

**INCIDENT
RESPONSE
PLAYBOOKS
AND
WORKFLOWS**

IR Playbooks

This repository contains all the Incident Response Playbooks and Workflows of Company's SOC. Each folder contains a Playbook that is broken down into 6 sections as per [NIST - 800.61 r2](#)

1- Preparation

This section should include the following information:

- List of *ALL* Assets
 - Servers
 - Endpoints (+critical ones)
 - Networks
 - Applications
 - Employees
 - Security Products
- Baselines
- Communication Plan
- Which Security Events
- Thresholds
- How to access Security Tools
 - How to provision access
- Create Playbooks
- Plan Exercises
 - Table Top
 - Hands On

2- Detection and Analysis

This section should include the following information:

- Gathering of Information
- Analyzing the Data
- Building Detections
- Root Cause Analysis
- Depth and Breadth of the Attack
 - Admin Rights
 - Affected Systems
- Techniques Used
- Indicators of Compromise / Indicators of Attack
 - Tactics Techniques and Procedures (TTP)
 - IP Address
 - Email Address
 - File Hash
 - Command Line
 - etc.

3- Containment, Eradication, and Recovery

This section should include the following information:

- Isolate Affected Systems
- Patch Threat Entry Point
- Predefine threshold
 - For Customers
 - For internal systems
 - For escalations
- Preauthorized actions
 - Per customers
 - Per environment
 - Prod
 - QA
 - Internet Facing
- How to Remove the Threat on All Affected Systems
- Get Systems Operational
- Rebuilt and Resume Service

4- Post-Incident Activity

- Lessons Learned
- New Detection
- New Hardening
- New Patch Management
- etc.

Account Compromised Playbook

- [Account Compromised Playbook](#)
 - [Scope](#)
 - [1. Preparation](#)
 - [Train Employees](#)
 - [Tool Access and Provisioning](#)
 - [Tool1](#)
 - [Tool2](#)
 - [Assets List](#)
 - [2. Detect](#)
 - [Workflow](#)
 - [Identify Threat Indicators](#)
 - [Alerts](#)
 - [Notifications](#)
 - [Identify Risks Factors](#)
 - [Common](#)
 - [Company Specific](#)
 - [Data Colletion](#)
 - [Categorize](#)
 - [Triage](#)
 - [3. Analyze](#)
 - [Workflow](#)
 - [AA1. Verify](#)
 - [AA2. List Compromised Credentials](#)
 - [AA3. Level of Access / Priviledges](#)
 - [Update Scope](#)
 - [Scope Validation](#)
 - [4. Contain / Eradicate](#)
 - [Workflow](#)
 - [Block](#)
 - [Validate User's Actions](#)
 - [Malware Infection?](#)
 - [Close Monitoring](#)
 - [All Affected Endpoints Contained?](#)
 - [New IOC Discovered?](#)
 - [5. Recover](#)
 - [Workflow](#)
 - [Update Defenses](#)
 - [All Affected Endpoints Recovered?](#)
 - [Validate Countermeasures](#)
 - [6. Post Incident](#)

- [Workflow](#)
- [Incident Review](#)
- [Update Mode of Operations](#)
- [Review Defensive Posture](#)
- [User Awareness Training](#)
- [References](#)

Scope

This Playbook covers the steps to take when accounts are compromised.
Of course, we also need to remediate the hosts where those accounts were used.

1. Preparation

▼ Expand/Colapse

- Create and maintain a list of
 - all domains owned by Company.
 - This can prevent you from taking actions against our own domains
 - all people of can register domains
- Create email templates
 - to notify all employees of ongoing phishing campaing against the organization
 - to contact hosting companies for domain(s) take down
 - to inform 3rd party to take actions against phishing on there infra (Microsoft, Fedex, Apple, etc.)
- Ensure that:
 - Mail anti-malware/anti-spam/anti-phish solutions are in place.
 - Users know how to report phish
 - Detection exists for office documents spawning processes
 - PowerShell
 - CMD
 - WMI
 - MSHTA
 - Etc.
- Perform Firedrill to ensure all aspects of the Playbook are working
 - After publication
 - At least once a year
 - Test/Validate:
 - [Customer's Cards](#)
 - Internal Contact and Escalation Paths
- Review threat intelligence for
 - threats to the organisation,
 - brands and the sector,
 - common patterns
 - newly developing risks and vulnerabilities
- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following
 - IR Playbooks
 - Network Architecture Diagram
 - Dataflow
- Identify and obtain the services of a 3rd party Cyber Forensic provider.
- Define Threat and Risk Indicators and Alerting pattern within the organisation's security information and event management (SIEM) solution.

Train Employees

- Conduct regular awareness campaigns to highlight information security risks faced by employees, including:
 - Phishing attacks and malicious emails;
 - Ransomware;
 - Reporting a suspected cyber incident.

Tool Access and Provisioning

Tool1

Please referer to [Tool1 Documentation](#)

Tool2

Please referer to [Tool2 Documentation](#)

Assets List

- A list of assets and owner should exists and be available for the following
 - Customers Assets
 - Owners
 - Contacts
 - Pre authorized actions
 - Company Assets (Including all filiale and business units)
 - Onwers
 - Contacts
 - Administrators
 - Pre authorized actions
- Type of assets inventory needed
 - Endpoints
 - Servers
 - Network Equipements
 - Security Appliances
 - Network Ranges
 - Public
 - Private
 - VPN / Out of Band
 - Employees
 - Partners
 - Clients

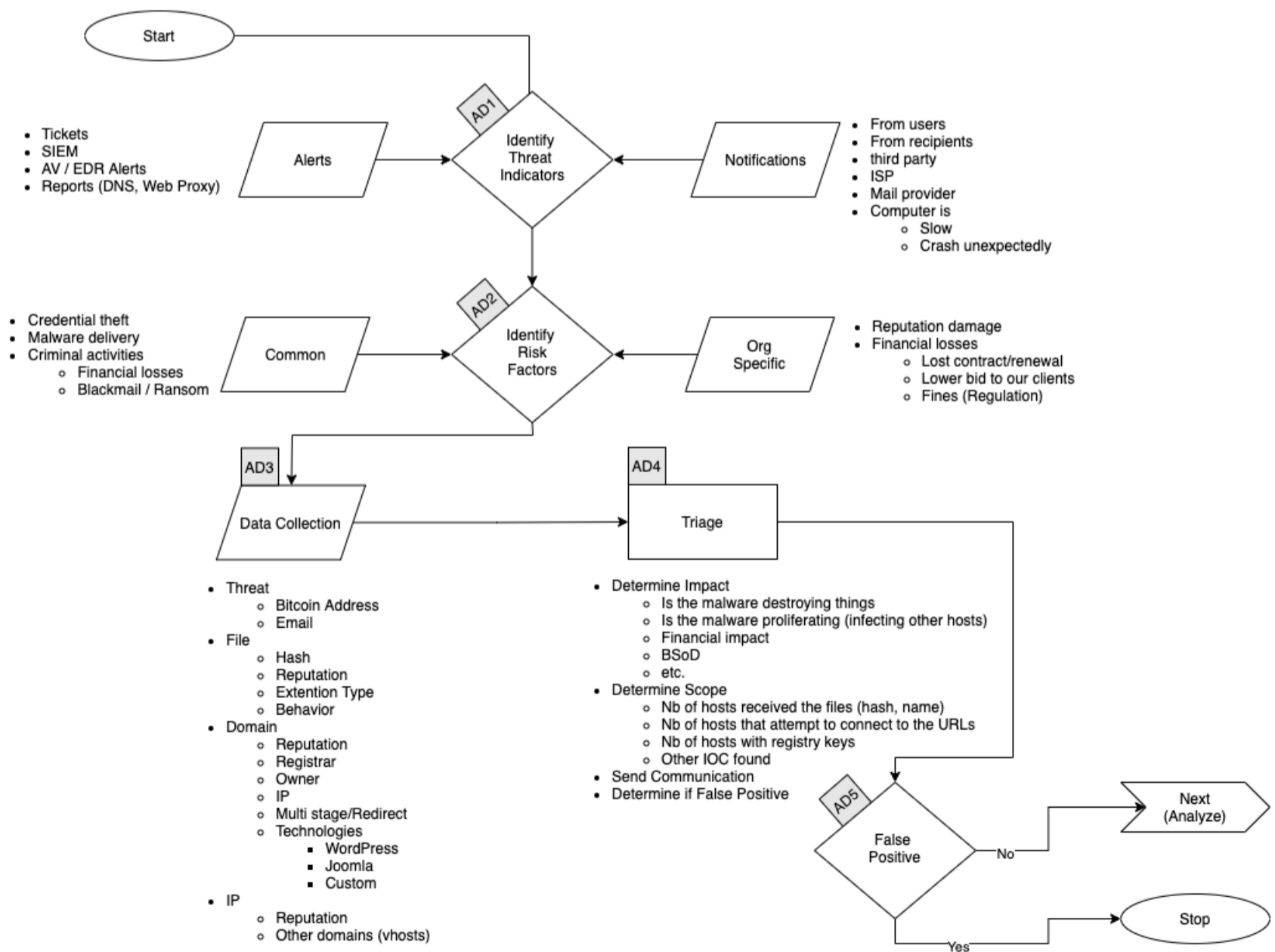
2. Detect

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Account Compromised - Detect



Identify Threat Indicators

▼ Expand/Colapse

Alerts

Alerts are generated by different systems owned by the Security/SOC team. The main sources for alerts are

- Tickets
- SIEM
- Anti-Virus / EDR
- Reports
 - DNS
 - Web Proxy
- Errors from mail servers

Notifications

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- Users (internal)
- Recipients of emails (external)
- Third Parties
- ISP
- Mail Providers

Identify Risks Factors

▼ Expand/Collapse

Common

- Credential Theft
- Malware Delivery
- Criminal Activities
 - Blackmail / Ransom

Company Specific

- Financial Losses
 - Lost of contract
 - Contract not renewed
 - Lower bid to our clients
 - Fines
 - Regulation

Data Collection

This section describes the information that should be collected and documented about the incident. There are a lot of resources to help you with that phase [here](#)

▼ Expand/Collapse

Domains

- Reputation
- Registrar
- Owner
- IP
- Multistage / Redirect
- Technologies of the site
 - WordPress
 - Joomla
 - Custom Page (credential phishing)

IP

- Reputation
- Owner
- Geo Localisation
- Other domains on that IP

Categorize

▼ Expand/Collapse

Determine type of

Triage

▼ Expand/Collapse

Determine

- Impact
 - Of
 - Financial
 - Data loss
- Scope (Nb of people)

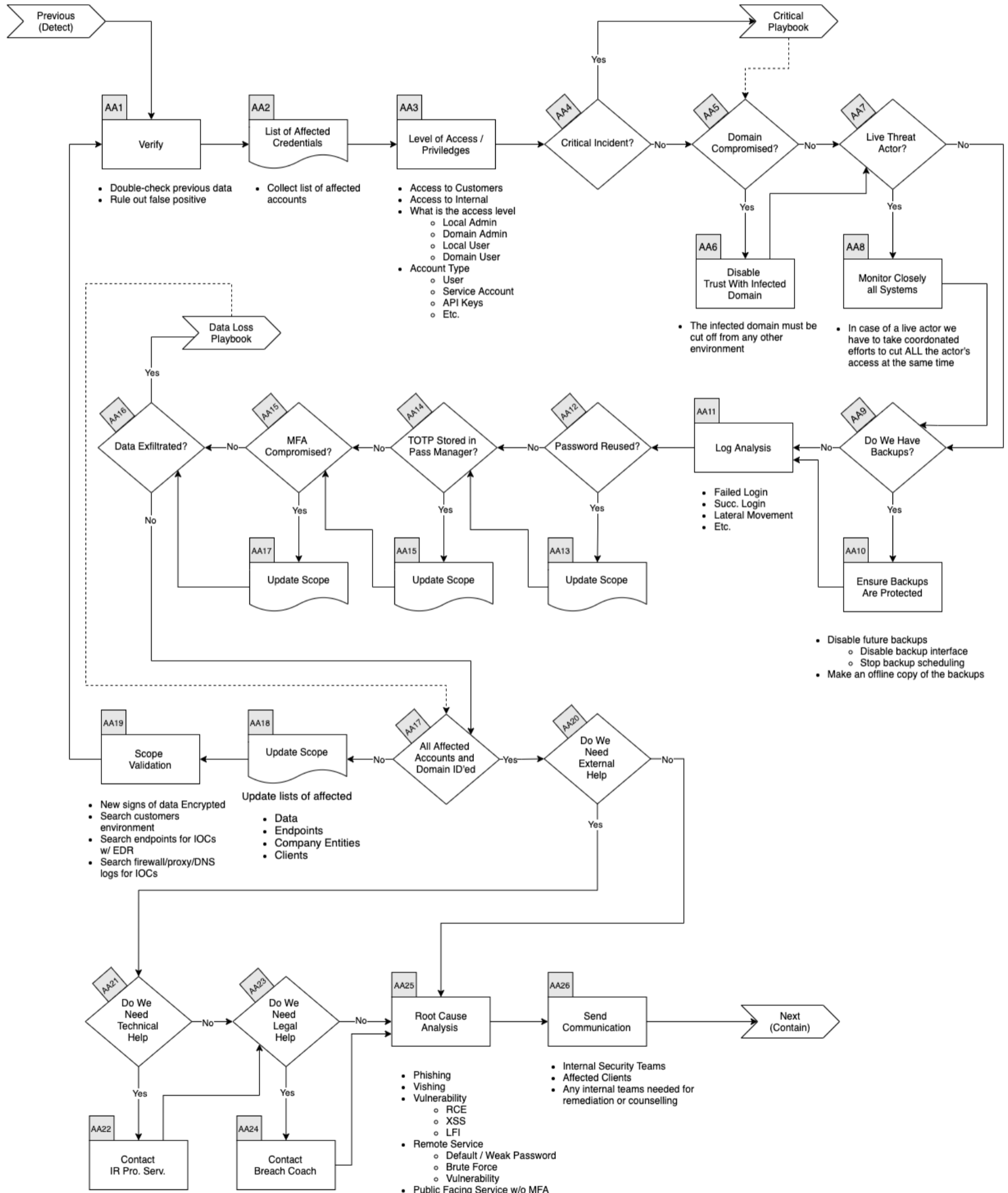
3. Analyze

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Account Compromised - Analyze



AA1. Verify

▼ Expand/Colapse

In conjunction with a senior member of the SOC

- Double check previous data
- Rule out False Positive

AA2. List Compromised Credentials

▼ Expand/Colapse

In the Compromised Assets TAB of the Event Log list:

- Compromised accounts
- Compromised machines
- Compromised domains

AA3. Level of Access / Priviledges

▼ Expand/Colapse

In conjunction with a senior member of the SOC

- Double check previous data
- Rule out False Positive

Update Scope

▼ Expand/Colapse

- Update lists of
 - affected endpoints
 - affected Company Entities
 - affected clients

Scope Validation

▼ Expand/Colapse

Have all the machines been identified? If you find futher traces of phishing or new IOCs go back through this step.

When you are done identifying all compromised:

- Hosts

And investigated all:

- URLs
- Domains
- IP
- Ports
- Files
- Hash

Go to the next phase <Contain/Eradicate>

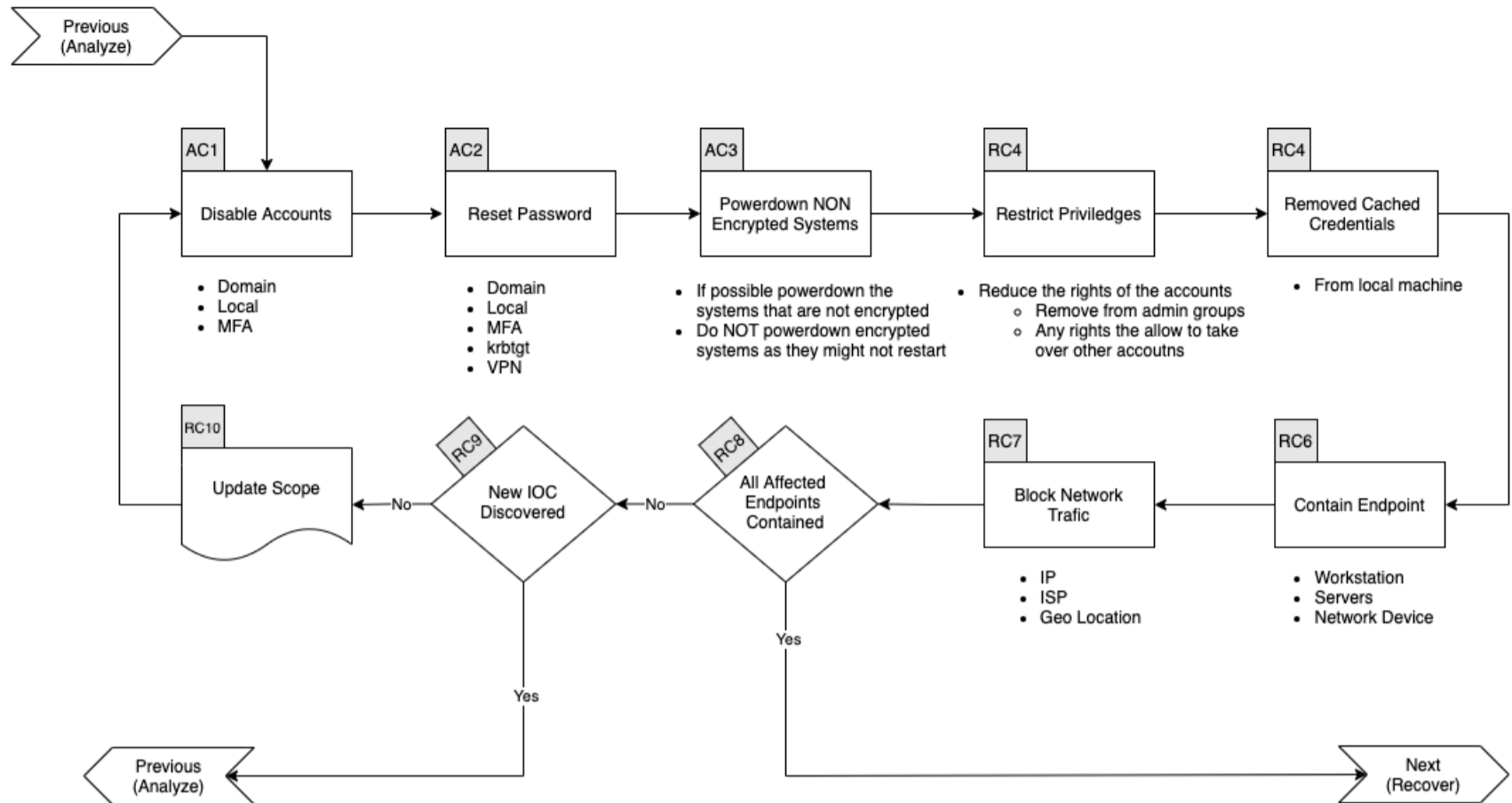
4. Contain / Eradicate

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Account Compromised - Contain / Eradicate



Block

▼ Expand/Colapse

- Update FW, Proxy, etc. rules
- Blackhole DNS
- Submit to Partners
 - AV/EDR Vendor
 - Web Filter Vendor
 - etc.

Validate User's Actions

▼ Expand/Colapse

Malware Infection?

▼ Expand/Colapse

If there was malicious attachments that were opened we need to assume the endpoint(s) was/were infected by a malware. Please continue to the [Malware Playbook](#)

Close Monitoring

▼ Expand/Colapse

- Monitor for
 - Related incoming messages
 - Internet connections to IOC
 - New files that matches hashes identified

All Affected Endpoints Contained?

▼ Expand/Colapse

If all affected endpoints have been contained, you can go to the next phase, otherwise continue bellow.

New IOC Discovered?

▼ Expand/Colapse

If there was new IOC discovered, go back to the [Analyze Phase](#)

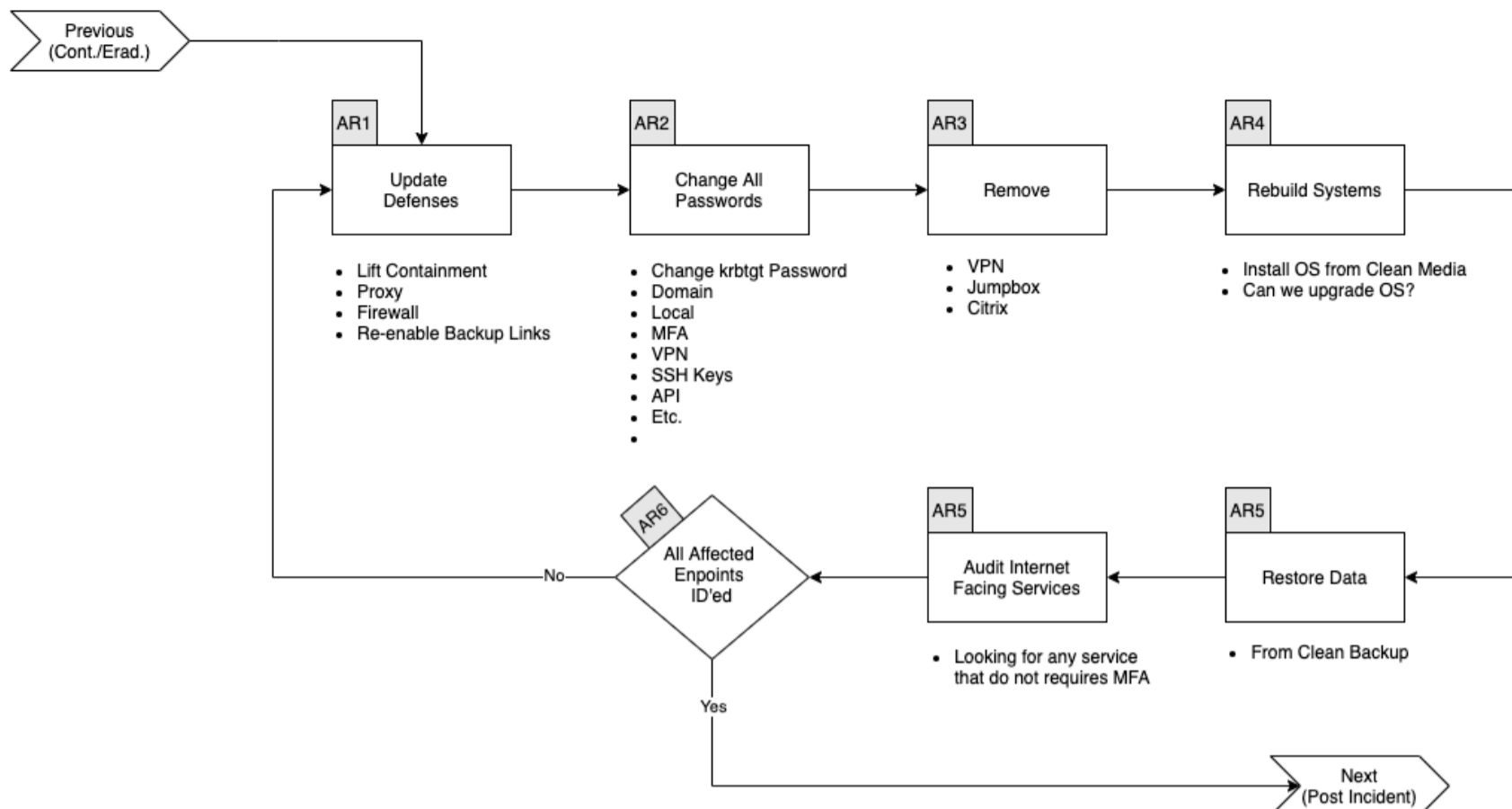
5. Recover

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Account Compromised - Recover



Update Defenses

▼ Expand/Colapse

Determine which of the following rules needs to be removed and which needs to stay in the following list:

- Firewall Rules
- EDR
 - ban hashes
 - ban domains
 - Containment
- Proxy Block

All Affected Endpoints Recovered?

▼ Expand/Colapse

If all affected endpoints have been contained, you can go to the next phase, otherwise continue bellow.

Validate Countermeasures

▼ Expand/Colapse

Determine if legitimate elements are blocked by:

- Proxy
- Firewall
- EDR

If so, go back to [Update Defenses](#) Otherwise go to the next phase

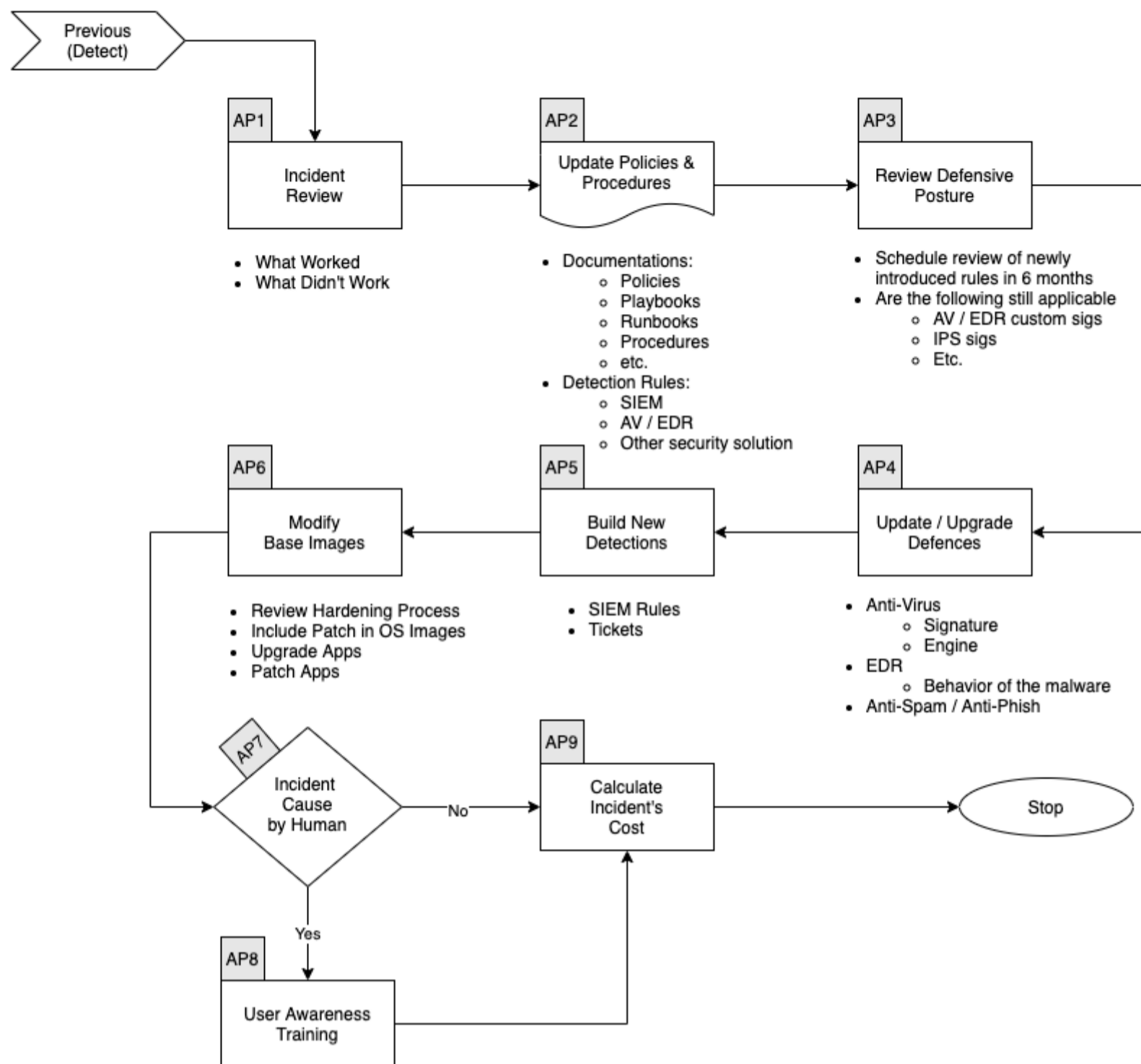
6. Post Incident

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

AccountCompromised - Post Incident



Incident Review

- ▼ Expand/Colapse
 - What worked
 - What didn't work

Update Mode of Operations

- ▼ Expand/Colapse
 - Update the following documents as required:

- Policies
- Processes
- Procedures
- Playbooks
- Runbooks

Update Detetion Rules in:

- SIEM
- Anti-Spam
- Malware Gataway
- EDR
- Other security solution

Review Defensive Posture

- ▼ Expand/Colapse
 - Schedule review of newly introduced rules in6 months
 - Are the following still applicatble
 - Firewall Rules
 - Proxy Rules for C2
 - AV / EDR custom Signatures
 - IPS Signatures

Critical Incident Playbook

Here are the steps to take when an incident is deemed critical.

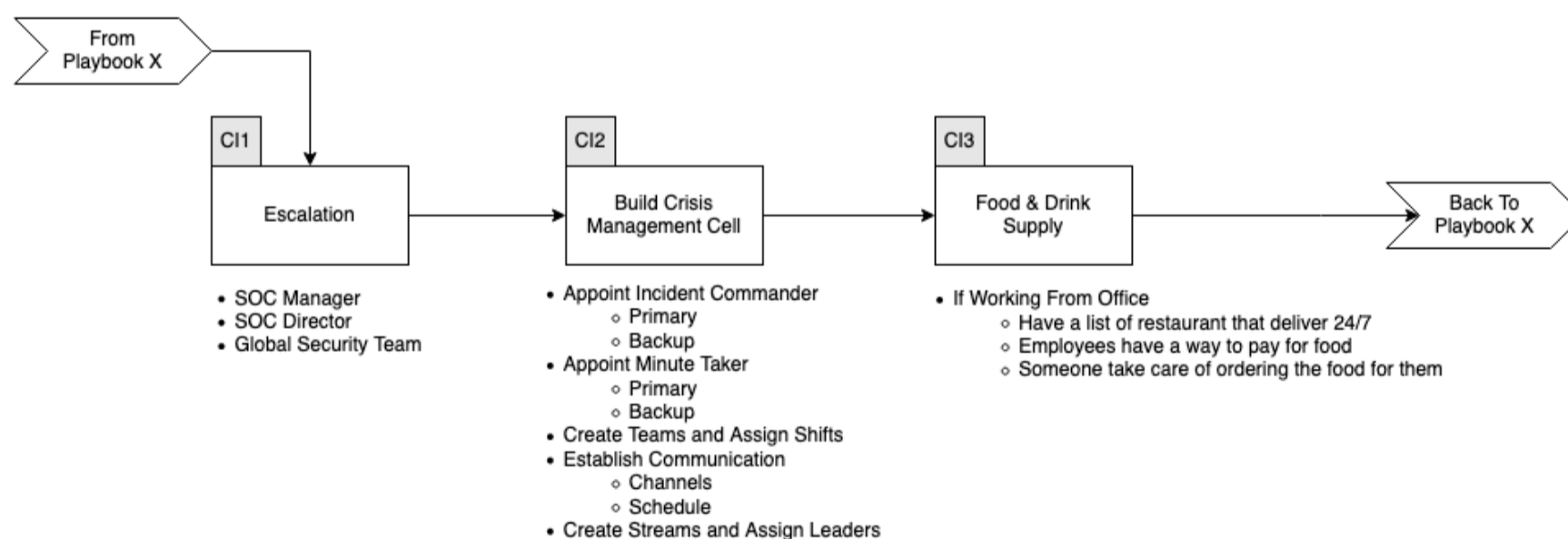
The fact that the incident is critical doesn't mean the Playbook can/should be ignored. It just means that every steps needs to occur faster, that more people will be working on the incident and that an Incident Commander will be appointed.

- [Critical Incident Playbook](#)
 - [Workflow](#)
 - [CI1 - Build a Crisis Management Cell](#)
 - [CI2 - Food & Drink Supply](#)
 - [CI3 - Define Communication Schedule](#)
 - [CI4 - Return to the Playbook](#)

Workflow

▼ Expand/Colapse

Critical Incident



CI1 - Build a Crisis Management Cell

▼ Expand/Colapse

The SOC Manager and Director will

- Appoint an Incident Commander and a backup
 - Responsible to call the shots
 - Ensuring the Playbooks are followed
 - No steps are forgotten
 - Steps are taken in the right order
 - This doesn't mean many steps cannot be taken simultaneously
 - Chain of Custody is maintain

- There's always someone taking notes
- Key person to gather all information
- Can authorize actions
 - Disconnect MPLS
 - Shutdown services/computer
- Can authorize spending
 - Equipement
 - VM
 - GCP
 - AWS
 - Digital Ocean
 - Software
- Appoint an "minute taker" and a backup
- Create
 - Alpha Team
 - Beta Team
 - Charlie Team
- Establish communication schedule
 - Stream Report
 - C Level communication
 - etc.

The goal of these teams is to

- Have people around the clock working on the incident
- Allow people to rest
- Have period of time for pass over
 - At least 1 hour (2 preferred)
 - Both Teams are working together
 - All updates are given

Each of the teams need to

- Have Stream Leads
 - Log review Stream
 - Depth and Breath of the attack
 - Vulnerability Assessment
 - To try and identify root cause
 - See if any other systems have the same Vulnerability
 - Forensics Stream
 - Understand what happened on the host(s)
 - Malware analysis
 - Identify IOC
 - Feed the Log Stream
 - Host Stream
 - Deploy security solution
 - Update security solution
 - Build new server
 - Install apps
 - Restore data
 - etc.
 - Dark Web / Social Media monitoring Stream (optional)
 - Is there any chatter about the breach
 - Is the data for sale
 - Is the data posted somewhere

CI2 - Food & Drink Supply

If working from the office we need to know how we will feed our staff.
 Someone will need to have a list of restaurants that deliver 24/7 to our locations.
 We don't want our team to eat fried chicken or pizza 3 times a day.

CI3 - Define Communication Schedule

During a critical incident information sharing is critical.
 We need to ensure everyone knows where and when to report information.

Define the following

- Who will attend each calls
- What platform will be used to communicate
- Technical call to sync information between the Streams
- C-Level information call
- Customers information call

CI4 - Return to the Playbook

Once the roles and teams have been formed, send the team that will take over away so they can rest and be ready to take over.
Finally return to the original(s) Playbook(s)

Good luck!

Data Loss Playbook

- [Data Loss Playbook](#)
 - [Scope](#)
 - [1. Preparation](#)
 - [Tool Access and Provisioning](#)
 - [Tool1](#)
 - [Tool2](#)
 - [Assets List](#)
 - [2. Detect](#)
 - [Workflow](#)
 - [DD1. Identify Threat Indicators](#)
 - [Alerts](#)
 - [Notifications](#)
 - [DD2. Indentify Risks Factors](#)
 - [Common](#)
 - [Company Specific](#)
 - [DD3. Data Colletion](#)
 - [DD4. Categorize](#)
 - [DD5. Is it Ransomware ?](#)
 - [DD6. Triage](#)
 - [3. Analyze](#)
 - [Workflow](#)
 - [DA1. Verify](#)
 - [DA2. Critical Incident](#)
 - [DA3. Identify IOCs](#)
 - [DA4. Malware](#)
 - [DA5. What Was Accessed](#)
 - [DA6. Update Scope](#)
 - [DA8. Scope Validation](#)
 - [DA9. External Help](#)
 - [DA11. Technical Help](#)
 - [DA12. Legal Help](#)
 - [DA14. Root Cause Analysis](#)
 - [DA15. Send Communication](#)
 - [4. Contain / Eradicate](#)
 - [Workflow](#)
 - [DC1. Compromised Credentials](#)
 - [DC3. Compromised or Lost MFA](#)
 - [DC5. Customer Data](#)
 - [DC7. Data Posted to the Internet](#)
 - [DC9. Insider Threat](#)
 - [DC11. Attacker Still Have Access?](#)
 - [DC12. Close Monitoring](#)

- [DC13. All Affected Data Lost Addressed?](#)
- [DC14. New Data Lost Discovered?](#)
- [5. Recover](#)
 - [Workflow](#)
 - [DR1. Rebuilt Systems](#)
 - [DR2. Vulnerability Scan](#)
 - [DR3. Update Defenses](#)
 - [DR4. Restore Service](#)
 - [DR5. All Affected Endpoints Restored?](#)
- [6. Post Incident](#)
 - [Workflow](#)
 - [DP1. Incident Review](#)
 - [DP2. Update Mode of Operations](#)
 - [DP3. Review Defensive Posture](#)
 - [DP4. Build New Detection](#)
 - [DP5. Modify Base Images](#)
 - [DP7. User Awareness Training](#)
 - [DP8. Calculate Incident's Cost](#)
- [References](#)

Scope

This Playbook covers the steps to take in case of Data Loss / Data Breach.

1. Preparation

▼ Expand/Colapse

- Create and maintain a list of
 - all domains owned by Company.
 - This can prevent you from taking actions against our own domains
 - all people of can register domains
- Create email template
 - to notify all employees of ongoing phishing campaing against the organization
 - to contact hosting companies for domain take down
 - to inform 3rd party to take actions against phishing on there infra (Microsoft, Fedex, Apple, etc.)
- Ensure that:
 - Mail anti-malware/anti-spam/anti-phish solutions are in place.
 - Users know how to report phish
 - Detection exists for office documents spawning processes
 - PowerShell
 - CMD
 - WMI
 - MSHTA
 - Etc.
- Perform Firedrill to ensure all aspects of the Playbook are working
 - After publication
 - At least once a year
 - Test/Validate:
 - [Customer's Cards](#)
 - Internal Contact and Escalation Paths
- Review threat intelligence for
 - threats to the organisation,
 - brands and the sector,
 - common patterns
 - newly developing risks and vulnerabilities
- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following
 - IR Playbgns to highlight information security risks faced by employees, including:
 - Phishing attacks and malicious emails;
 - Ransomware;
 - Reporting a suspected cyber incident.

Tool Access and Provisioning

Tool1

Please referer to [Tool1 Documentation](#)

Tool2

Assets List

- A list of assets and owner should exists and be available for the following
 - Customers Assets
 - Owners
 - Contacts
 - Pre authorized actions
 - Company Assets (Including all filiale and business units)
 - Owners
 - Contacts
 - Administrators
 - Pre authorized actions
- Type of assets inventory needed
 - Endpoints
 - Servers
 - Network Equipements
 - Security Appliances
 - Network Ranges
 - Public
 - Private
 - VPN / Out of Band
 - Employees
 - Partners
 - Clients

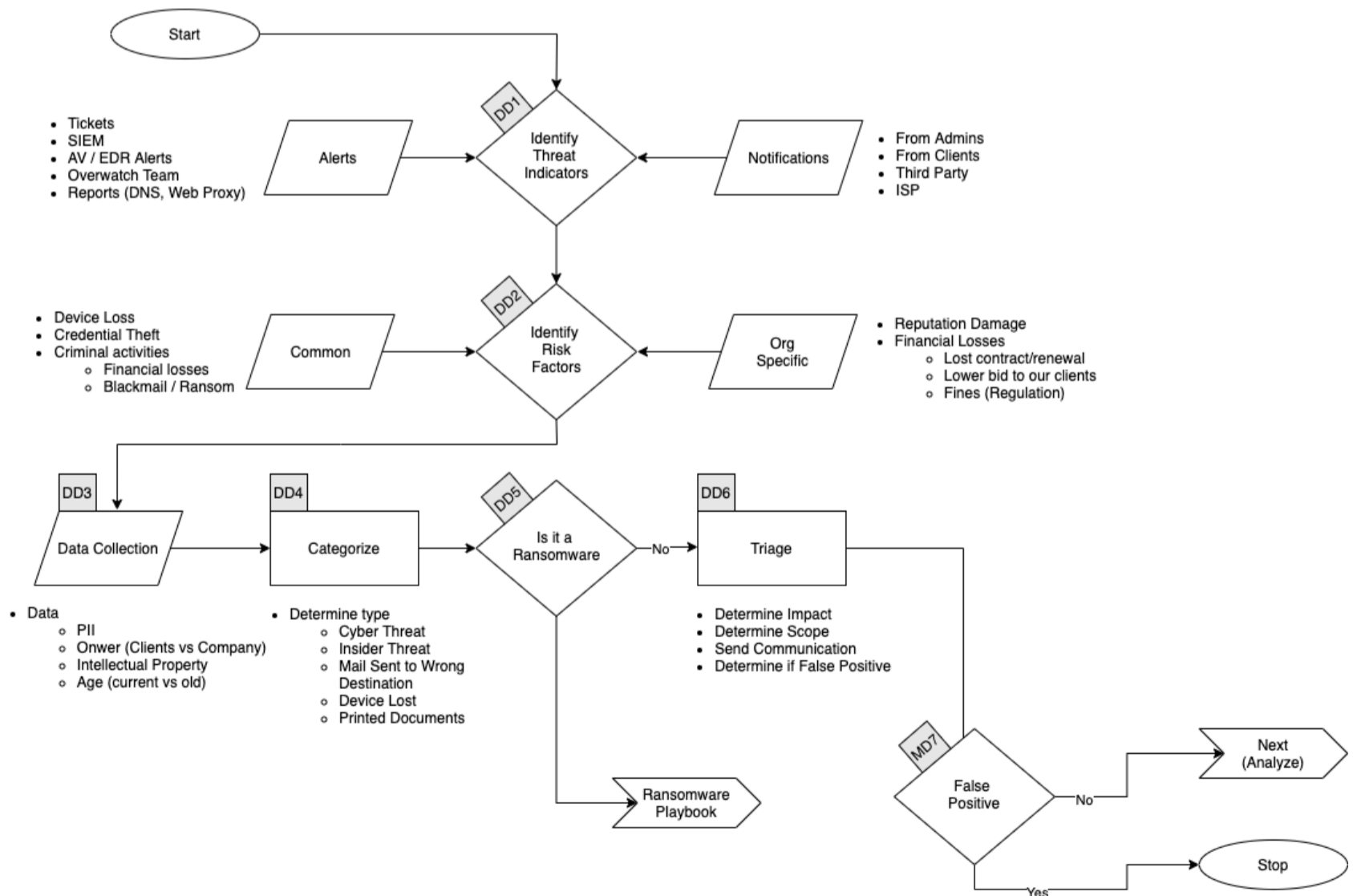
2. Detect

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

DataLoss - Detect



DD1. Identify Threat Indicators

▼ Expand/Colapse

Alerts

Alerts are be generated by differents systems owned by the Security/SOC team. The main sources for alerts are

- Tickets
- SIEM
- Anti-Virus / EDR
- Reports
 - DNS
 - Web Proxy

Notifications

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- System Administrators
- Clients
- Third Parties
- ISP

DD2. Identify Risks Factors

▼ Expand/Collapse

Common

- Credential Theft
- Device Loss
 - Laptop
 - Phone
- Criminal Activities
 - Blackmail / Ransom

Company Specific

- Reputation Damage
- Financial Losses
 - Lost of contract
 - Contract not renewed
 - Lower bid to our clients
 - Fines
 - Regulation

DD3. Data Collection

This section describe the information that should be collected and documented about the incident
There is a lot of resources to help you with that phase [here](#)

▼ Expand/Collapse

Type Data

- Personally identifiable information (PII)
- Intellectual Property
- Age of the Data
 - Current
 - Old
- Owner of the Data
 - Company
 - Clients

DD4. Categorize

▼ Expand/Collapse

Determine type of Data Loss we are dealing with.

- Cyber Threat
- Insider Threat
- Mail Sent to Wrong Destination
- Device Lost
 - Laptop
 - Phone
- Printed Documents

DD5. Is it Ransomware ?

If the Data Loss is caused by a Ransomware please refer to the [Ransomware Playbook](#)

DD6. Triage

▼ Expand/Colapse

- Determine Impact
- Determine Scope
 - Number of Documents / Records
 - Number of Clients
 - Number of Company Entities
 - Number of Individuals
- Send Communication
- Determine if False Positive

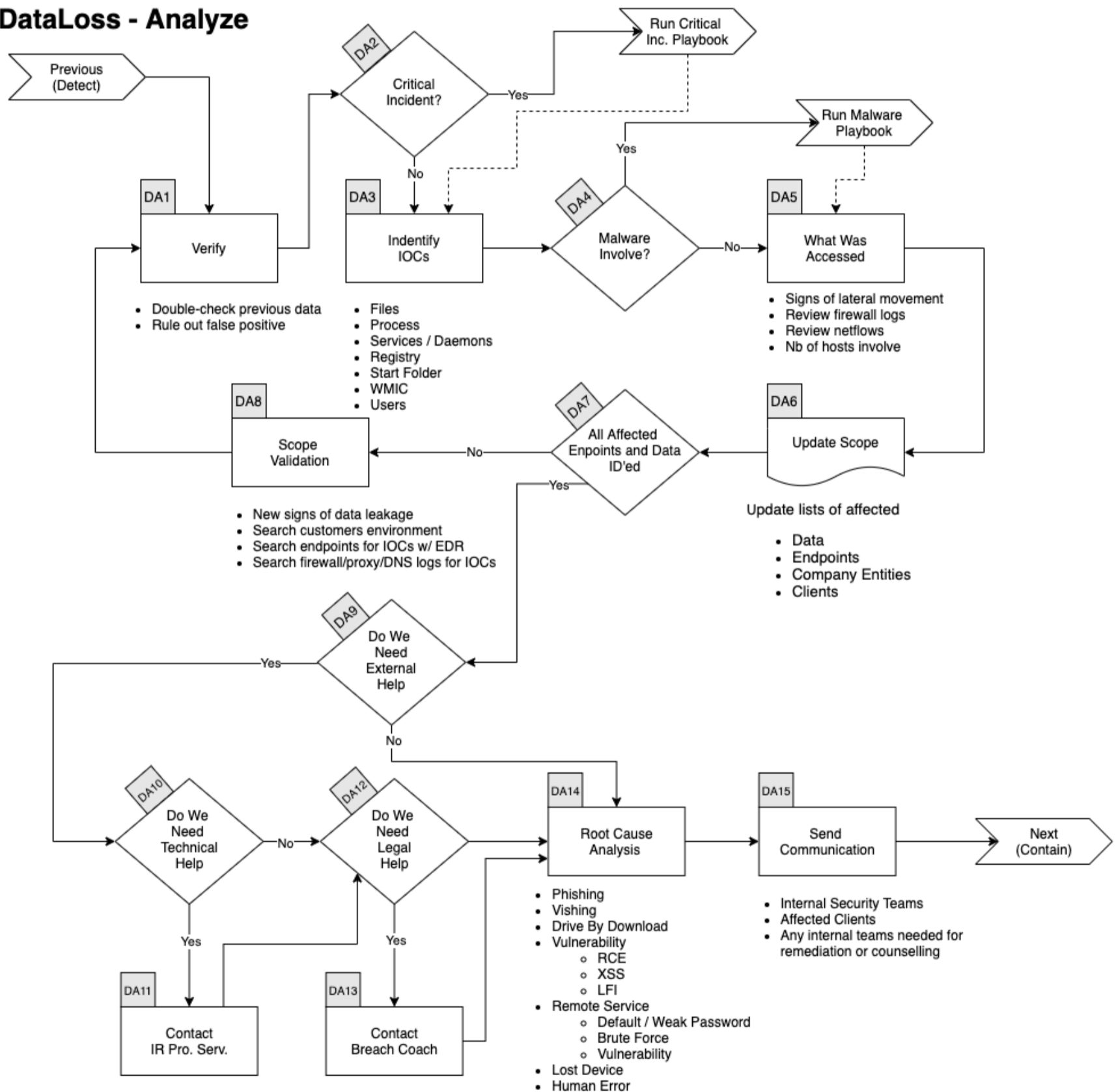
3. Analyze

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

DataLoss - Analyze



DA1. Verify

▼ Expand/Colapse

In conjunction with a senior member of the SOC

- Double check previous data
- Rule Out False Positive

DA2. Critical Incident

If this incident is deemed **Major or Critical** by the senior analyst go to the [Critical Incident Playbook](#)

DA3. Identify IOCs

▼ Expand/Colapse

- Data
 - All Files Lost
 - Records Stolen
 - MFA Token
 - Credentials
 - PII
- Validate hashes
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
- Validate links
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [URLScan](#)
- ID other addresses, domains, IPs
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [Talos Intelligence](#)
- Search Threat Intel sources
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [Talos Intelligence](#)
- Disk forensics on recipient's endpoint

DA4. Malware

If **Malware** was involve in the incident refer to the [Malware Playbook](#)

DA5. What Was Accessed

▼ Expand/Colapse

Did the attack touched other systems?

Look for:

- Signs of Lateral Movement
- Review Firewall Logs
- Review Netflows
- Assess the Number of Hosts Involved
- Number of Clients Affected
 - Perform the same research for all affected clients

DA6. Update Scope

▼ Expand/Colapse

- Update lists of affected
 - Data
 - Endpoints
 - Company Entities
 - Clients

DA8. Scope Validation

▼ Expand/Colapse

Have all the machines and data been identified? If you find futher traces of phishing or new IOCs go back to [Verify Step](#).

When you are done identifying all :

- Data that was Lost
- Affected Endpoints
- Affected Company Entities
- Affected Customers

And if applicable investigated all:

- URLs
- Domains
- IP
- Ports
- Files
- Hash

You can proceed with the next steps.

DA9. External Help

Does Company have all the knowledge and resources to handle the crisis alone?

DA11. Technical Help

If the Incident Commander feels we need Technical help or resources to handle the incident he can reach out to our Incident Response Partner.

We have a retainer with the following company and we can reach them at : xxxx@yyy.com or 555-555-5555

DA12. Legal Help

If there are Legal implication such as

- GDPR
- Criminal Charges
- Regulation
- Laws

DA14. Root Cause Analysis

▼ Expand/Colapse

Identify how this incident happened.

- Phishing Emails
- Voice Phishing
- Drive-by Download
- Vulnerability
 - Remote Code Execution
 - Cross-Site Scripting
- Remote Services
 - Default / Weak Password
 - Brute Force
 - Vulnerability
- Lost Device
- Human Error

DA15. Send Communication

▼ Expand/Colapse

Contact any relevant of the following party

- Internal Security Team
- Affected Clients
- Any internal teams needed for remediation or counselling

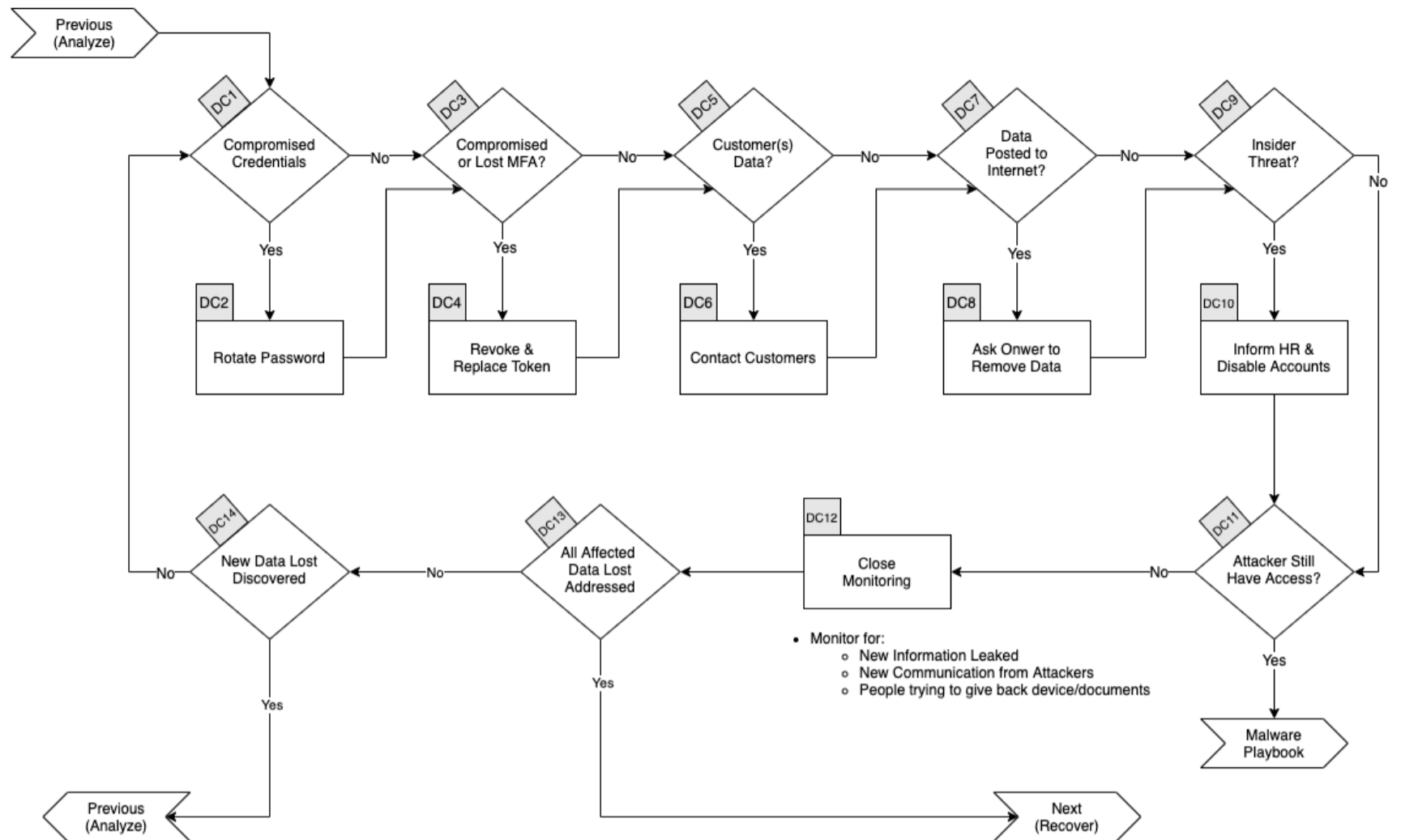
4. Contain / Eradicate

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

DataLoss - Contain / Eradicate



DC1. Compromised Credentials

▼ Expand/Colapse

If any credentials are suspected to have been accessed, stolen or used they will all need to be changed. This applies to:

- Local Passwords
- Network Passwords
- Remote Passwords
- Etc.

DC3. Compromised or Lost MFA

▼ Expand/Colapse

If any Multi Factor Authentication token/code were accessed, stolen or used they will all need to be

- Revoke
- Replace.

DC5. Customer Data

▼ Expand/Colapse

If any if customer data was accessed or leaked we will need to send communication to all affected clients using the approved [Customer Communication Template](#).

DC7. Data Posted to the Internet

▼ Expand/Colapse

If the site is controlled by a public company, we can ask them to remove the information. Usually writing at abuse@company.com is a good place to start.

DC9. Insider Threat

▼ Expand/Colapse

If the information was intentionally leaked/sold by an employee, we need to:

- Contact HR
- Disable User Account
- Disable any MFA token

We will potentially need to send physical security to the employee's desk to seize his/her laptop and other devices.

DC11. Attacker Still Have Access?

If there is any sign of the attacker still being in the network, go to the [Malware Playbook](#)

DC12. Close Monitoring

▼ Expand/Colapse

- Monitor for
 - New information leaked
 - New communication from Attackers
 - People trying to give back device(s)/document(s)

DC13. All Affected Data Lost Addressed?

▼ Expand/Colapse

If all affected data have been addressed, you can go to the [Recover phase](#), otherwise continue below.

DC14. New Data Lost Discovered?

▼ Expand/Colapse

If there was new leaked data/devices discovered, go back to the [Analyze Phase](#)

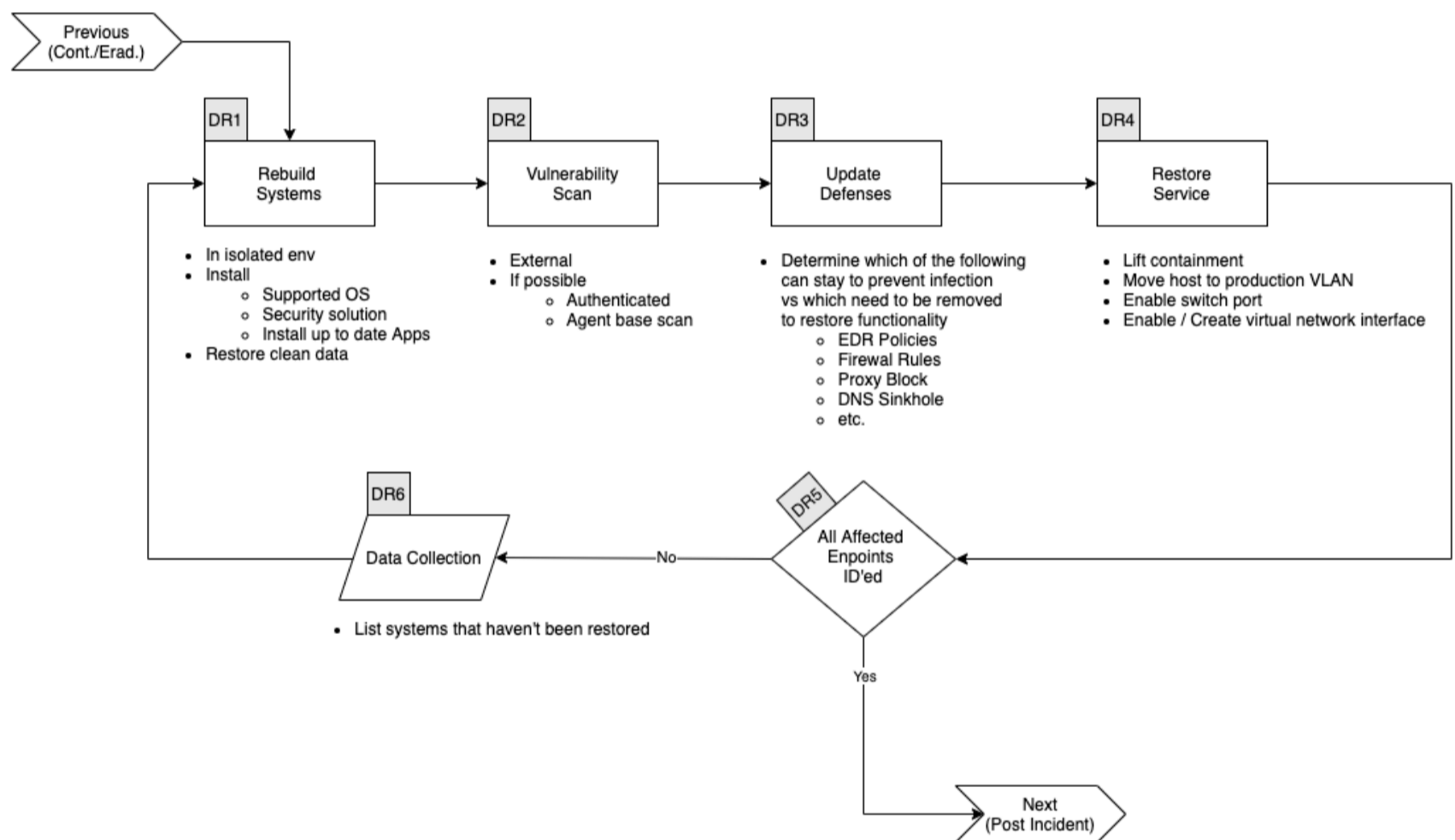
5. Recover

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

DataLoss - Recover



DR1. Rebuilt Systems

▼ Expand/Colapse

In an isolated environment:

- Install - Supported OS - Security solutions - Up to date applications - Restore data (from a clean backup)

DR2. Vulnerability Scan

▼ Expand/Colapse

Perform:

- External VA
- If possible
 - Authenticated scan
 - Agent base scan

DR3. Update Defenses

▼ Expand/Colapse

Determine which of the following rules needs to be removed and which needs to stay in the following list:

- Firewall Rules

- EDR
 - Ban hashes
 - Ban domains
 - Containment
- Proxy Block
- DNS Sinkhole
- Etc.

DR4. Restore Service

▼ Expand/Colapse

Depending on the containment applied to the host, perform all the following that applies:

- Lift containment in EDR console
- Move host to production VLAN
- Enable switch port
- Enable/Create virtual network interface
- etc.

DR5. All Affected Endpoints Restored?

▼ Expand/Colapse

If all affected endpoints have been restored, you can go to the [Post Incident](#) phase, otherwise continue bellow.

- List systems that haven't been restored
- Go to [README.md#rebuild-systems]

6. Post Incident

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

 [Data Loss Workflow](#)

DP1. Incident Review

▼ Expand/Colapse

- What worked
- What didn't work

DP2. Update Mode of Operations

▼ Expand/Colapse

Update the following documents as required:

- Policies
- Processes
- Procedures
- Playbooks
- Runbooks

Update Detetion Rules in:

- SIEM
- Anti-Spam
- Malware Gataway
- EDR
- Other security solution

DP3. Review Defensive Posture

▼ Expand/Colapse

- Schedule review of newly introduced rules in 6 months
- Are the following still applicatble
 - Firewall Rules
 - Proxy Rules for C2
 - AV / EDR custom Signatures
 - IPS Signatures

DP4. Build New Detection

▼ Expand/Colapse

If the Data Loss was not caused by a lost device, we need to build new detections

- Mail Service
- Anti-Spam / Anti-Phish
- ATT&CK Techniques
- etc.

DP5. Modify Base Images

▼ Expand/Colapse

If the Data Loss was caused by a lack of hardening or sufficient patch level:

- Review hardening processes
- Include critical patches in base Images
- etc.

DP7. User Awareness Training

▼ Expand/Colapse

If the incident was caused by a human error

- Create / Select new mandatory training
 - Cyber Education Vendor
 - From Youtube videos
 - Built by internal teams

DP8. Calculate Incident's Cost

▼ Expand/Colapse

Calculate the incident's Cost

- Time Spent
- Ransom paid
- Downtime
- Fines / Penalties
- etc.

Malware Playbook

- [Malware Playbook](#)
 - [Scope](#)
 - [1. Preparation](#)
 - [Tool Access and Provisioning](#)
 - [Tool1](#)
 - [Tool2](#)
 - [Assets List](#)
 - [2. Detect](#)
 - [Workflow](#)
 - [MD1. Identify Threat Indicators](#)
 - [Alerts](#)
 - [Notifications](#)
 - [MD2. Identify Risks Factors](#)
 - [Common](#)
 - [Company Specific](#)
 - [MD3. Data Collection](#)
 - [MD4. Categorize](#)
 - [MD5. Is it a Ransomware ?](#)
 - [MD6. Is it a Worm ?](#)
 - [MD7. Triage](#)
 - [MD8. Is it a False Positive?](#)
 - [3. Analyze](#)
 - [Workflow](#)
 - [MA1. Verify](#)
 - [MA2. Is this a Major/Critical Incident?](#)
 - [MA3. Identify IOCs](#)
 - [MA4. Extract IOCs](#)
 - [MA5. Submit Samples to Partners](#)
 - [MA6. Scan Enterprise](#)
 - [MA7. What Was Access](#)
 - [MA8. Update Scope](#)
 - [MA9. Scope Validation](#)
 - [MA11. Do We Need External Help?](#)
 - [MA16. Root Cause Analysis](#)
 - [MA17. Determine Mitre ATT&CK Stage](#)
 - [MA18. Was Any Data Exfiltrated?](#)
 - [MA19. Send communication](#)
 - [4. Contain / Eradicate](#)
 - [Workflow](#)
 - [MC1. Does the host have EDR?](#)
 - [MC4. Contain Affected Hosts](#)
 - [MC7. Action Taken by User/Computer](#)

- [MC8. Admin Rights?](#)
- [MC11. Did Vendor Release New Signature?](#)
- [MC14. Close Monitoring](#)
- [MC15. All Affected Endpoints Contained?](#)
- [MC16. New IOC Discovered?](#)
- [5. Recover](#)
 - [Workflow](#)
 - [MR1. Rebuilt Systems](#)
 - [MR2. Vulnerability Scan](#)
 - [MR3. Patch Vulnerabilities](#)
 - [MR4. Update Defenses](#)
 - [MR5. Restore Service](#)
 - [MR6. All Affected Endpoints Restored?](#)
 - [MR8. Validate Countermeasures](#)
 - [MR9. Was Malware Known Before](#)
- [6. Post Incident](#)
 - [Workflow](#)
 - [MP1. Incident Review](#)
 - [MP2. Update Policies & Procedures](#)
 - [MP3. Review Defensive Posture](#)
 - [MP4. Update & Upgrade Defenses](#)
 - [MP5. Build New Detections](#)
 - [MP6. Modify Base Images](#)
 - [MP8. User Awareness Training](#)
 - [MP9. Calculate Incident's Cost](#)
- [References](#)

Scope

This Playbook covers

1. Preparation

▼ Expand/Colapse

- Create and maintain a list of
 - all domains owned by Company.
 - This can prevent you from taking actions against our own domains
 - all people of can register domains
- Create email template
 - to notify all employees of ongoing phishing campaing against the organization
 - to contact hosting companies for domain take down
 - to inform 3rd party to take actions against phishing on there infra (Microsoft, Fedex, Apple, etc.)
- Ensure that:
 - Mail anti-malware/anti-spam/anti-phish solutions are in place.
 - Users know how to report phish
 - Detection exists for office documents spawning processes
 - PowerShell
 - CMD
 - WMI
 - MSHTA
 - Etc.
- Perform Firedrill to ensure all aspects of the Playbook are working
 - After publication
 - At least once a year
 - Test/Validate:
 - [Customer's Cards](#)
 - Internal Contact and Escalation Paths
- Review threat intelligence for
 - threats to the organisation,
 - brands and the sector,
 - common patterns
 - newly developing risks and vulnerabilities
- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following
 - IR Playbgns to highlight information security risks faced by employees, including:
 - Phishing attacks and malicious emails;
 - Ransomware;
 - Reporting a suspected cyber incident.

Tool Access and Provisioning

Tool1

Please refer to [Tool1 Documentation](#)

Tool2

Please refer to [Tool2 Documentation](#)

Assets List

- A list of assets and owner should exist and be available for the following
 - Customers Assets
 - Owners
 - Contacts
 - Pre authorized actions
 - Company Assets (Including all filiales like and business units)
 - Owners
 - Contacts
 - Administrators
 - Pre authorized actions
- Type of assets inventory needed
 - Endpoints
 - Servers
 - Network Equipements
 - Security Appliances
 - Network Ranges
 - Public
 - Private
 - VPN / Out of Band
 - Employees
 - Partners
 - Clients

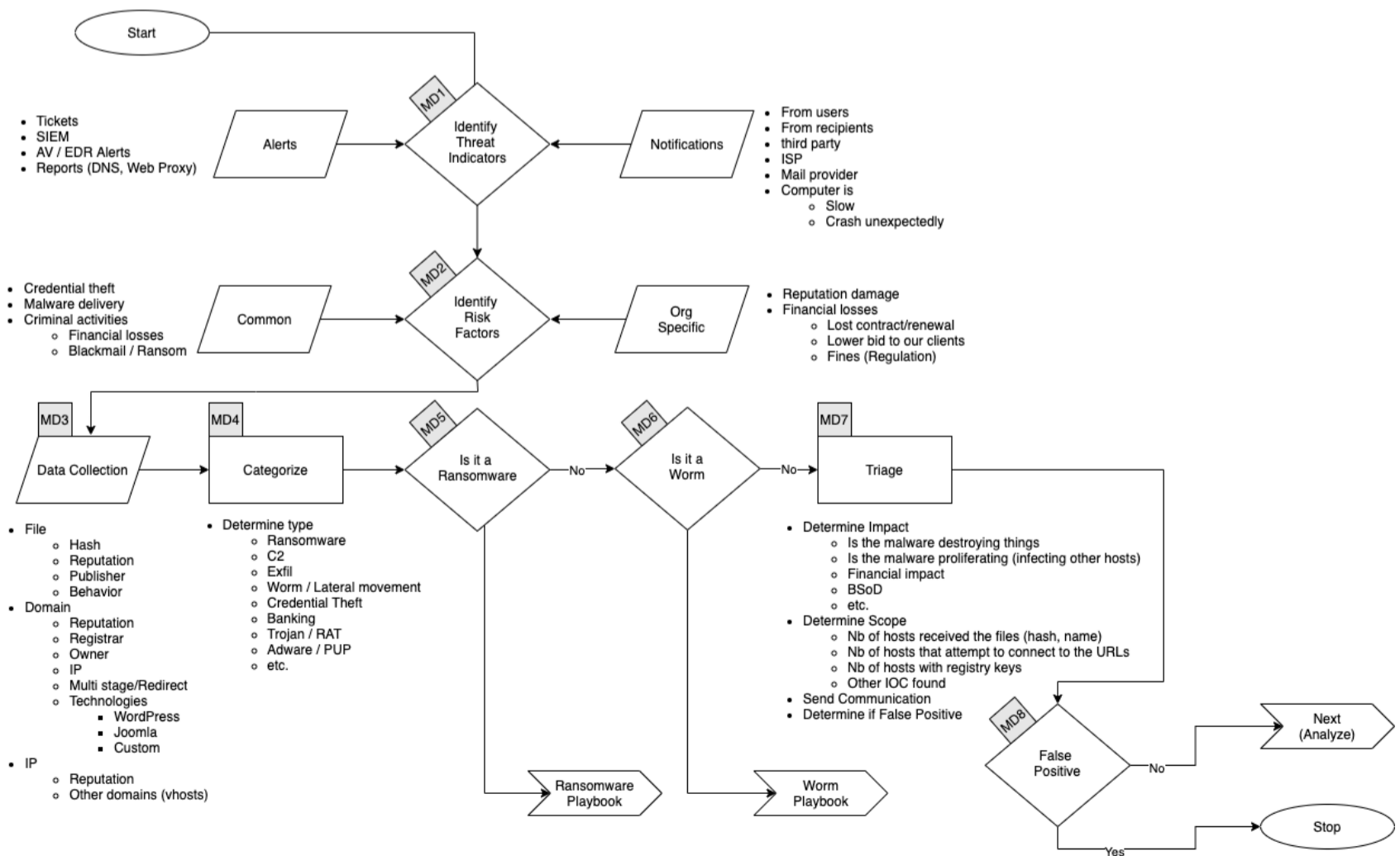
2. Detect

▼ Expand/Collapse

Workflow

▼ Expand/Collapse

Malware - Detect



MD1. Identify Threat Indicators

▼ Expand/Colapse

Alerts

Alerts are generated by different systems owned by the Security/SOC team. The main sources for alerts are

- Tickets
- SIEM
- Anti-Virus / EDR
- Reports
 - DNS
 - Web Proxy
- Errors from mail servers

Notifications

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- Users (internal)
- Recipients of emails (external)
- Third Parties
- ISP
- Mail Providers
- Computer is
 - Slow
 - Crash unexpectedly

MD2. Identify Risks Factors

▼ Expand/Colapse

Common

- Credential Theft
- Malware Delivery
- Criminal Activities
 - Blackmail / Ransom

Company Specific

- Reputation damage
- Financial Losses
 - Lost of contract
 - Contract not renewed
 - Lower bid to our clients
 - Fines
 - Regulation

MD3. Data Collection

This section describes the information that should be collected and documented about the incident

There is a lot of resources to help you with that phase [here](#)

▼ Expand/Colapse

Files

- Hash
- Reputation
- Publisher
- Behavior

Domains

- Reputation
- Registrar
- Owner
- IP
- Multistage / Redirect
- Technologies of the site
 - WordPress
 - Joomla

- Custom Page (credential phish)

IP

- Reputation
- Owner
- Geo Localisation
- Other domains on that IP

MD4. Categorize

▼ Expand/Colapse

Determine type of malware

- Ransomware
- C2
- Exfiltration
- Worm / Lateral Movement
- Credential Theft
- Banking
- Trojan / RAT
- Adware / PUP
- etc.

MD5. Is it a Ransomware ?

As time is VERY sensitive in the case of a Ransomware:

- Send a communication to the Security Mailing List
- Ping everyone in the Security Teams Chat
- Go to the [Ransomware Playbook](#)
 - If the Playbook doesn't exist, follow this one

MD6. Is it a Worm ?

As time is sensitive in the case of a Worm:

- Send a communication to the Security Mailing List
- Ping everyone in the Security Teams Chat
- Go to the [Worm Playbook](#)
 - If the Playbook doesn't exist, follow this one

MD7. Triage

▼ Expand/Colapse

Determine

- Impact
 - Of the malware destroying things
 - Is the malware proliferating (infecting other hosts)
 - Financial
 - Blue Screen of Death (or other crash)
 - Data loss
 - etc.
- Scope: Number and list of hosts that
 - Have the files
 - Hash
 - File name
 - RegEx match (ie: INVOICE-12345.docx where 12345 is 5 random digit)
 - Attempted to connect to the
 - URLs
 - IP
 - Ports
 - That have the registry keys
 - Any other IOCs found

MD8. Is it a False Positive?

If it's a False Positive:

- Document and close the incident

If it's a True Positive:

- Send communication to
 - Security Team
 - Admin Teams
 - Affected Syntac Entities
 - Affected Clients
- Go to Analyze phase

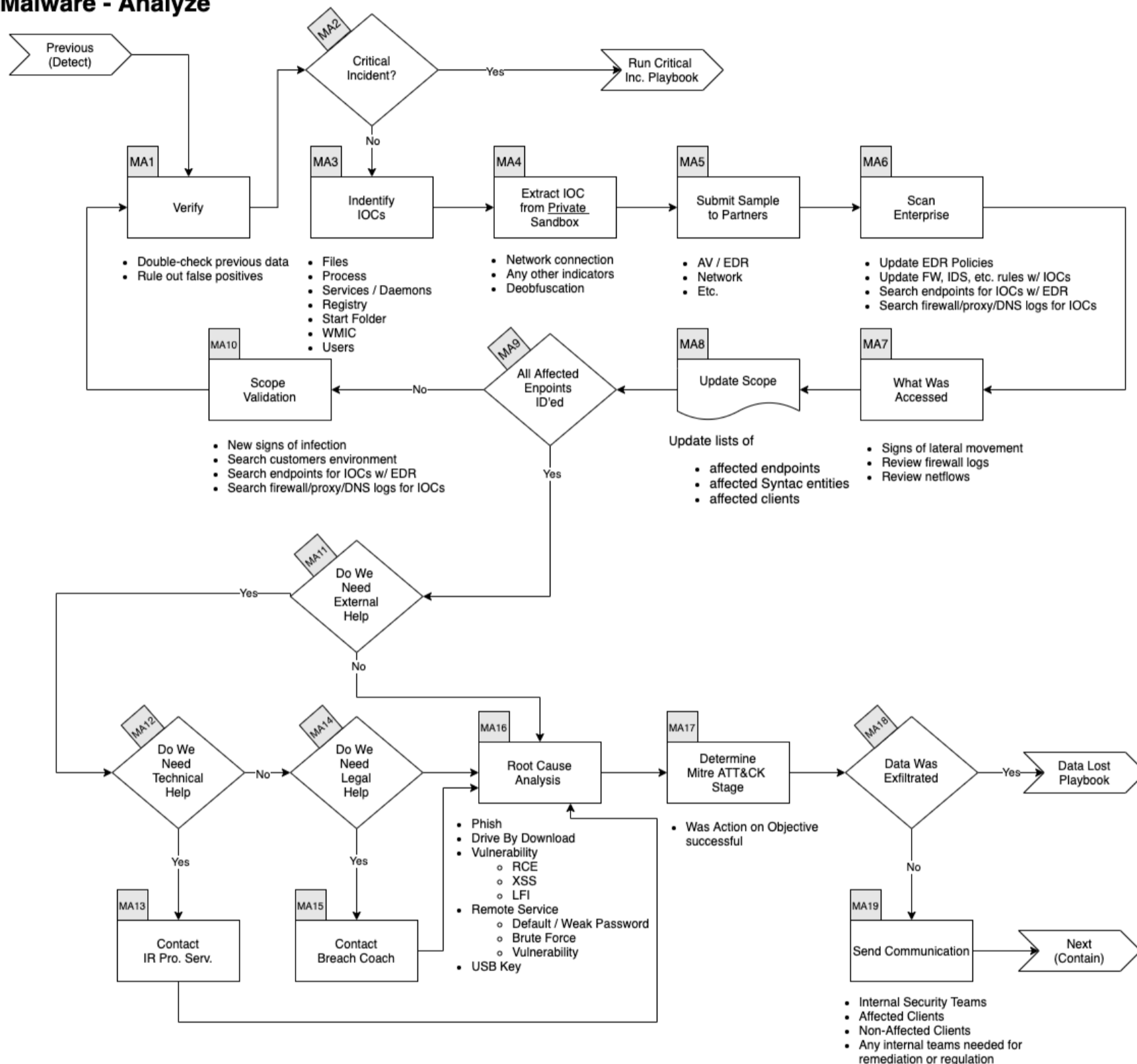
3. Analyze

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Malware - Analyze



MA1. Verify

▼ Expand/Colapse

In conjunction with a senior member of the SOC

- Double check previous data
- Rule out False Positive

MA2. Is this a Major/Critical Incident?

If this incident is deemed **Major or Critical** by the senior analyst go to the [Critical Incident Playbook](#)

MA3. Identify IOCs

▼ Expand/Colapse

Don't forget to look at **ALL** the tabs of the tools. Not just detection rate.

For example, the tabs **Details** and **Behavior** of VirusTotal are very informative about who published the file and what the file did to the system.

- Validate file hashes
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
- Validate links
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [URLScan](#)
- ID other addresses, domains, IPs
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [Talos Intelligence](#)
 - [Domain Dossier](#)
- Search Threat Intel sources
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [Talos Intelligence](#)
- Disk forensics on endpoint (if required)

MA4. Extract IOCs

▼ Expand/Colapse

Using a *PRIVATE* sandbox run the malware sample (files) and try to access the URLs

Collect the following informations:

- Network connections
- Registries modifications
- Files
 - dropped
 - accessed
 - modified
- Deobfuscated script
 - From Script Block (for PowerShell)
- New services
 - Created
 - Launched
- New scheduled tasks
- New WMI provider(s)

MA5. Submit Samples to Partners

▼ Expand/Colapse

If the malware(s) was not detected/blocked by the security stack

- Submit Samples to Security Vendor
- Submit URLs, IP, Domains

MA6. Scan Enterprise

▼ Expand/Colapse

- Update AV / EDR
 - Engine
 - Ruleset
 - Policies
- Update FW, IDS, etc. rules with IOCs
- Search endpoints for IOCs with EDR
- Search SIEM for IOCs
- Search Firewall, Proxy, DNS logs for IOCs

MA7. What Was Access

▼ Expand/Colapse

- Look for signs of lateral Movement
- Review firewall logs
 - Network appliances (ie: Cisco ASA)
 - endpoint (ie: Windows local firewall, EDR, AV, etc.)
- Review netflows

MA8. Update Scope

▼ Expand/Colapse

- Update lists of
 - affected endpoints
 - affected Company Entities
 - affected clients

MA9. Scope Validation

▼ Expand/Colapse

Have all the machines been identified? If you find futher traces of infection or new IOCs go back to the [Verify Step](#).

When you are done identifying all compromised:

- Hosts

And investigated all:

- URLs
- Domains
- IP
- Ports
- Files
- Hash

MA11. Do We Need External Help?

▼ Expand/Colapse

Depending on the depth and breath of the infection we might need so conseilling. Evalatuete of we need

- Technical, Hands On, Response, etc. support
- Legal conseilling (data breach, lots of clients affected, etc.)

If it's the case, contact our partners and activate the retainer.

MA16. Root Cause Analysis

▼ Expand/Colapse

How did this infection started?

- Phish
- Drive by download
- Vulnerability
 - RCE
 - XSS
 - LFI
- Remote services
 - Default / Weak password
 - Brute Force
 - Vulnerability
- USB key/drive

MA17. Determine Mitre ATT&CK Stage

▼ Expand/Colapse

The [Mitre ATT&CK Framework]() as various [Tactics] that are part of a [Cyber Kill Chain]. It is important to know at which stage of the Kill Chain the attack was detected and stoped.

Document your ticket with the following information:

- Stage of detection
- Stage of prevention
- Was action on objective completed
 - File encrypted
 - Data exfiltrated
 - Account takeover
 - Etc.

If data was exfiltrated go to the [Data Lost Playbook](#)

MA18. Was Any Data Exfiltrated?

If we know or **suspect** that data was exfiltrated by the adversaries go to [Data Loss Playbook](#)

MA19. Send communication

▼ Expand/Colapse

- Send a update communication to
 - Security Team
 - Admin Teams
 - Affected Syntac Entities
 - Affected Clients

Go to the next phase <Contain/Eradicate>

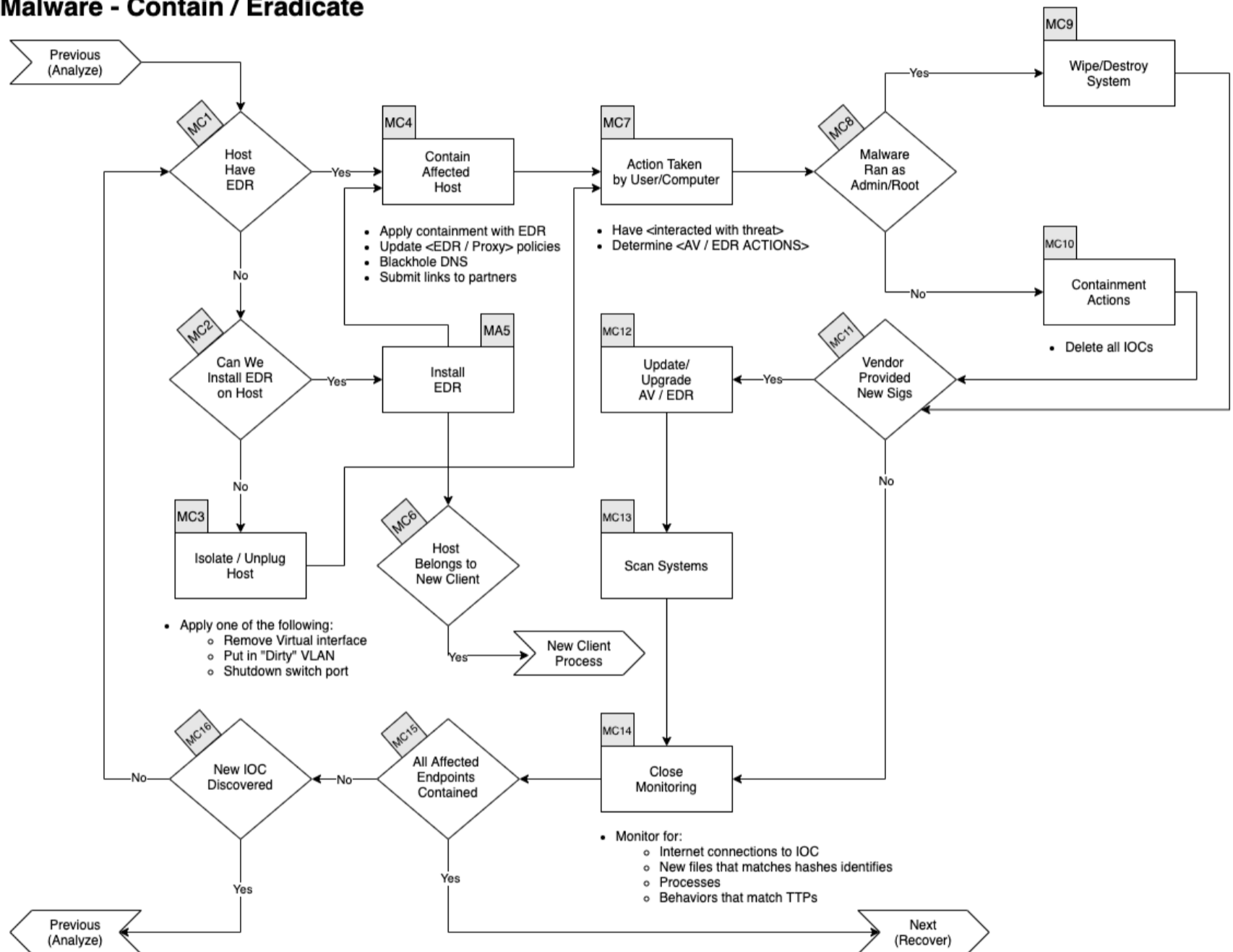
4. Contain / Eradicate

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Malware - Contain / Eradicate



MC1. Does the host have EDR?

▼ Expand/Colapse

If the host **have** an EDR installed go to the [Contain Section](#)

If the host **does not have** an EDR, is it possible to install one?

Yes:

- Install EDR
- Go to [Contain section](#)

No: Isolate / Unplug the host

- Apply one of the following containment strategy
 - Remove/shutdown virtual interface
 - Put in "Dirty" VLAN
 - Shutdown switch port
- Go to [Action Taken section](#)

MC4. Contain Affected Hosts

▼ Expand/Colapse

- Update FW, Proxy, etc. rules
- Blackhole DNS
- Submit to Partners
 - AV/EDR Vendor
 - Web Filter Vendor
 - etc.

MC7. Action Taken by User/Computer

▼ Expand/Colapse

Did the user:

- Launch the malware
 - Open the document(s)
 - Run the executable
 - Launch the script

Did the computer / EDR:

- Connect to external site(s)
- Write files to disk
- Modified registry keys
- New services
 - Created
 - Launched
- New scheduled tasks
- New WMI provider(s)
- Block excution
- Quarantine file(s)

MC8. Admin Rights?

▼ Expand/Colapse

In order to select the right eradication strategy we need to know in which context the malware was executed.

Was the user admin/root of the machine or any other machines in the environment?

Yes:

- Wipe physical machine
- Delete virtual machine

No:

- Delete all IOCs
 - Files
 - Registry keys
 - Services
 - Scheduled Tasks
 - WMI provider(s)
 - etc.

MC11. Did Vendor Release New Signature?

▼ Expand/Colapse

Did the security vendor of the AV / EDR released a new engine, signature, policy to address the malware?

No:

- Go to [Close Monitoring](#)

Yes:

- Upgrade security solution
- Update signatures
- Activate policy
- Scan systems enterprise wide
 - Include customers if requiered

MC14. Close Monitoring

- ▼ Expand/Colapse
 - Monitor for:
 - Internet connections to IOC
 - New files that matches hashes identified
 - Processes
 - Behaviors that matched identified TTPs

MC15. All Affected Endpoints Contained?

- ▼ Expand/Colapse
 - If all affected endpoints have been contained, you can go to the phase, otherwise continue bellow.

MC16. New IOC Discovered?

- ▼ Expand/Colapse
 - If there was new IOC discovered, go back to the [Analyze Phase](#)
 - Otherwise continue with [host containment](#)

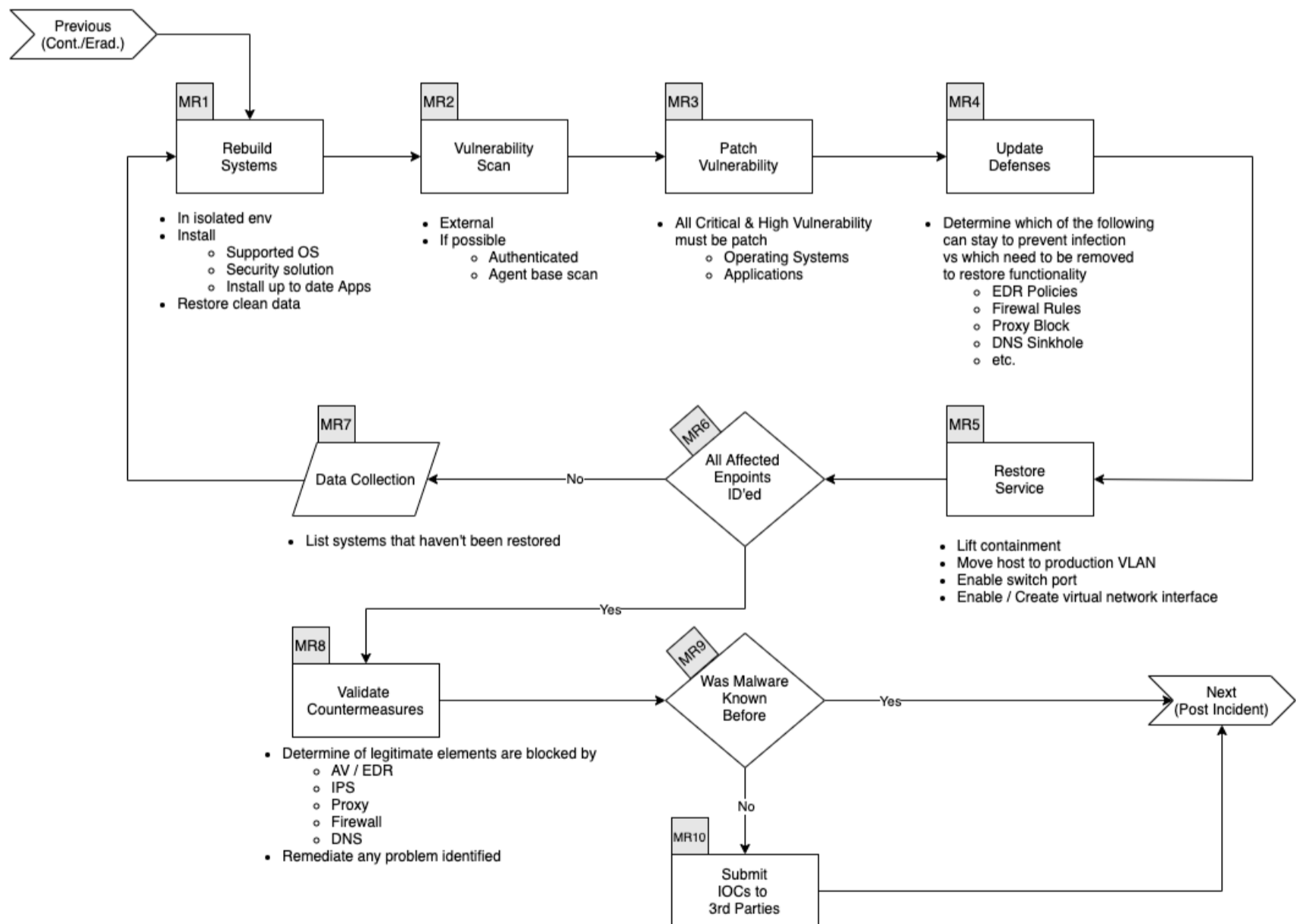
5. Recover

- ▼ Expand/Colapse

Workflow

- ▼ Expand/Colapse

Malware - Recover



MR1. Rebuilt Systems

- ▼ Expand/Colapse
 - In an isolated environment:
 - Install - Supported OS - Security solutions - Up to date applications - Restore data (from a clean backup)

MR2. Vulnerability Scan

- ▼ Expand/Colapse
 - Perform:
 - External VA
 - If possible

- Authenticated scan
- Agent base scan

MR3. Patch Vulnerabilities

▼ Expand/Colapse

Any **Critical** or **High** vulnerability needs to be patched **before** the service is reestablish. This include, but it not limited to

- Operating Systems
- Applications
- Network Appliances

Medium and Low vulnerability should be patched if possible, but should not be mandatory for restoring the service/lifting containment.

MR4. Update Defenses

▼ Expand/Colapse

Determine which of the following rules needs to be removed and which needs to stay in the following list:

- Firewall Rules
- EDR
 - Ban hashes
 - Ban domains
 - Containment
- Proxy Block
- DNS Sinkhole
- Etc.

MR5. Restore Service

▼ Expand/Colapse

Depending on the containment applied to the host, perform all the following that applies:

- Lift containment in EDR console
- Move host to production VLAN
- Enable switch port
- Enable/Create virtual network interface
- etc.

MR6. All Affected Endpoints Restored?

▼ Expand/Colapse

If all affected endpoints have been restored, you can go to the phase, otherwise continue bellow.

- List systems that haven't been restored
- Go to [README.md#rebuild-systems]

MR8. Validate Countermeasures

▼ Expand/Colapse

Determine if legitimate elements are blocked by:

- AV / EDR
- IPS
- Proxy
- Firewall
- DNS
- Etc.

If so, apply the corrective action to restore functionality

MR9. Was Malware Known Before

▼ Expand/Colapse

If the malware was **not known** before the incident

- Validate with the Global Security Team if you can submit the sample to 3rd parties like
 - VirusTotal
 - Hybrid-Analysis
 - Any.run
 - Threat Grig
 - Google Safe Browsing
 - OpenIOC

- Etc.

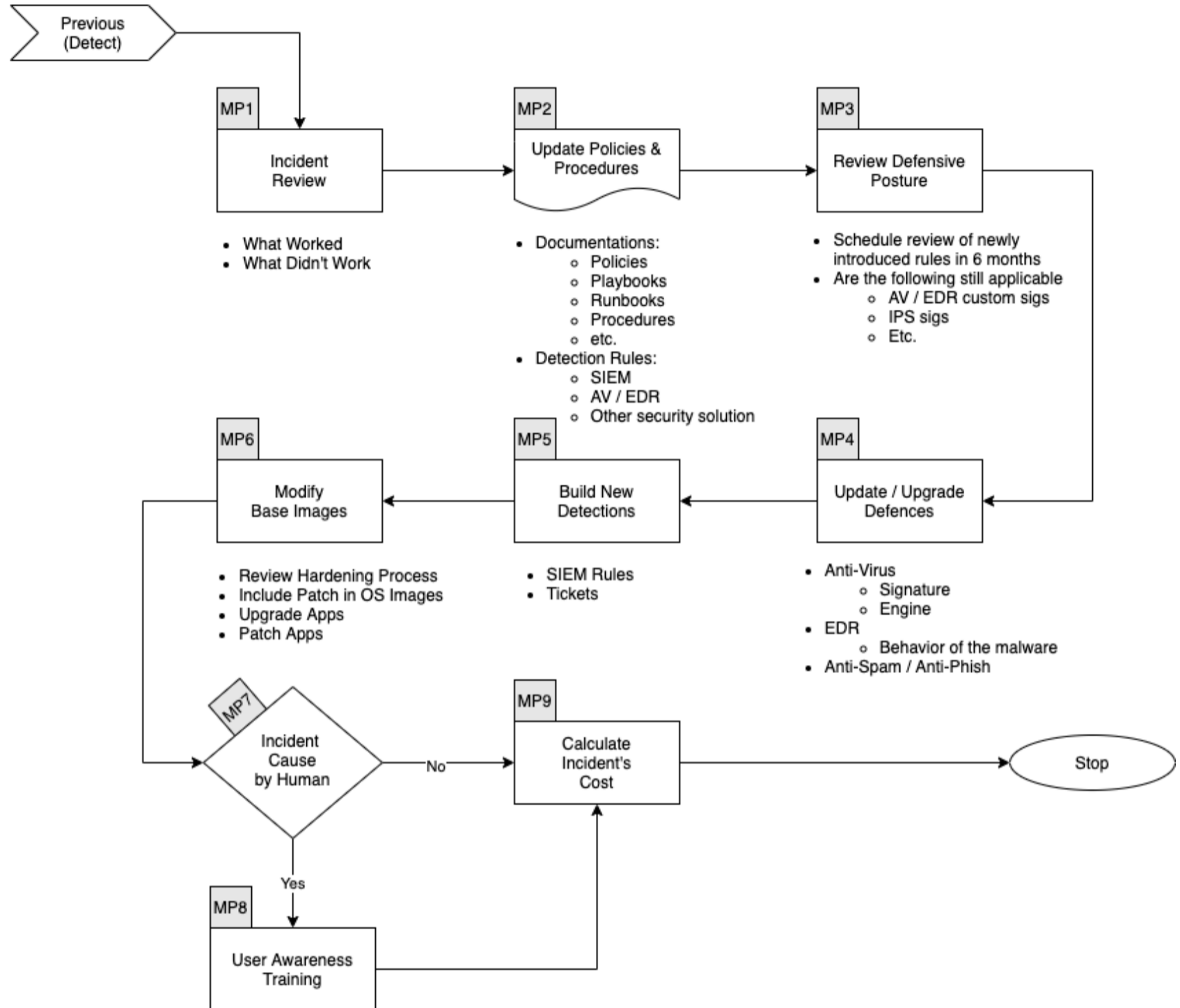
6. Post Incident

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Malware - Post Incident



MP1. Incident Review

▼ Expand/Colapse

- What worked
- What didn't work

MP2. Update Policies & Procedures

▼ Expand/Colapse

Update the following documents as required:

- Policies
- Processes
- Procedures
- Playbooks
- Runbooks

Update Detetion Rules in:

- SIEM
- Malware Gataway
- AV / EDR
- IPS
- Other security solution

MP3. Review Defensive Posture

▼ Expand/Colapse

- Schedule review of newly introduced rules in 6 months
- Are the following still applicatble
 - Firewall Rules
 - Proxy Rules for C2
 - AV / EDR custom Signatures
 - IPS Signatures
 - Etc.

MP4. Update & Upgrade Defenses

▼ Expand/Colapse

As we still have multiple AV & EDR Vendor, we must ensure **ALL** of them can detect this malware family in the future.

Malware Sample should be sent to **ALL** AV and EDR vendor we work with. Once the AV/EDR vendor confirms they can detect the sample we need to make sure:

- Anti-Virus
 - Signatures are updated for all
 - Company Entities
 - Customers (Regardless of the region)
 - Engine are upgraded for all
 - Company Entities
 - Customers (Regardless of the region)
- EDR Rules
 - To detect the behaviors of the malware
- Mail Service
- Anti-Spam / Anti-Phish
- etc.

MP5. Build New Detections

▼ Expand/Colapse

SIEM Rules could be created to catch this type of behaviors and create tickets.

MP6. Modify Base Images

▼ Expand/Colapse

If the Malware Infection was caused by a lack of hardening or insufficient patch level:

- Review hardening processes
- Include critical patches in base images
- Consider upgrading application
- Apply Security Patch to application
- etc.

MP8. User Awareness Training

▼ Expand/Colapse

If the incident was caused by a human error

- Create / Select new mandatory training
 - From Security Education Vendor
 - From Youtube video
 - Built by internal teams

MP9. Calculate Incident's Cost

▼ Expand/Colapse

Phishing Playbook

- [Phishing Playbook](#)
 - [Scope](#)
 - [1. Preparation](#)
 - [Tool Access and Provisioning](#)
 - [Tool1](#)
 - [Tool2](#)
 - [Assets List](#)
 - [2. Detect](#)
 - [Workflow](#)
 - [Identify Threat Indicators](#)
 - [Alerts](#)
 - [Notifications](#)
 - [Identify Risks Factors](#)
 - [Common](#)
 - [Company Specific](#)
 - [Data Colletion](#)
 - [Categorize](#)
 - [Triage](#)
 - [3. Analyze](#)
 - [Workflow](#)
 - [Verify](#)
 - [Identify IOCs](#)
 - [Scan Enterprise](#)
 - [Update Scope](#)
 - [Update Scope](#)
 - [Scope Validation](#)
 - [4. Contain / Eradicate](#)
 - [Workflow](#)
 - [Block](#)
 - [Validate User's Actions](#)
 - [Malware Infection?](#)
 - [Delete Emails](#)
 - [Close Monitoring](#)
 - [All Affected Endpoints Contained?](#)
 - [New IOC Discovered?](#)
 - [5. Recover](#)
 - [Workflow](#)
 - [Update Defenses](#)
 - [All Affected Endpoints Recovered?](#)
 - [Validate Countermeasures](#)

- [6. Post Incident](#)
 - [Workflow](#)
 - [Incident Review](#)
 - [Update Mode of Operations](#)
 - [Review Defensive Posture](#)
 - [User Awareness Training](#)
- [References](#)

Scope

This Playbook covers

1. Preparation

▼ Expand/Colapse

- Create and maintain a list of
 - all domains owned by Company.
 - This can prevent you from taking actions against our own domains
 - all people of can register domains
- Create email template
 - to notify all employees of ongoing phishing campaing against the organization
 - to contact hosting companies for domain take down
 - to inform 3rd party to take actions against phishing on there infra (Microsoft, Fedex, Apple, etc.)
- Ensure that:
 - Mail anti-malware/anti-spam/anti-phish solutions are in place.
 - Users know how to report phish
 - Detection exists for office documents spawning processes
 - PowerShell
 - CMD
 - WMI
 - MSHTA
 - Etc.
- Perform Firedrill to ensure all aspects of the Playbook are working
 - After publication
 - At least once a year
 - Test/Validate:
 - [Customer's Cards](#)
 - Internal Contact and Escalation Paths
- Review threat intelligence for
 - threats to the organisation,
 - brands and the sector,
 - common patterns
 - newly developing risks and vulnerabilities
- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following
 - IR Playbgns to highlight information security risks faced by employees, including:
 - Phishing attacks and malicious emails;
 - Ransomware;
 - Reporting a suspected cyber incident.

Tool Access and Provisioning

Tool1

Please referer to [Tool1 Documentation](#)

Tool2

Please referer to [Tool2 Documentation](#)

Assets List

- A list of assets and owner should exists and be available for the following
 - Customers Assets
 - Owners
 - Contacts
 - Pre authorized actions
 - Company Assets (Including all filiale and business units)
 - Owners
 - Contacts

- Administrators
- Pre authorized actions
- Type of assets inventory needed
 - Endpoints
 - Servers
 - Network Equipements
 - Security Appliances
 - Network Ranges
 - Public
 - Private
 - VPN / Out of Band
 - Employees
 - Partners
 - Clients

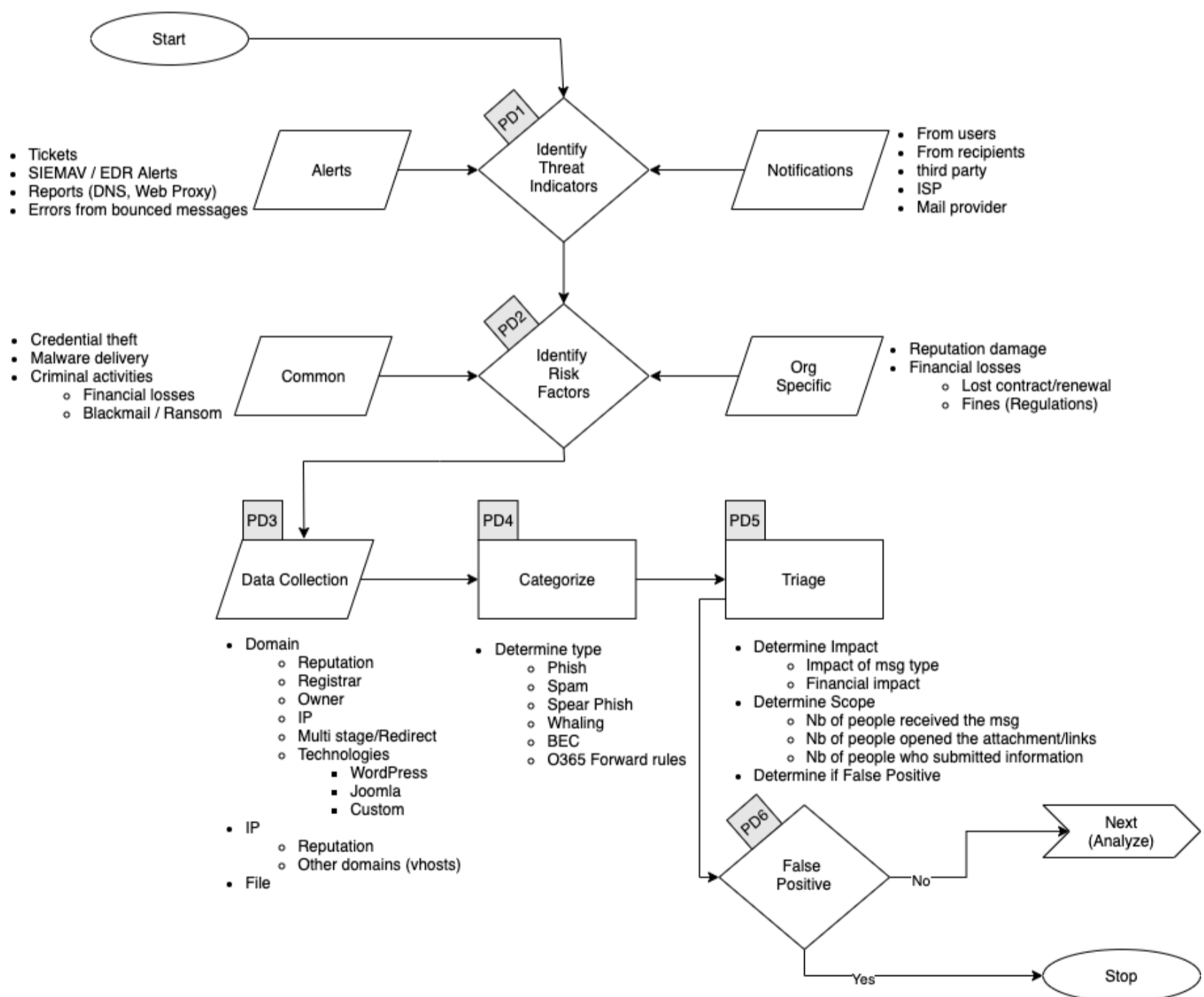
2. Detect

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Phishing - Detect



Identify Threat Indicators

▼ Expand/Colapse

Alerts

Alerts are generated by different systems owned by the Security/SOC team. The main sources for alerts are

- Tickets
- SIEM
- Anti-Virus / EDR
- Reports
 - DNS

- Web Proxy
- Errors from mail servers

Notifications

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- Users (internal)
- Recipients of emails (external)
- Third Parties
- ISP
- Mail Providers

Identify Risks Factors

▼ Expand/Collapse

Common

- Credential Theft
- Malware Delivery
- Criminal Activities
 - Blackmail / Ransom

Company Specific

- Financial Losses
 - Lost of contract
 - Contract not renewed
 - Lower bid to our clients
 - Fines
 - Regulation

Data Collection

This section describe the information that should be collected and documented about the incident

There is a lot of resources to help you with that phase [here](#)

▼ Expand/Collapse

Domains

- Reputation
- Registrar
- Owner
- IP
- Multistage / Redirect
- Technologies of the site
 - WordPress
 - Joomla
 - Custom Page (credential phish)

IP

- Reputation
- Owner
- Geo Localisation
- Other domains on that IP

Categorize

▼ Expand/Collapse

Determine type of email

- Phish
 - Company Site rip-off
 - Common brand
 - Apple
 - FedEx
 - Netflix
 - Etc.
 - Company 3rd Party
 - O365
 - Other Cloud base solutions

- Spear Phish
- Whaling
- Spam
- BEC
- O365 Forward Rules

Triage

- ▼ Expand/Collapse
Determine

- Impact
 - Of the message
 - Financial
 - Data loss
- Scope (Nb of people)
 - Received the message
 - Opened the attachments
 - Clicked on the links
 - Submitted information

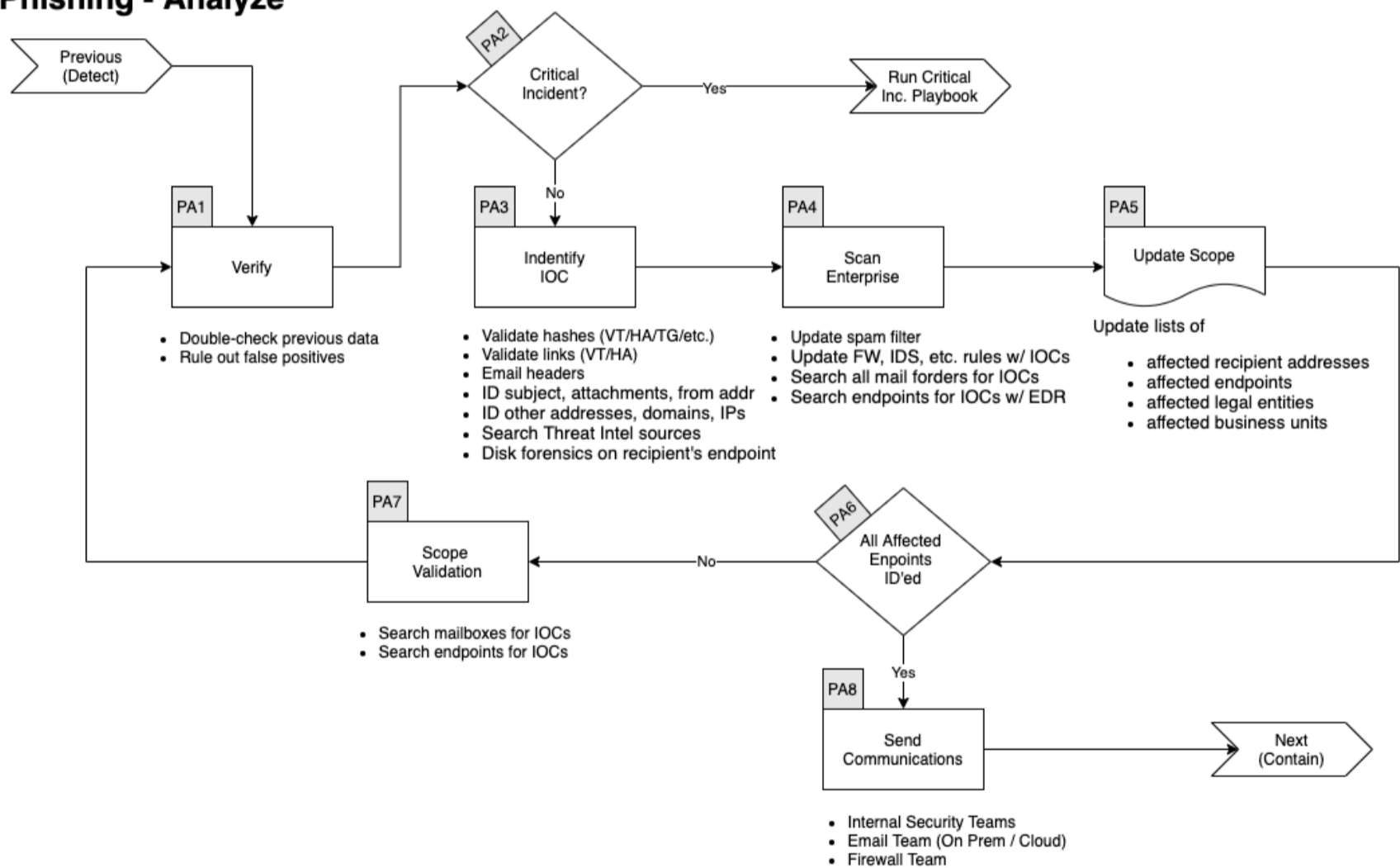
3. Analyze

- ▼ Expand/Collapse

Workflow

- ▼ Expand/Collapse

Phishing - Analyze



Verify

- ▼ Expand/Collapse
In conjunction with a senior member of the SOC

- Double check previous data
- Rule out False Positive

Identify IOCs

- ▼ Expand/Collapse
 - Validate hashes
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - Validate links

- [VirusTotal](#)
- [Hybrid Analysis](#)
- [URLScan](#)
- ID subject, attachments, from addr
- ID other addresses, domains, IPs
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [Talos Intelligence](#)
- Search Threat Intel sources
 - [VirusTotal](#)
 - [Hybrid Analysis](#)
 - [Talos Intelligence](#)
- Disk forensics on recipient's endpoint

Scan Enterprise

- ▼ Expand/Colapse
 - Update spam filter
 - Update FW, IDS, etc. rules w/ IOCs
 - Search all mail folders for IOCs
 - Search endpoints for IOCs w/ EDR

Update Scope

- ▼ Expand/Colapse
 - Update lists of
 - affected recipient addresses
 - affected endpoints
 - affected enclaves
 - affected business units

Update Scope

- ▼ Expand/Colapse
 - Update lists of
 - affected recipient addresses
 - affected endpoints
 - affected enclaves
 - affected business units

Scope Validation

- ▼ Expand/Colapse

Have all the machines been identified? If you find futher traces of phishing or new IOCs go back through this step.

When you are done identifying all compromised:

- Hosts
- Mailboxes

And investigated all:

- URLs
- Domains
- IP
- Ports
- Files
- Hash

Go to the next phase <Contain/Eradicate>

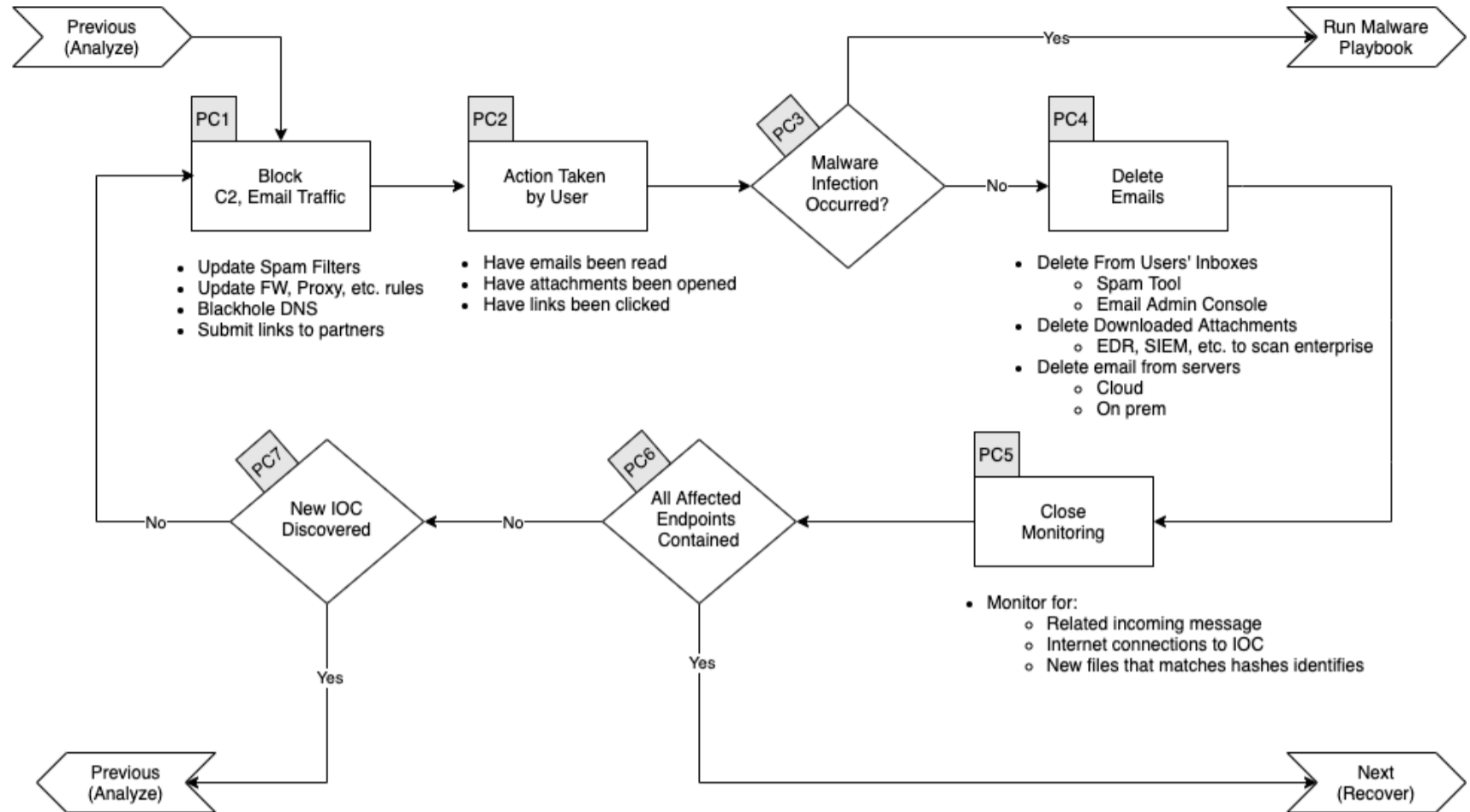
4. Contain / Eradicate

- ▼ Expand/Colapse

Workflow

- ▼ Expand/Colapse

Phishing - Contain / Eradicate



Block

▼ Expand/Colapse

- Update Spam Filters
- Update FW, Proxy, etc. rules
- Blackhole DNS
- Submit to thrid parties
 - [Google Safe Browsing](#)
 - Web Filter Vendor
 - etc.

Validate User's Actions

▼ Expand/Colapse

- Have emails been read
- Have attachments been opened
- Have links been clicked

Malware Infection?

▼ Expand/Colapse

If there was malicious attachments that were opened we need to assume the endpoint(s) was/were infected by a malware. Please continue to the [Malware Playbook](#)

Delete Emails

▼ Expand/Colapse

- Delete From Users' Inboxes
 - Spam Tool
 - Email Admin Console
 - Cloud & On-Prem
- Delete Downloaded Attachments
 - EDR, SIEM, etc. to scan enterprise

Close Monitoring

▼ Expand/Colapse

- Monitor for
 - Related incoming messages
 - Internet connections to IOC
 - New files that matches hashes identified

All Affected Endpoints Contained?

▼ Expand/Colapse

If all affected endpoints have been contained, you can go to the next phase, otherwise continue bellow.

New IOC Discovered?

▼ Expand/Collapse

If there was new IOC discovered, go back to the [Analyze Phase](#)

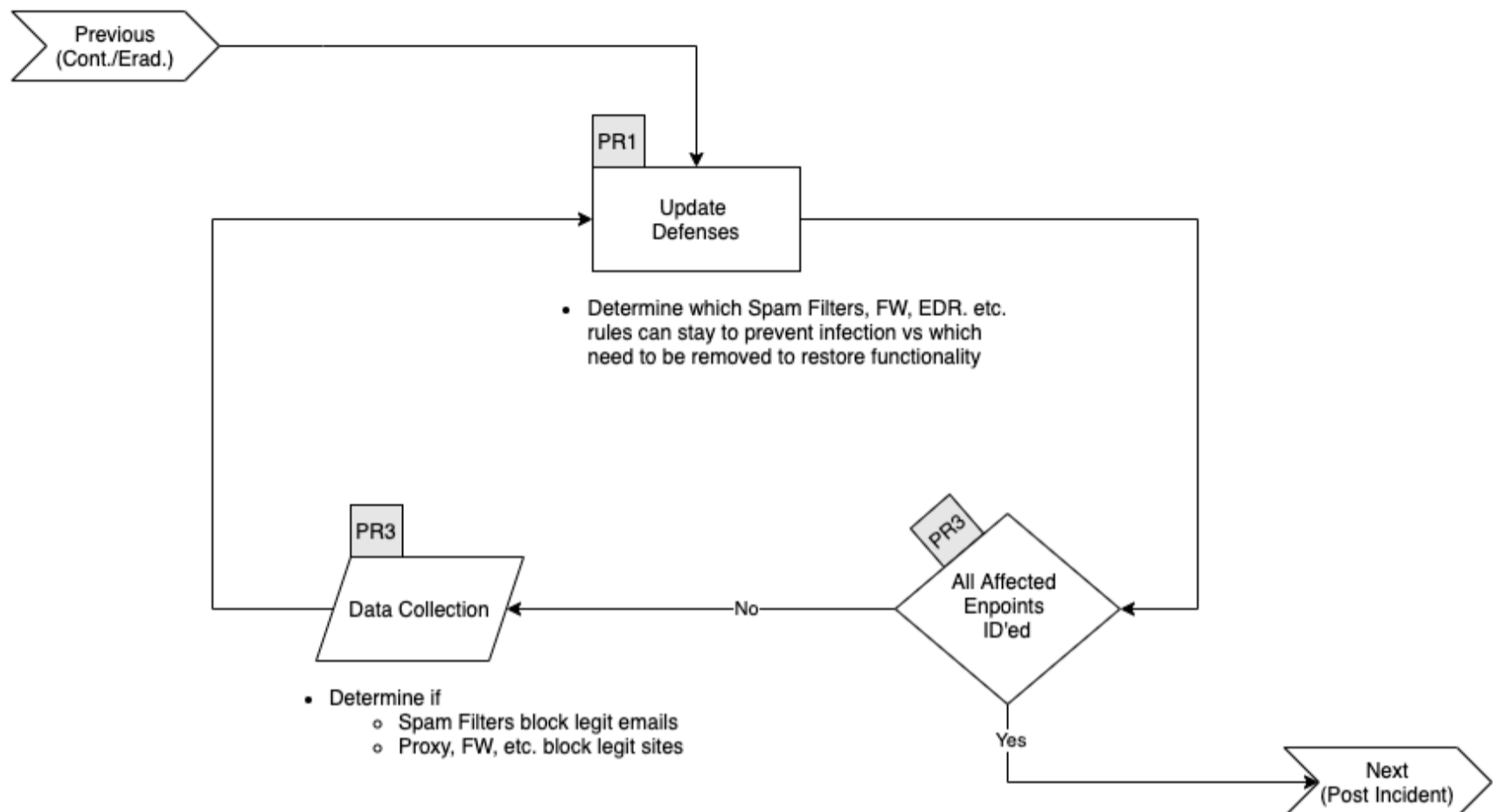
5. Recover

▼ Expand/Collapse

Workflow

▼ Expand/Collapse

Phishing - Recover



Update Defenses

▼ Expand/Collapse

Determine which of the following rules needs to be removed and which needs to stay in the following list:

- Spam Filters
- Firewall Rules
- EDR
 - ban hashes
 - ban domains
 - Containment
- Proxy Block

All Affected Endpoints Recovered?

▼ Expand/Collapse

If all affected endpoints have been contained, you can go to the next phase, otherwise continue below.

Validate Countermeasures

▼ Expand/Collapse

Determine if legitimate elements are blocked by:

- Spam Filters
- Proxy
- Firewall
- EDR

If so, go back to [Update Defenses](#) Otherwise go to the next phase

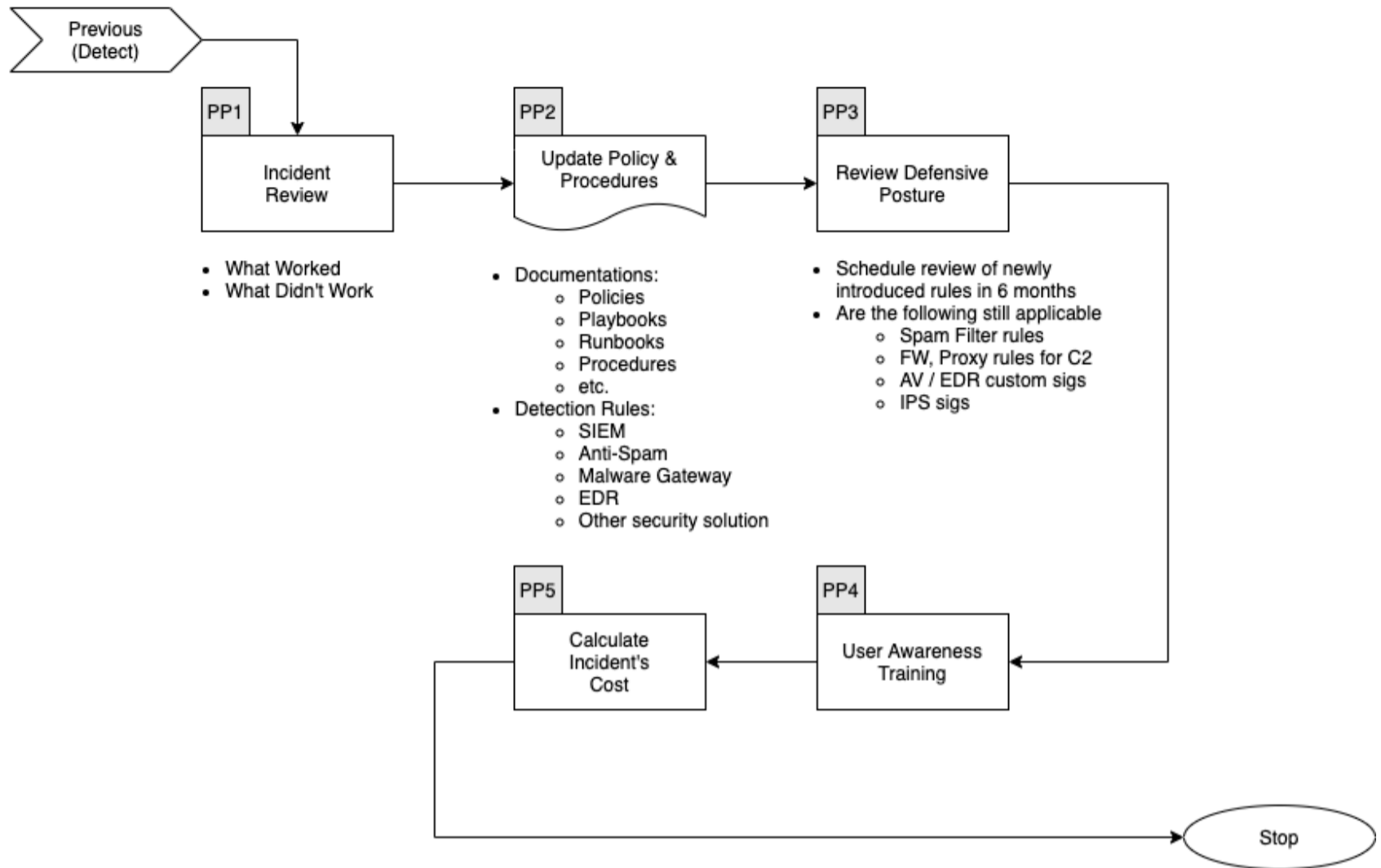
6. Post Incident

▼ Expand/Collapse

Workflow

▼ Expand/Colapse

Phishing - Post Incident



Incident Review

▼ Expand/Colapse

- What worked
- What didn't work

Update Mode of Operations

▼ Expand/Colapse

Update the following documents as required:

- Policies
- Processes
- Procedures
- Playbooks
- Runbooks

Update Detetion Rules in:

- SIEM
- Anti-Spam
- Malware Gataway
- EDR
- Other security solution

Review Defensive Posture

▼ Expand/Colapse

- Schedule review of newly introduced rules in 6 months
- Are the following still applicatble
 - Spam Filter Rules
 - Firewall Rules
 - Proxy Rules for C2
 - AV / EDR custom Signatures
 - IPS Signatures

User Awareness Training

▼ Expand/Colapse

- Ensure that the user receives Phishing training

- How to recognize Phish
- How to report Phish
- Danger of following links
- Danger of opening attachments
- Danger of complying with scammers requests

Ransom Playbook

- [Ransom Playbook](#)
 - [Scope](#)
 - [1. Preparation](#)
 - [Tool Access and Provisioning](#)
 - [Tool1](#)
 - [Tool2](#)
 - [Assets List](#)
 - [2. Detect](#)
 - [Workflow](#)
 - [RD1. Identify Threat Indicators](#)
 - [Alerts](#)
 - [Notifications](#)
 - [RD2. Indentify Risks Factors](#)
 - [Common](#)
 - [Company Specific](#)
 - [RD3. Data Colletion](#)
 - [Categorize](#)
 - [RD4. Triage](#)
 - [3. Analyze](#)
 - [Workflow](#)
 - [RA1. Verify](#)
 - [RA2. Identify type of Ransom](#)
 - [RA4. Assess if the Threat Actor is still in the Network](#)
 - [RA6. Do We Have Backup?](#)
 - [RA8. Is the infected environment \(AD\) trusted by other environment?](#)
 - [RA10. Identify Threat Actor/Ransomware Family.](#)
 - [RA11. Identify Affected Systems Type](#)
 - [RA12. Do We Pay the Ransom?](#)
 - [RA14. Was Data Exfiltrated?](#)
 - [RA15. Were All Endpoints and Data Identified?](#)
 - [RA16. Update Scope](#)
 - [RA17. Scope Validation](#)
 - [RA18. External Help](#)
 - [RA19. Technical Help](#)
 - [RA21. Legal Help](#)
 - [RA23. Root Cause Analysis](#)
 - [RA24. Send Communication](#)
 - [4. Contain / Eradicate](#)
 - [Workflow](#)
 - [RC1. Block Systems to Systems Communications](#)
 - [RC2. Stop Backups](#)
 - [RC3. Powerdown NON Encrypted Systems](#)

- [RC4. Disconnect Share Drives](#)
- [RC5. Malware Infection](#)
- [RC6. Active Directory Clean Up](#)
- [RC7. Monitor Closely](#)
- [RC9. New IOC Discovered](#)
- [5. Recover](#)
 - [Workflow](#)
 - [RR1. Update Defenses](#)
 - [RR2. Change All Passwords](#)
 - [RR3. Remove](#)
 - [RR4. Rebuild Systems](#)
 - [RR5. Restore Data](#)
- [6. Post Incident](#)
 - [Workflow](#)
 - [RP1. Incident Review](#)
 - [RP2. Update Mode of Operations](#)
 - [RP3. Review Defensive Posture](#)
 - [RP4. Update & Upgrade Defenses](#)
 - [RP5. Build New Detection](#)
 - [RP6. Modify Base Images](#)
 - [RP7. User Awareness Training](#)
 - [RP9. Calculate Incident's Cost](#)
- [References](#)

Scope

This Playbook covers various type of Ransom we could be faced with. The most common being Ransomware but we try to also account for other types.

It was built to be run in parallele with the [Malware Playbook](#) and possibly the [Critical Playbook](#)

1. Preparation

▼ Expand/Colapse

- Create and maintain a list of
 - all domains owned by Company.
 - This can prevent you from taking actions against our own domains
 - all people of can register domains
- Create email template
 - to notify all employees of ongoing phishing campaing against the organization
 - to contact hosting companies for domain take down
 - to inform 3rd party to take actions against phishing on there infra (Microsoft, Fedex, Apple, etc.)
- Ensure that:
 - Mail anti-malware/anti-spam/anti-phish solutions are in place.
 - Users know how to report phish
 - Detection exists for office documents spawning processes
 - PowerShell
 - CMD
 - WMI
 - MSHTA
 - Etc.
- Perform Firedrill to ensure all aspects of the Playbook are working
 - After publication
 - At least once a year
 - Test/Validate:
 - [Customer's Cards](#)
 - Internal Contact and Escalation Paths
- Review threat intelligence for
 - threats to the organisation,
 - brands and the sector,
 - common patterns
 - newly developing risks and vulnerabilities
- Ensure appropriate access to any necessary documentation and information, including out-of-hours access, for the following
 - IR Playbgnns to highlight information security risks faced by employees, including:
 - Phishing attacks and malicious emails;
 - Ransomware;
 - Reporting a suspected cyber incident.

Tool Access and Provisioning

Tool1

Please referer to [Tool1 Documentation](#)

Tool2

Please referer to [Tool2 Documentation](#)

Assets List

- A list of assets and owner should exists and be available for the following
 - Customers Assets
 - Owners
 - Contacts
 - Pre authorized actions
 - Company Assets (Including all filiale and business units)
 - Owners
 - Contacts
 - Administrators
 - Pre authorized actions
- Type of assets inventory needed
 - Endpoints
 - Servers
 - Network Equipements
 - Security Appliances
 - Network Ranges
 - Public
 - Private
 - VPN / Out of Band
 - Employees
 - Partners
 - Clients

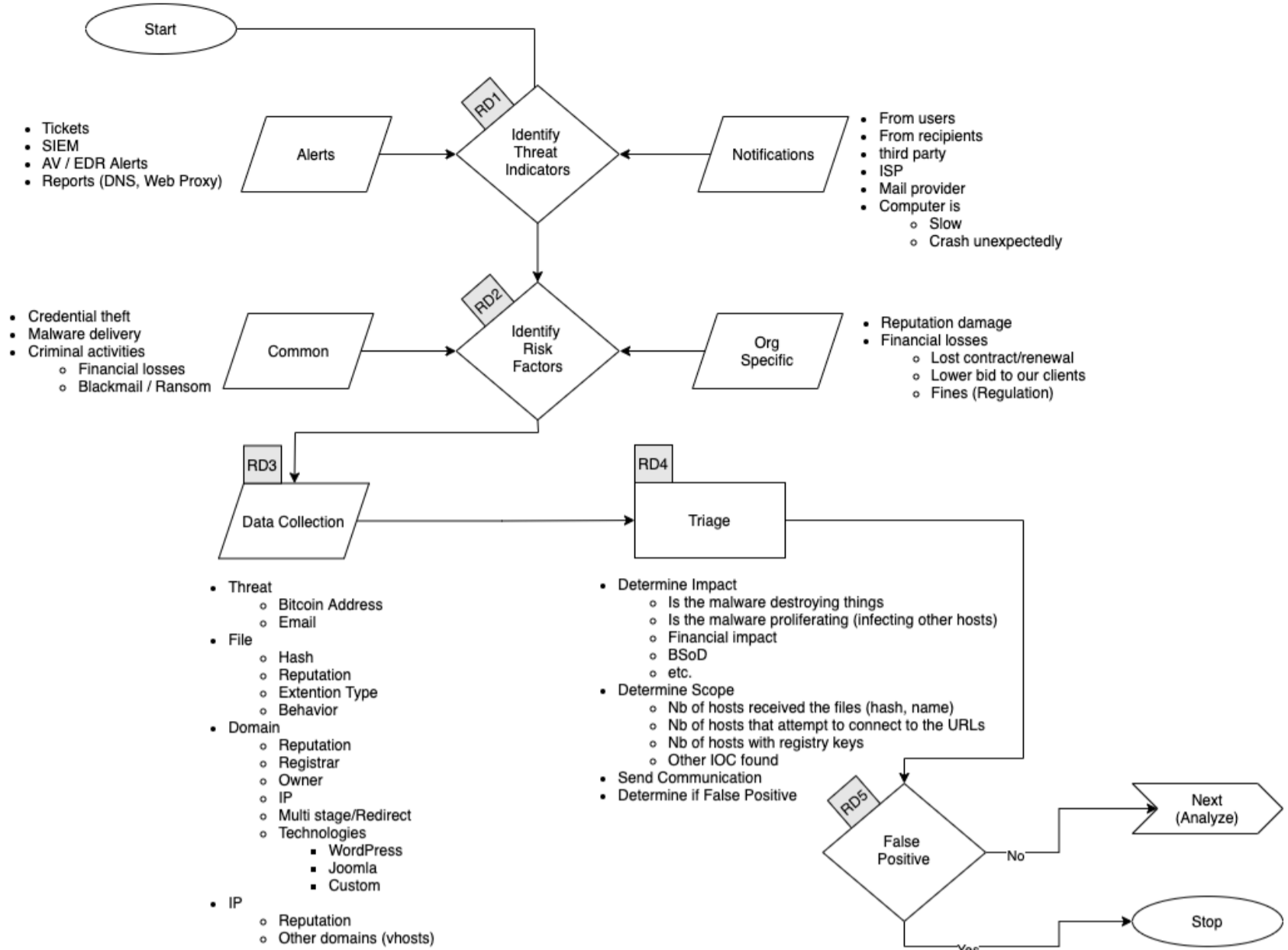
2. Detect

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Ransom - Detect



RD1. Identify Threat Indicators

▼ Expand/Colapse

Alerts

Alerts are generated by different systems owned by the Security/SOC team. The main sources for alerts are

- Tickets
- SIEM
- Anti-Virus / EDR
- Reports
 - DNS
 - Web Proxy
- Errors from mail servers

Notifications

Notifications are coming from external sources usually via email, Teams or phone. The main sources for notifications are

- Users (internal)
- Recipients of emails (external)
- Third Parties
- ISP
- Mail Providers

RD2. Identify Risks Factors

▼ Expand/Colapse

Common

- Credential Theft
- Malware Delivery
- Criminal Activities
 - Blackmail / Ransom

Company Specific

- Financial Losses
 - Lost of contrat
 - Contract not renewed
 - Lower bid to our clients
 - Fines
 - Regulation

RD3. Data Colletion

This section describe the information that should be collected and documented about the incident
 There is a lot of ressources to help you with that phase [here](#)

▼ Expand/Colapse

Domains

- Reputation
- Registrar
- Owner
- IP
- Multistage / Redirect
- Technologies of the site
 - WordPress
 - Joomla
 - Custom Page (credential phish)

IP

- Reputation
- Owner
- Geo Localisation
- Other domains on that IP

Categorize

▼ Expand/Colapse Determine type of

RD4. Triage

▼ Expand/Colapse Determine

- Impact
 - Of
 - Financial
 - Data loss
- Scope (Nb of people)

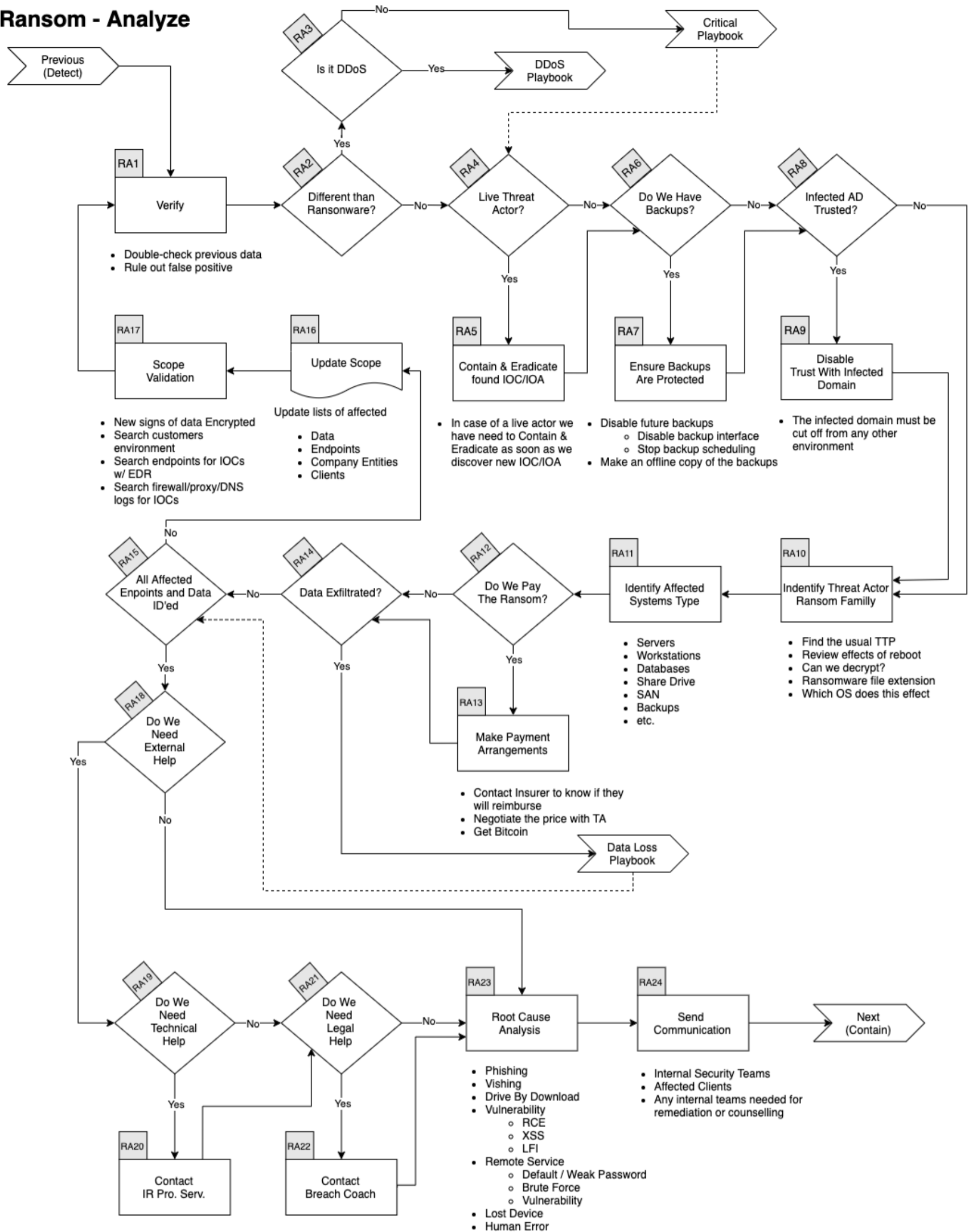
3. Analyze

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Ransom - Analyze



RA1. Verify

▼ Expand/Collapse

In conjunction with a senior member of the SOC

- Double check previous data
- Rule out False Positive

RA2. Identify type of Ransom

▼ Expand/Collapse

The first thing we need to do is understand which type of Ransom we are dealing with.

- Is this a Ransomware?
- Is this a DDoS related Ransom?
 - For now, we do not have a DDoS Playbook, so referer to the [Critical Playbook](#)

If it's another type, you should follow the [Critical Playbook](#) and escalate to the SOC and/or Security management.

RA4. Assess if the Threat Actor is still in the Network

▼ Expand/Colapse

Depending if the actor has successfully encrypted the data or if they are still actively trying, the speed at which we must act is different.

If the actor is still in the network, the containment effort needs to be taken as fast as possible and the Contain & Eradicate actions will be intertwined with the Analysis.

RA6. Do We Have Backup?

▼ Expand/Colapse

If we have backups, we must make sure they are protected and not overwritten. Here's some of the steps that needs to be taken:

- Disable future backups
 - Disable backup Interface
 - Stop backup scheduling
- Make an offline copy of the backup

RA8. Is the infected environment (AD) trusted by other environment?

▼ Expand/Colapse

In order to prevent the adversaries to reach other domains that could be linked, we need to

- Disable any Trust from that domain to others
- In some cases, we might need to disconnect the MPLS Link
 - This needs management approval (refer to the [Critical Playbook](#))

RA10. Identify Threat Actor/Ransomware Family

▼ Expand/Colapse

Using the various artefacts, we need to identify who our adversary is. This will help

- Know the TTP they typically use
- Potentially identify the Initial Access technique
- Understand how they move laterally
 - WMI
 - PSEXEC
 - RDP
 - Etc.
- Understand the effect of a reboot on the machine
- Is there a known decryptor
 - This is increasingly less frequent
- Which OS version are targeted

Things that we can use to identify the adversary:

- Ransomware note
- Malware payload
- Encrypted file extensions
- Email / Web portal
- Bitcoin addresses
- etc.

RA11. Identify Affected Systems Type

▼ Expand/Colapse

In order to remediate properly and engage the right team(s) we need to understand which type of systems were affected:

- Servers
 - OS version
 - Kernel
- Workstations
 - OS version
 - Service Pack
- Databases
- Share Drives
- SAN
- Backups
- Etc.

RA12. Do We Pay the Ransom?

▼ Expand/Colapse

Depending on the state of the backups, the type of devices that was encrypted, we might need to pay the ransom.

NOTE: This decision must be taken by the Board (or the client(s)), but we are here to help advice.

Here are some things to think about if we decide to pay:

- Will the insurer cover/reimburse?
- Most of threat actors are open to negotiation and we should **always** negotiate the price down
- We need to get Bitcoin on a trusted exchange

RA14. Was Data Exfiltrated?

▼ Expand/Collapse

If data was exfiltrated we need to refer to the [Data Loss Playbook](#)

RA15. Were All Endpoints and Data Identified?

▼ Expand/Collapse

If we have found new affected endpoints or data go to the next section.

If we have identified all endpoints and data you can jump to [Do we need external help](#)

- Update FW, IDS, etc. rules w/ IOCs
- Search endpoints for IOCs w/ EDR

RA16. Update Scope

▼ Expand/Collapse

- Update lists of
 - affected endpoints
 - affected Company Entities
 - affected clients

RA17. Scope Validation

▼ Expand/Collapse

Have all the machines been identified? If you find further traces of phishing or new IOCs go back through this step.

When you are done identifying all compromised:

- Hosts
- Data

You can continue to the next phase.

RA18. External Help

▼ Expand/Collapse

Does Company have all the knowledge and resources to handle the crisis alone?

RA19. Technical Help

▼ Expand/Collapse

The Incident Commander can reach out to a 3rd Party Incident Responder

- xxxx@yyyy.com
- 555-555-1212

RA21. Legal Help

▼ Expand/Collapse

If there are legal implications such as

- GDPR
- Criminal Charges
- Regulation
- Laws

The Incident Commander can reach out to a Breach Coach / Cyber Insurer

- aaa@bbb.com
- 555-555-1212

RA23. Root Cause Analysis

▼ Expand/Collapse

Identify how this incident happened.

- Phishing Emails
- Voice Phishing
- Drive-by Download
- Vulnerability
 - Remote Code Execution
 - Cross-Site Scripting
- Remote Services
 - Default / Weak Password
 - Brute Force
 - Vulnerability
- Lost Device
- Human Error

RA24. Send Communication

▼ Expand/Colapse

Contact any relevant of the following party

- Internal Security Team
- Affected Clients
- Any internal teams needed for remediation or counselling

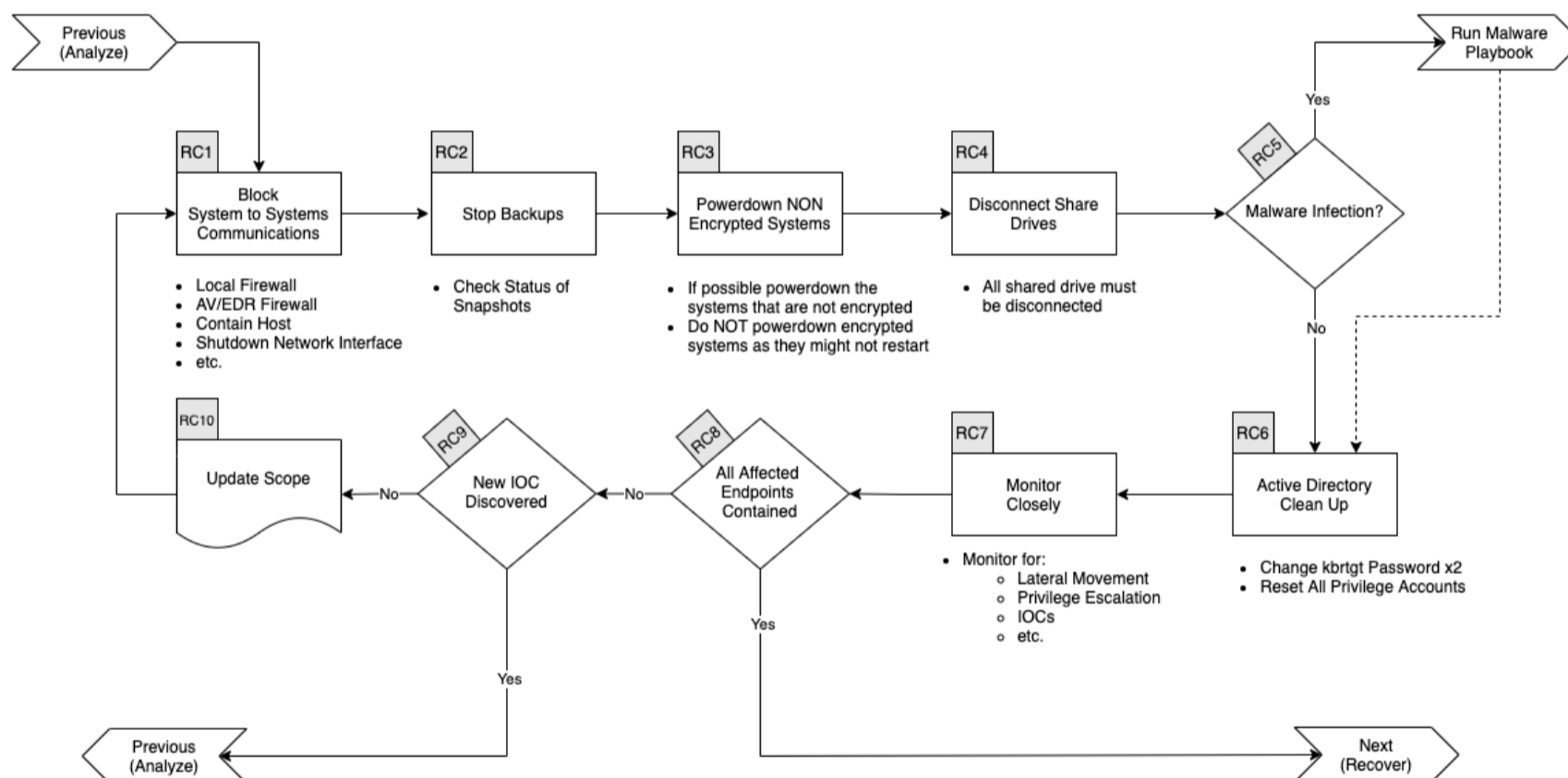
4. Contain / Eradicate

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Ransom - Contain / Eradicate



RC1. Block Systems to Systems Communications

▼ Expand/Colapse

The first things we need to do with ransomware is to block systems to systems communication. We can do this using various methods such as: - EDR containment function - Local Firewall - This could be circumvented if the adversary is still on the system - AV/EDR Firewall - Shutdown Network Interface - This mostly apply to VM - Disable the switch port on the router - Etc.

RC2. Stop Backups

▼ Expand/Colapse

- Check status of Snapshots

RC3. Powerdown NON Encrypted Systems

▼ Expand/Colapse

- If possible powerdown the systems that are not encrypted
- Do NOT powerdown encrypted systems as they might not restart

RC4. Disconnect Share Drives

- ▼ Expand/Colapse
 - All shared drive must be disconnected

RC5. Malware Infection

- ▼ Expand/Colapse
 - If there is a Malware infection run the [Malware Playbook](#)

RC6. Active Directory Clean Up

- ▼ Expand/Colapse
 - In most cases these actions should be sufficient:

- Change kbrtgt Password twice
- Reset All Privilege Accounts

In cases where we believe Domain Admin account(s) were compromised we have to do the following **before** the steps above:

- Restore the AD from backup that predate the initial compromised
- If no backup exists:
 - Consider rebuilding the AD from scratch.
 - Change how we protect sensitive Accounts

The decision to rebuilt from strach should come from the higher management of the Global-Security Team or of the client's security team.

RC7. Monitor Closely

- ▼ Expand/Colapse
 - Monitor for:
 - Lateral Movement
 - Privilege Escalation
 - IOCs
 - etc.

RC9. New IOC Discovered

- ▼ Expand/Colapse
 - Go back to [Ransom Analyze](#)

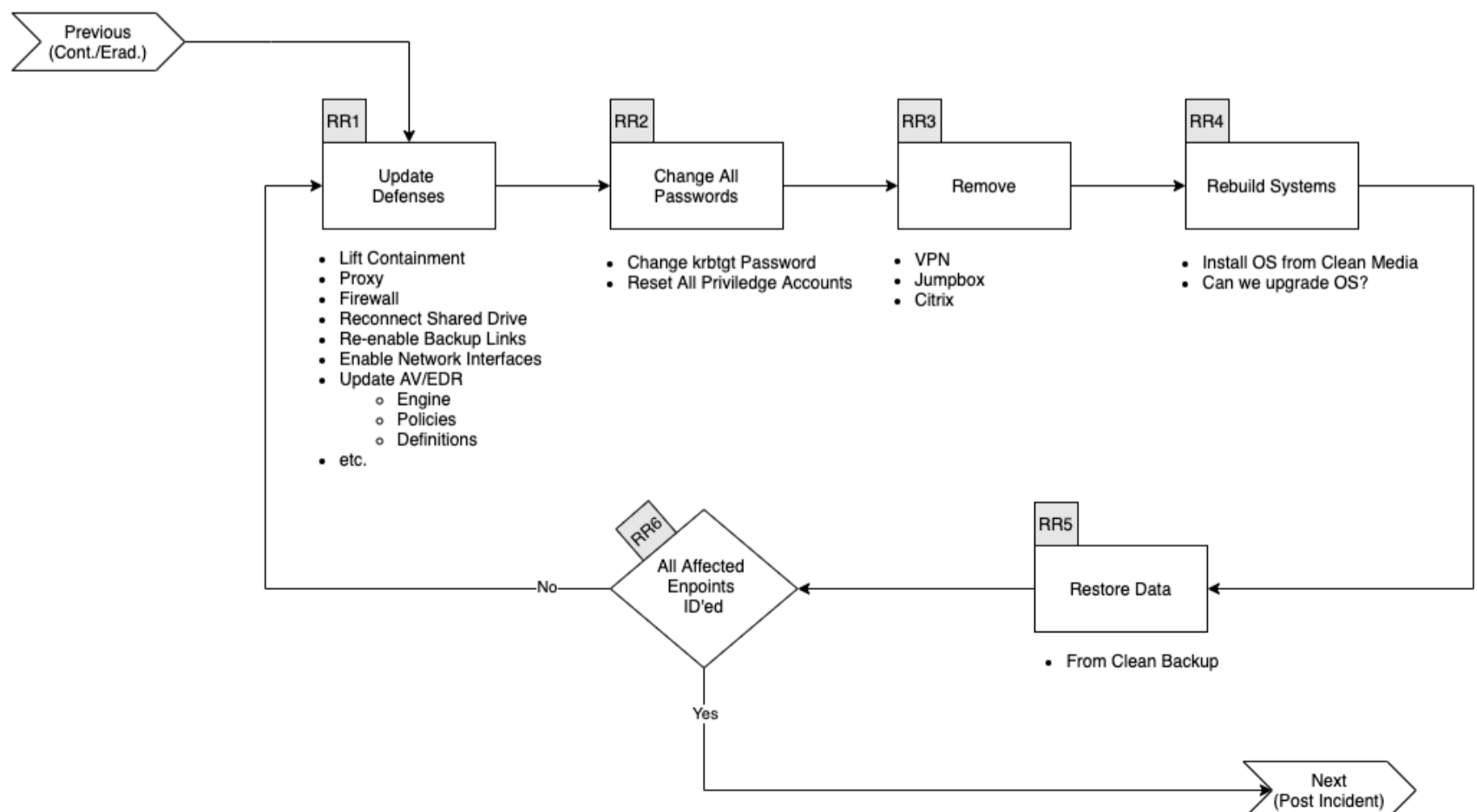
5. Recover

- ▼ Expand/Colapse

Workflow

- ▼ Expand/Colapse

Ransom - Recover



RR1. Update Defenses

▼ Expand/Colapse

Determine which of the following actions need to be performed:

- Lift Containment
- Proxy Block
- Firewall Rules
- Reconnect Shared Drives
- Re-enable Backup Links
- Enable Network Interfaces
- Update EDR/AV
 - Engine
 - Policies
 - Definitions

RR2. Change All Passwords

▼ Expand/Colapse

- Change krbtgt Password
- Reset All Priviledge Accounts

RR3. Remove

▼ Expand/Colapse

- VPN
- Jumpbox
- Citrix

RR4. Rebuild Systems

▼ Expand/Colapse

- Install OS from Clean Media
- Can we upgrade OS?

RR5. Restore Data

▼ Expand/Colapse

- Use a clean backup

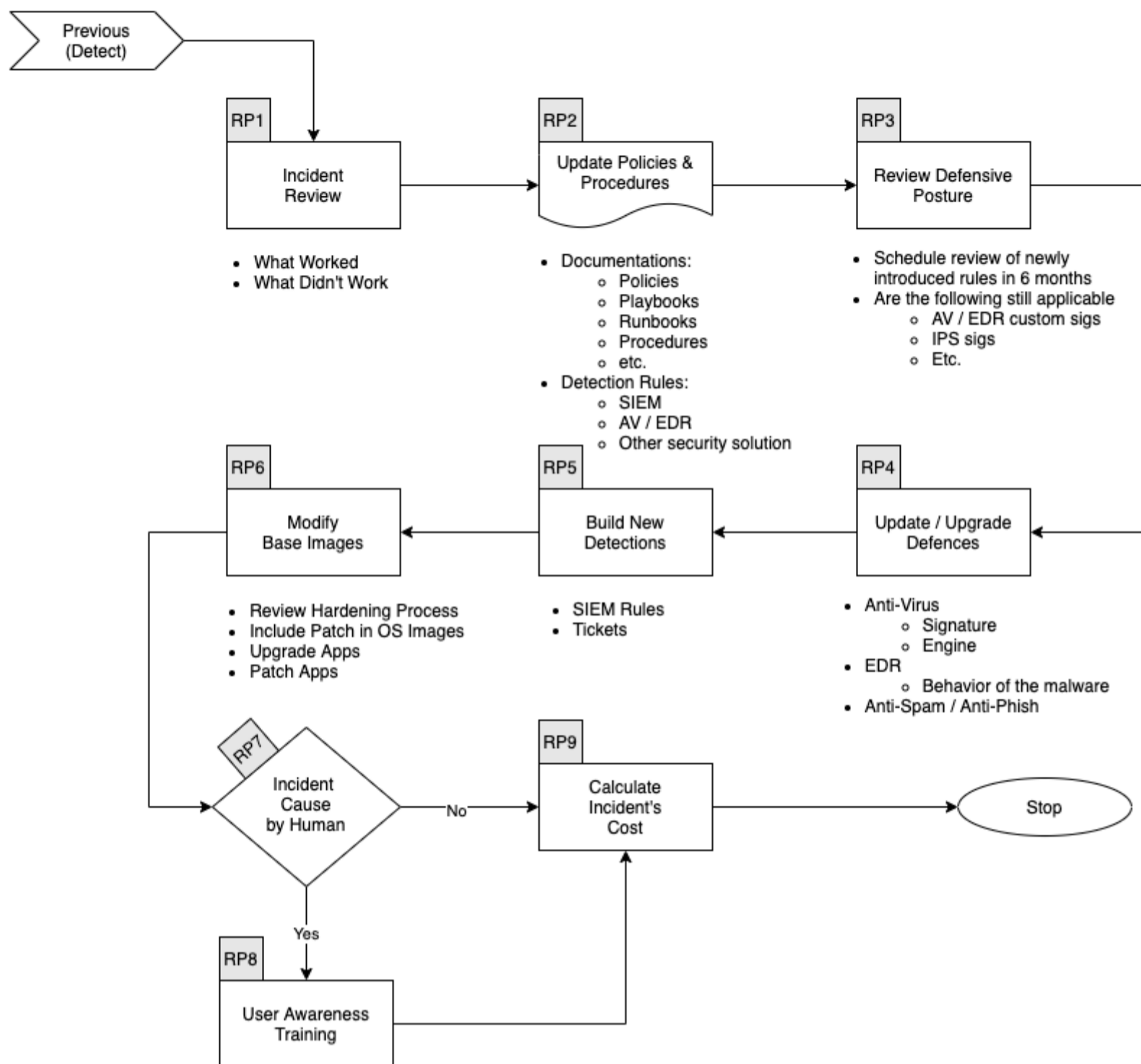
6. Post Incident

▼ Expand/Colapse

Workflow

▼ Expand/Colapse

Ransom - Post Incident



RP1. Incident Review

- ▼ Expand/Colapse
 - What worked
 - What didn't work

RP2. Update Mode of Operations

- ▼ Expand/Colapse
 - Update the following documents as required:

- Policies
- Processes
- Procedures
- Playbooks
- Runbooks

Update Detetion Rules in:

- SIEM
- Anti-Spam
- Malware Gataway
- EDR
- Other security solution

RP3. Review Defensive Posture

- ▼ Expand/Colapse
 - Schedule review of newly introduced rules in6 months
 - Are the following still applicatble
 - Firewall Rules
 - Proxy Rules for C2
 - AV / EDR custom Signatures

- IPS Signatures

RP4. Update & Upgrade Defenses

▼ Expand/Colapse

Various security solutions might need to be updated or upgraded to prevent a similar incident from occurring again.

Here are a few items to consider:

- Anti-Virus
 - Signatures
 - Engine
- EDR
 - Behaviour (TTP)
 - Custom Detection
- Anti-Spam
 - Filter
- Anti-Phishing

RP5. Build New Detection

▼ Expand/Colapse

If the incident was detected late in the Kill Chain, we need to try to improve our detection to catch a similar incident earlier.

We could for instance:

- Create SIEM rules
- Generate SNOW tickets
- Create Miro Plays
- etc.

RP6. Modify Base Images

▼ Expand/Colapse

If the Ransom was caused by a lack of hardening or sufficient patch level:

- Review hardening processes
- Include critical patches in base Images
- etc.

RP7. User Awareness Training

▼ Expand/Colapse

If the incident was caused by a human error

- Create / Select new mandatory training
 - From Security Education Vendor
 - From Youtube video
 - Built by internal teams

RP9. Calculate Incident's Cost

▼ Expand/Colapse

Calculate the incident's Cost

- Time Spent
- Ransom paid
- Downtime
- Fines / Penalties
- etc.