**Account Compromised Playbook**

**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**

**Summary**

- Create and maintain a list of

- all domains owned by Organisation.

- 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 campaign against the organisation

- to contact hosting organisation for domain(s) take down

- to inform 3rd party to take actions against phishing on their infra (Microsoft, Amazon, 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 dry drill to ensure all aspects of the Playbook are working

- After publication

- At least once a quarter

- Test/Validate:

- Internal Contact and Escalation Paths

- Review threat intelligence for

- threats to the organisation,

- trends for 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**

**Tools**

Please referrer to [DCOT Handbook]

**Assets List**

- A list of assets and owner should exist and be available for the following

- Customers Assets

- Owners

- Contacts

- Pre approved/authorized actions

- Organisation Assets

- Owners

- Contacts

- Administrators

- Pre approved/authorized actions

- Type of assets inventory needed

- Endpoints

- Servers

- Network Equipment

- Security Appliances

- Network Ranges

- Public

- Private

- VPN / Out of Band

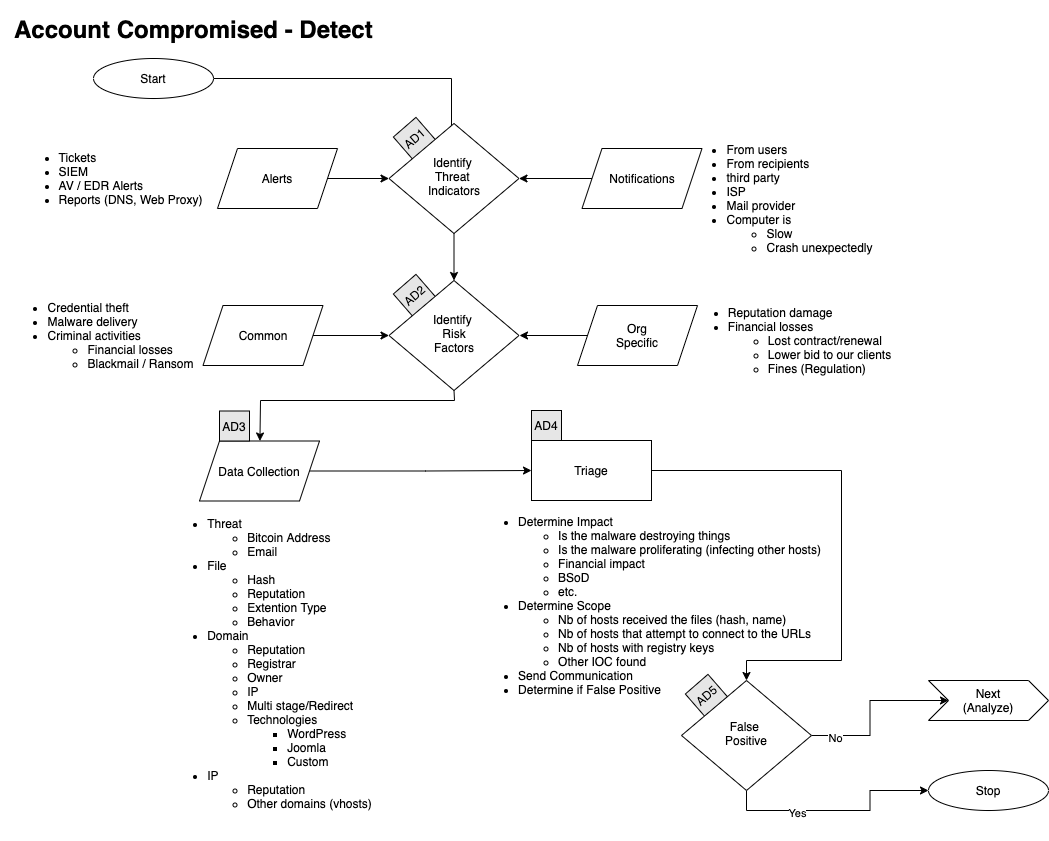
- Employees

- Partners

- Clients

**2. Detect**

**Workflow**



**Identify Threat Indicators**

**Alerts**

Alerts are be generated by different systems. 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**

**Common**

- Credential Theft

- Malware Delivery

- Criminal Activities

- Blackmail / Ransom

**Organisation 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.

**Domains**

- Reputation

- Registrar

- Owner

- IP

- Multistage / Redirect

- Technologies of the site

- WordPress

- Joomla

- Custom Page (credential phish)

**Intellectual Property**

- Reputation

- Owner

- Geo Localisation

- Other domains on that IP

**Categorize**

**Determine type of**

**Triage**

**Determine**

- Impact

- Of

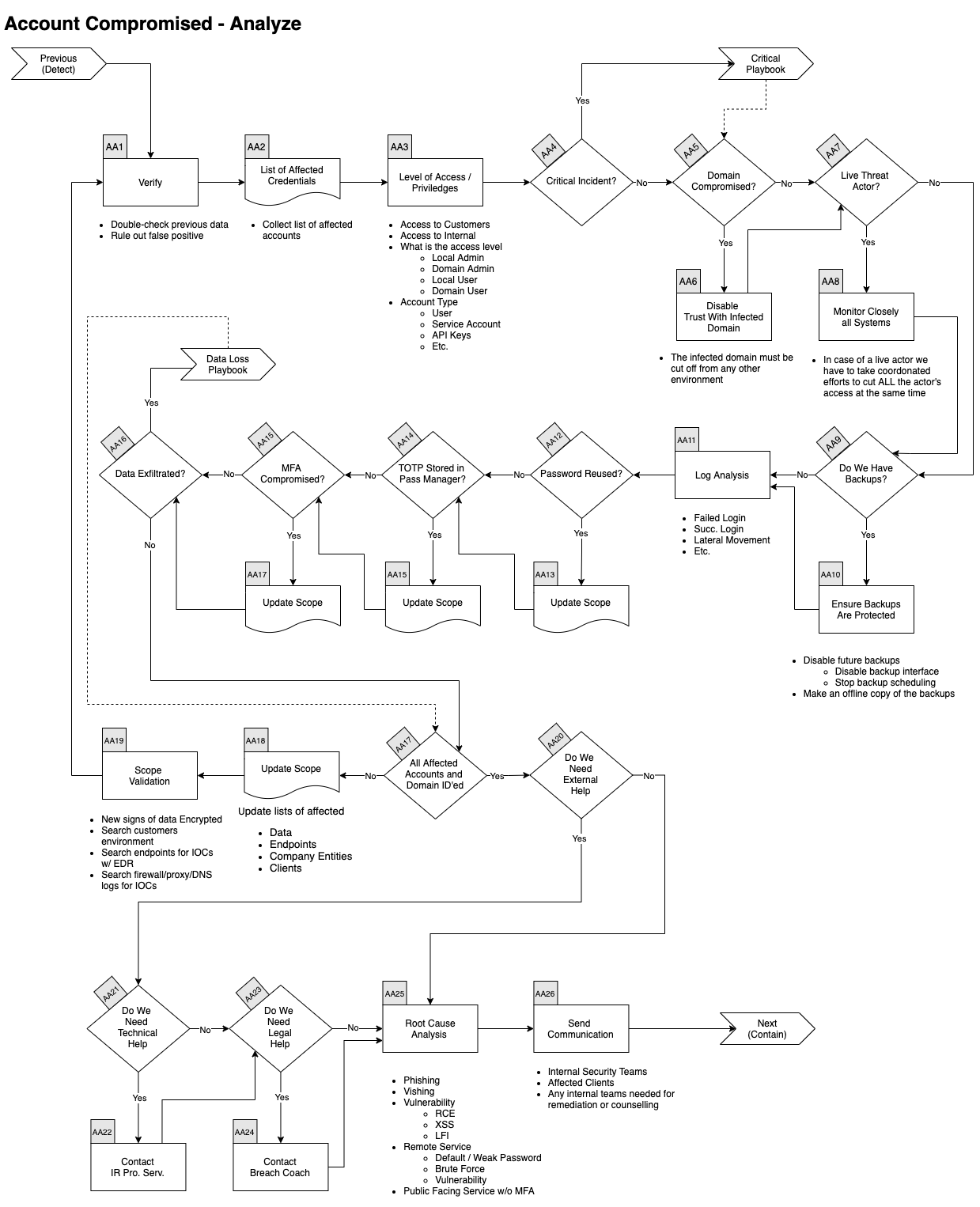
- Financial

- Data loss

- Scope (Nb of people)

**3. Analyse**

Workflow



**Verify**

In conjunction with a senior member of the DCOT

- Double check previous data

- Rule out False Positive

**List Compromised Credentials**

**In the Compromised Assets TAB of the Event Log list:**

- Compromised accounts

- Compromised machines

- Compromised domains

**Level of Access / Privileges**

In conjunction with a senior member of the DCOT

- Double check previous data

- Rule out False Positive

**Update Scope**

- Update lists of

- affected endpoints

- affected Company Entities

- affected clients

**Scope Validation**

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

And investigated all:

- URLs

- Domains

- IP

- Ports

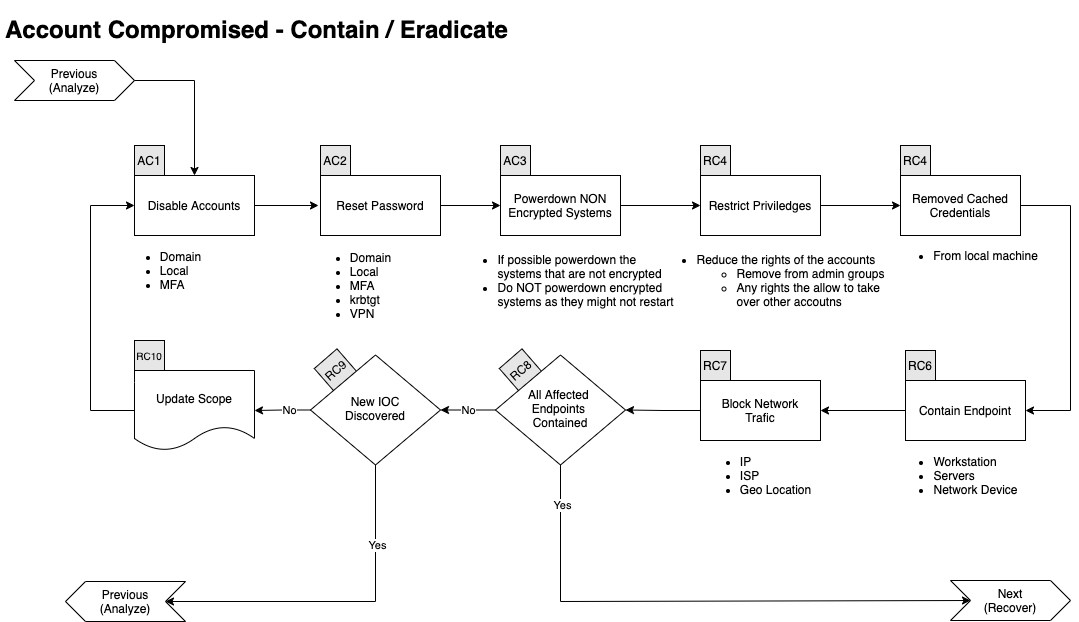
- Files

- Hash

Go to the next phase **Contain/Eradicate**

**Contain / Eradicate**

**Workflow**

**Block**

- Update FW, Proxy, etc. rules

- Blackhole DNS

- Submit to Partners

- AV/EDR Vendor

- Web Filter Vendor

- etc.

**Validate User's Actions**

**Malware Infection**

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**

- Monitor for

- Related incoming messages

- Internet connections to IOC

- New files that matches hashes identified

**All Affected Endpoints Contained**

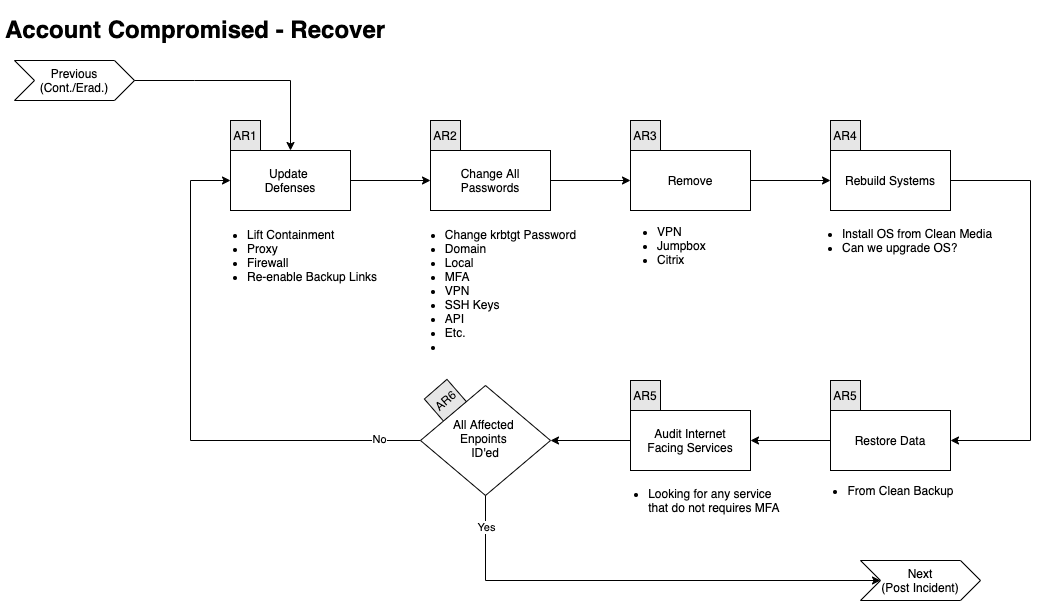
If all affected endpoints have been contained, you can go to the next phase, otherwise continue below.

**New IOC Discovered**

If there was new IOC discovered, go back to the **Analyse Phase.**

**Recover**

**Workflow**

 **Update Defences**

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**

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

**Validate Countermeasures**

Determine if legitimate elements are blocked by:

- Proxy

- Firewall

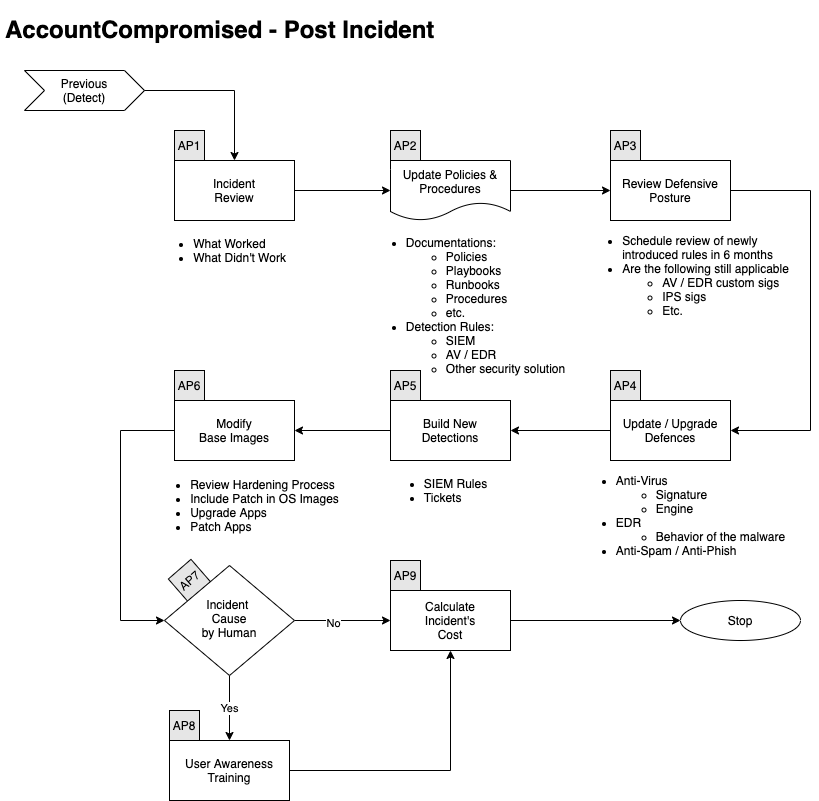
- EDR

If so, go back to **Update Defences.**

Otherwise go to the next phase **Post Incident.**

**Post Incident**

**Workflow**



**Incident Review**

- What worked

- What didn't work

**Update Mode of Operations**

**Update the following documents as required:**

- Policies

- Processes

- Procedures

- Playbooks

- Runbooks

**Update Detection Rules in:**

- SIEM

- Anti-Spam

- Malware Gateway

- EDR

- Other security solution

**Review Defensive Posture**

- Schedule review of newly introduced rules in6 months

- Are the following still applicable

- Firewall Rules

- Proxy Rules for C2

- AV / EDR custom Signatures

- IPS/IDS Signatures

**User Awareness Training**

**References**

This Playbook was built using the following references:

https://www.dfir.training/index.php?option=com\_jreviews&format=ajax&url=media/download&m=14tt1&1600804844570

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf