the use of cloud services and taking steps to manage those risks through the use of the CASB solution and other security controls.
6. Compliance management: Ensuring that the use of cloud services and the CASB solution aligns with relevant security and privacy regulations and taking steps to address any compliance gaps that are identified.

Effective governance of a CASB solution is critical for ensuring that the solution is used effectively and efficiently, and for protecting sensitive data and systems in the cloud. This requires the collaboration of multiple stakeholders within an organization, including security teams, compliance teams, and business leaders.

8. Database Activity Monitoring

Database Activity Monitoring (DAM) is a security and compliance management solution that tracks and records database activity in real-time. It is used to monitor and control access to sensitive data and to ensure that database activity is consistent with regulatory requirements.

DAM typically collects data from database logs, system logs, and other sources, and analyses this data to detect unauthorized access, data theft, and other potential security threats. The solution provides real-time alerts to security personnel and can also be used to generate reports that can be used to assess the overall security posture of an organization's database environment. Some of the key benefits of DAM include:

1. Increased visibility into database activity: DAM provides a centralized view of database activity, making it easier to identify and respond to security incidents and data breaches.
2. Improved security and compliance: DAM helps organizations meet regulatory requirements, such as PCI DSS, HIPAA, and GDPR, by monitoring and controlling access to sensitive data.
3. Real-time alerting and reporting: DAM can generate real-time alerts for security personnel and provide detailed reports to help organizations understand their database security posture.
4. Enhanced threat detection: DAM uses advanced analytics and machine learning algorithms to detect unusual database activity and potential security threats, providing early warning for organizations to respond to incidents.

Overall, DAM is a valuable tool for organizations looking to improve the security and compliance of their database environment and to protect sensitive data from theft or unauthorized access. This is not to be confused with Digital Asset Management which also shortens to DAM.

8.1 Sales cue- Questions to ask and answers to give

8.1.1 Questions to ask prospective client

For discovering Database Activity Monitoring, here are some questions you may want to ask potential buyers:

1. What type of databases are you monitoring (e.g., Oracle, SQL Server, MySQL)?
2. What type of monitoring do you need (e.g., real-time monitoring, auditing, compliance reporting)?
3. What security and privacy requirements do you have for monitoring database activity?
4. What kind of data do you need to monitor (e.g., sensitive data, specific tables, users, or transactions)?
5. How would you like to receive alerts and reports (e.g., email, SMS, dashboards)?
6. What is your budget for a database activity monitoring solution?

7. How will you integrate the solution with your existing security infrastructure (e.g., firewalls, intrusion detection systems, security information and event management [SIEM] tools)?
8. Do you need a cloud-based solution or an on-premises solution?
9. What level of support and maintenance do you require?
10. Can you provide examples of the types of suspicious activity you would like the solution to detect?

8.1.2 Questions prospective clients will ask of sales

Clients evaluating solutions for Database Activity Monitoring may have a variety of questions based on their specific needs and requirements. Here are some common questions they ask:

1. What types of databases are supported (e.g., Oracle, SQL Server, MySQL)?
2. Can you monitor real-time database activity and generate alerts?
3. What types of activities can be monitored (e.g., user access, SQL statements, data modifications)?
4. How does the solution handle sensitive data, such as credit card numbers or personally identifiable information (PII)?
5. Can you generate reports for compliance and auditing purposes?
6. Can you configure the system to alert on specific types of activity (e.g., unauthorized access attempts)?
7. How does the solution integrate with other security tools, such as firewalls, intrusion detection systems, and security information and event management (SIEM) tools?
8. Is the solution cloud-based or on-premise, and what are the deployment options?
9. What level of support and maintenance is included?
10. Can you provide a demo or a free trial so we can test the product before making a purchase?

Free trials will need licenses to be allocated for checking the solution on databases. Clients won't be able to share live production or test database for doing this trial and may dodge the purchase unless needed. It is best to qualify these opportunities properly

It is recommended to provide clear and concise answers to these questions, and to demonstrate how the solution addresses the client's specific requirements and concerns. Additionally, it may be helpful to provide relevant case studies or client references to show how the solution has benefited similar organizations.

8.1.3 Payment terms to agree with the clients

All Database Activity Monitoring technology owners ask for advance payments, almost always 100% in advance. So, unless clients pay similarly, the service providers come under heavy cash-flow situations. Therefore, agreeing on 100% advance payments or back-to-back (client pays services/ system integrator and system integrator pays Database Activity Monitoring

technology owners via distributors) payment options with clients always keeps the cash-registers green and healthy.

The payment terms for Database Activity Monitoring solutions can vary depending on the specific solution. Here are some common payment terms that you can discuss with clients:

1. Licensing model: Determine the licensing model that works best for your organization. Some solutions use a per-user, per-device, or per-database model, while others use a subscription-based model.
2. Term length: Consider the term length for the agreement. Options may include a monthly, annual, or multi-year contract.
3. Upfront payment vs. recurring payment: Decide whether you prefer to make an upfront payment for the entire term or to spread payments out over time.
4. Payment schedule: Agree on a payment schedule that works for both parties, such as monthly, quarterly, or annually.
5. Discounts: Negotiate any discounts for prepayment or long-term commitment.
6. Maintenance and support: Determine the cost of maintenance and support and whether it is included in the licensing fee or if it is an additional cost.
7. Upgrade policy: Clarify the policy for upgrades and determine whether there is an additional cost for upgrades.
8. Renewal terms: Discuss the terms for renewing the agreement and any changes to the pricing structure.
9. Termination clause: Review the termination clause and determine the conditions under which the agreement can be terminated and the process for doing so.

It's important to have a clear understanding of the payment terms and to have everything in writing to avoid misunderstandings or disputes later on.

8.2 Pre-sales cue: Solution building complexities

8.2.1 Sizing the solution

Sizing a Database Activity Monitoring (DAM) solution involves determining the resources (e.g., CPU, memory, storage) and capacity needed to run the solution effectively for your organization. Here are some factors to consider when sizing a DAM solution:

1. Database size: The size of your database will impact the resources needed to run the DAM solution. Larger databases will typically require more resources.
2. Number of databases: Consider the number of databases you need to monitor. If you have multiple databases, you'll need to factor in the resources required for each database.
3. User concurrency: Determine the number of users who will be accessing the database at the same time and factor this into the resources required for the DAM solution.
4. Data volume: Consider the volume of data that will be generated and processed by the DAM solution. Larger data volumes may require additional storage and processing resources.

5. Reporting and alerting requirements: Determine the reporting and alerting requirements for the DAM solution and factor in the resources needed to generate these reports and alerts.
6. Integration with other tools: If you plan to integrate the DAM solution with other security tools, such as firewalls, intrusion detection systems, or security information and event management (SIEM) tools, factor in the resources required for the integration.

It's important to size the DAM solution appropriately to ensure it can effectively monitor and protect client's database. You may need to work with the Database activity Monitoring technology owner and/or system integrator to determine the appropriate resources needed.

8.2.2 To what will Database Activity Monitoring solution connect to?

A Database Activity Monitoring (DAM) solution typically connects to the database servers or systems it is monitoring. This can include databases such as Oracle, SQL Server, MySQL, or other database management systems.

The DAM solution uses various methods to connect to the database servers, such as database APIs or database log files. Once connected, the DAM solution can monitor database activity, including user access, SQL statements, and data modifications, and generate alerts or reports for compliance and auditing purposes.

In some cases, the DAM solution may also connect to other security tools, such as firewalls, intrusion detection systems, or security information and event management (SIEM) tools, to provide a comprehensive security solution. This integration can help you centralize security event data, automate security workflows, and respond to security incidents more efficiently.

8.2.3 Implementation steps of Database Activity Monitoring solution

The implementation of a Database Activity Monitoring (DAM) solution typically involves the following steps:

1. Assessment: Perform an assessment of your current database environment to determine the scope of the implementation. This may include determining the types of databases to be monitored, the volume of data, and the number of users.
2. Planning: Develop a plan for the implementation, including the resources needed, the timeline, and any dependencies. This is also a good time to decide on any customization or integration requirements.
3. Installation: Install the DAM solution on the necessary servers or systems. This may include configuring the solution to connect to the database servers, setting up the database monitoring rules, and configuring the alerts and reports.
4. Configuration: Configure the DAM solution to meet your specific requirements, including setting up the monitoring rules, alerts, and reports. This may also include configuring the solution to integrate with other security tools, such as firewalls, intrusion detection systems, or security information and event management (SIEM) tools.

5. Testing: Test the DAM solution to ensure it is working as expected. This may include testing the monitoring rules, alerts, and reports, as well as testing the integration with other security tools.
6. Deployment: Deploy the DAM solution into production. This may include training end-users, migrating existing data, and updating any processes or procedures.
7. Ongoing maintenance: Perform ongoing maintenance and support for the DAM solution, including updating the solution as needed, monitoring the solution, and responding to any issues.

It's important to work with a DAM technology owner, a system integrator, and a managed security services provider who has experience with DAM solutions to ensure a successful implementation and operations.

8.2.4 What can go wrong in Database Activity Monitoring solution

Like any software solution, a Database Activity Monitoring (DAM) solution can encounter issues that affect its performance and reliability. Here are some common problems that can occur with DAM solutions:

1. Configuration errors: Configuration errors can result in incorrect monitoring, alerting, or reporting. For example, the monitoring rules may be misconfigured, leading to false positives or false negatives.
2. Integration issues: If the DAM solution is integrated with other security tools, such as firewalls, intrusion detection systems, or security information and event management (SIEM) tools, integration issues can occur. This can result in incorrect data being reported or alerts not being generated when necessary.
3. Performance issues: The DAM solution can impact the performance of the database servers, leading to slowdowns or even outages. This is especially important if the DAM solution is monitoring large databases or high-concurrency environments.
4. False positive alerts: The DAM solution may generate false positive alerts, which can be time-consuming to investigate and can distract from more serious security incidents.
5. Data privacy and security: The DAM solution may access sensitive data stored in the database, so it's important to ensure that the solution is secure, and that sensitive data is protected.
6. Complexity: The DAM solution may be complex to configure and manage, requiring specialized knowledge and expertise to set up and maintain.

It's important to thoroughly test the DAM solution before deploying it into production and to monitor the solution regularly to detect and resolve any issues that may arise. Additionally, it's important to work with a DAM technology owner, a system integrator, and a managed security services provider who has experience with DAM solutions to ensure a successful implementation.

8.2.5 What Service Levels can be committed/ expected?

Service Level Agreements (SLAs) in antivirus services can vary depending on the specific needs of an organization and the level of service offered by the provider. In the context of a Database Activity Monitoring (DAM) solution, some common service levels that can be committed include:

1. Availability: The percentage of time that the DAM solution is available and accessible to users. This may be expressed as an uptime guarantee, such as 99.9% availability.
2. Response time: The amount of time it takes for the provider to respond to a service request or issue. This may be expressed as a guaranteed response time, such as 2 hours.
3. Resolution time: The amount of time it takes for the provider to resolve a service request or issue. This may be expressed as a guaranteed resolution time, such as 4 hours.
4. Operations and Management- The detailed daily, weekly, monthly monitoring and management activities
5. Maintenance windows: The times during which the DAM solution may be unavailable for maintenance or upgrades. This may be expressed as a weekly or monthly maintenance window, during which the solution may be offline.
6. Data backup and recovery: The procedures for backing up and recovering data in the event of a disaster or data loss. This may include a guarantee for the recovery time objective (RTO) and recovery point objective (RPO).
7. Support hours: The hours during which the provider is available to provide support for the DAM solution. This may include 24x7 support or support during business hours.
8. Escalation procedures: The procedures for escalating issues to higher levels of support, if necessary.
9. Documentation and training: The availability of documentation and training materials to assist with the use and maintenance of the DAM solution.

The SLA should be reviewed regularly to ensure that the service levels continue to meet the needs of the client and to make any necessary updates. For cloud-based databases, the exact nature of the database activity monitoring changes slightly and must be discussed based on agreed ‘Shared Responsibility’ matrices with cloud services providers and client. Please keep in mind, it is not always possible to accurately provide a resolution time commitment and hence, take penalty conditions in contracts.

8.2.6 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.

2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

8.3 Delivery cue- Database Activity Monitoring operations

8.3.1 Daily Activities

Daily DAM operation activities typically include the following tasks:

1. Performance monitoring: This involves monitoring the performance metrics of the database such as response time, CPU utilization, memory usage, and disk space utilization.
2. Security monitoring: This involves monitoring the database for any security breaches or unauthorized access attempts. This can include monitoring for SQL injection attacks, unauthorized access attempts, and other security threats.
3. Backup and recovery monitoring: This involves monitoring the status of backup and recovery operations to ensure that data is being backed up and can be recovered in the event of a disaster.
4. Error and exception monitoring: This involves monitoring the database for any errors or exceptions that occur, such as deadlocks, constraint violations, and other issues.
5. Query monitoring: This involves monitoring the performance of individual SQL queries to identify any long-running or resource-intensive queries that may be affecting the performance of the database.
6. Auditing: This involves tracking changes made to the database, such as changes to data, schema, or configuration, to ensure that the database remains in compliance with internal policies and regulations.

These activities can help ensure the reliability, security, and performance of the database and its associated applications, and can help prevent outages or other issues that could affect the availability of the database.

8.3.2 Weekly Activities

Weekly DAM operation activities typically include the following tasks:

1. Capacity planning: This involves analysing database usage patterns to determine the future resource requirements of the database and to plan for capacity upgrades or optimizations as needed.
2. Database maintenance: This involves performing routine maintenance tasks such as index rebuilding, statistics updating, and checking for database consistency.
3. Data integrity checks: This involves running checks on the data stored in the database to ensure that it is accurate and complete and that it meets the requirements of the applications that use it.
4. Software and patch updates: These involve checking for and installing any available software or patch updates to keep the database software and its associated components up-to-date and secure.
5. Disaster recovery testing: This involves testing the disaster recovery process and procedures to ensure that the database can be recovered in the event of a disaster.
6. User access review: This involves reviewing the access permissions and roles of database users to ensure that they follow security policies and to identify any potential security risks.

These weekly activities can help maintain the health and stability of the database and its associated applications and can help prevent issues that could affect the availability and performance of the database.

8.3.3 Monthly Activities

Monthly DAM operation activities typically include the following tasks:

1. Data archiving: This involves archiving old or infrequently used data to free up disk space and improve performance.
2. Database replication monitoring: If the database is configured for replication, this involves monitoring the status of the replication processes to ensure that data is being replicated correctly and consistently.
3. Performance tuning: This involves analysing database performance metrics and making any necessary adjustments to improve performance, such as modifying indexes, tuning queries, and adjusting configuration settings.
4. License compliance review: This involves reviewing the licenses for any software and tools used in conjunction with the database to ensure that they are in compliance with licensing agreements and to avoid any potential legal issues.

5. Data backup review: This involves reviewing the backup procedures and processes to ensure that they follow disaster recovery policies and to identify any potential issues that need to be addressed.
6. Data retention policy review: This involves reviewing the data retention policy to ensure that it follows regulations and to determine if any changes need to be made.

These monthly activities can help maintain the long-term health and stability of the database and can help ensure that the database remains in compliance with internal policies, regulations, and best practices.

8.3.4 What does an L1 DAM Engineer do?

An L1 Database Activity Monitoring Engineer is a entry-level position responsible for monitoring and maintaining the health and performance of a database. The specific responsibilities of an L1 Database Activity Monitoring Engineer may vary depending on the organization, but some common tasks include:

1. Performance monitoring: Monitoring the performance of the database and its associated applications, including response time, CPU utilization, memory usage, and disk space utilization.
2. Error and exception handling: Identifying and resolving errors and exceptions that occur in the database, such as deadlocks, constraint violations, and other issues.
3. Backup and recovery monitoring: Monitoring the status of backup and recovery operations to ensure that data is being backed up and can be recovered in the event of a disaster.
4. Security monitoring: Monitoring the database for any security breaches or unauthorized access attempts and taking appropriate action to prevent or resolve any issues.
5. Query optimization: Optimizing the performance of individual SQL queries to improve the overall performance of the database.
6. Reporting: Generating and distributing reports on the performance and availability of the database to stakeholders and management.
7. Escalation: Escalating issues to higher-level support teams when necessary.

The L1 Database Activity Monitoring Engineer is typically the first point of contact for database-related issues, and they are responsible for ensuring that the database is running smoothly and efficiently. The role requires a basic understanding of database technologies, as well as the ability to troubleshoot and resolve technical issues.

8.3.5 What does an L2 DAM Engineer do?

An L2 Database Activity Monitoring Engineer is a mid-level position responsible for providing advanced support for the monitoring and maintenance of a database. This role is typically responsible for more complex tasks than an L1 Database Activity Monitoring Engineer, and may include the following responsibilities:

1. Performance tuning: Analysing performance metrics and making adjustments to improve the performance of the database, such as modifying indexes, tuning queries, and adjusting configuration settings.
2. Data backup and recovery: Configuring and maintaining backup and recovery procedures to ensure that data can be recovered in the event of a disaster.
3. Security management: Implementing security measures to protect the database from unauthorized access and other security threats.
4. Software and patch management: Installing software and patch updates to keep the database software and its associated components up-to-date and secure.
5. Capacity planning: Analysing database usage patterns to determine future resource requirements and plan for capacity upgrades or optimizations.
6. Database replication: Configuring and monitoring database replication processes to ensure that data is being replicated correctly and consistently.
7. Technical leadership: Providing technical guidance and support to junior-level support engineers and serving as a subject matter expert for the database environment.

The L2 Database Activity Monitoring Engineer is responsible for ensuring the stability, performance, and security of the database, and for providing advanced technical support for complex issues that cannot be resolved by the L1 support team. This role requires a strong understanding of database technologies and the ability to diagnose and resolve complex technical problems.

8.3.6 What does an L3 DAM Engineer do?

An L3 Database Activity Monitoring Engineer is a senior-level position responsible for providing expert-level support for the monitoring and maintenance of a database. This role typically involves the following responsibilities:

1. Architecture and design: Designing and implementing database solutions to meet the needs of the organization, including recommending hardware and software configurations, and developing backup and recovery strategies.
2. Problem resolution: Investigating and resolving complex and critical issues related to the database, such as performance bottlenecks, security breaches, and data integrity issues.
3. Technical leadership: Providing technical guidance and support to junior-level support engineers and serving as a subject matter expert for the database environment.
4. Vendor management: Interfacing with vendors and other external organizations to resolve technical issues and to ensure that the database software and hardware are functioning optimally.
5. Strategic planning: Developing and implementing long-term strategies for the database environment, including capacity planning, software upgrades, and disaster recovery planning.

6. Training: Providing training and mentorship to junior-level support engineers and other stakeholders to enhance their technical knowledge and capabilities.

The L3 Database Activity Monitoring Engineer is responsible for ensuring the overall health and stability of the database environment, and for providing expert-level support for complex technical issues. This role requires a deep understanding of database technologies and a strong ability to diagnose and resolve complex technical problems, as well as excellent leadership and communication skills.

8.3.7 Reports

DAM operation reports typically include the following:

1. Performance reports: These reports provide information on the performance of the database and its associated applications, including response time, CPU utilization, memory usage, and disk space utilization.
2. Error and exception reports: These reports provide information on errors and exceptions that occur in the database, such as deadlocks, constraint violations, and other issues.
3. Backup and recovery reports: These reports provide information on the status of backup and recovery operations, including backup completion times, backup sizes, and the success or failure of recovery operations.
4. Security reports: These reports provide information on security-related events and incidents, such as unauthorized access attempts, security breaches, and other security threats.
5. Query optimization reports: These reports provide information on the performance of individual SQL queries, including execution time and the number of rows returned.
6. Capacity planning reports: These reports provide information on the usage patterns of the database and its associated resources, including disk space utilization, memory usage, and CPU utilization.
7. Compliance reports: These reports provide information on the database environment's compliance with various regulatory standards and policies, such as data privacy regulations and industry standards.

These reports provide valuable information to stakeholders and management about the performance, security, and overall health of the database environment, and are used to make informed decisions about database-related issues and initiatives.

8.3.8 Governance of EMM, MDM, or MTD solution

The governance of a database activity monitoring solution involves the establishment of policies, procedures, and standards to ensure the effective, secure, and compliant use of the solution. It involves the following key elements:

1. Ownership and responsibility: Defining the roles and responsibilities of stakeholders involved in the implementation, maintenance, and use of the database activity monitoring solution.

2. Data classification and protection: Establishing policies for the protection of sensitive and confidential data, including the implementation of data access controls and encryption.
3. Compliance: Ensuring that the database activity monitoring solution complies with relevant regulations, standards, and policies, such as data privacy regulations and industry standards.
4. Security: Implementing security measures to protect the database activity monitoring solution from unauthorized access and other security threats, such as firewalls, access controls, and encryption.
5. Monitoring and reporting: Establishing procedures for the regular monitoring and reporting of database activity, including the identification of unusual activity and the initiation of appropriate action.
6. Auditing: Conducting regular audits of the database activity monitoring solution to ensure compliance with policies and standards and to identify areas for improvement.
7. Incident response: Developing and implementing a plan for responding to security incidents, such as data breaches or unauthorized access attempts, to minimize the risk of data loss or damage.
8. Continuous improvement: Continuously reviewing and improving the governance of the database activity monitoring solution to ensure its effectiveness and efficiency.

Effective governance of a database activity monitoring solution is essential for ensuring the security and compliance of the database environment and for supporting the overall success of the solution.

9. Managed Security Services

Managed Security Services (MSS) is a type of service provided by an external vendor or service provider that offers a comprehensive suite of security solutions and services designed to protect an organization's information technology (IT) assets. This includes services such as monitoring, threat detection, incident response, and management of security technologies and devices, such as firewalls, intrusion detection systems, and security information and event management (SIEM) systems.

The objective of MSS is to help organizations mitigate security risks and respond to security incidents in a timely and effective manner, without having to invest in internal resources or expertise. MSS providers offer a range of security services, from basic monitoring and threat detection to more advanced services such as security analytics and incident response.

9.1 Advantages of Managed Security Services

Advantages of using MSS include:

1. Expertise: MSS providers have dedicated security experts and specialized tools to provide round-the-clock monitoring and protection of an organization's IT assets.
2. Scalability: MSS services can be scaled to meet the changing needs of an organization, allowing for flexibility and cost-effectiveness.
3. Continuous improvement: MSS providers continuously monitor and assess the latest security threats and trends and update their services to keep pace with evolving security risks.
4. Cost savings: By outsourcing security services, organizations can reduce the cost of hiring and training in-house security staff, and reduce the costs associated with security software and hardware.

MSS is a valuable service for organizations of all sizes that need to secure their IT assets and ensure compliance with security regulations and standards, without having to invest in internal security resources and expertise.

9.2 How are Managed Detection & Response Services different

Managed Detection and Response (MDR) and Managed Security Services (MSS) are two different approaches to managing an organization's security needs. While both provide managed security solutions, there are some key differences between MDR and MSS:

1. Focus: MDR focuses specifically on detecting and responding to security threats, while MSS is a broader service that includes a range of security solutions and services, such as monitoring, threat detection, incident response, and management of security technologies and devices.
2. Level of service: MDR typically provides a higher level of service and expertise compared to MSS, as it focuses specifically on detecting and responding to security threats.
3. Cost: MDR is generally more expensive than MSS, as it provides a higher level of service and expertise.

4. Customization: MDR is typically a more customized service, as it focuses specifically on the security needs of an individual organization, while MSS is a more standardized service that is delivered to many different organizations.
5. Monitoring: MDR provides continuous monitoring and threat detection, while MSS may provide monitoring as part of a broader suite of security services.

Ultimately, the choice between MDR and MSS depends on the specific security needs and requirements of an organization. MDR is ideal for organizations that require a higher level of security and expertise, while MSS may be a better option for organizations that need a broader range of security services or have limited budgets.

9.3 What is a Security Operations Centre?

A Security Operations Centre (SOC) is a centralized team responsible for the security of an organization's information systems and assets. To effectively fulfil this role, a SOC typically requires the following components:

1. Security Information and Event Management (SIEM) software: A SIEM tool is used to collect and analyse security-related data from a variety of sources, such as logs and alerts from firewalls, intrusion detection systems, and other security devices.
2. Threat intelligence sources: A SOC should subscribe to and incorporate information from trusted sources of threat intelligence to help identify and prioritize potential security threats.
3. Vulnerability management tools: These tools help identify and remediate vulnerabilities in systems and applications that could be exploited by attackers.
4. Incident response plan: A documented incident response plan outlines the steps the SOC will take in the event of a security incident, including communication with stakeholders, escalation procedures, and incident resolution procedures.
5. Security analyst team: A team of experienced security analysts with the necessary skills and knowledge to operate the SOC, analyse security data, and respond to security incidents.
6. Management support: Effective SOC management is critical for ensuring that the SOC has the resources and support it needs to operate effectively.
7. Continuous improvement: A SOC should be designed with continuous improvement in mind, and should regularly assess and improve its processes, technology, and staffing to ensure that it remains effective over time.

This is by no means an exhaustive list, and the exact components of a SOC will vary based on the specific needs and requirements of the organization.

9.4 How is NG-SOC different from SOC?

NG SOC (Next-Generation Security Operations Centre) and SOC (Security Operations Centre) are terms used to describe the centralized management and coordination of an organization's security activities. While both are focused on providing a centralized approach to security, there are some key differences between the two:

1. Technology: NG SOCs typically leverage advanced security technologies, such as artificial intelligence, machine learning, and automation, to enhance the efficiency and effectiveness of security operations. SOCs may use these technologies to some extent, but they are not typically their primary focus.
2. Focus: NG SOCs are designed to be proactive in detecting and responding to security threats, while SOCs are focused on monitoring and reacting to security incidents.
3. Integration: NG SOCs are typically more integrated with other parts of an organization's IT infrastructure, such as network and endpoint security solutions, while SOCs may be more siloed.
4. Processes: NG SOCs typically have more mature and streamlined security processes and workflows, such as incident response and threat hunting, compared to SOCs.
5. Collaboration: NG SOCs typically promote greater collaboration between different parts of an organization, such as IT and security teams, to enhance security operations, while SOCs may have limited collaboration between different teams.

Ultimately, the choice between an NG SOC and a SOC depends on the specific security needs and requirements of an organization. An NG SOC is ideal for organizations that require a more proactive and integrated approach to security, while a SOC may be a better option for organizations with limited budgets or resources.

9.5 SOAR, UEBA, CTI: What are these?

SOAR, UEBA, and CTI are all related to security operations and threat management. Here's a brief overview of each term:

1. SOAR (Security Orchestration, Automation, and Response): SOAR refers to a set of security technologies and processes that automate and streamline security operations. The goal of SOAR is to improve the efficiency and effectiveness of security operations, and to reduce the time it takes to detect and respond to security incidents.
2. UEBA (User and Entity Behaviour Analytics): UEBA is a type of security solution that leverages machine learning and artificial intelligence to analyse user and entity behaviour to detect security threats and anomalies. UEBA is designed to be more proactive and effective in detecting security threats, compared to traditional security solutions that rely on predefined rules and signatures.
3. CTI (Cyber Threat Intelligence): CTI refers to information and intelligence about current and emerging cyber threats, vulnerabilities, and attack methods. CTI is used by security teams to enhance their understanding of the threat landscape and to better defend against security threats.

These three terms are related in that they are all part of a comprehensive approach to security operations and threat management. SOAR, UEBA, and CTI can be used together to automate and streamline security operations, improve the detection and response to security incidents, and provide valuable intelligence and context to security teams.

9.6 SOAR- Tell me more

SOAR (Security Orchestration, Automation, and Response) is a security operations approach that combines technology and processes to automate and streamline security operations. The goal of SOAR is to improve the efficiency and effectiveness of security operations, and to reduce the time it takes to detect and respond to security incidents. SOAR typically consists of the following components:

1. Security orchestration: This component automates the coordination of security technologies and processes to respond to security incidents. Security orchestration allows security teams to automate complex, time-consuming, and repetitive security tasks, such as triage and incident response.
2. Security automation: This component automates the execution of security processes and workflows, such as incident response and threat hunting. Security automation helps to reduce the time it takes to detect and respond to security incidents, and to reduce the risk of human error.
3. Security response: This component manages the actual response to security incidents, including the collection of relevant information, the execution of response procedures, and the tracking of incident resolution.

SOAR can be used in conjunction with other security technologies, such as SIEMs (Security Information and Event Management), threat intelligence platforms, and security analytics, to provide a comprehensive approach to security operations. The benefits of SOAR include:

1. Improved efficiency and effectiveness of security operations: SOAR streamlines and automates security processes, reducing the time it takes to detect and respond to security incidents, and improving the accuracy of security operations.
2. Reduced risk of human error: SOAR minimizes the risk of human error by automating complex and repetitive security tasks.
3. Enhanced incident response: SOAR provides a centralized and coordinated approach to incident response, improving the speed and efficiency of incident resolution.
4. Improved threat visibility: SOAR provides a more complete and comprehensive view of security incidents, improving the ability of security teams to detect and respond to threats.

9.7 UEBA: tell me more

UEBA (User and Entity Behaviour Analytics) is a type of security solution that leverages machine learning and artificial intelligence to analyse user and entity behaviour to detect security threats and anomalies. UEBA is designed to be more proactive and effective in detecting security threats, compared to traditional security solutions that rely on predefined rules and signatures.

UEBA works by collecting and analysing data from multiple sources, such as network logs, endpoint logs, and user activity logs, to build a baseline of normal user and entity behaviour. The UEBA system then uses machine learning algorithms to identify unusual or suspicious behaviour that may indicate a security threat.

UEBA can detect a wide range of security threats, including insider threats, advanced persistent threats (APTs), and credential theft. UEBA can also be used to detect violations of security policies, such as the unauthorized access of sensitive data. The benefits of UEBA include:

1. Proactive threat detection: UEBA goes beyond traditional security solutions by proactively detecting security threats, rather than relying on predefined rules and signatures.
2. Improved accuracy: UEBA uses machine learning algorithms to analyse user and entity behaviour, improving the accuracy of threat detection.
3. Enhanced visibility: UEBA provides a comprehensive view of user and entity behaviour, improving the visibility of security threats and anomalies.
4. Reduced false positives: UEBA reduces the number of false positives generated by traditional security solutions, reducing the workload of security teams, and improving the overall efficiency of security operations.

UEBA is typically used in conjunction with other security technologies, such as SIEMs (Security Information and Event Management) and security orchestration and automation (SOAR) solutions, to provide a comprehensive approach to security operations.

9.8 CTI: Tell me more

CTI (Cyber Threat Intelligence) is information gathered and analysed about the threats faced by an organization in the cyberspace. CTI enables organizations to understand the nature and potential impact of cyber threats and to develop appropriate responses and defences.

CTI is derived from multiple sources, including open-source intelligence (OSINT), proprietary data, and data from other organizations that have been targeted by similar threats. This information is analysed and used to develop a comprehensive understanding of the threat landscape, including the motivations and tactics of threat actors, the tools and techniques they use, and the potential impact of their actions. The benefits of CTI include:

1. Improved threat visibility: CTI provides organizations with a better understanding of the threat landscape, enabling them to detect and respond to security incidents more effectively.
2. Enhanced threat response: CTI provides organizations with the information they need to develop effective responses to security incidents, including the identification of threat actors, their motivations and tactics, and the tools and techniques they use.
3. Improved threat prevention: CTI enables organizations to develop more effective security measures by providing insight into the tactics and techniques used by threat actors and the potential impact of their actions.
4. Better incident management: CTI provides organizations with the information they need to manage security incidents more effectively, including the identification of the threat actors and their motivations, and the potential impact of their actions.

CTI is used by organizations of all sizes, including government agencies, large corporations, and small businesses, to improve the security of their networks and systems and to protect

against cyber threats. CTI is typically used in conjunction with other security technologies, such as SIEMs (Security Information and Event Management) and security orchestration and automation (SOAR) solutions, to provide a comprehensive approach to security operations.

9.9 Sales cue- Questions to ask and answers to give

9.9.1 How to discover potential buyers for managed security services

There are several ways to discover potential buyers for managed security services:

1. Market research: Conduct market research to understand the market demand for managed security services. Identify the industries and verticals that need such services.
2. Networking: Attend relevant industry events, join professional organizations and network with potential buyers and industry leaders.
3. Cold outreach: Reach out to potential buyers directly through cold emails or calls. Research potential buyers, personalize your approach and make a compelling case for your managed security services.
4. Online advertising: Utilize online advertising platforms such as Google Ads, LinkedIn Ads or Facebook Ads to target your audience and drive traffic to your website.
5. Referrals: Ask for referrals from current clients, partners, or industry professionals. Word-of-mouth can be a powerful tool for finding new business opportunities.
6. Partner with complementary companies: Partner with companies that offer complementary services to your managed security services, such as IT service providers or cloud solution providers.

Remember, the key is to identify your target market and understand their needs. Once you know who your ideal buyer is, you can tailor your marketing efforts to reach them effectively.

9.9.2 Questions to ask prospective client

When speaking with potential buyers of managed security services, it's important to understand their current security posture, challenges, and goals. Here are some questions that can help you gather this information:

1. Can you describe your current security infrastructure and processes?
2. What security challenges are you currently facing?
3. What are your security goals for the next 12-24 months?
4. How do you currently manage and respond to security incidents?
5. Have you ever experienced a security breach or cyber-attack? If so, how did you handle it?
6. What is your current budget for security services?

7. Have you worked with a managed security service provider in the past? If so, what was your experience like?
8. How do you prioritize and make decisions about your security investments?
9. What criteria are you using to evaluate managed security service providers?
10. When are you looking to implement a managed security service solution?

Asking these questions can help you understand the potential buyer's current security needs and priorities and determine if your managed security services would be a good fit for them. It's also a good opportunity to showcase your expertise and build a rapport with the potential buyer.

9.9.3 Questions prospective clients will ask of sales

Prospective clients evaluating Managed Security Services or Managed Detection and Response services may have a variety of questions based on their specific needs and requirements. Here are some common questions that clients ask:

1. What security services do you offer?
2. What is included in your managed security services package?
3. How do you monitor and detect security threats?
4. How do you respond to security incidents?
5. How do you ensure the privacy and security of my data?
6. How do you stay current with the latest security threats and technologies?
7. How do you handle communication and collaboration with my internal security team?
8. Can you provide references from current clients?
9. What is your pricing model and what is the cost of your services?
10. What is your process for on-boarding new clients?
11. What level of support do you provide for your managed security services?
12. How do you measure the success of your managed security services?
13. Can you provide examples of security incidents that you have successfully resolved for your clients?
14. What measures do you have in place to ensure the continuity and availability of your services?
15. How do you handle security incidents outside of normal business hours?

By asking these questions, clients can gain a better understanding of the provider's capabilities and ensure that they can meet security needs and provide the level of service required.

9.9.4 What to cover in cybersecurity capability presentation

A presentation on cybersecurity capability should typically cover the following topics:

1. Overview of cybersecurity and its importance in today's digital world
2. Threat landscape and the different types of cyber attacks
3. Importance of proactive measures, such as risk assessments and vulnerability management
4. Security policies, procedures, and standards to ensure compliance and governance
5. Incident response planning and management, including communication and reporting processes
6. Security awareness training for employees and end-users
7. Emerging technologies and trends in cybersecurity, such as cloud security and IoT security
8. Key performance indicators (KPIs) and metrics for measuring the effectiveness of cybersecurity capability
9. Cybersecurity budget and investment considerations.

9.9.5 Payment terms to agree with the clients

When agreeing on payment terms with potential buyers for managed security services, there are several factors to consider:

1. Service level agreement (SLA): Outline the expected level of service, response times, and availability in an SLA.
2. Pricing model: Decide on a pricing model that works best for both parties. This could be a monthly retainer, project-based, or a combination of both.
3. Payment schedule: Determine the payment schedule, whether it is monthly, quarterly, or annually.
4. Payment method: Agree on a payment method, whether it is by credit card, bank transfer, or another method.
5. Late payment fees: Consider including late payment fees in the contract to encourage timely payment.
6. Renewal terms: Discuss renewal terms, such as automatic renewals, notice periods, and rate adjustments.
7. Termination clause: Include a termination clause that outlines the conditions under which either party can terminate the agreement.

It's important to have clear and agreed-upon payment terms to avoid misunderstandings and disputes down the line. A written agreement that outlines the payment terms, along with the SLA and other relevant details, can provide a clear understanding of the expectations and responsibilities of both parties.

9.10 Pre-sales cue: Solution building complexities

9.10.1 Benchmarks for SOC manpower sizing

There is no one-size-fits-all answer to the question of how to size a security operations centre (SOC) team, as the size of the SOC will depend on the size of the organization and the level of security risk it faces. However, there are a few benchmarking methods that can be used to help determine the optimal size of a SOC team:

1. Analyse the size of the organization: A SOC should have enough manpower to cover the size of the organization and the number of systems and devices it manages.
2. Assess the level of risk: The level of risk faced by the organization will influence the size of the SOC team. A higher level of risk will require a larger SOC team to manage the increased volume of incidents and threats.
3. Consider industry benchmarks: Some industry groups have established benchmarks for the size of SOC teams. For example, the SANS Institute recommends that organizations have one SOC analyst for every 1,000 to 2,000 devices or systems managed. The SANS Institute recommends a ratio of one SOC analyst for every 1,000 to 2,000 devices or systems managed because it provides an appropriate level of staffing to manage a large number of systems while still allowing each analyst to focus on specific tasks and responsibilities. This ratio is intended to provide the right balance between having enough resources to manage the organization's security posture effectively, while avoiding over-burdening the security team with too many systems to manage.

   However, the exact staffing ratio will vary based on the complexity of the organization's infrastructure, the types of systems and data being protected, and the level of threat activity the organization is experiencing. In some cases, a smaller ratio may be more appropriate, while in others a larger ratio may be required. Ultimately, the goal is to have a staffing ratio that allows the SOC to effectively manage the organization's security posture, respond to security incidents, and continuously improve the organization's security posture over time.
4. Look at the volume of incidents: The volume of incidents that the SOC must handle will also impact the size of the team. The more incidents the SOC handles, the more personnel it will need to manage the workload.
5. Delivery model: Consider a mix of onsite and remote monitoring solutions as is appropriate for the client requirements.
6. Analyse staffing trends: Organizations should also analyse trends in their staffing needs over time and plan for future growth. For example, if the volume of incidents is increasing, the SOC team should also grow in size to manage the increased workload.

These are just a few of the many factors that can influence the size of a SOC team. Ultimately, the goal of SOC manpower sizing is to have enough personnel to manage the volume of incidents and threats faced by the organization while also ensuring that the SOC is cost-effective and efficient.

9.10.2 How are SIEM licenses sized for?

To size the number of Security Information and Event Management (SIEM) licenses required for an organization, the following factors should be considered:

1. Data volume: The amount of data that needs to be collected and analysed by the SIEM solution, which may include logs from network devices, servers, and applications.
2. Log retention period: The duration for which logs need to be stored for compliance, auditing, and investigation purposes.
3. Compliance requirements: The regulatory and industry-specific requirements that must be met, which may dictate the types of logs that need to be collected and the retention period.
4. Use case requirements: The specific use cases for the SIEM solution, such as threat detection, incident response, and compliance monitoring, which may require different types of data to be collected and analysed.
5. IT environment complexity: The complexity of the IT environment, including the number of devices, applications, and users, which may impact the performance and scalability of the SIEM solution.

Once these factors have been assessed, the number of SIEM licenses required can be estimated based on the data volume, log retention period, and other requirements. It is also important to consider factors such as redundancy and failover to ensure high availability and continuity of the SIEM solution. It is recommended to consult with the SIEM vendor or a trusted SIEM partner to help determine the appropriate licensing for an organization's specific needs.

9.10.3 EPS Vs Number of devices Vs Log Volume?

EPS, number of devices, and log volume are all important factors to consider when sizing a Security Information and Event Management (SIEM) solution. Here is a brief overview of these factors:

1. EPS (Events Per Second): EPS is the rate at which events are generated in an IT environment. SIEM solutions are often licensed based on the EPS capacity they can handle, as this directly impacts the performance and scalability of the solution. This can vary wildly between SIEM solutions. There are several factors that can impact the EPS (Events Per Second) capacity of a Security Information and Event Management (SIEM) solution. Here are some of the key factors:
    a. **Log volume:** The volume of logs generated by the devices being monitored. These devices have different configurations. A device configuration is a set of settings and parameters that determine how a particular device operates and interacts with other devices in an IT environment.

       Device configuration is an important aspect of IT management as it can impact the security, performance, and functionality of the device and the overall IT environment. Device configuration typically includes settings such as network configuration, authentication and access controls, software and firmware

versions, hardware settings, and other parameters that determine the behaviour of the device. These settings can be configured manually or through automated tools and may vary depending on the type and function of the device. For example, a router or a switch may have a configuration that determines how it routes traffic between different networks, while a server may have a configuration that specifies which applications and services are running and how they are configured.

Proper device configuration is critical for ensuring the security and stability of an IT environment. Incorrect or insecure configurations can leave devices vulnerable to attacks and can cause performance or stability issues. Therefore, it is important to maintain accurate and up-to-date device configurations and to regularly review and audit device configurations to ensure they are aligned with security policies and best practices.

Important to note: Same firewall model generates different EPS for different clients because of the way the configuration has been fine-tuned. SIEM solutions collect, process, and analyze logs to detect potential security incidents, so the log volume directly impacts the EPS capacity of the SIEM solution.

b. **Event complexity**: The complexity of the events being generated, including the number of fields and the size of the events. More complex events generally require more processing power and can reduce the EPS capacity of the SIEM solution. Here are some examples of event complexity in a Security Information and Event Management (SIEM) solution:

    i. Events with a large number of fields: Some events may contain a large number of fields or attributes, which can make them more complex to process and analyse. For example, a system log that contains detailed information about a user's activity may include dozens of fields, each with its own value.

    ii. Events with complex data structures: Some events may have complex data structures that make them more difficult to parse and analyse. For example, events that contain nested objects or arrays can require more processing power to handle.

    iii. Encrypted events: Events that are encrypted can be more complex to analyse since they require decryption before they can be processed. Decrypting events can be resource-intensive and can impact the EPS capacity of the SIEM solution.

    iv. Malformed events: Events that are incorrectly formatted or that contain errors can be more complex to analyse since they may not conform to the expected data structure. This can require additional processing power and can impact the performance of the SIEM solution.

    v. Custom events: Custom events that are not part of a pre-defined data model can be more complex to process since they may require custom

parsing and analysis rules. Custom events can be especially challenging for SIEM solutions that do not support custom data models.

All these factors can impact the complexity of events in a SIEM solution and can impact the EPS capacity of the solution. It is important to carefully consider event complexity when designing and sizing a SIEM solution to ensure it can handle the expected volume and complexity of events in the IT environment.

c. **Use case requirements**: The specific use cases for the SIEM solution, such as threat detection, incident response, and compliance monitoring, which may require different types of data to be collected and analyzed. Some use cases may generate more events than others, which can impact the EPS capacity. Use cases are an important part of a Security Information and Event Management (SIEM) solution and are used to identify potential security threats or incidents in an organization's IT environment. They help security analysts to identify patterns and anomalies in log and event data that may be indicative of a security breach or other security incident.

   Use cases can be tailored to specific types of threats or incidents, such as malware infections, account compromises, or data exfiltration attempts. They can also be designed to meet compliance requirements or to support incident response procedures.

   Effective use cases typically involve a combination of log sources, filtering criteria, correlation rules, and automated responses, such as generating alerts, blocking traffic, or quarantining infected devices.

   Developing and maintaining effective use cases is an ongoing process, as threat actors are constantly evolving their tactics and techniques. Regular review and updating of use cases is important to ensure that they remain relevant and effective in detecting potential security incidents.

d. **Filtering and correlation rules**: Filtering and correlation are two important processes in the context of cybersecurity and Security Information and Event Management (SIEM) solutions.

   The number and complexity of filtering and correlation rules applied to the events being processed. These rules can reduce the EPS capacity by increasing the processing time required for each event.

   Filtering is the process of narrowing down a large volume of log and event data to a smaller set of relevant events. This is typically done by applying filters or rules to the data, such as filtering out events that are not relevant to a particular use case or security incident. Filtering helps to reduce the amount of data that needs to be processed and analysed by a SIEM solution, which can improve performance and reduce false positives.

   Correlation is the process of analysing the relationship between different events to identify patterns or anomalies that may be indicative of a security threat or incident. Correlation rules are typically defined based on a specific use case or security incident, and can involve looking for patterns in event

timestamps, source and destination IP addresses, usernames, and other data. Correlation helps to identify potential threats or incidents that may not be visible when looking at individual events in isolation.

Together, filtering and correlation help to identify and investigate potential security threats or incidents in an organization's IT environment. By applying filtering rules to reduce the amount of data that needs to be analysed, and by using correlation rules to identify patterns and anomalies in the remaining data, security analysts can more effectively identify and respond to potential security threats.

e. **Hardware and software resources**: The hardware and software resources available to the SIEM solution, including CPU, memory, and storage capacity. Insufficient resources can limit the EPS capacity of the SIEM solution.

2. Number of devices: The number of devices that need to be monitored by the SIEM solution, including network devices, servers, endpoints, and cloud environments. This factor is also related to EPS, as more devices generally generate more events.
3. Log volume: The volume of logs generated by the devices being monitored. SIEM solutions collect, process, and analyse logs to detect potential security incidents, so the log volume is a critical factor to consider when sizing the solution.

It is important to carefully consider all of these factors when designing and sizing a SIEM solution to ensure it can handle the required EPS capacity and meet the organization's security requirements. It is also recommended to consult with the SIEM vendor or a trusted SIEM partner to help determine the appropriate sizing for an organization's specific needs.

9.10.4 Typical Server EPS

The typical server EPS (events per second) can vary greatly depending on the type of server, the applications running on it, and the level of logging enabled. In general, servers with high network traffic, such as web servers or application servers, tend to generate a higher volume of events than servers that are used for file storage or other less network-intensive tasks.

According to industry benchmarks, a typical EPS for a server can range from a few hundred to several thousand events per second, depending on the server type and workload. For example, a busy web server can generate tens of thousands of requests per second, each of which may generate one or more log events. Similarly, an application server may generate a high volume of events related to user activity, database queries, and other application-specific events. Some other studies mention low EPS examples as follows:

1. Windows Domain Servers- EPS hover around 35-40
2. Windows App Servers on HA- EPS hovers around 1-2
3. DB Servers on HA- EPS hovers around 1-2
4. Exchange Servers- EPS hovers around 3-5
5. DNS Servers- EPS hovers below 1
6. Linux Servers- EPS hovers below 0.5

7. Proxies- EPS hovers around 12-15

It is important to carefully consider the EPS capacity of a Security Information and Event Management (SIEM) solution when designing and sizing a solution. The EPS capacity required will depend on the number of servers, network devices, and other log sources that need to be monitored, as well as the expected EPS from each source. Sizing a SIEM solution requires careful consideration of EPS, as well as other factors such as log volume, storage capacity, and processing power, to ensure that the solution can effectively handle the expected workload. It is best to discuss the configurations in detail with client teams to get a right fix on the EPS.

9.10.5 Typical Firewall EPS

The typical Firewall EPS (events per second) can vary depending on the size and complexity of the network being monitored, as well as the number and types of security rules configured on the firewall.

In general, firewalls generate a relatively high volume of events compared to other network devices, as they are responsible for controlling access to the network and enforcing security policies. According to industry benchmarks, a typical firewall can generate anywhere from several hundred to several thousand events per second.

The EPS capacity of a Security Information and Event Management (SIEM) solution should be carefully considered when designing and sizing a solution for monitoring firewall logs. The EPS capacity required will depend on the number of firewalls being monitored, as well as the expected EPS from each firewall.

In addition, effective monitoring of firewall logs requires careful filtering and correlation to distinguish normal network traffic from potential security threats. This can involve filtering out known benign traffic, such as internal network traffic or traffic from trusted sources, to reduce the volume of data that needs to be analysed. Correlation rules can then be used to identify potential security threats, such as traffic from suspicious or unknown sources, or traffic that violates established security policies.

Overall, effective monitoring of firewall logs is an essential component of a comprehensive security monitoring strategy, and requires careful consideration of EPS capacity, log volume, and filtering and correlation techniques to ensure that potential security threats are identified and addressed in a timely manner.

9.10.6 Typical Kubernetes EPS

The typical Kubernetes EPS (events per second) can vary depending on the size and complexity of the Kubernetes cluster, as well as the number and types of applications running on it. Kubernetes is a container orchestration platform that is used to deploy and manage containerized applications at scale, and it generates log and event data related to container creation, deletion, and other cluster management activities.

In general, the EPS for a Kubernetes cluster can range from several hundred to several thousand events per second. This can include events related to container lifecycle management, cluster health monitoring, and application logging.

The EPS capacity of a Security Information and Event Management (SIEM) solution should be carefully considered when designing and sizing a solution for monitoring a Kubernetes cluster. The EPS capacity required will depend on the number of Kubernetes nodes and applications, as well as the expected EPS from each source.

In addition, special consideration should be given to the unique logging and monitoring requirements of a Kubernetes cluster, including the need to monitor container logs, as well as the logs generated by Kubernetes system components such as the API server, *etcd,* and the **scheduler.** Effective monitoring of a Kubernetes cluster requires a combination of log aggregation, filtering, and correlation, and may require specialized tools and expertise.

9.10.7 What is etcd of kubernetes

In Kubernetes parlance, etcd is a distributed key-value store that is used by Kubernetes as a central registry for storing configuration data, state information, and metadata about the Kubernetes cluster. etcd is a critical component of a Kubernetes cluster, as it is used to maintain consistency and coordination between the various nodes in the cluster, and to store information about the state of the system.

In Kubernetes, etcd is used to store information such as the state of running pods, the configuration of services and endpoints, and the status of the cluster's various components. etcd can also be used to store custom data and metadata that is specific to a particular Kubernetes deployment.

Since etcd is a critical component of a Kubernetes cluster, it is important to monitor its logs and events to ensure that the cluster is functioning correctly and to detect any potential issues or failures. Monitoring etcd logs can help to identify issues such as node failures, network outages, and other issues that can impact the stability and performance of the Kubernetes cluster.

In addition to monitoring etcd logs, it is also important to ensure that the etcd cluster is configured securely and that appropriate access controls are in place to protect sensitive data stored in the registry. Overall, effective monitoring and management of etcd is essential for maintaining the stability and security of a Kubernetes cluster.

9.10.8 What is scheduler of kubernetes

The scheduler is a key component of a Kubernetes cluster that is responsible for scheduling pods onto nodes in the cluster. When a new pod is created in the cluster, the scheduler examines the resource requirements and constraints of the pod and selects a suitable node on which to run the pod.

The Kubernetes scheduler uses a number of different strategies and policies to make scheduling decisions, including spreading pods across different nodes to ensure high availability, optimizing resource utilization by co-locating related pods on the same node, and

ensuring that pods with specific constraints (such as hardware requirements or location) are scheduled on the appropriate nodes.

Since the scheduler is a critical component of a Kubernetes cluster, it is important to monitor its logs and events to ensure that the scheduling process is functioning correctly and to detect any potential issues or failures. Monitoring the scheduler can help to identify issues such as scheduling conflicts, resource constraints, and other issues that can impact the stability and performance of the Kubernetes cluster.

In addition to monitoring the scheduler logs, it is important to ensure that the scheduler is configured correctly and that appropriate access controls are in place to protect sensitive data stored in the scheduler. Overall, effective monitoring and management of the scheduler is essential for maintaining the stability and security of a Kubernetes cluster.

9.10.9 Implementation steps of SIEM solution

The implementation of a Security Information and Event Management (SIEM) solution typically involves the following steps:

1. Define the requirements: Identify the key business and technical requirements for the SIEM solution, including the types of data sources that will be monitored, the expected volume of events, and the use cases and compliance requirements that need to be addressed.
2. Design the architecture: Design the overall architecture of the SIEM solution, including the deployment model, the hardware and software components required, and the network topology. Ensure that the architecture can support the expected volume of events and is scalable and resilient.
3. Implement the solution: Install and configure the SIEM solution, including the data collection and parsing mechanisms, the event processing and storage infrastructure, and any correlation and reporting features. Configure the system to align with the defined requirements and use cases.
4. Configure the data sources: Configure the various data sources, such as firewalls, servers, and network devices, to send logs and events to the SIEM solution. Ensure that the correct data is being collected and that the data is being normalized and parsed correctly.
5. Test the system: Test the SIEM solution to ensure that it is collecting and processing events correctly, that the correlation and reporting features are functioning correctly, and that the system is providing the desired results for the defined use cases and compliance requirements.
6. Deploy the system: Deploy the SIEM solution in the production environment and monitor the system to ensure that it is functioning correctly and meeting the defined requirements.
7. Tune and optimize the system: Continuously monitor and tune the SIEM system to ensure that it is providing the desired results, and optimize the system for performance, scalability, and efficiency.

8. Train the staff: Train the staff responsible for managing and monitoring the SIEM solution and ensure that they have the necessary skills and knowledge to operate and maintain the system effectively.
9. Maintain and support the system: Maintain and support the SIEM solution over its lifecycle, including ongoing system maintenance, updates, and upgrades, and provide support for the staff responsible for managing and monitoring the system.

Overall, the implementation of a SIEM solution is a complex process that requires careful planning, design, and implementation to ensure that the system is functioning correctly and meeting the defined requirements and use cases.

9.10.10 Integrating SOAR with SIEM solution

The integration of a Security Orchestration, Automation, and Response (SOAR) solution with a Security Information and Event Management (SIEM) solution typically involves the following steps:

1. Identify Use Cases: Identify the use cases that need to be addressed by the SOAR and SIEM solutions. This could include use cases such as alert triage and investigation, incident response, threat hunting, and compliance reporting.
2. Plan Integration: Plan the integration of the SOAR and SIEM solutions by identifying the data sources that will be used to feed the SIEM solution and the use cases that will be addressed by the SOAR solution.
3. Configure Data Sources: Configure the various data sources such as firewalls, servers, and network devices to send logs and events to the SIEM solution. Ensure that the correct data is being collected and that the data is being normalized and parsed correctly.
4. Integrate the SIEM Solution: Integrate the SIEM solution with the SOAR solution by configuring the SIEM solution to forward relevant alerts or events to the SOAR solution. This could involve configuring the SIEM solution to send alerts to the SOAR solution through APIs or other integration mechanisms.
5. Develop Playbooks: Develop playbooks in the SOAR solution to automate the response to specific types of events or incidents. This could involve defining the actions to be taken, the conditions under which those actions are triggered, and the workflows that are required to support the response.
6. Test the System: Test the SOAR and SIEM solutions to ensure that they are functioning correctly and that the automated response and remediation features are working as expected.
7. Deploy the System: Deploy the SOAR and SIEM solutions in the production environment and monitor the system to ensure that it is functioning correctly and meeting the defined requirements.
8. Train the Staff: Train the staff responsible for managing and monitoring the SOAR and SIEM solutions and ensure that they have the necessary skills and knowledge to operate and maintain the systems effectively.

9. Maintain and Support the System: Maintain and support the SOAR and SIEM solutions over their lifecycle, including ongoing system maintenance, updates, and upgrades, and provide support for the staff responsible for managing and monitoring the systems.

Overall, the integration of a SOAR solution with a SIEM solution can provide significant benefits in terms of improved incident response times, reduced workload for security teams, and enhanced overall security posture.

9.10.11 What can go wrong in SIEM, SOAR, UEBA solution

There are several things that can go wrong with SIEM, SOAR, and UEBA solutions. Here are some common issues:

1. Poor Data Quality: SIEM, SOAR, and UEBA solutions rely on data from various sources. If the data is incomplete, inconsistent, or inaccurate, it can result in false positives or false negatives, leading to missed or unnecessary alerts.
2. Configuration Errors: Incorrect configuration of the SIEM, SOAR, or UEBA solution can result in incorrect alerts, missed alerts, or system failure.
3. Lack of Context: A lack of context can lead to an inability to properly identify and respond to security events. The absence of contextual data such as device or user information, can lead to difficulties in identifying the source of a threat, and can make it difficult to prioritize events and incidents.
4. Alert Fatigue: SIEM, SOAR, and UEBA solutions can generate a large volume of alerts, which can lead to alert fatigue. This happens when security analysts are overwhelmed by the number of alerts, and they can miss critical alerts or make mistakes while triaging them.
5. Integration Issues: Integrating SIEM, SOAR, and UEBA solutions with other security tools and systems can be challenging. Integration issues can lead to data loss, duplication, or other problems that affect the overall security posture of the organization.
6. Lack of Expertise: Implementing and managing SIEM, SOAR, and UEBA solutions requires specialized skills and knowledge. A lack of expertise can lead to poor system performance, incorrect configuration, or other problems.
7. Overreliance on Technology: SIEM, SOAR, and UEBA solutions are tools that require human expertise to be effective. Overreliance on technology can lead to a false sense of security and leave the organization vulnerable to threats that are not detected by the system.

To mitigate these risks, it is important to establish a robust security program that includes regular testing and validation of the SIEM, SOAR, and UEBA solutions. It is also essential to have trained personnel with the appropriate skills and knowledge to manage and operate the system effectively. Finally, it is important to monitor the system continuously to ensure that it is functioning correctly and meeting the defined requirements.

9.10.12 Why can't any vendor commit resolution time/ SLA accurately?

Accurately providing a resolution time commitment in cybersecurity is challenging for several reasons:

1. Complexity of security incidents: Cybersecurity incidents can range from simple malware infections to complex, multi-faceted attacks that are difficult to fully understand and resolve. This makes it difficult to accurately predict the amount of time it will take to resolve a given incident.
2. Evolving threats: The nature of cyber threats is constantly evolving, with new and more sophisticated attacks appearing all the time. This means that even experienced cybersecurity teams may encounter new and unexpected challenges when attempting to resolve an incident, which can make it difficult to provide accurate resolution time commitments.
3. Interdependencies: Many cybersecurity incidents involve multiple systems and technologies and resolving one issue may require resolving multiple underlying issues. This can make it difficult to accurately predict the amount of time it will take to fully resolve an incident.
4. Limited information: In many cases, the information available about a cybersecurity incident may be limited or incomplete, making it difficult to accurately assess the scope of the issue and predict the amount of time it will take to resolve.

Given these challenges, it is not always possible to accurately provide a resolution time commitment in cybersecurity. Instead, cybersecurity teams may aim to provide a range of possible resolution times, or a commitment to resolve the incident as quickly as possible, while ensuring that all necessary steps are taken to thoroughly resolve the issue and prevent future incidents.

9.11 Delivery cue- Managed Security Services operations

9.11.1 Daily Activities of an L1 Security Engineer

The daily activities of an L1 (Level 1) Security Engineer can vary depending on the specific organization and the size and complexity of the IT environment. However, some common activities include:

1. Monitoring security alerts: An L1 Security Engineer is responsible for monitoring various security systems, such as firewalls, intrusion detection systems, and anti-virus software, for alerts and potential threats.
2. Responding to security incidents: When a security incident occurs, the L1 Security Engineer is typically the first responder, responsible for triaging the incident, determining the extent of the problem, and taking appropriate action to contain and resolve the issue.
3. Performing security scans: An L1 Security Engineer may run regular security scans to identify vulnerabilities in the network and systems and take steps to remediate those vulnerabilities.

4. Performing security audits: The L1 Security Engineer may also be responsible for performing security audits of systems, applications, and network configurations to ensure they follow security policies and standards.
5. Keeping systems updated: Keeping systems and software up to date is a critical aspect of security. The L1 Security Engineer is responsible for ensuring that all systems and software are patched and updated to the latest version.
6. Documenting and reporting: An L1 Security Engineer must keep detailed records of all security incidents, including the cause, resolution, and any preventive measures taken. They are also responsible for preparing regular security reports for management and other stakeholders.
7. Collaborating with other teams: The L1 Security Engineer may also collaborate with other IT teams, such as system administrators, network engineers, and developers, to ensure that security best practices are followed, and that security is integrated into all aspects of the IT environment.

These are some of the common activities performed by an L1 Security Engineer. The specific tasks and responsibilities may vary based on the organization, but the main goal is always to protect the organization's information and systems from security threats.

9.11.2 Daily Activities of an L2 Security Engineer

The daily activities of a Level 2 (L2) Security Engineer are typically more advanced and complex than those of a Level 1 (L1) Security Engineer. In addition to the tasks performed by L1 Security Engineers, L2 Security Engineers may be responsible for:

1. Investigating and resolving complex security incidents: L2 Security Engineers are responsible for investigating and resolving complex security incidents that require a higher level of technical expertise. This may involve analysing log files, network traffic, and other technical data to determine the root cause of the incident and to develop an appropriate response plan.
2. Designing and implementing security solutions: L2 Security Engineers may be involved in the design and implementation of new security solutions, such as firewalls, intrusion detection systems, and data encryption technologies. They may also be involved in the configuration and deployment of these solutions.
3. Developing and maintaining security policies: L2 Security Engineers are responsible for developing, updating, and maintaining security policies and procedures. This includes conducting regular security reviews, conducting risk assessments, and working with other teams to ensure that security policies are effectively implemented and followed.
4. Mentoring and training L1 Security Engineers: L2 Security Engineers may also be involved in mentoring and training L1 Security Engineers, providing guidance and support on complex security issues, and helping to develop their technical skills.
5. Collaborating with other security teams: L2 Security Engineers may work with other security teams, such as threat intelligence teams, incident response teams, and security operations centres, to coordinate and share information about security threats and incidents.

6. Staying current with the latest security technologies and techniques: L2 Security Engineers must stay current with the latest security technologies and techniques in order to effectively defend against emerging threats. This may involve attending training courses, participating in online communities, and conducting independent research.

These are some of the common activities performed by a Level 2 (L2) Security Engineer. The specific tasks and responsibilities may vary based on the organization, but the main goal is always to protect the organization's information and systems from security threats.

9.11.3 Daily Activities of an L3 Security Engineer

The daily activities of a Level 3 (L3) Security Engineer are typically more advanced and strategic in nature compared to those of a Level 1 (L1) and Level 2 (L2) Security Engineer. In addition to the tasks performed by L1 and L2 Security Engineers, L3 Security Engineers may be responsible for:

1. Designing and implementing security architecture: L3 Security Engineers are often responsible for designing and implementing the overall security architecture for an organization. This includes designing and implementing security solutions, such as firewalls, intrusion detection systems, and data encryption technologies.
2. Developing and implementing security strategies: L3 Security Engineers are responsible for developing and implementing security strategies that align with the overall business goals and objectives of the organization. This may involve conducting risk assessments, developing incident response plans, and implementing security awareness training programs.
3. Collaborating with senior management: L3 Security Engineers are often the primary point of contact between the security team and senior management. They are responsible for communicating security risks, recommendations, and incidents to senior management, and for ensuring that the organization's security posture aligns with the overall business strategy.
4. Responding to security incidents: L3 Security Engineers are involved in responding to complex security incidents, such as data breaches and cyber-attacks. This may involve leading a cross-functional incident response team, coordinating with law enforcement, and communicating with stakeholders.
5. Staying current with the latest security technologies and techniques: L3 Security Engineers must stay current with the latest security technologies and techniques in order to effectively defend against emerging threats. This may involve attending training courses, participating in online communities, and conducting independent research.
6. Mentoring and managing L1 and L2 Security Engineers: L3 Security Engineers may also be involved in mentoring and managing L1 and L2 Security Engineers, providing guidance and support on complex security issues, and helping to develop their technical skills.

These are some of the common activities performed by a Level 3 (L3) Security Engineer. The specific tasks and responsibilities may vary based on the organization, but the main goal is always to protect the organization's information and systems from security threats.

9.11.4 What are daily activities of Security Threat Hunter?

The daily activities of a Security Threat Hunter may vary depending on the specific organization, but in general, a Security Threat Hunter is responsible for proactively searching for and identifying potential security threats to the organization's systems and networks. Some common daily activities include:

1. Analysing log data and network traffic: Security Threat Hunters use various tools to analyse log data and network traffic, looking for anomalies and signs of potential security threats. This may include using security information and event management (SIEM) systems, intrusion detection systems (IDS), and security orchestration, automation, and response (SOAR) platforms.
2. Conducting threat research: Security Threat Hunters regularly conduct research to stay current with the latest security threats, attack methods, and malware families. They may also work with threat intelligence providers to obtain information about emerging threats.
3. Collaborating with other security teams: Security Threat Hunters often work closely with other security teams, such as incident response teams, vulnerability management teams, and threat intelligence teams. They collaborate on security incidents and share information about potential threats.
4. Developing and refining threat hunting techniques: Security Threat Hunters are responsible for developing and refining the techniques and processes used to identify potential security threats. They may also develop custom scripts, algorithms, and queries to automate parts of the threat hunting process.
5. Responding to security incidents: When a potential security threat is identified, Security Threat Hunters may be involved in the initial stages of responding to the incident. This may include gathering additional information, determining the extent of the threat, and coordinating with other security teams to develop a response plan.
6. Reporting on findings: Security Threat Hunters are responsible for documenting their findings and providing regular reports to senior management. This includes providing recommendations for improving the organization's security posture, as well as reporting on the effectiveness of current security measures.

These are some of the common activities performed by a Security Threat Hunter. The specific tasks and responsibilities may vary based on the organization, but the main goal is always to proactively identify and respond to security threats before they can cause harm to the organization.

9.11.5 Daily Managed Security Services Activities

The daily managed security services activities can vary depending on the specific security services being provided by the managed security services provider (MSSP). However, here are some common activities that are typically performed by MSSPs:

1. Log Monitoring: The MSSP will monitor logs from security devices such as firewalls, intrusion detection/prevention systems, and other security devices for any security events or alerts.
2. Incident Response: The MSSP will investigate and respond to security events or incidents that are detected and escalate to the client as needed.
3. Vulnerability Management: The MSSP will perform vulnerability scans and assessments to identify vulnerabilities in the client's infrastructure and provide recommendations for remediation.
4. Threat Intelligence: The MSSP will monitor threat intelligence sources to identify emerging threats and provide threat intelligence reports to the client.
5. Patch Management: The MSSP will assist with the management of patching and updates for security devices and systems.
6. Configuration Management: The MSSP will assist with the management of security device configurations to ensure they are properly configured to provide maximum security.
7. Policy Management: The MSSP will assist with the development and management of security policies, ensuring they are aligned with industry best practices and regulatory requirements.
8. Reporting: The MSSP will provide regular reporting to the client on security events, incident response, vulnerability assessments, and other security-related activities.
9. Security Awareness Training: The MSSP may provide security awareness training to the client's employees, helping to reduce the risk of security incidents caused by human error.

These activities can help ensure that the client's infrastructure is secure and can help reduce the risk of security incidents that can impact the business. It is important to work closely with the MSSP to ensure that the security services provided align with the specific needs of the organization.

9.11.6 Weekly Managed Security Services Activities

The weekly managed security services activities can vary depending on the specific security services being provided by the managed security services provider (MSSP). However, here are some common activities that are typically performed by MSSPs on a weekly basis:

1. Vulnerability Assessment and Remediation: The MSSP will perform a vulnerability assessment to identify any new vulnerabilities in the client's infrastructure that have been discovered since the last assessment. The MSSP will then assist the client with remediation efforts to address any identified vulnerabilities.
2. Security Policy Review: The MSSP will review the client's security policies to ensure that they are up-to-date and aligned with industry best practices and regulatory requirements. Any necessary updates or changes to policies will be recommended.
3. Security Awareness Training: The MSSP may provide weekly security awareness training to the client's employees to help reduce the risk of security incidents caused by human error.

4. System and Device Configuration Management: The MSSP will review the configuration of security devices and systems to ensure that they are properly configured to provide maximum security. Any necessary changes to configurations will be recommended.
5. Network Traffic Analysis: The MSSP will perform a review of network traffic logs to identify any anomalies or suspicious activity that may indicate a security incident.
6. Review of Incident Response and Escalation Procedures: The MSSP will review the client's incident response and escalation procedures to ensure that they are up-to-date and aligned with industry best practices.
7. Security Operations Centre (SOC) Review: The MSSP will review the performance of the SOC, including the effectiveness of the security devices and systems being used, as well as the performance of the SOC staff.

These activities can help ensure that the client's infrastructure remains secure and can help reduce the risk of security incidents that can impact the business. It is important to work closely with the MSSP to ensure that the security services provided align with the specific needs of the organization.

9.11.7 Monthly Managed Security Services Activities

The monthly managed security services activities can vary depending on the specific security services being provided by the managed security services provider (MSSP). However, here are some common activities that are typically performed by MSSPs on a monthly basis:

1. Firewall Rule Review: The MSSP will review the firewall rules to ensure that they are properly configured and aligned with the client's security policies.
2. Patch Management: The MSSP will review and manage patching of servers, applications, and other devices in the client's environment to address known vulnerabilities.
3. Log Retention and Archiving: The MSSP will review and manage retention policies for log data in compliance with regulatory requirements.
4. Network Access Controls: The MSSP will review and manage network access controls to ensure only authorized individuals have access to sensitive resources.
5. Threat Intelligence Review: The MSSP will review threat intelligence feeds and other sources of security threat information to identify emerging threats.
6. User Behaviour Analytics: The MSSP will review user behaviour data to identify any unusual patterns that may indicate a security incident.
7. Disaster Recovery and Business Continuity Planning: The MSSP will review the client's disaster recovery and business continuity plans to ensure they are up-to-date and aligned with industry best practices.

These activities can help ensure that the client's infrastructure remains secure and can help reduce the risk of security incidents that can impact the business. It is important to work

closely with the MSSP to ensure that the security services provided align with the specific needs of the organization.

9.11.8 Managed Security Services Reports

Here are some common types of managed security services reports:

1. Security Operations Centre (SOC) Reports: These reports provide an overview of the activities that have been conducted by the SOC team, including incident investigations, threat intelligence analysis, and vulnerability assessments.
2. Threat and Vulnerability Management Reports: These reports provide an overview of the threats and vulnerabilities that have been identified in the client's environment, including details about the severity of the risks and recommendations for remediation.
3. Compliance and Audit Reports: These reports provide an overview of the client's compliance posture, including any areas of non-compliance and recommendations for remediation. They may also include information about audit findings and recommendations.
4. Incident Response Reports: These reports provide an overview of security incidents that have been identified and the response actions that have been taken to remediate the incident.
5. User Behaviour Analytics Reports: These reports provide an overview of user activity and any unusual patterns that may indicate a security incident or risk.
6. Security Risk Assessment Reports: These reports provide an overview of the risks that the client faces in their environment, including details about the likelihood and impact of different types of security incidents.
7. Executive Summary Reports: These reports provide a high-level overview of the security posture of the organization and are typically presented to executives and other high-level stakeholders. They may include information about trends in security incidents, key risk areas, and recommendations for improvement.

These reports can help organizations stay informed about their security posture, identify areas of risk, and make informed decisions about their security strategy. It is important to work with your managed security services provider to ensure that the reports provided align with the specific needs of your organization.

9.11.9 Governance of Managed Security Services solution

The governance of a Managed Security Services (MSS) solution is critical to ensure that the security services provided are aligned with the needs of the organization, and that the MSS provider is meeting their obligations under the service agreement. Here are some key elements of governance for an MSS solution:

1. Service Level Agreements (SLAs): The SLAs define the scope of the services provided by the MSS provider and the performance metrics that will be used to measure the

effectiveness of the services. They should be reviewed and updated regularly to ensure they remain aligned with the organization's needs.

2. Performance Monitoring: The organization should regularly monitor the performance of the MSS provider to ensure they are meeting their obligations under the SLAs. This can include reviewing reports, conducting periodic audits, and reviewing feedback from end-users.
3. Risk Management: The MSS solution should be subject to the same risk management processes as other areas of the organization's IT infrastructure. This includes conducting risk assessments, implementing appropriate controls, and regularly reviewing and updating security policies and procedures.
4. Incident Management: The organization should have a well-defined incident management process in place that includes procedures for reporting, investigating, and responding to security incidents. This process should be aligned with the MSS provider's incident management processes.
5. Change Management: The organization should have a well-defined change management process in place that includes procedures for reviewing and approving changes to the MSS solution. This process should be aligned with the MSS provider's change management processes.
6. Contract Management: The organization should have a well-defined contract management process in place that includes procedures for reviewing and updating the service agreement with the MSS provider. This process should be aligned with the organization's procurement and vendor management processes.

Effective governance of an MSS solution can help ensure that the organization's security needs are met, that the MSS provider is meeting their obligations, and that risks are appropriately managed. It is important to work closely with the MSS provider to ensure that the governance framework is appropriate for the specific needs of the organization.

9.12 Delivery cure- List of incident response playbooks SOC maintains

A Security Operations Centre (SOC) should maintain a number of incident response playbooks to ensure effective and efficient responses to various security incidents. Some of the playbooks that a SOC should maintain are:

1. Ransomware Response Playbook: A playbook that outlines the steps to be taken in the event of a ransomware attack.
2. Data Breach Response Playbook: A playbook that outlines the steps to be taken in the event of a data breach.
3. Distributed Denial of Service (DDoS) Response Playbook: A playbook that outlines the steps to be taken in the event of a DDoS attack.
4. Phishing Attack Response Playbook: A playbook that outlines the steps to be taken in the event of a phishing attack.
5. Advanced Persistent Threat (APT) Response Playbook: A playbook that outlines the steps to be taken in the event of an APT attack.

6. Malware Response Playbook: A playbook that outlines the steps to be taken in the event of a malware attack.
7. Insider Threat Response Playbook: A playbook that outlines the steps to be taken in the event of an insider threat.
8. Network Intrusion Response Playbook: A playbook that outlines the steps to be taken in the event of a network intrusion.
9. Third-Party Risk Management Response Playbook: A playbook that outlines the steps to be taken in the event of a risk associated with a third-party vendor.
10. Incident Communication and Coordination Playbook: A playbook that outlines the steps to be taken in communicating and coordinating with internal stakeholders and external partners during an incident.

These are some of the playbooks that a SOC maintains to ensure effective and efficient responses to various security incidents. The playbooks should be reviewed and updated regularly to ensure they are current and effective.

9.12.1 Ransomware response playbook

A ransomware response playbook is a set of guidelines that outlines the steps to be taken in the event of a ransomware attack. The following is a general outline of a ransomware response playbook:

1. Initial Response: The first step is to quickly assess the situation and determine the extent of the ransomware attack. This includes determining the affected systems and the type of ransomware involved.
2. Containment: The next step is to contain the attack to prevent it from spreading further. This may involve disconnecting infected systems from the network, shutting down access to shared resources, and disabling network shares.
3. Backup and Recovery: Once the attack has been contained, the next step is to restore the affected systems from a recent backup. If a backup is not available, the affected systems may need to be restored from a fresh install.
4. Investigation: A thorough investigation of the attack should be conducted to determine the cause of the infection and the scope of the damage. This may include reviewing system logs, examining the ransomware payload, and interviewing relevant personnel.
5. Notification: Organizations should inform relevant stakeholders, such as law enforcement agencies and incident response teams, of the attack.
6. Remediation: Once the investigation has been completed, it is important to implement measures to prevent similar attacks from happening in the future. This may involve applying security patches, updating software, and changing security configurations.
7. Communication: Regular communication should be maintained with stakeholders throughout the response process to keep them informed of the progress and resolution of the attack.

This is a general outline of a ransomware response playbook. The specific steps and procedures may vary depending on the specific requirements of the organization, but the goal is always to respond quickly and effectively to minimize the impact of a ransomware attack.

9.12.2 Data Breach Response Playbook

A data breach response playbook is a document that outlines the steps an organization should take in the event of a data breach. The following is a general outline of a data breach response playbook:

1. Initial Response: The first step in responding to a data breach is to initiate the incident response plan and assemble the incident response team. This may involve activating an incident response hotline or email address and notifying key stakeholders, such as the CEO, legal counsel, and the public relations department.
2. Assessment: The next step is to assess the scope and impact of the data breach. This may involve reviewing system and network logs, interviewing employees, and assessing the data that has been compromised.
3. Containment: The next step is to contain the breach to prevent further damage. This may involve shutting down systems, disconnecting affected devices from the network, or disabling access to affected data.
4. Investigation: The next step is to conduct a thorough investigation to determine the cause of the breach and identify any additional systems or data that may have been impacted.
5. Remediation: The next step is to remediate any vulnerabilities that were exploited during the breach. This may involve patching systems, changing passwords, and implementing additional security controls.
6. Notification: The next step is to determine if notification is required, and if so, who needs to be notified. This may involve notifying affected individuals, regulatory agencies, and the media.
7. Incident Reporting: The final step is to document the incident and create an incident report. This report should include details about the scope and impact of the breach, as well as recommendations for future mitigation and prevention efforts.

It's important to note that this is just a general outline, and that each data breach incident may require different steps and response activities. The specific steps taken will depend on the scope and impact of the breach, as well as the specific details of the organization's network, systems, and data. Additionally, legal requirements for data breach notification may vary from country to country, so it's important to be familiar with the relevant laws and regulations in your jurisdiction.

9.12.3 Distributed Denial of Service (DDoS) Response Playbook

A Distributed Denial of Service (DDoS) response playbook is a document that outlines the steps an organization should take in the event of a DDoS attack. The following is a general outline of a DDoS response playbook:

1. Initial Response: The first step in responding to a DDoS attack is to initiate the incident response plan and assemble the incident response team. This may involve activating an incident response hotline or email address and notifying key stakeholders, such as the CEO, legal counsel, and the public relations department.
2. Monitoring: The next step is to monitor network and system logs to identify the source and scope of the DDoS attack. This may involve using intrusion detection systems, firewalls, and other security tools to monitor network traffic.
3. Containment: The next step is to contain the attack to prevent further damage. This may involve filtering out malicious traffic, diverting traffic to other servers, or blocking incoming traffic from specific IP addresses.
4. Analysis: The next step is to analyse the attack traffic to determine the type and source of the attack. This may involve reviewing log files, network traffic data, and other sources of information to determine the specifics of the attack.
5. Mitigation: The next step is to implement mitigation strategies to counteract the attack. This may involve using DDoS protection services, filtering traffic at the network level, or using traffic shaping techniques.
6. Post-Attack Review: The final step is to conduct a post-attack review to determine what worked and what didn't, and to identify areas for improvement in the future. This may involve analysing network logs, incident response reports, and other sources of information to determine what can be done to prevent similar attacks in the future.

It's important to note that this is just a general outline, and that each DDoS attack incident may require different steps and response activities. The specific steps taken will depend on the type and severity of the attack, as well as the specific details of the organization's network and systems. Additionally, the response strategies that are most effective for countering DDoS attacks can vary depending on the specifics of the attack and the capabilities of the organization's network and security infrastructure.

9.12.4 Phishing Attack Response Playbook

A Phishing Attack Response Playbook is a document that outlines the steps an organization should take in the event of a phishing attack. The following is a general outline of a Phishing Attack Response Playbook:

1. Initial Response: The first step in responding to a phishing attack is to initiate the incident response plan and assemble the incident response team. This may involve activating an incident response hotline or email address and notifying key stakeholders, such as the CEO, legal counsel, and the public relations department.
2. Verification: The next step is to verify that a phishing attack has actually taken place. This may involve reviewing email headers, examining the structure of the phishing email, or checking the authenticity of links contained in the email.
3. Containment: The next step is to contain the attack to prevent further damage. This may involve disabling access to the phishing email, resetting passwords for affected users, or taking other measures to prevent unauthorized access to sensitive information.

4. Analysis: The next step is to analyse the phishing email to determine the type and source of the attack. This may involve reviewing log files, email headers, and other sources of information to determine the specifics of the attack.
5. Notification: The next step is to notify affected individuals or organizations. This may involve sending notifications to users who have been targeted by the phishing email, or alerting stakeholders who may be at risk of being targeted in the future.
6. Remediation: The next step is to remediate the issue and address any vulnerabilities that may have contributed to the phishing attack. This may involve updating software, implementing stronger authentication measures, or providing additional security training for employees.
7. Post-Attack Review: The final step is to conduct a post-attack review to determine what worked and what didn't, and to identify areas for improvement in the future. This may involve analysing log files, incident response reports, and other sources of information to determine what can be done to prevent similar attacks in the future.

It's important to note that this is just a general outline and that each phishing attack incident may require different steps and response activities. The specific steps taken will depend on the type and severity of the attack, as well as the specific details of the organization's network and systems. Additionally, the response strategies that are most effective for countering phishing attacks can vary depending on the specifics of the attack and the capabilities of the organization's security infrastructure.

9.12.5 Advanced Persistent Threat (APT) Response Playbook

An Advanced Persistent Threat (APT) Response Playbook is a detailed set of procedures that outlines the steps an organization should take when responding to an APT attack. The goal of an APT Response Playbook is to help organizations effectively and efficiently respond to APT attacks, minimize damage, and restore normal operations as quickly as possible. The following are the steps that are typically included in an APT Response Playbook:

1. Preparation: Establishing an incident response team, developing a communications plan, and conducting regular tabletop exercises to test the response plan.
2. Detection: Monitoring network activity and logging all events to detect any signs of an APT attack.
3. Containment: Isolating the infected systems and networks to prevent the spread of the attack.
4. Analysis: Identifying the scope of the attack, determining the source and the methods used by the attacker, and determining what data may have been stolen or compromised.
5. Remediation: Removing the malware and patching any vulnerabilities that were exploited in the attack.
6. Recovery: Restoring normal operations, including restoring any data that was lost or compromised during the attack.
7. Review and Lessons Learned: Evaluating the response plan, documenting what worked well and what can be improved for future incidents.

It's important to note that this is just a general outline and each organization's APT Response Playbook should be tailored to its specific needs and requirements. Additionally, it's important for organizations to regularly review and update their playbooks to stay current with the evolving threat landscape.

9.12.6 Malware Response Playbook

A Malware Response Playbook is a detailed set of procedures that outlines the steps an organization should take when responding to a malware attack. The goal of a Malware Response Playbook is to help organizations effectively and efficiently respond to malware attacks, minimize damage, and restore normal operations as quickly as possible. The following are the steps that are typically included in a Malware Response Playbook:

1. Preparation: Establishing an incident response team, developing a communications plan, and conducting regular tabletop exercises to test the response plan.
2. Detection: Monitoring network activity and logging all events to detect any signs of a malware attack.
3. Containment: Isolating the infected systems and networks to prevent the spread of the malware.
4. Analysis: Identifying the scope of the attack, determining the source and methods used by the attacker, and determining what data may have been stolen or compromised.
5. Remediation: Removing the malware and patching any vulnerabilities that were exploited in the attack.
6. Recovery: Restoring normal operations, including restoring any data that was lost or compromised during the attack.
7. Review and Lessons Learned: Evaluating the response plan, documenting what worked well and what can be improved for future incidents.

It's important to note that this is just a general outline and each organization's Malware Response Playbook should be tailored to its specific needs and requirements. Additionally, it's important for organizations to regularly review and update their playbooks to stay current with the evolving threat landscape.

9.12.7 Insider Threat Response Playbook

An Insider Threat Response Playbook is a set of procedures and guidelines for responding to security incidents caused by insiders, such as employees, contractors, or third-party vendors. The goal of an Insider Threat Response Playbook is to help organizations quickly identify, contain, and mitigate the impact of insider threat incidents, while also protecting the rights and privacy of the affected individuals. The following are the steps that are typically included in an Insider Threat Response Playbook:

1. Preparation: Establishing an incident response team, developing a communications plan, and conducting regular tabletop exercises to test the response plan.

2. Detection: Monitoring employee behaviour and system activity, and establishing processes for reporting suspicious activity.
3. Containment: Limiting the scope of the incident and preventing further damage by isolating systems, revoking access, and disabling accounts.
4. Analysis: Gathering and preserving evidence, identifying the scope of the attack, and determining the motive and methods used by the insider.
5. Remediation: Removing the threat, repairing any damage, and restoring normal operations.
6. Recovery: Restoring normal operations and any data that was lost or compromised during the attack.
7. Review and Lessons Learned: Evaluating the response plan, documenting what worked well and what can be improved for future incidents.

It's important to note that this is just a general outline and each organization's Insider Threat Response Playbook should be tailored to its specific needs and requirements. Additionally, it's important for organizations to regularly review and update their playbooks to stay current with the evolving threat landscape.

9.12.8 Network Intrusion Response Playbook

A Network Intrusion Response Playbook is a set of procedures and guidelines for responding to security incidents that involve unauthorized access to an organization's network. The goal of a Network Intrusion Response Playbook is to help organizations quickly identify, contain, and mitigate the impact of network intrusions, while also protecting sensitive information and systems. The following are the steps that are typically included in a Network Intrusion Response Playbook:

1. Preparation: Establishing an incident response team, developing a communications plan, and conducting regular tabletop exercises to test the response plan.
2. Detection: Monitoring network activity and establishing processes for reporting suspicious activity.
3. Containment: Limiting the scope of the incident and preventing further damage by isolating systems, revoking access, and disabling accounts.
4. Analysis: Gathering and preserving evidence, identifying the scope of the attack, and determining the methods used by the attacker.
5. Remediation: Removing the threat, repairing any damage, and restoring normal operations.
6. Recovery: Restoring normal operations and any data that was lost or compromised during the attack.
7. Review and Lessons Learned: Evaluating the response plan, documenting what worked well and what can be improved for future incidents.

It's important to note that this is just a general outline and each organization's Network Intrusion Response Playbook should be tailored to its specific needs and requirements.

Additionally, it's important for organizations to regularly review and update their playbooks to stay current with the evolving threat landscape.

9.12.9 Third-Party Risk Management Response Playbook

A Third-Party Risk Management Response Playbook is a set of procedures and guidelines for responding to security incidents that involve third-party vendors or partners. The goal of a Third-Party Risk Management Response Playbook is to help organizations quickly identify and respond to risks associated with third-party relationships, while also protecting sensitive information and systems. The following are the steps that are typically included in a Third-Party Risk Management Response Playbook:

1. Preparation: Developing a third-party risk management program, establishing a relationship with third-party vendors, and conducting regular risk assessments.
2. Identification: Monitoring the security posture of third-party vendors and identifying any potential risks.
3. Response: Responding to incidents or breaches, including containment, investigation, and remediation.
4. Recovery: Restoring normal operations and any data that was lost or compromised during the incident.
5. Review and Lessons Learned: Evaluating the response plan, documenting what worked well and what can be improved for future incidents and implementing any necessary changes to the third-party risk management program.

It's important to note that this is just a general outline and each organization's Third-Party Risk Management Response Playbook should be tailored to its specific needs and requirements. Additionally, it's important for organizations to regularly review and update their playbooks to stay current with the evolving threat landscape and to ensure the security of their third-party relationships.

9.12.10 Incident Communication and Coordination Playbook

An Incident Communication and Coordination Playbook is a set of procedures and guidelines for communicating and coordinating during a security incident. The goal of an Incident Communication and Coordination Playbook is to ensure that all stakeholders, both internal and external, are informed and aware of the incident and are able to work together effectively to resolve it. The following are the steps that are typically included in an Incident Communication and Coordination Playbook:

7. Preparation: Defining roles and responsibilities, establishing communication channels, and conducting regular drills and tabletop exercises.
8. Activation: Determining when an incident is considered an emergency and activating the incident response team.
9. Notification and Escalation: Notifying the relevant stakeholders and escalating the incident to the appropriate level of management.
10. Coordination: Coordinating with internal and external stakeholders, including law enforcement, regulatory agencies, and other organizations.

11. Communication: Providing regular updates to stakeholders and managing the flow of information during the incident.
12. Closure: Wrapping up the incident, documenting what worked well and what can be improved for future incidents and communicating the final outcome to stakeholders.

It's important to note that this is just a general outline and each organization's Incident Communication, and Coordination Playbook should be tailored to its specific needs and requirements. Additionally, it's important for organizations to regularly review and update their playbooks to ensure that their incident response plan remains effective and up to date.

========== **END**==========

About the authors

As a CISO and Head, Cybersecurity, Sudhansu M Nayak specialises and spearheads enterprise cybersecurity (IT/ OT), cloud, and data transformation solutions. He advises CxOs and Executive Boards on cyber risks and techno-operational mitigation, data privacy and protection, and compliance and governance.

As an avid consultant to multiple think-tanks, he contributes to building of various components of national cybersecurity policies. His research and views have been cited in Centre for Land Warfare Studies (CLAWS), The Cyber Defense Review, (Army Cyber Institute, Australia), DQChannels, TechPanda, and others.

To bridge the cybersecurity skill-gaps, he mentors, corporates, students, and startups. A passionate speaker, he talks on Cybersecurity and its engagement in international policies and digital transformation. His current research is focussed on the interplay of cybersecurity with global peace, state espionage, climate change, international trade, and strategic diplomacy.

In his free time, Sudhansu writes on Indian temples, experiments on indo-continental dishes, and dabbles in photography.

Twitter: @smnayak

LinkedIn: https://www.linkedin.com/in/sudhansunayak/

OpenAI is an artificial intelligence research organization founded in 2015 by a group of prominent technology leaders, including Elon Musk, Sam Altman, Greg Brockman, and others. OpenAI's mission is to develop and promote friendly AI for the betterment of humanity, while also considering and addressing potential risks and challenges posed by artificial intelligence. OpenAI conducts research in a variety of fields related to AI, including deep learning, reinforcement learning, natural language processing, robotics, and more. It also develops and releases software tools and platforms for machine learning and AI development, including the popular deep learning framework TensorFlow. OpenAI has made significant contributions to the field of AI, and its work has been widely recognized and awarded.