INCIDENT RESPONSE WORKFLOWS (SCENARIOS & EXAMPLES)

BY IZZMIER IZZUDDIN

General

1. Preparation

- List of all assets
  - Servers
  - Endpoints
  - 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

- Gathering of information
- Analysing 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

3. Containment, Eradication, and Recovery

- 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 learn
- New detection
- New hardening
- New patch management

1. Account Compromised

Scenario: An employee's email account has been compromised, leading to unauthorized access to sensitive data and potential further infiltration into the network.

Incident Response Analysis

1. Preparation

List of All Assets

Servers

- **Web Server**: Hostname: web01, IP: 192.168.1.10, OS: Ubuntu 20.04
- **Database Server**: Hostname: db01, IP: 192.168.1.20, OS: MySQL 8.0
- **Email Server**: Hostname: mail01, IP: 192.168.1.30, OS: Exchange Server 2019

Endpoints

- **Workstations**: 50 Windows 10 PCs
- **Laptops**: 20 MacBook Pros
- **Mobile Devices**: 10 iPhones, 10 Android devices

Networks

- **Corporate Network**: 192.168.0.0/16
- **Guest Network**: 172.16.0.0/16
- **DMZ**: 10.0.0.0/24

Applications

- **CRM**: Salesforce
- **ERP**: SAP
- **Office Suite**: Microsoft Office 365
- **Communication**: Slack, Zoom

Employees

- **Total Employees**: 150
- **Key Roles**: IT Admins, HR, Finance, Sales, Executives

Security Products

- **Antivirus**: Symantec Endpoint Protection

- **Firewall**: Cisco ASA 5500
- **SIEM**: Splunk
- **IDS/IPS**: Snort
- **MFA**: Duo Security

Baselines

- **Normal Network Traffic**: Defined and documented with Splunk
- **System Performance Metrics**: Established benchmarks for CPU, memory, and disk usage
- **User Behaviour**: Normal login times, locations, and activities

Communication Plan

- **Incident Response Team**: Defined roles and contact info for all members
- **Internal Notifications**: Procedures for informing executives, IT staff, and affected users
- **External Notifications**: Criteria for informing customers, partners, and regulatory bodies

Security Events

- **Authentication Failures**
- **Unusual Login Locations**
- **Unauthorized Access Attempts**
- **Data Exfiltration Attempts**
- **Privilege Escalation Attempts**

Thresholds

- **Login Failures**: More than 5 failed logins within 10 minutes
- **Unusual Locations**: Logins from unrecognized countries
- **Data Transfer**: Uploads exceeding 1 GB from a single user

Access to Security Tools

- **Provision Access**: Procedures for granting and revoking access to security tools like Splunk, Duo, Snort
- **Documentation**: User guides and training materials for security tools

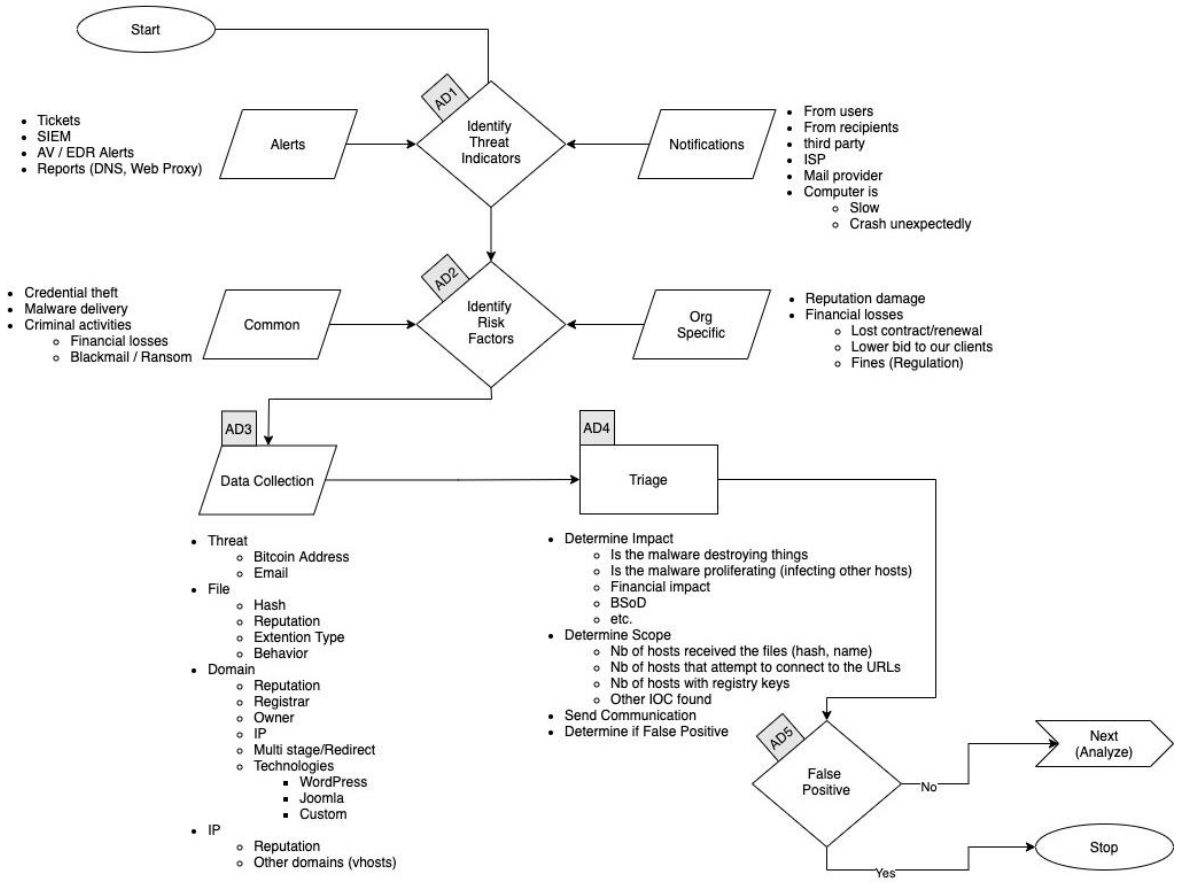
Create Playbooks

- **Account Compromise**: Step-by-step actions for detection, containment, and recovery
- **Malware Infection**: Procedures for identification and removal
- **Data Breach**: Steps for notification, containment, and legal compliance

Plan Exercises

- **Tabletop Exercises**: Quarterly simulations of common incidents
- **Hands-On Drills**: Annual red team/blue team exercises

2. Detect



Gathering of Information

- **Logs**: Authentication logs, access logs, and network traffic logs from Splunk
- **Alerts**: Review alerts from SIEM, IDS/IPS, and antivirus
- **User Reports**: Analyse reports from users about suspicious activity

Logs

Authentication Log Extracts:

2024-06-01 09:12:34,auth,login,failed,user=jdoe,ip=192.168.1.50

2024-06-01 09:12:37,auth,login,failed,user=jdoe,ip=192.168.1.50

2024-06-01 09:12:40,auth,login,failed,user=jdoe,ip=192.168.1.50

2024-06-01 09:12:43,auth,login,success,user=jdoe,ip=192.168.1.50

2024-06-01 10:05:12,auth,login,success,user=jdoe,ip=203.0.113.25

2024-06-01 10:07:45,auth,login,failed,user=jdoe,ip=203.0.113.25

Email Server Log:

2024-06-01
10:05:14,email,send,success,user=jdoe,to=malicious@example.com,subject=Confidential Data,ip=203.0.113.25

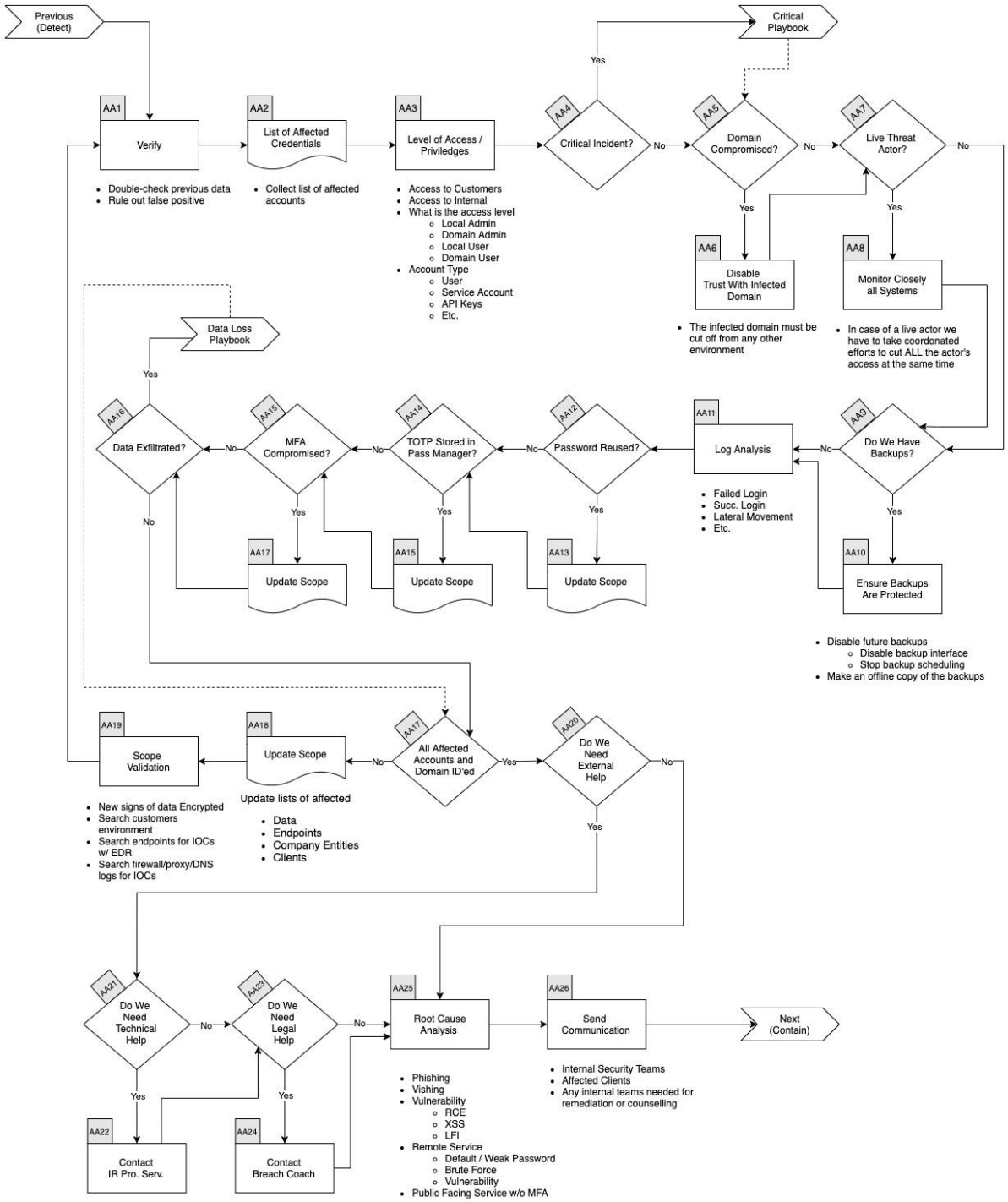
2024-06-01
10:10:22,email,send,failed,user=jdoe,to=malicious@example.com,subject=Further Info,ip=203.0.113.25

Firewall Log:

2024-06-01
10:05:13,firewall,allow,source_ip=203.0.113.25,dest_ip=192.168.1.30,port=443

2024-06-01
10:07:47,firewall,deny,source_ip=203.0.113.25,dest_ip=192.168.1.20,port=3306

3. Analyse



Analyse Data

- **Login Attempts**: Multiple failed login attempts followed by a successful login from an internal IP, then an unusual login from an external IP.
- **Geolocation**: The external IP (203.0.113.25) is from an unrecognized location.
- **Access Patterns**: Email account used to send sensitive information to an external address.

Building Detections

- **Custom SIEM Rules**: Create rules to flag logins from unusual locations, rapid login failures followed by success, and large data transfers.
- **Behavioural Analysis**: Monitor deviations from normal login locations and times.

Root Cause Analysis

- **Initial Point of Compromise**: Likely a phishing attack that obtained the user's credentials.
- **Affected Accounts**: User jdoe's email account is compromised.

Depth and Breadth of the Attack

- **Admin Rights**: Check if jdoe has any administrative privileges (confirmed: no admin rights).
- **Affected Systems**: Email server primarily affected, attempted access to the database server.

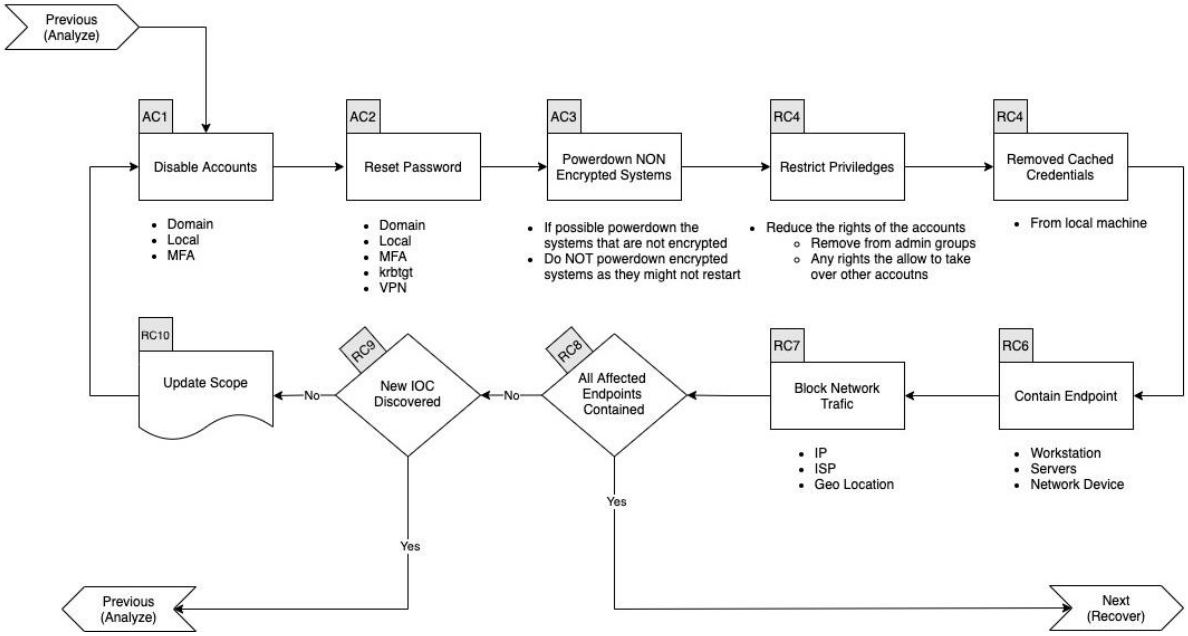
Techniques Used

- **Phishing**: Possible credential theft via a phishing email.
- **Unauthorized Access**: Use of stolen credentials to access email.

Indicators of Compromise / Indicators of Attack

- **Tactics, Techniques, and Procedures (TTP)**: Use of compromised credentials to access email and send sensitive data.
- **IP Addresses**: Malicious activity from IP 203.0.113.25.
- **Email Addresses**: Email sent to malicious@example.com.

4. Contain / Eradicate



Isolate Affected Systems

- **Immediate Isolation**: Disable user jdoe's email account.
- **Quarantine**: Block IP 203.0.113.25 at the firewall.

Patch Threat Entry Point

- **Update Software**: Ensure email server is up to date with the latest security patches.
- **Change Credentials**: Force a password reset for user jdoe and all employees as a precaution.

Predefined Threshold

- **For Customers**: Notify any customers whose data may have been affected.
- **For Internal Systems**: Escalate to the IT security team.
- **For Escalations**: Involve higher management and, if necessary, external cybersecurity consultants.

Preauthorized Actions

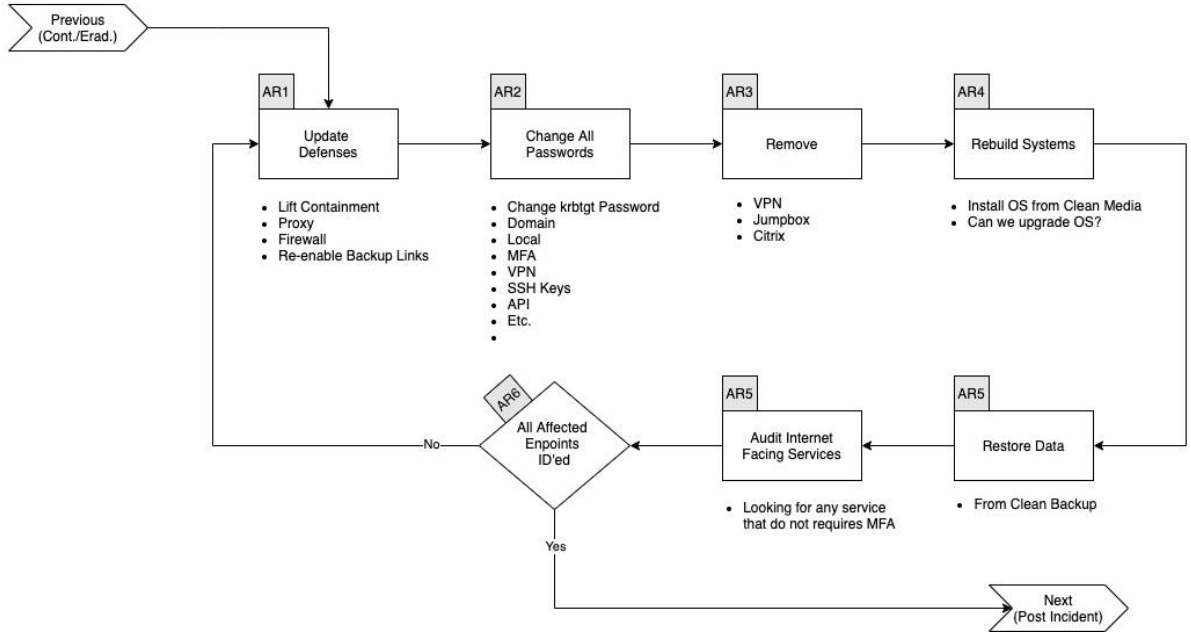
- **Per Customers**: Execute predefined response actions such as notifying customers and providing support.
- **Per Environment**: Differentiate actions for production and other environments.

How to Remove the Threat on All Affected Systems

- **Antivirus Scans**: Run comprehensive scans on all endpoints.

- **Manual Inspection**: Conduct manual checks on critical systems.

5. Recover



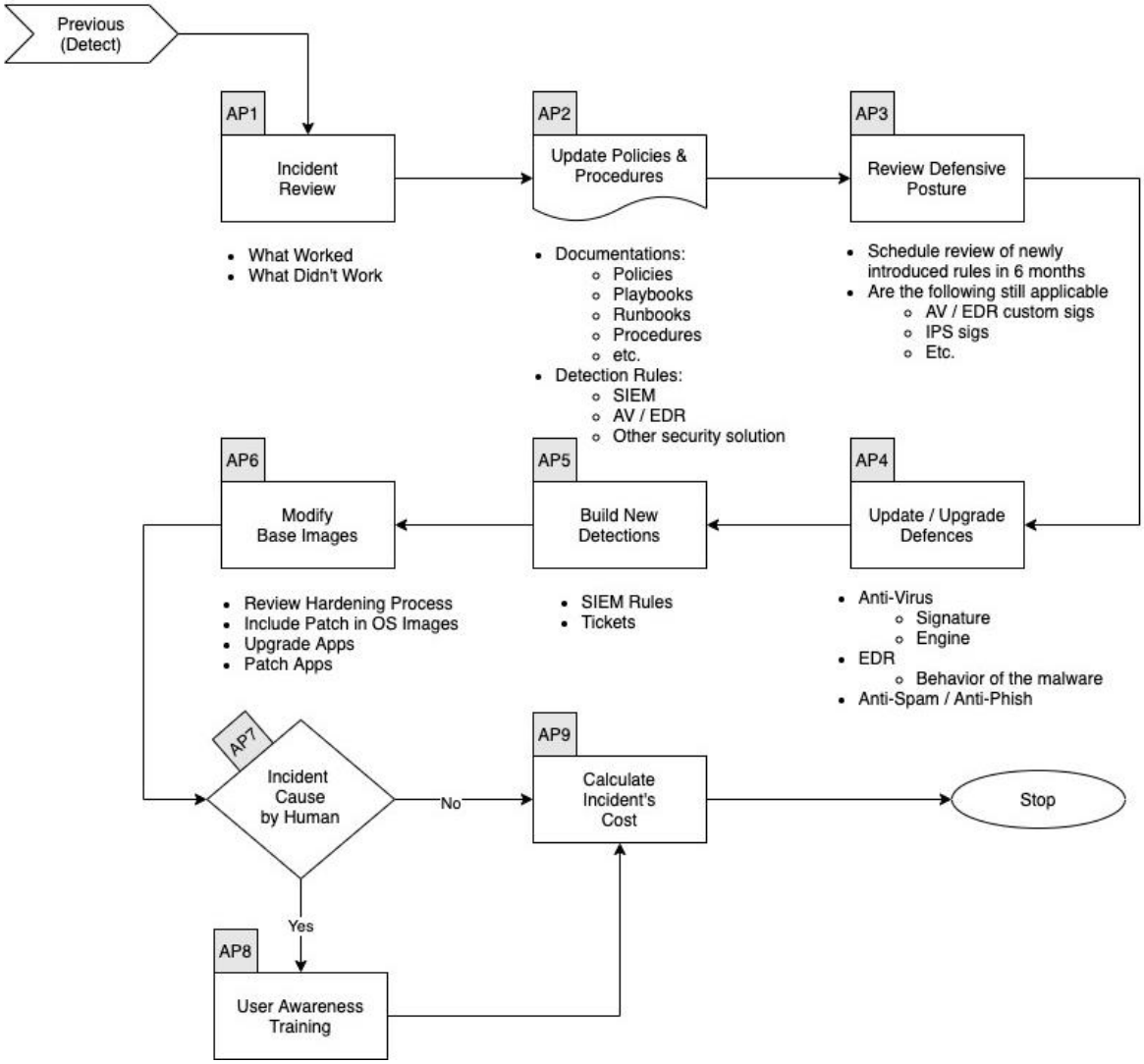
Get Systems Operational

- **Restore Services**: Ensure the email server and other systems are free of threats and restore normal operations.
- **Monitoring**: Implement heightened monitoring for any signs of residual threats.

Rebuild and Resume Service

- **Reimage Systems**: Rebuild systems from clean backups if necessary.
- **Verification**: Verify the integrity and security of all restored systems.

6. Post Incident



Lessons Learned

- **Review**: Conduct a post-mortem analysis to identify what worked and what didn't.
- **Documentation**: Update incident response documentation with new insights.

New Detection

- **Enhance Monitoring**: Improve detection rules and monitoring based on the incident analysis.
- **Training**: Provide additional training to staff based on lessons learned.

New Hardening

- **Security Enhancements**: Implement new security measures such as stronger MFA, improved email filtering.

- **Policy Updates**: Revise security policies to address gaps identified during the incident.

New Patch Management

- **Regular Updates**: Ensure all systems are regularly updated with the latest patches.
- **Automated Deployment**: Implement automated patch management solutions to reduce manual effort and errors.

2. Data Loss

Scenario: Sensitive data from the company's financial database was found to be exfiltrated by an unauthorized external entity.

Incident Response Analysis

1. Preparation

List of All Assets

Servers

- **Web Server**: Hostname: web01, IP: 192.168.1.10, OS: Ubuntu 20.04
- **Database Server**: Hostname: db01, IP: 192.168.1.20, OS: MySQL 8.0
- **Email Server**: Hostname: mail01, IP: 192.168.1.30, OS: Exchange Server 2019

Endpoints

- **Workstations**: 50 Windows 10 PCs
- **Laptops**: 20 MacBook Pros
- **Mobile Devices**: 10 iPhones, 10 Android devices

Networks

- **Corporate Network**: 192.168.0.0/16
- **Guest Network**: 172.16.0.0/16
- **DMZ**: 10.0.0.0/24

Applications

- **CRM**: Salesforce
- **ERP**: SAP
- **Office Suite**: Microsoft Office 365
- **Communication**: Slack, Zoom

Employees

- **Total Employees**: 150
- **Key Roles**: IT Admins, HR, Finance, Sales, Executives

Security Products

- **Antivirus**: Symantec Endpoint Protection

- **Firewall**: Cisco ASA 5500
- **SIEM**: Splunk
- **IDS/IPS**: Snort
- **MFA**: Duo Security

Baselines

- **Normal Network Traffic**: Defined and documented with Splunk
- **System Performance Metrics**: Established benchmarks for CPU, memory, and disk usage
- **User Behaviour**: Normal login times, locations, and activities

Communication Plan

- **Incident Response Team**: Defined roles and contact info for all members
- **Internal Notifications**: Procedures for informing executives, IT staff, and affected users
- **External Notifications**: Criteria for informing customers, partners, and regulatory bodies

Security Events

- **Authentication Failures**
- **Unusual Login Locations**
- **Unauthorized Access Attempts**
- **Data Exfiltration Attempts**
- **Privilege Escalation Attempts**

Thresholds

- **Login Failures**: More than 5 failed logins within 10 minutes
- **Unusual Locations**: Logins from unrecognized countries
- **Data Transfer**: Uploads exceeding 1 GB from a single user

Access to Security Tools

- **Provision Access**: Procedures for granting and revoking access to security tools like Splunk, Duo, Snort
- **Documentation**: User guides and training materials for security tools

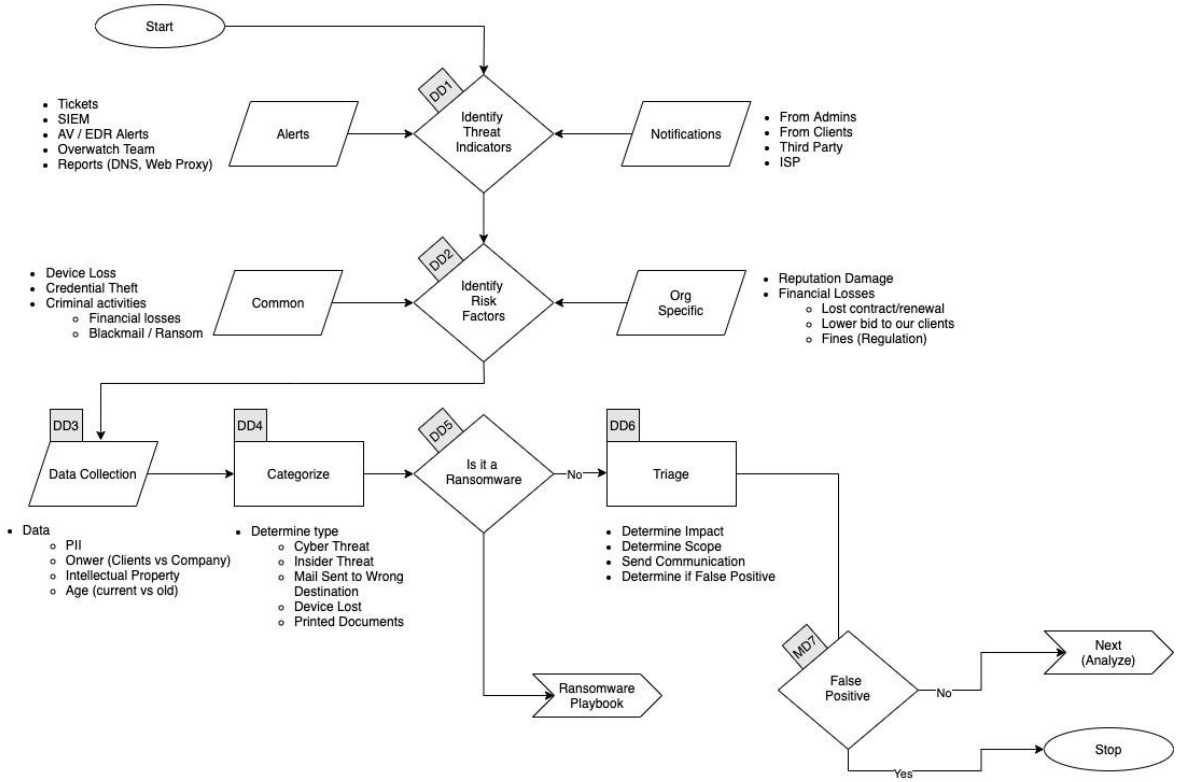
Create Playbooks

- **Account Compromise**: Step-by-step actions for detection, containment, and recovery
- **Malware Infection**: Procedures for identification and removal
- **Data Breach**: Steps for notification, containment, and legal compliance

Plan Exercises

- **Tabletop Exercises**: Quarterly simulations of common incidents
- **Hands-On Drills**: Annual red team/blue team exercises

2. Detect



Gathering of Information

- **Logs**: Authentication logs, access logs, and network traffic logs from Splunk
- **Alerts**: Review alerts from SIEM, IDS/IPS, and antivirus
- **User Reports**: Analyse reports from users about suspicious activity

Logs

Database Server Access Logs:

2024-06-15 14:35:12,db_access,login,success,user=finance_user,ip=192.168.1.75

2024-06-15 14:45:37,db_access,query,select,table=financial_data,user=finance_user,ip=192.168.1.75

2024-06-15 14:46:02,db_access,export,success,table=financial_data,rows=1000,user=finance_user,ip=192.168.1.75

2024-06-15 15:10:12,db_access,login,failed,user=finance_user,ip=203.0.113.55

2024-06-15 15:12:45,db_access,login,success,user=finance_user,ip=203.0.113.55

2024-06-15 15:20:22,db_access,query,select,table=financial_data,user=finance_user,ip=203.0.113.55

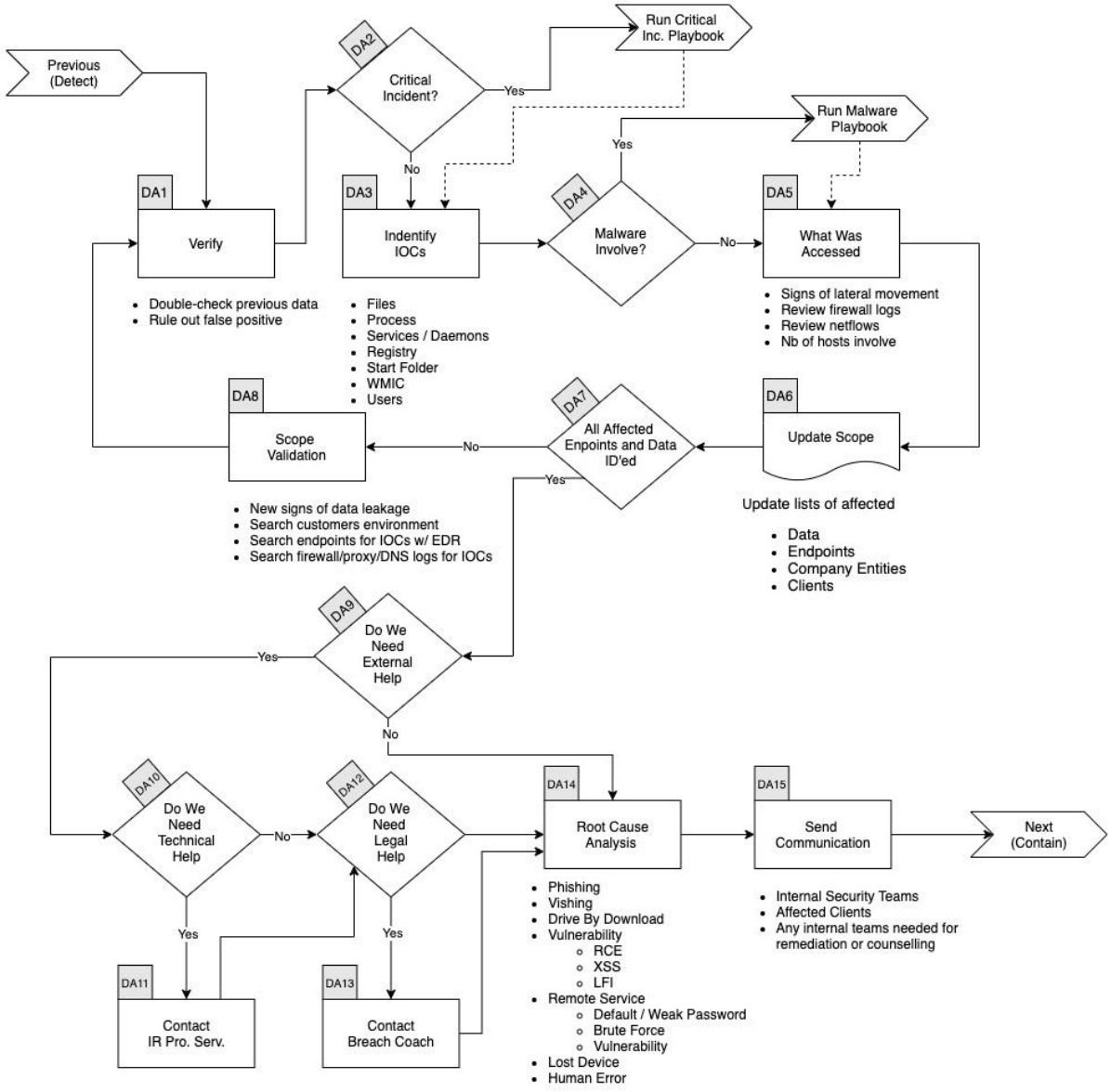
2024-06-15 15:22:10,db_access,export,success,table=financial_data,rows=5000,user=finance_user,ip=203.0.113.55

Firewall Log:

2024-06-15 15:12:46,firewall,allow,source_ip=203.0.113.55,dest_ip=192.168.1.20,port=3306

2024-06-15 15:22:15,firewall,allow,source_ip=203.0.113.55,dest_ip=203.0.113.100,port=443

3. Analyse



Analyse Data

- **Login Attempts**: Multiple successful logins from an internal IP followed by successful login from an external IP.
- **Data Export**: Large volumes of data exported from the financial database.
- **Geolocation**: External IP (203.0.113.55) is from an unrecognized location, suggesting unauthorized access.

Building Detections

- **Custom SIEM Rules**: Create rules to flag large data exports and logins from unusual locations.

- **Behavioural Analysis**: Monitor deviations from normal login patterns and data access behaviours.

Root Cause Analysis

- **Initial Point of Compromise**: Unauthorized access via a compromised user account (finance_user).
- **Affected Accounts**: User finance_user's account is compromised.

Depth and Breadth of the Attack

- **Admin Rights**: Verify if finance_user has any administrative privileges (confirmed: no admin rights).
- **Affected Systems**: Database server primarily affected with unauthorized data export.

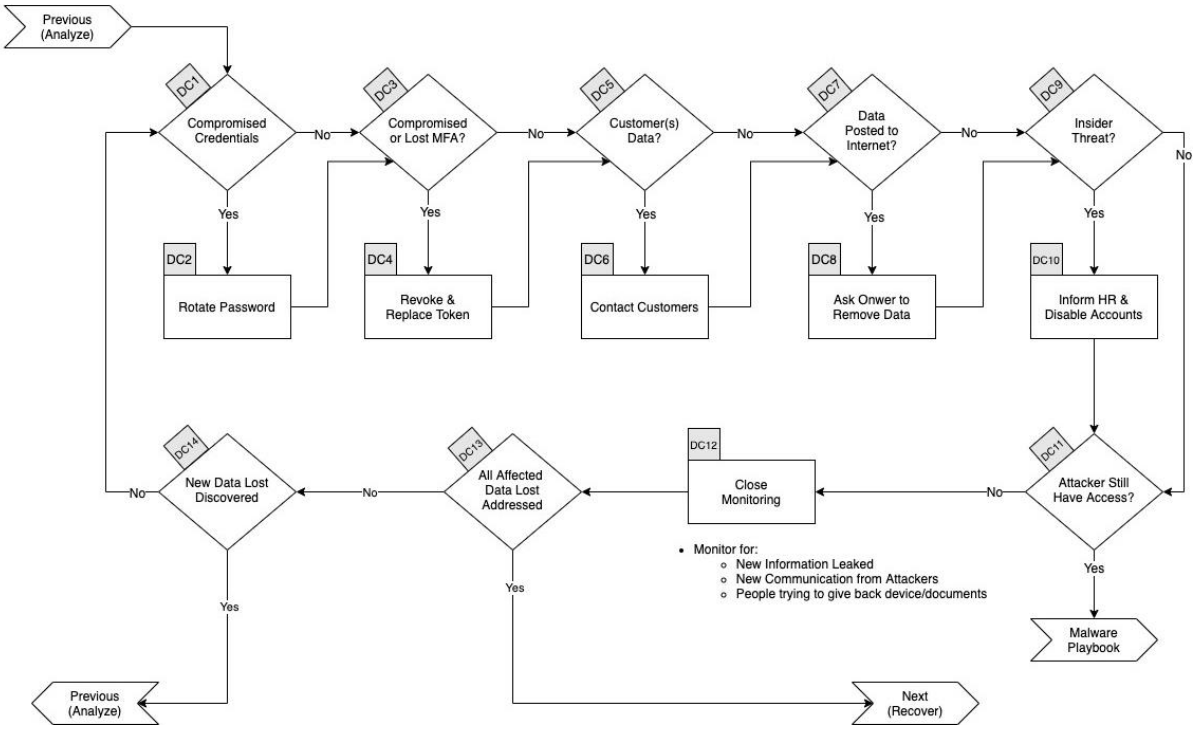
Techniques Used

- **Credential Theft**: Possible phishing attack or credential stuffing leading to unauthorized access.
- **Unauthorized Data Export**: Large-scale export of financial data.

Indicators of Compromise / Indicators of Attack

- **Tactics, Techniques, and Procedures (TTP)**: Use of compromised credentials to access and export sensitive data.
- **IP Addresses**: Malicious activity from IP 203.0.113.55.
- **Command Line**: Unusual command line activity on the database server (if available).

4. **Contain / Eradicate**



Isolate Affected Systems

- **Immediate Isolation**: Disable user finance_user's account.
- **Quarantine**: Block IP 203.0.113.55 at the firewall.

Patch Threat Entry Point

- **Update Software**: Ensure the database server and related applications are up to date with the latest security patches.
- **Change Credentials**: Force a password reset for user finance_user and all employees as a precaution.

Predefined Threshold

- **For Customers**: Notify any customers whose data may have been affected.
- **For Internal Systems**: Escalate to the IT security team.
- **For Escalations**: Involve higher management and, if necessary, external cybersecurity consultants.

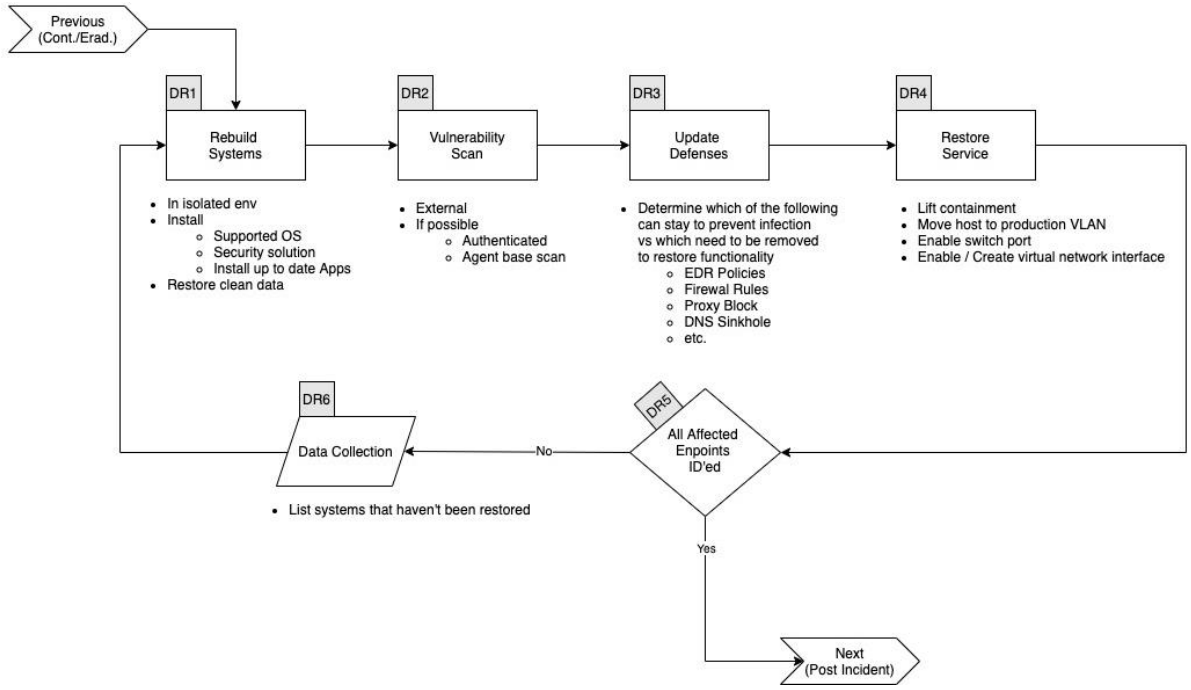
Preauthorized Actions

- **Per Customers**: Execute predefined response actions such as notifying customers and providing support.
- **Per Environment**: Differentiate actions for production and other environments.

How to Remove the Threat on All Affected Systems

- **Antivirus Scans**: Run comprehensive scans on all endpoints.
- **Manual Inspection**: Conduct manual checks on critical systems.

5. Recover



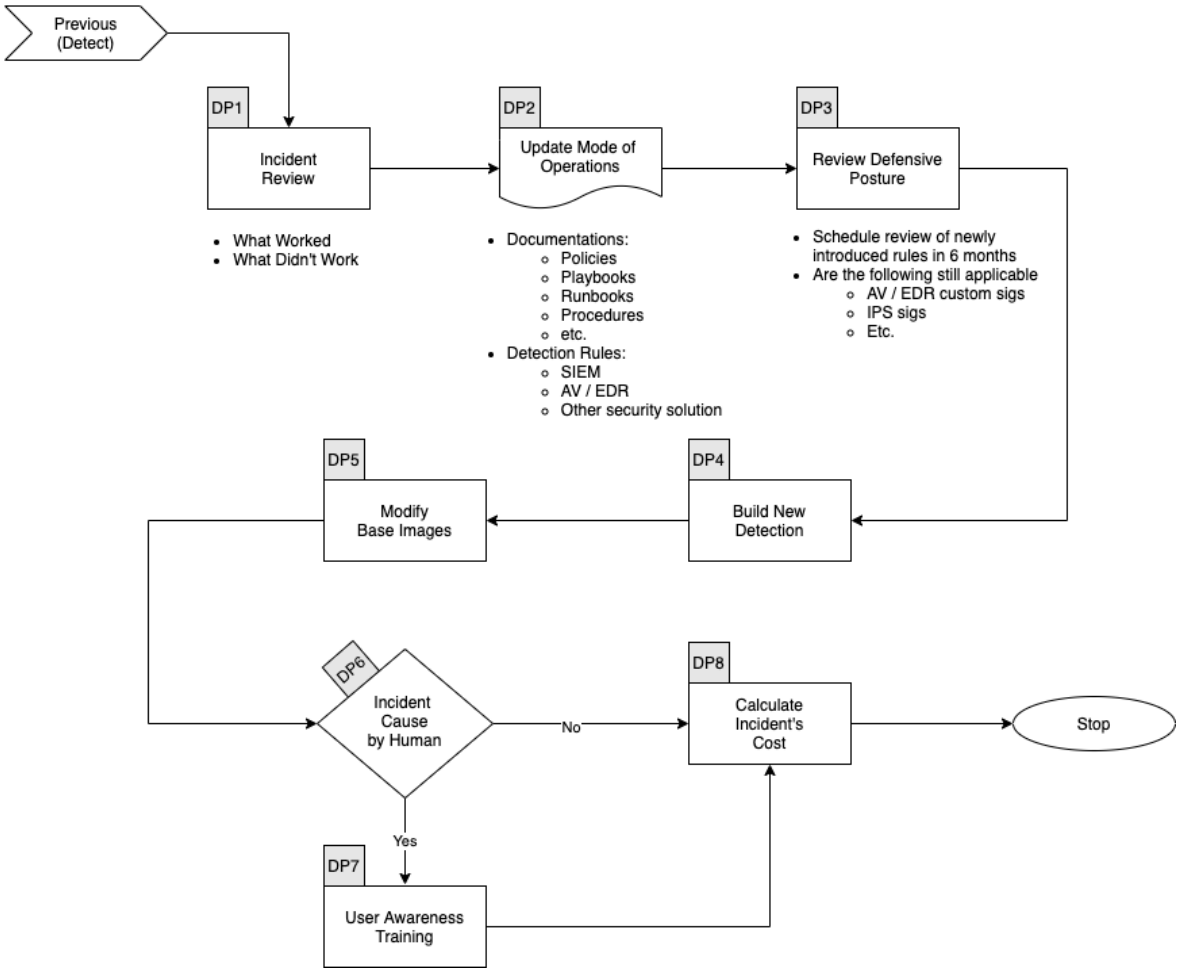
Get Systems Operational

- **Restore Services**: Ensure the database server and other systems are free of threats and restore normal operations.
- **Monitoring**: Implement heightened monitoring for any signs of residual threats.

Rebuild and Resume Service

- **Reimage Systems**: Rebuild systems from clean backups if necessary.
- **Verification**: Verify the integrity and security of all restored systems.

6. Post Incident



Lessons Learned

- **Review**: Conduct a post-mortem analysis to identify what worked and what didn't.
- **Documentation**: Update incident response documentation with new insights.

New Detection

- **Enhance Monitoring**: Improve detection rules and monitoring based on the incident analysis.
- **Training**: Provide additional training to staff based on lessons learned.

New Hardening

- **Security Enhancements**: Implement new security measures such as stronger MFA, improved email filtering.
- **Policy Updates**: Revise security policies to address gaps identified during the incident.

New Patch Management

- **Regular Updates**: Ensure all systems are regularly updated with the latest patches.
- **Automated Deployment**: Implement automated patch management solutions to reduce manual effort and errors.

3. Malware

Scenario: A sophisticated malware infection has been detected on multiple employee workstations, leading to unauthorized access and potential data exfiltration.

Incident Response Analysis

1. Preparation

List of All Assets

Servers

- **Web Server**: Hostname: web01, IP: 192.168.1.10, OS: Ubuntu 20.04
- **Database Server**: Hostname: db01, IP: 192.168.1.20, OS: MySQL 8.0
- **Email Server**: Hostname: mail01, IP: 192.168.1.30, OS: Exchange Server 2019

Endpoints

- **Workstations**: 50 Windows 10 PCs
- **Laptops**: 20 MacBook Pros
- **Mobile Devices**: 10 iPhones, 10 Android devices

Networks

- **Corporate Network**: 192.168.0.0/16
- **Guest Network**: 172.16.0.0/16
- **DMZ**: 10.0.0.0/24

Applications

- **CRM**: Salesforce
- **ERP**: SAP
- **Office Suite**: Microsoft Office 365
- **Communication**: Slack, Zoom

Employees

- **Total Employees**: 150
- **Key Roles**: IT Admins, HR, Finance, Sales, Executives

Security Products

- **Antivirus**: Symantec Endpoint Protection

- **Firewall**: Cisco ASA 5500
- **SIEM**: Splunk
- **IDS/IPS**: Snort
- **MFA**: Duo Security

Baselines

- **Normal Network Traffic**: Defined and documented with Splunk
- **System Performance Metrics**: Established benchmarks for CPU, memory, and disk usage
- **User Behavior**: Normal login times, locations, and activities

Communication Plan

- **Incident Response Team**: Defined roles and contact info for all members
- **Internal Notifications**: Procedures for informing executives, IT staff, and affected users
- **External Notifications**: Criteria for informing customers, partners, and regulatory bodies

Security Events

- **Authentication Failures**
- **Unusual Login Locations**
- **Unauthorized Access Attempts**
- **Data Exfiltration Attempts**
- **Privilege Escalation Attempts**

Thresholds

- **Login Failures**: More than 5 failed logins within 10 minutes
- **Unusual Locations**: Logins from unrecognized countries
- **Data Transfer**: Uploads exceeding 1 GB from a single user

Access to Security Tools

- **Provision Access**: Procedures for granting and revoking access to security tools like Splunk, Duo, Snort
- **Documentation**: User guides and training materials for security tools

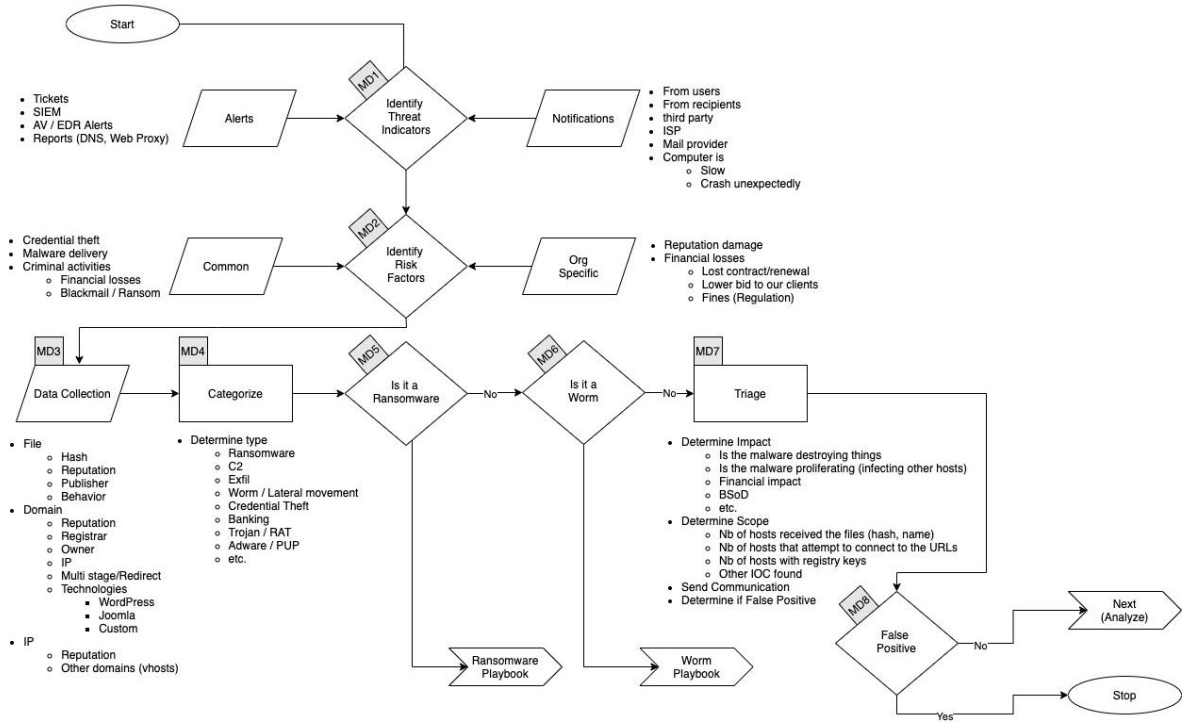
Create Playbooks

- **Account Compromise**: Step-by-step actions for detection, containment, and recovery
- **Malware Infection**: Procedures for identification and removal
- **Data Breach**: Steps for notification, containment, and legal compliance

Plan Exercises

- **Tabletop Exercises**: Quarterly simulations of common incidents
- **Hands-On Drills**: Annual red team/blue team exercises

2. Detect



Gathering of Information

- **Logs**: Authentication logs, access logs, and network traffic logs from Splunk
- **Alerts**: Review alerts from SIEM, IDS/IPS, and antivirus
- **User Reports**: Analyse reports from users about suspicious activity

Logs

Endpoint Antivirus Logs:

2024-06-22 08:32:10,av,alert,malware_detected,threat=Trojan.Generic,action=quarantine,device=192.168.1.50,user=jdoe

2024-06-22 08:35:12,av,alert,malware_detected,threat=Trojan.Generic,action=quarantine,device=192.168.1.51,user=asmith

2024-06-22 08:40:15,av,alert,malware_detected,threat=Ransomware.WannaCry,action=remove,device=192.168.1.52,user=bwong

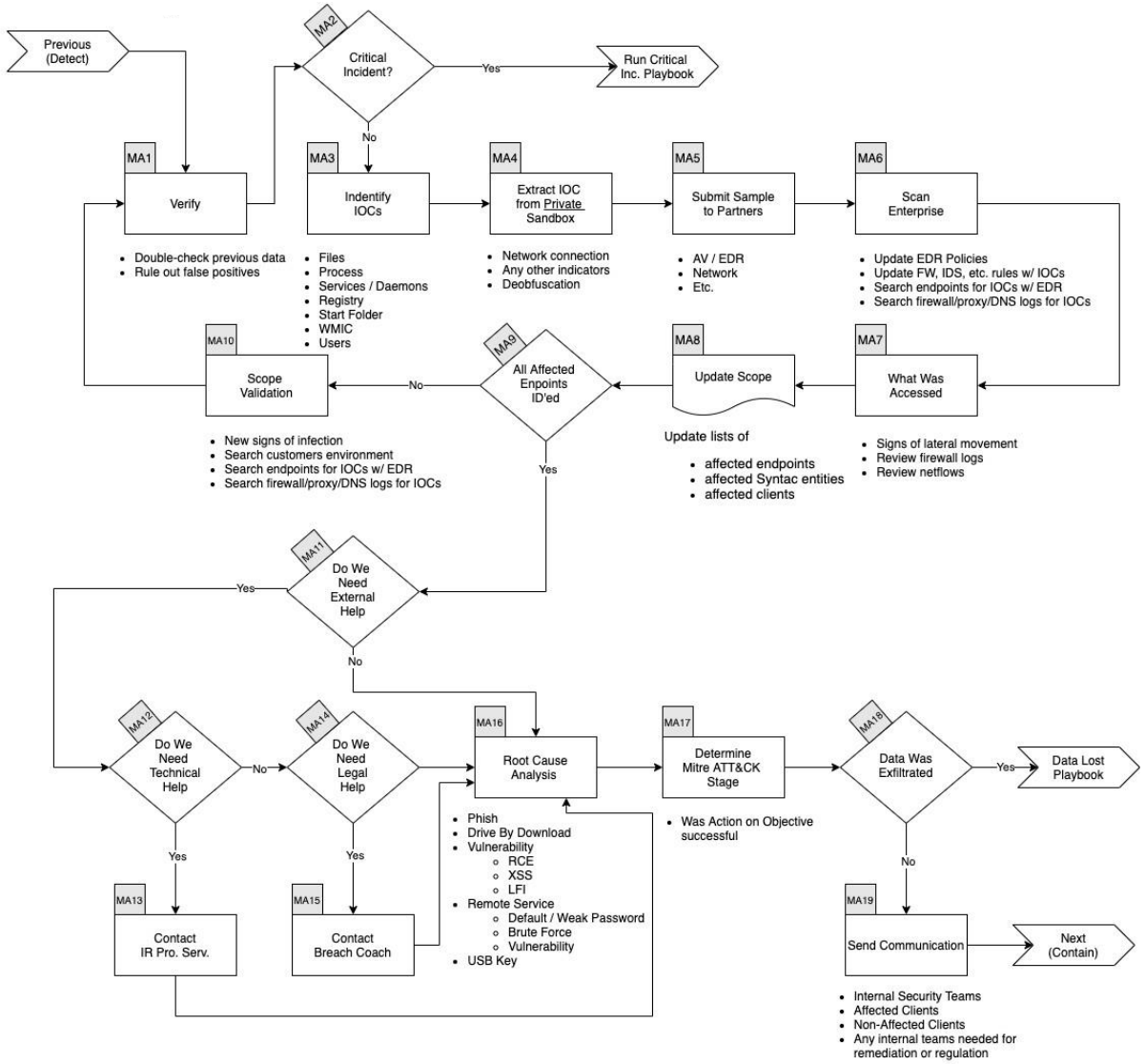
Network Traffic Logs:

2024-06-22 08:32:11,network,connection,allowed,src_ip=192.168.1.50,dst_ip=203.0.113.100,port=80

2024-06-22 08:35:13,network,connection,blocked,src_ip=192.168.1.51,dst_ip=203.0.113.101,port=443

2024-06-22 08:40:16,network,connection,allowed,src_ip=192.168.1.52,dst_ip=203.0.113.102,port=80

3. Analyse



Analyse Data

- **Malware Detection**: Multiple workstations have detected and quarantined malware.
- **Network Activity**: Suspicious outbound connections from infected devices to external IPs.

Building Detections

- **Custom SIEM Rules**: Create rules to flag malware alerts from antivirus logs and unusual outbound traffic.
- **Behavioural Analysis**: Monitor deviations from normal network activity patterns.

Root Cause Analysis

- **Initial Point of Compromise**: Malware likely introduced via a phishing email or malicious download.
- **Affected Accounts**: Users jdoe, asmith, and bwong are affected.

Depth and Breadth of the Attack

- **Admin Rights**: Verify if affected users have administrative privileges (confirmed: no admin rights).
- **Affected Systems**: Multiple workstations with detected malware infections.

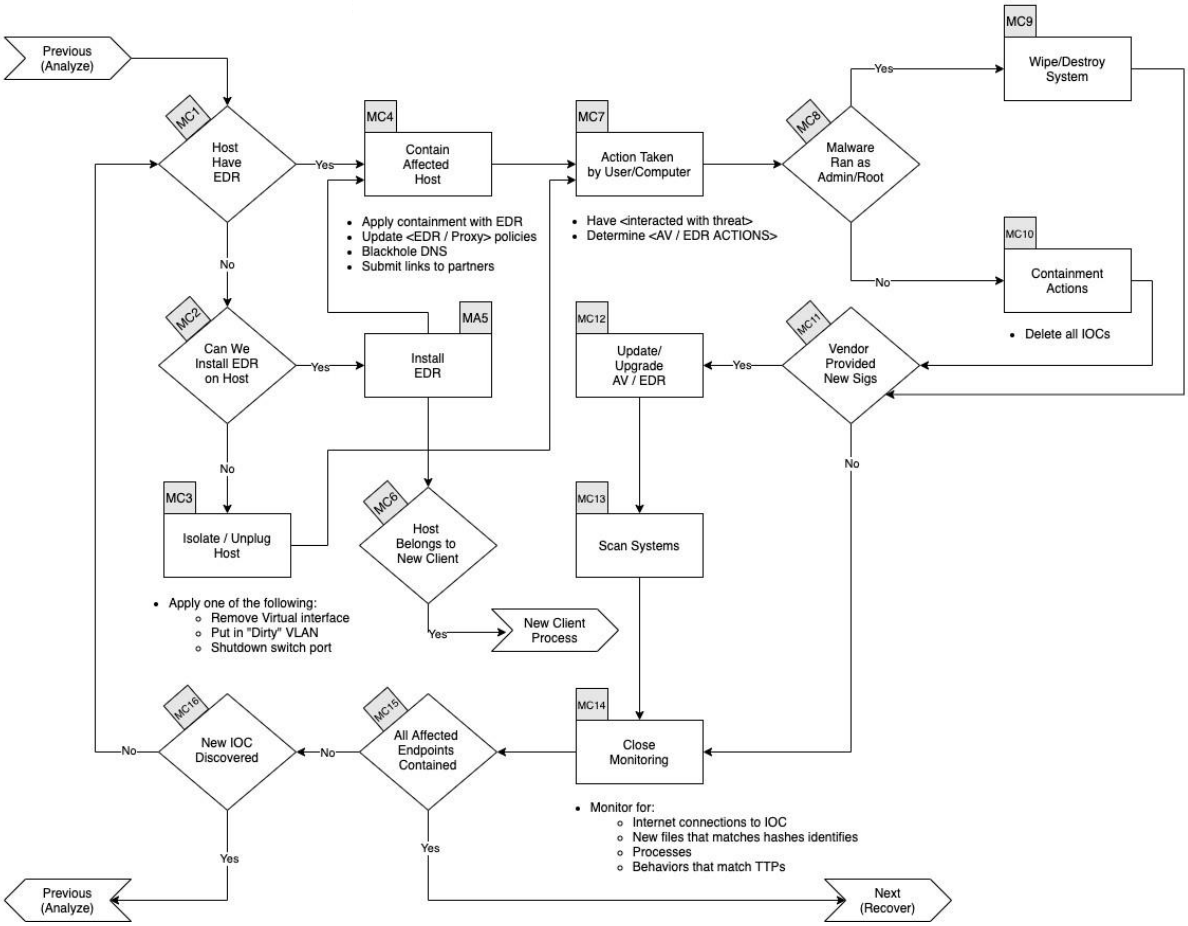
Techniques Used

- **Phishing**: Possible entry point via phishing email.
- **Malware Payload**: Trojan.Generic and Ransomware.WannaCry detected.

Indicators of Compromise / Indicators of Attack

- **Tactics, Techniques, and Procedures (TTP)**: Use of phishing emails to deliver malware payloads.
- **IP Addresses**: Malicious outbound connections to IPs 203.0.113.100, 203.0.113.101, and 203.0.113.102.
- **File Hashes**: Identify hashes of detected malware files.
- **Command Line**: N/A (not available in logs).

4. Contain / Eradicate



Isolate Affected Systems

- **Immediate Isolation**: Disconnect infected workstations from the network.
- **Quarantine**: Quarantine affected devices.

Patch Threat Entry Point

- **Update Software**: Ensure all systems are updated with the latest security patches.
- **Change Credentials**: Force a password reset for affected users and all employees as a precaution.

Predefined Threshold

- **For Customers**: Notify any customers whose data may have been affected.
- **For Internal Systems**: Escalate to the IT security team.
- **For Escalations**: Involve higher management and, if necessary, external cybersecurity consultants.

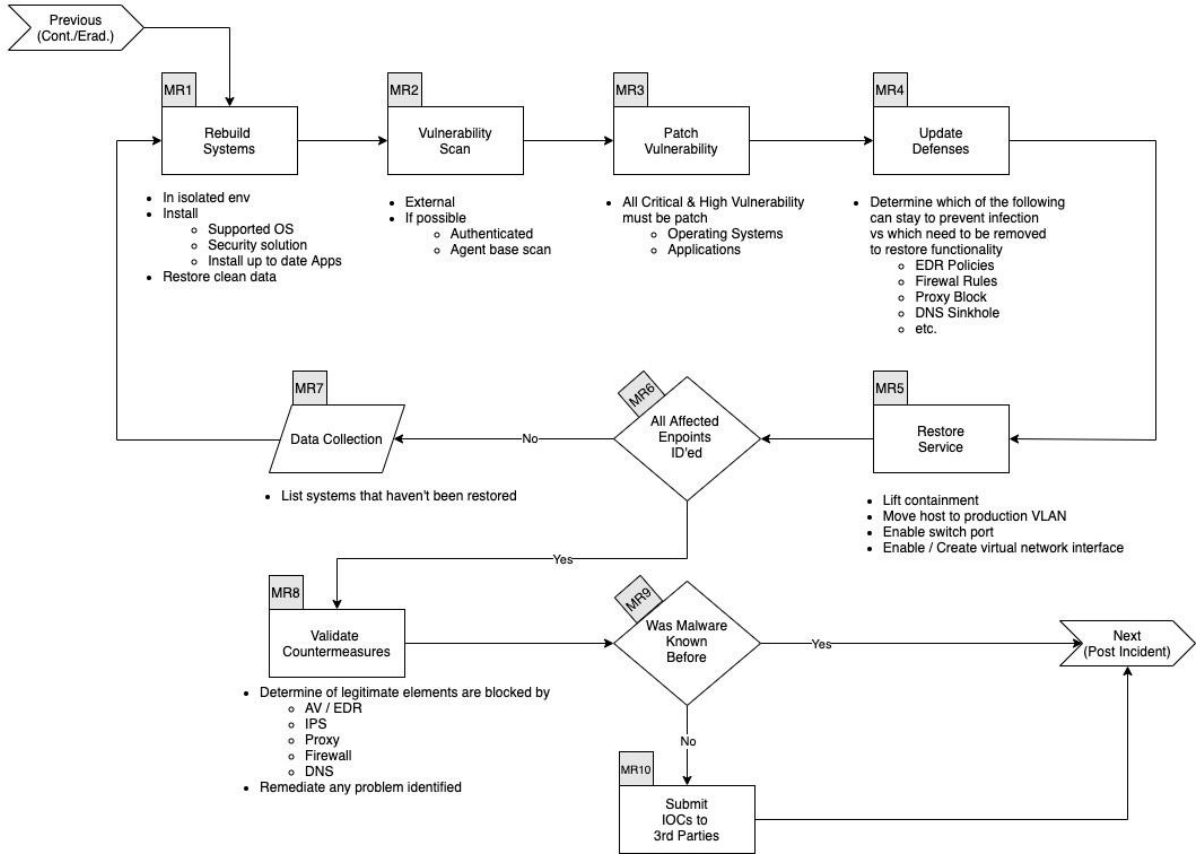
Preauthorized Actions

- **Per Customers**: Execute predefined response actions such as notifying customers and providing support.
- **Per Environment**: Differentiate actions for production and other environments.

How to Remove the Threat on All Affected Systems

- **Antivirus Scans**: Run comprehensive scans on all endpoints to ensure all malware is removed.
- **Manual Inspection**: Conduct manual checks on critical systems.

5. Recover



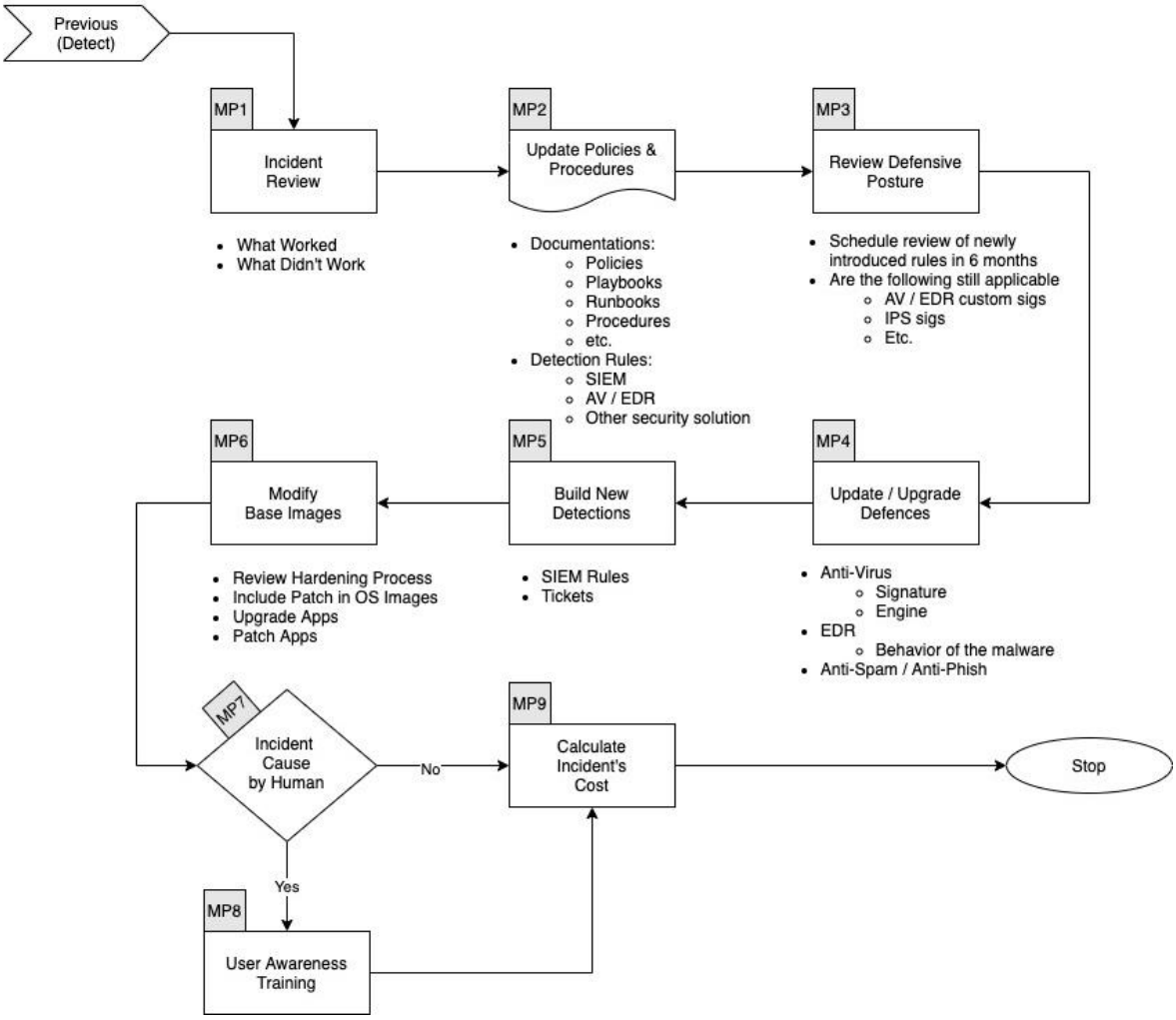
Get Systems Operational

- **Restore Services**: Ensure all infected workstations and systems are free of threats and restore normal operations.
- **Monitoring**: Implement heightened monitoring for any signs of residual threats.

Rebuild and Resume Service

- **Reimage Systems**: Rebuild systems from clean backups if necessary.
- **Verification**: Verify the integrity and security of all restored systems.

6. Post Incident



Lessons Learned

- **Review**: Conduct a post-mortem analysis to identify what worked and what didn't.
- **Documentation**: Update incident response documentation with new insights.

New Detection

- **Enhance Monitoring**: Improve detection rules and monitoring based on the incident analysis.
- **Training**: Provide additional training to staff based on lessons learned.

New Hardening

- **Security Enhancements**: Implement new security measures such as stronger MFA, improved email filtering.
- **Policy Updates**: Revise security policies to address gaps identified during the incident.

New Patch Management

- **Regular Updates**: Ensure all systems are regularly updated with the latest patches.
- **Automated Deployment**: Implement automated patch management solutions to reduce manual effort and errors.

4. Phishing

Scenario: Multiple employees received a phishing email that led to compromised credentials and unauthorized access to the company's internal systems.

Incident Response Analysis

1. Preparation

List of All Assets

Servers

- **Web Server**: Hostname: web01, IP: 192.168.1.10, OS: Ubuntu 20.04
- **Database Server**: Hostname: db01, IP: 192.168.1.20, OS: MySQL 8.0
- **Email Server**: Hostname: mail01, IP: 192.168.1.30, OS: Exchange Server 2019

Endpoints

- **Workstations**: 50 Windows 10 PCs
- **Laptops**: 20 MacBook Pros
- **Mobile Devices**: 10 iPhones, 10 Android devices

Networks

- **Corporate Network**: 192.168.0.0/16
- **Guest Network**: 172.16.0.0/16
- **DMZ**: 10.0.0.0/24

Applications

- **CRM**: Salesforce
- **ERP**: SAP
- **Office Suite**: Microsoft Office 365
- **Communication**: Slack, Zoom

Employees

- **Total Employees**: 150
- **Key Roles**: IT Admins, HR, Finance, Sales, Executives

Security Products

- **Antivirus**: Symantec Endpoint Protection

- **Firewall**: Cisco ASA 5500
- **SIEM**: Splunk
- **IDS/IPS**: Snort
- **MFA**: Duo Security

Baselines

- **Normal Network Traffic**: Defined and documented with Splunk
- **System Performance Metrics**: Established benchmarks for CPU, memory, and disk usage
- **User Behaviour**: Normal login times, locations, and activities

Communication Plan

- **Incident Response Team**: Defined roles and contact info for all members
- **Internal Notifications**: Procedures for informing executives, IT staff, and affected users
- **External Notifications**: Criteria for informing customers, partners, and regulatory bodies

Security Events

- **Authentication Failures**
- **Unusual Login Locations**
- **Unauthorized Access Attempts**
- **Data Exfiltration Attempts**
- **Privilege Escalation Attempts**

Thresholds

- **Login Failures**: More than 5 failed logins within 10 minutes
- **Unusual Locations**: Logins from unrecognized countries
- **Data Transfer**: Uploads exceeding 1 GB from a single user

Access to Security Tools

- **Provision Access**: Procedures for granting and revoking access to security tools like Splunk, Duo, Snort
- **Documentation**: User guides and training materials for security tools

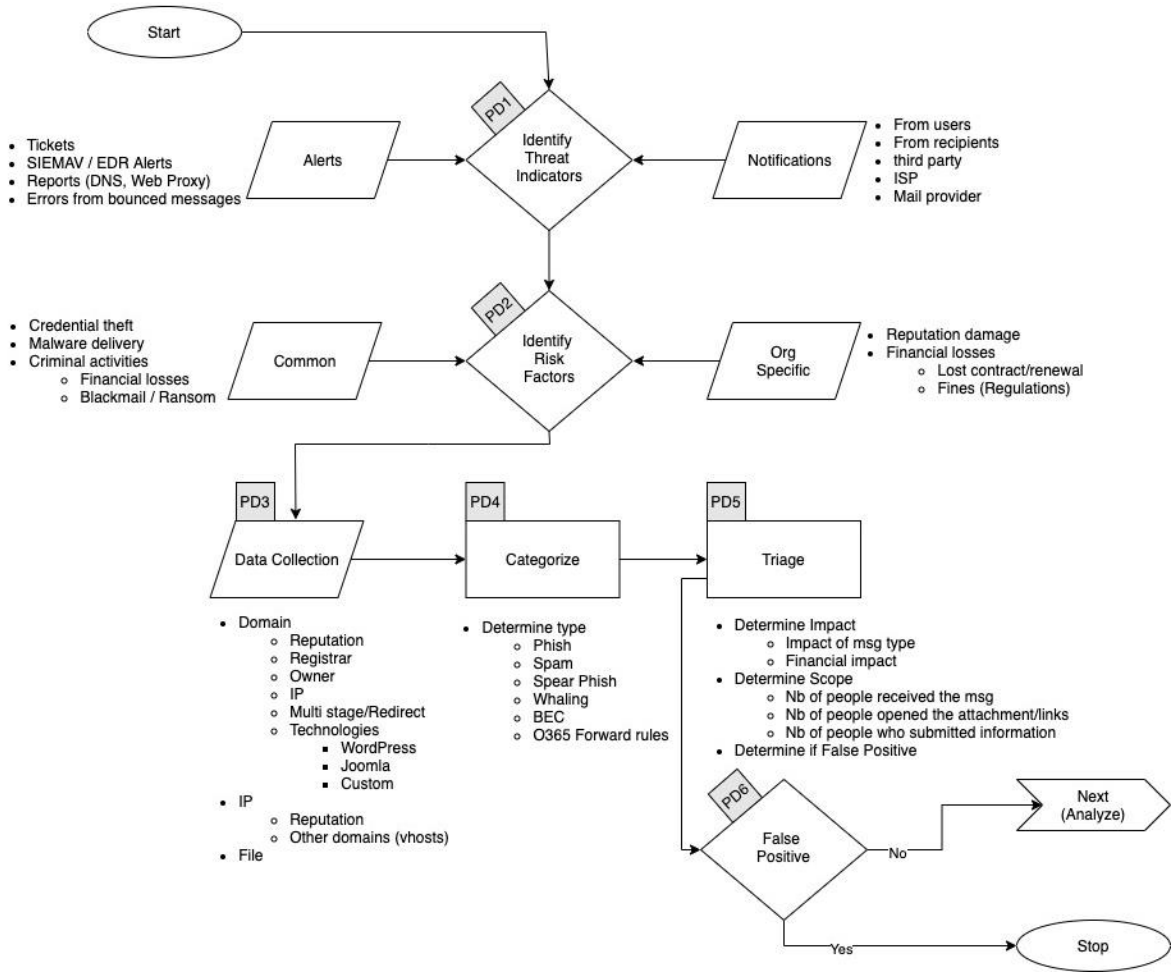
Create Playbooks

- **Account Compromise**: Step-by-step actions for detection, containment, and recovery
- **Malware Infection**: Procedures for identification and removal
- **Phishing Attack**: Steps for identifying phishing attempts, removing malicious emails, and securing compromised accounts

Plan Exercises

- **Tabletop Exercises**: Quarterly simulations of common incidents
- **Hands-On Drills**: Annual red team/blue team exercises

2. Detect



Gathering of Information

- **Logs**: Email logs, authentication logs, and network traffic logs from Splunk
- **Alerts**: Review alerts from SIEM, IDS/IPS, and antivirus
- **User Reports**: Analyse reports from users about suspicious emails

Logs

Email Server Logs:

2024-06-25 09:12:32,email,received,sender=attacker@example.com,recipient=jsmith@company.com,subject="Urgent: Update Your Password",ip=203.0.113.50

2024-06-25 09:15:47,email,received,sender=attacker@example.com,recipient=adoe@company.com,subject="Urgent: Update Your Password",ip=203.0.113.50

2024-06-25 09:17:53,email,received,sender=attacker@example.com,recipient=bwong@company.com,subject="Urgent: Update Your Password",ip=203.0.113.50

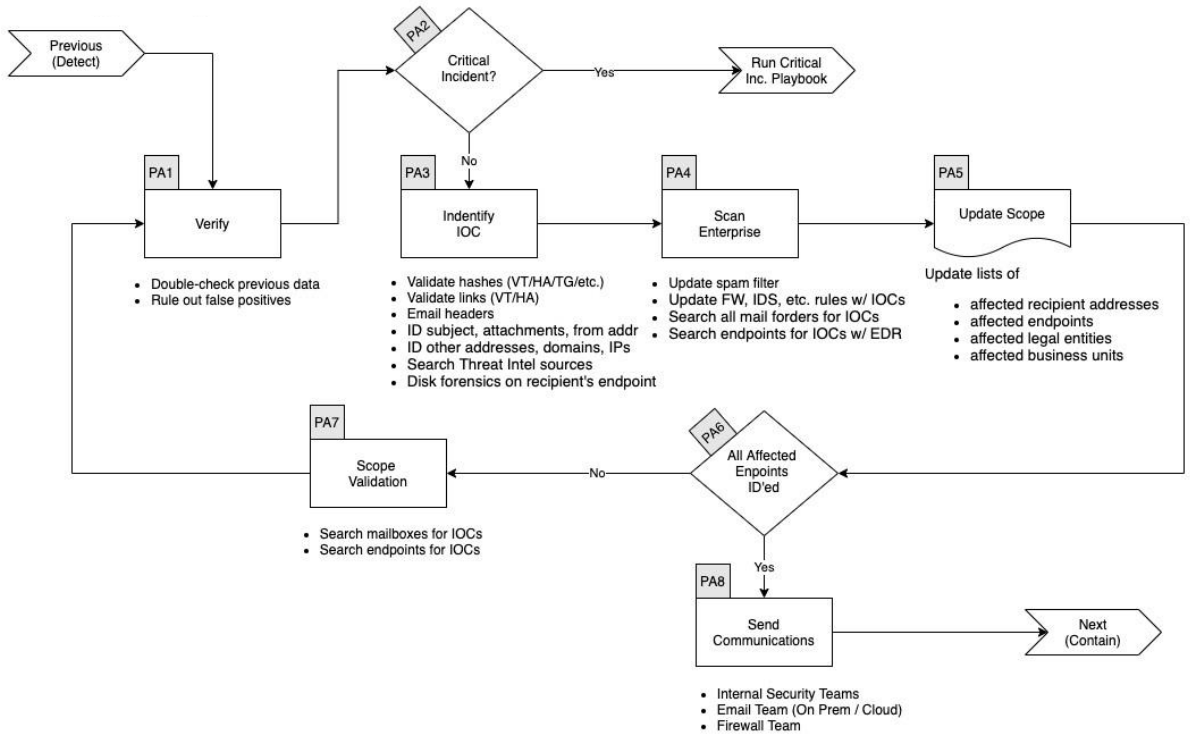
Authentication Logs:

2024-06-25 09:30:12,auth,login,success,user=jsmith,ip=203.0.113.60

2024-06-25 09:35:15,auth,login,failed,user=adoe,ip=203.0.113.60

2024-06-25 09:40:20,auth,login,success,user=adoe,ip=203.0.113.60

3. Analyse



Analyse Data

- **Email Analysis**: Multiple phishing emails received from attacker@example.com.
- **Login Attempts**: Successful logins from an external IP (203.0.113.60) shortly after phishing emails were received.

Building Detections

- **Custom SIEM Rules**: Create rules to flag emails from suspicious domains and detect unusual login attempts.
- **Behavioural Analysis**: Monitor deviations from normal email and login patterns.

Root Cause Analysis

- **Initial Point of Compromise**: Phishing emails led to users providing their credentials to the attacker.
- **Affected Accounts**: Users jsmith and adoe.

Depth and Breadth of the Attack

- **Admin Rights**: Verify if affected users have administrative privileges (confirmed: no admin rights).
- **Affected Systems**: Email accounts and potentially other internal systems accessed using compromised credentials.

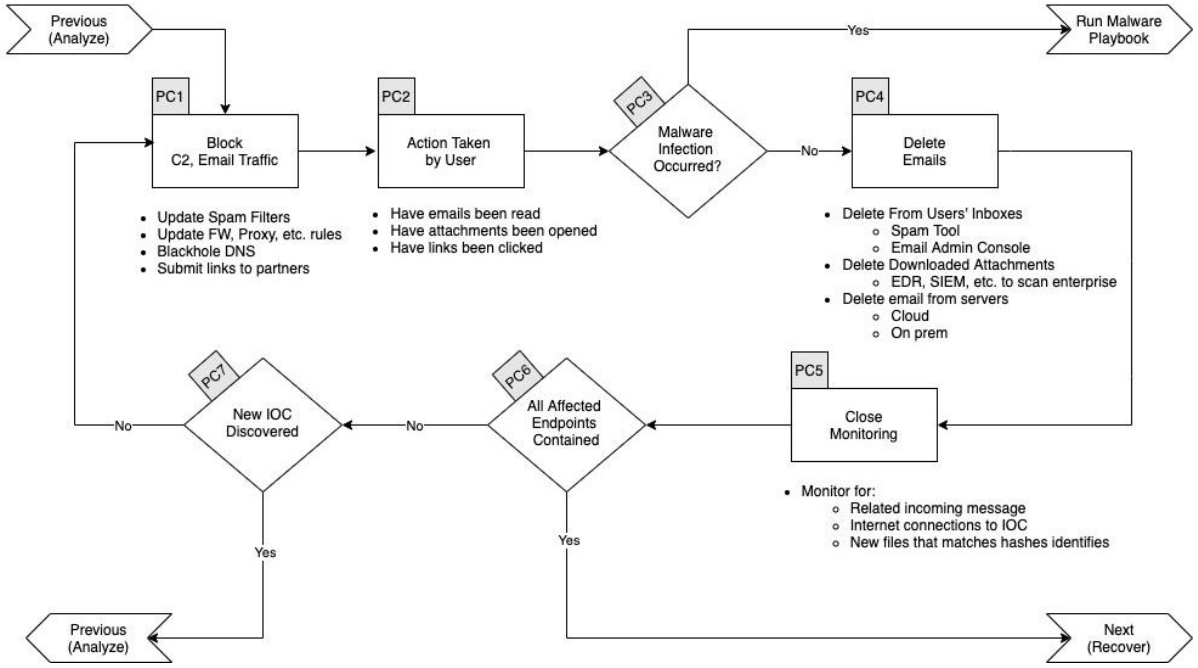
Techniques Used

- **Phishing**: Attacker used phishing emails to harvest credentials.
- **Unauthorized Access**: Attacker used harvested credentials to log into internal systems.

Indicators of Compromise / Indicators of Attack

- **Tactics, Techniques, and Procedures (TTP)**: Use of phishing emails to steal credentials.
- **IP Addresses**: Malicious activity from IP 203.0.113.60 and 203.0.113.50.
- **Email Content**: Subject line "Urgent: Update Your Password" from attacker@example.com.

4. Contain / Eradicate



Isolate Affected Systems

- **Immediate Isolation**: Disable compromised accounts jsmith and adoe.
- **Quarantine**: Block IPs 203.0.113.60 and 203.0.113.50 at the firewall.

Patch Threat Entry Point

- **Update Software**: Ensure all systems are updated with the latest security patches.
- **Change Credentials**: Force a password reset for compromised users and all employees as a precaution.

Predefined Threshold

- **For Customers**: Notify any customers whose data may have been accessed or affected.
- **For Internal Systems**: Escalate to the IT security team.
- **For Escalations**: Involve higher management and, if necessary, external cybersecurity consultants.

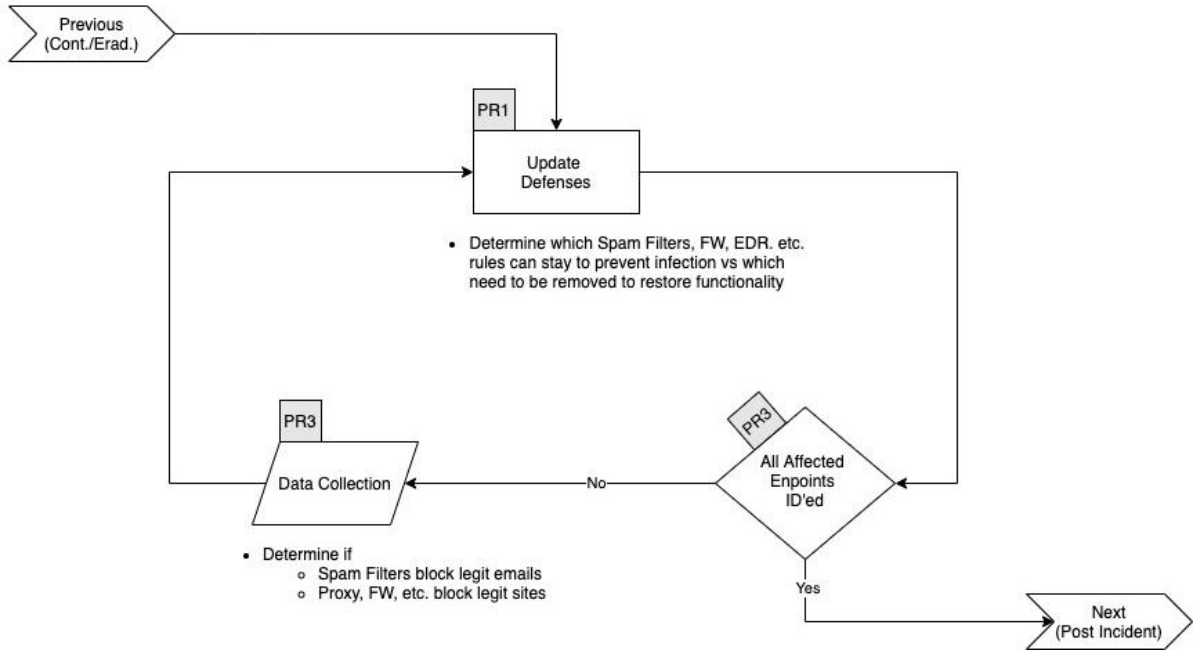
Preauthorized Actions

- **Per Customers**: Execute predefined response actions such as notifying customers and providing support.
- **Per Environment**: Differentiate actions for production and other environments.

How to Remove the Threat on All Affected Systems

- **Email Filtering**: Implement stronger email filtering rules to block similar phishing emails.
- **Antivirus Scans**: Run comprehensive scans on all endpoints to ensure no malware was introduced.

5. Recover



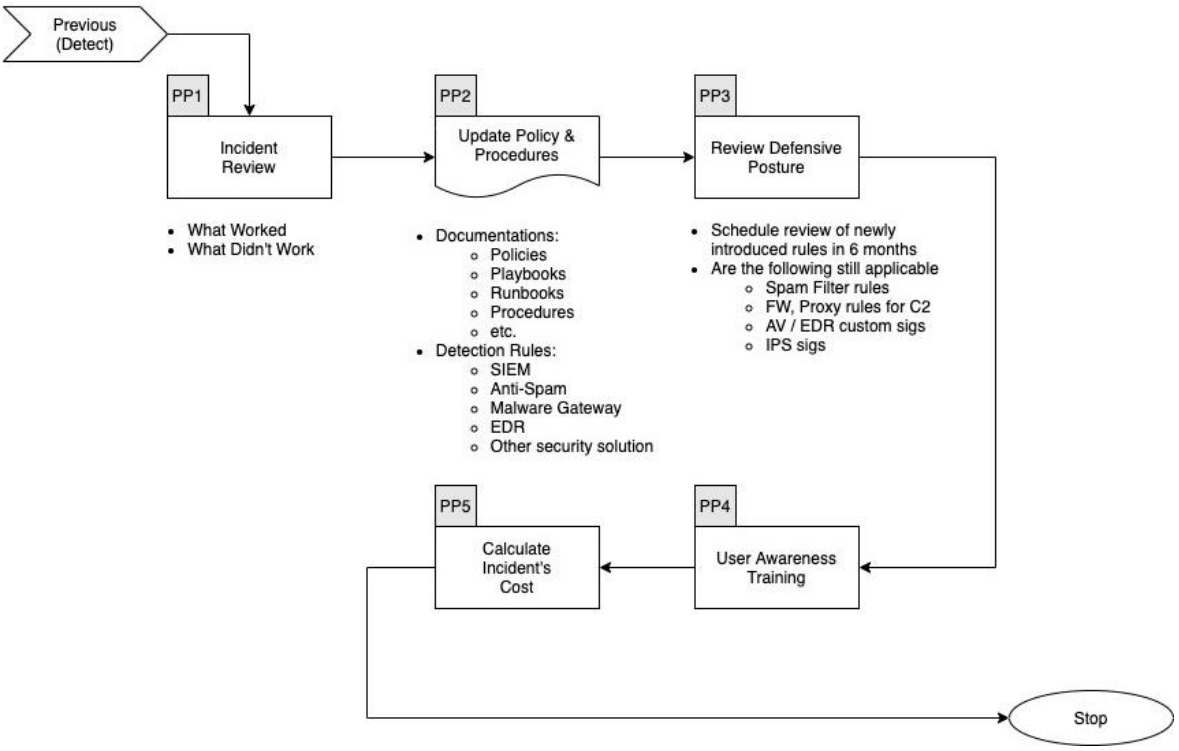
Get Systems Operational

- **Restore Services**: Ensure email accounts and other systems are secure and restore normal operations.
- **Monitoring**: Implement heightened monitoring for any signs of residual threats.

Rebuild and Resume Service

- **Reimage Systems**: Rebuild systems from clean backups if necessary.
- **Verification**: Verify the integrity and security of all restored systems.

6. Post Incident



Lessons Learned

- **Review**: Conduct a post-mortem analysis to identify what worked and what didn't.
- **Documentation**: Update incident response documentation with new insights.

New Detection

- **Enhance Monitoring**: Improve detection rules and monitoring based on the incident analysis.
- **Training**: Provide additional training to staff based on lessons learned.

New Hardening

- **Security Enhancements**: Implement new security measures such as stronger MFA, improved email filtering.
- **Policy Updates**: Revise security policies to address gaps identified during the incident.

New Patch Management

- **Regular Updates**: Ensure all systems are regularly updated with the latest patches.
- **Automated Deployment**: Implement automated patch management solutions to reduce manual effort and errors.

5. Ransomware

Scenario: A ransomware attack has encrypted multiple critical systems within the organization, demanding payment for the decryption keys.

Incident Response Analysis

1. Preparation

List of All Assets

Servers

- **Web Server**: Hostname: web01, IP: 192.168.1.10, OS: Ubuntu 20.04
- **Database Server**: Hostname: db01, IP: 192.168.1.20, OS: MySQL 8.0
- **Email Server**: Hostname: mail01, IP: 192.168.1.30, OS: Exchange Server 2019
- **File Server**: Hostname: file01, IP: 192.168.1.40, OS: Windows Server 2019

Endpoints

- **Workstations**: 50 Windows 10 PCs
- **Laptops**: 20 MacBook Pros
- **Mobile Devices**: 10 iPhones, 10 Android devices

Networks

- **Corporate Network**: 192.168.0.0/16
- **Guest Network**: 172.16.0.0/16
- **DMZ**: 10.0.0.0/24

Applications

- **CRM**: Salesforce
- **ERP**: SAP
- **Office Suite**: Microsoft Office 365
- **Communication**: Slack, Zoom

Employees

- **Total Employees**: 150
- **Key Roles**: IT Admins, HR, Finance, Sales, Executives

Security Products

- **Antivirus**: Symantec Endpoint Protection
- **Firewall**: Cisco ASA 5500
- **SIEM**: Splunk
- **IDS/IPS**: Snort
- **MFA**: Duo Security

Baselines

- **Normal Network Traffic**: Defined and documented with Splunk
- **System Performance Metrics**: Established benchmarks for CPU, memory, and disk usage
- **User Behaviour**: Normal login times, locations, and activities

Communication Plan

- **Incident Response Team**: Defined roles and contact info for all members
- **Internal Notifications**: Procedures for informing executives, IT staff, and affected users
- **External Notifications**: Criteria for informing customers, partners, and regulatory bodies

Security Events

- **Authentication Failures**
- **Unusual Login Locations**
- **Unauthorized Access Attempts**
- **Data Exfiltration Attempts**
- **Privilege Escalation Attempts**
- **Mass File Encryption**

Thresholds

- **Login Failures**: More than 5 failed logins within 10 minutes
- **Unusual Locations**: Logins from unrecognized countries
- **Data Transfer**: Uploads exceeding 1 GB from a single user
- **File Modifications**: Sudden spike in file encryption or modifications

Access to Security Tools

- **Provision Access**: Procedures for granting and revoking access to security tools like Splunk, Duo, Snort

- **Documentation**: User guides and training materials for security tools

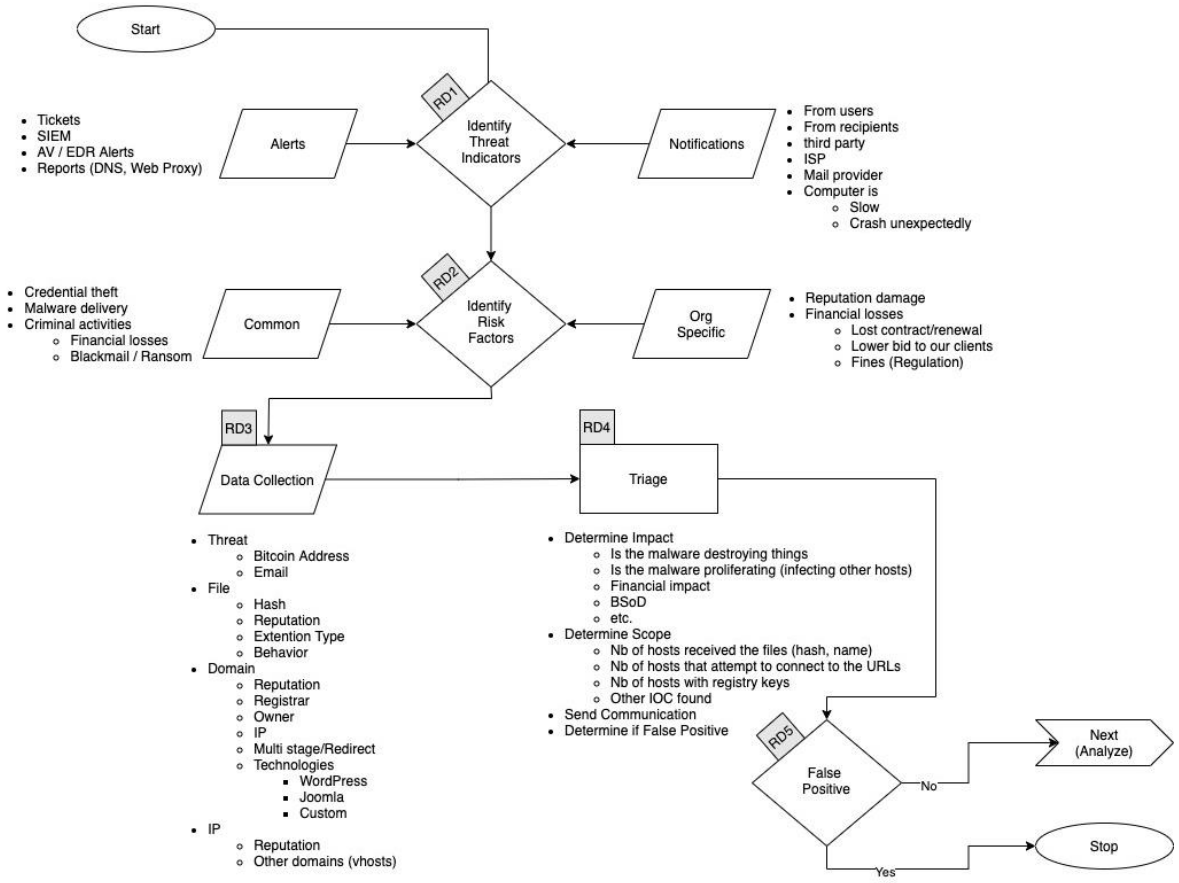
Create Playbooks

- **Account Compromise**: Step-by-step actions for detection, containment, and recovery
- **Malware Infection**: Procedures for identification and removal
- **Phishing Attack**: Steps for identifying phishing attempts, removing malicious emails, and securing compromised accounts
- **Ransomware Attack**: Comprehensive guide for responding to ransomware, including isolation, communication, and recovery steps

Plan Exercises

- **Tabletop Exercises**: Quarterly simulations of common incidents
- **Hands-On Drills**: Annual red team/blue team exercises

2. Detect



Gathering of Information

- **Logs**: Authentication logs, access logs, and network traffic logs from Splunk
- **Alerts**: Review alerts from SIEM, IDS/IPS, and antivirus
- **User Reports**: Analyse reports from users about unusual system behaviour

Logs

Endpoint Antivirus Logs:

2024-06-26 10:12:10,av,alert,ransomware_detected,threat=Ransomware.LockBit,action=quarantine,device=192.168.1.50,user=jdoe

2024-06-26 10:15:12,av,alert,ransomware_detected,threat=Ransomware.LockBit,action=quarantine,device=192.168.1.51,user=asmith

2024-06-26 10:20:15,av,alert,ransomware_detected,threat=Ransomware.LockBit,action=quarantine,device=192.168.1.52,user=bwong

Network Traffic Logs:

2024-06-26 10:12:11,network,connection,allowed,src_ip=192.168.1.50,dst_ip=203.0.113.200,port=443

2024-06-26 10:15:13,network,connection,allowed,src_ip=192.168.1.51,dst_ip=203.0.113.200,port=443

2024-06-26 10:20:16,network,connection,allowed,src_ip=192.168.1.52,dst_ip=203.0.113.200,port=443

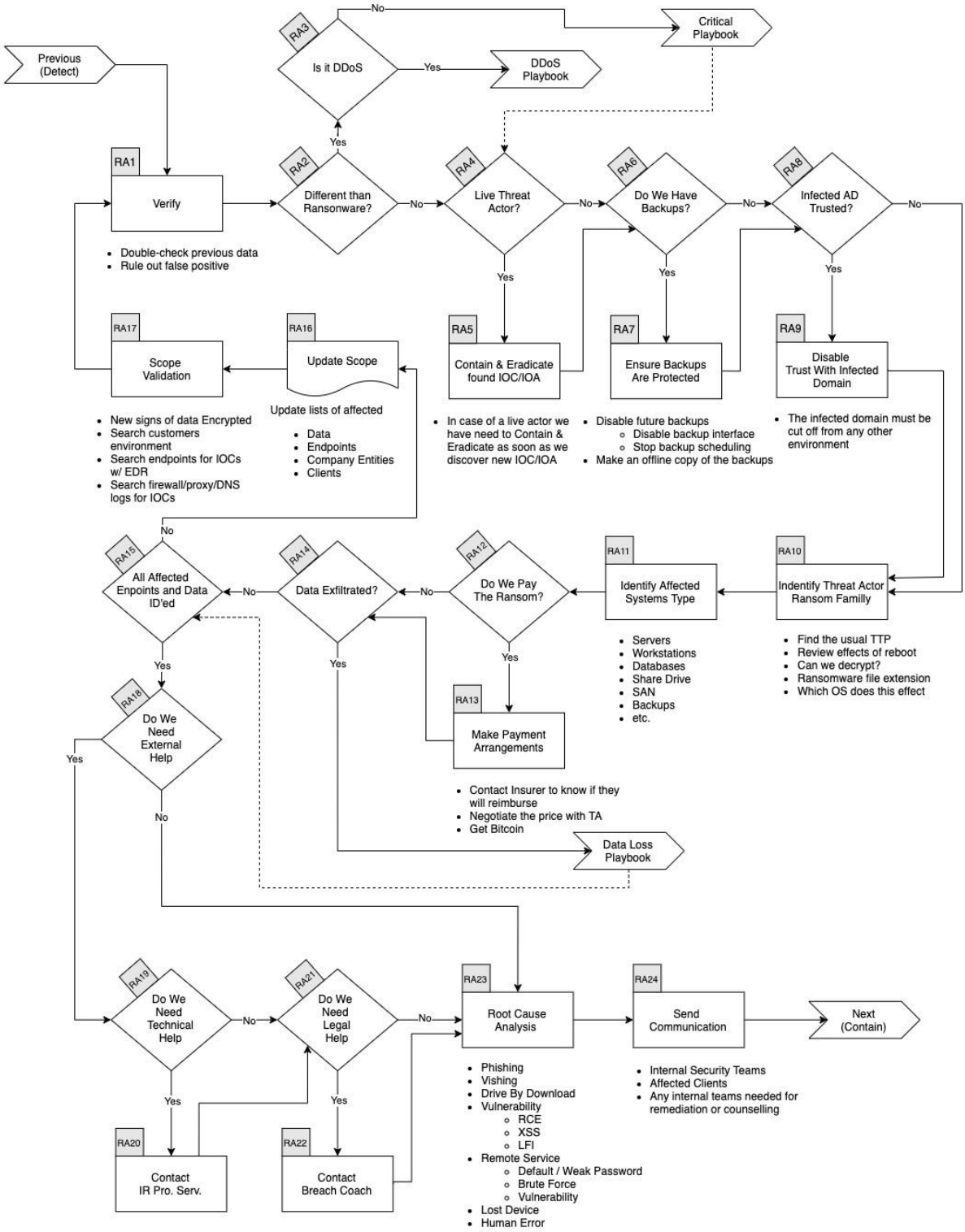
File Server Logs:

2024-06-26 10:12:10,file,modified,path=/share/docs/file1.docx,user=jdoe

2024-06-26 10:15:12,file,modified,path=/share/docs/file2.docx,user=asmith

2024-06-26 10:20:15,file,modified,path=/share/docs/file3.docx,user=bwong

3. Analyse



Analyse Data

- **Ransomware Detection**: Multiple workstations have detected and quarantined ransomware.

- **Network Activity**: Suspicious outbound connections to external IPs (203.0.113.200).
- **File Modifications**: Sudden spike in file modifications on the file server.

Building Detections

- **Custom SIEM Rules**: Create rules to flag ransomware alerts from antivirus logs and unusual file modifications.
- **Behavioural Analysis**: Monitor deviations from normal network and file activity patterns.

Root Cause Analysis

- **Initial Point of Compromise**: Likely introduced via phishing email or malicious download.
- **Affected Accounts**: Users jdoe, asmith, and bwong are affected.

Depth and Breadth of the Attack

- **Admin Rights**: Verify if affected users have administrative privileges (confirmed: no admin rights).
- **Affected Systems**: Multiple workstations and file server with encrypted files.

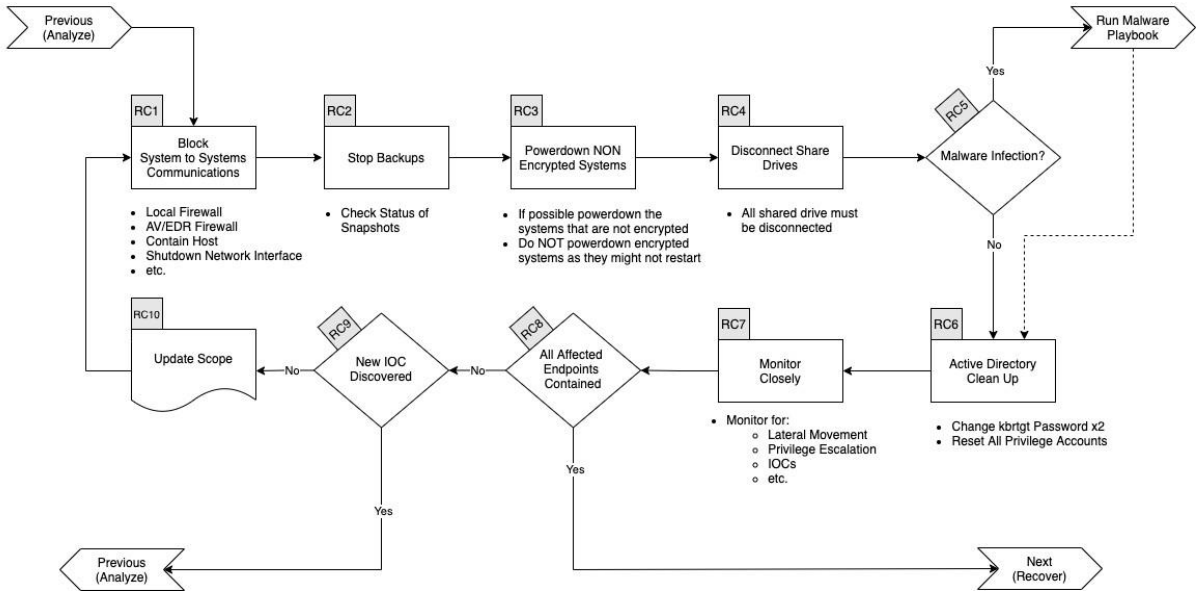
Techniques Used

- **Phishing**: Possible entry point via phishing email.
- **Ransomware Payload**: LockBit ransomware detected.

Indicators of Compromise / Indicators of Attack

- **Tactics, Techniques, and Procedures (TTP)**: Use of phishing emails to deliver ransomware payloads.
- **IP Addresses**: Malicious outbound connections to IP 203.0.113.200.
- **File Modifications**: Unusual file modifications and encryptions.

Contain / Eradicate



Isolate Affected Systems

- **Immediate Isolation**: Disconnect infected workstations from the network.
- **Quarantine**: Quarantine affected devices to prevent further spread.

Patch Threat Entry Point

- **Update Software**: Ensure all systems are updated with the latest security patches.
- **Change Credentials**: Force a password reset for affected users and all employees as a precaution.

Predefined Threshold

- **For Customers**: Notify any customers whose data may have been affected.
- **For Internal Systems**: Escalate to the IT security team.
- **For Escalations**: Involve higher management and, if necessary, external cybersecurity consultants.

Preauthorized Actions

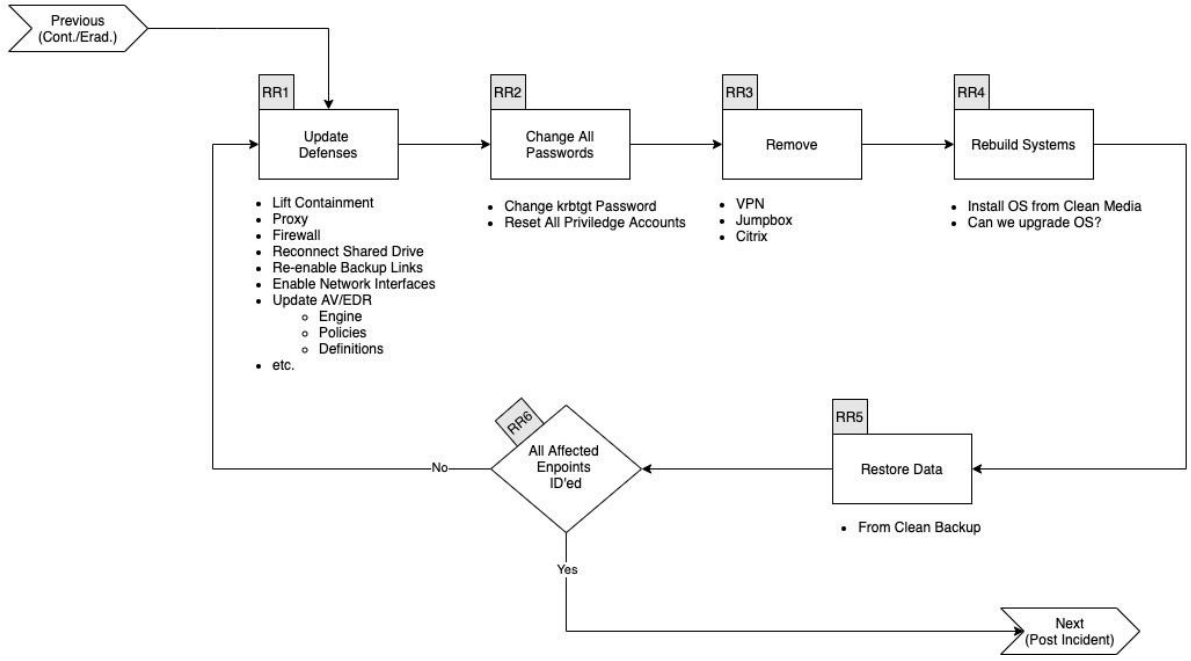
- **Per Customers**: Execute predefined response actions such as notifying customers and providing support.
- **Per Environment**: Differentiate actions for production and other environments.

How to Remove the Threat on All Affected Systems

- **Antivirus Scans**: Run comprehensive scans on all endpoints to ensure all ransomware is removed.

- **Manual Inspection**: Conduct manual checks on critical systems.

4. Recover



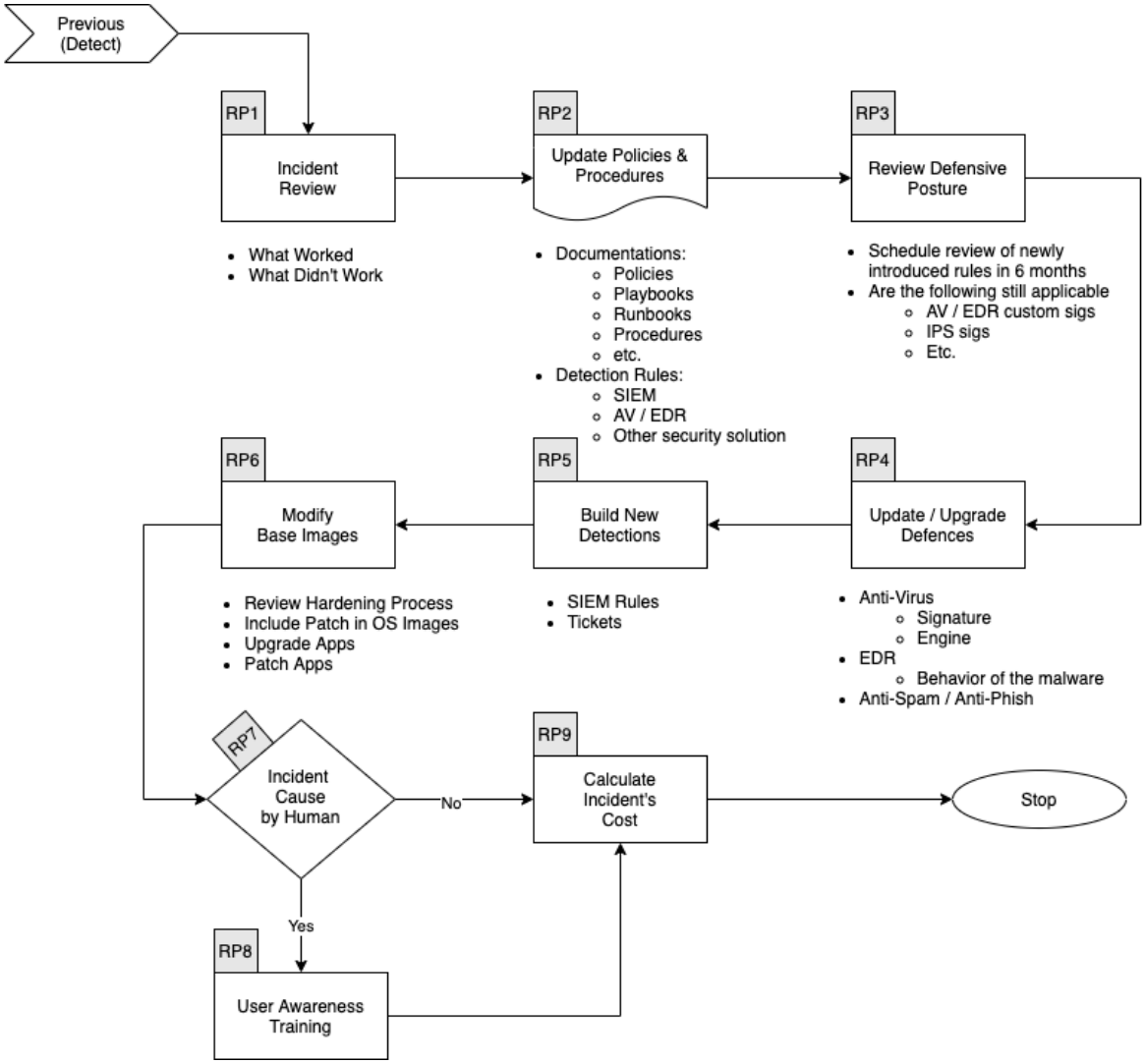
Get Systems Operational

- **Restore Services**: Ensure all infected workstations and systems are free of threats and restore normal operations.
- **Monitoring**: Implement heightened monitoring for any signs of residual threats.

Rebuild and Resume Service

- **Reimage Systems**: Rebuild systems from clean backups if necessary.
- **Verification**: Verify the integrity and security of all restored systems.

5. Post Incident



Lessons Learned

- **Review**: Conduct a post-mortem analysis to identify what worked and what didn't.
- **Documentation**: Update incident response documentation with new insights.

New Detection

- **Enhance Monitoring**: Improve detection rules and monitoring based on the incident analysis.
- **Training**: Provide additional training to staff based on lessons learned.

New Hardening

- **Security Enhancements**: Implement new security measures such as stronger MFA, improved email filtering.

- **Policy Updates**: Revise security policies to address gaps identified during the incident.

New Patch Management

- **Regular Updates**: Ensure all systems are regularly updated with the latest patches.
- **Automated Deployment**: Implement automated patch management solutions to reduce manual effort and errors.