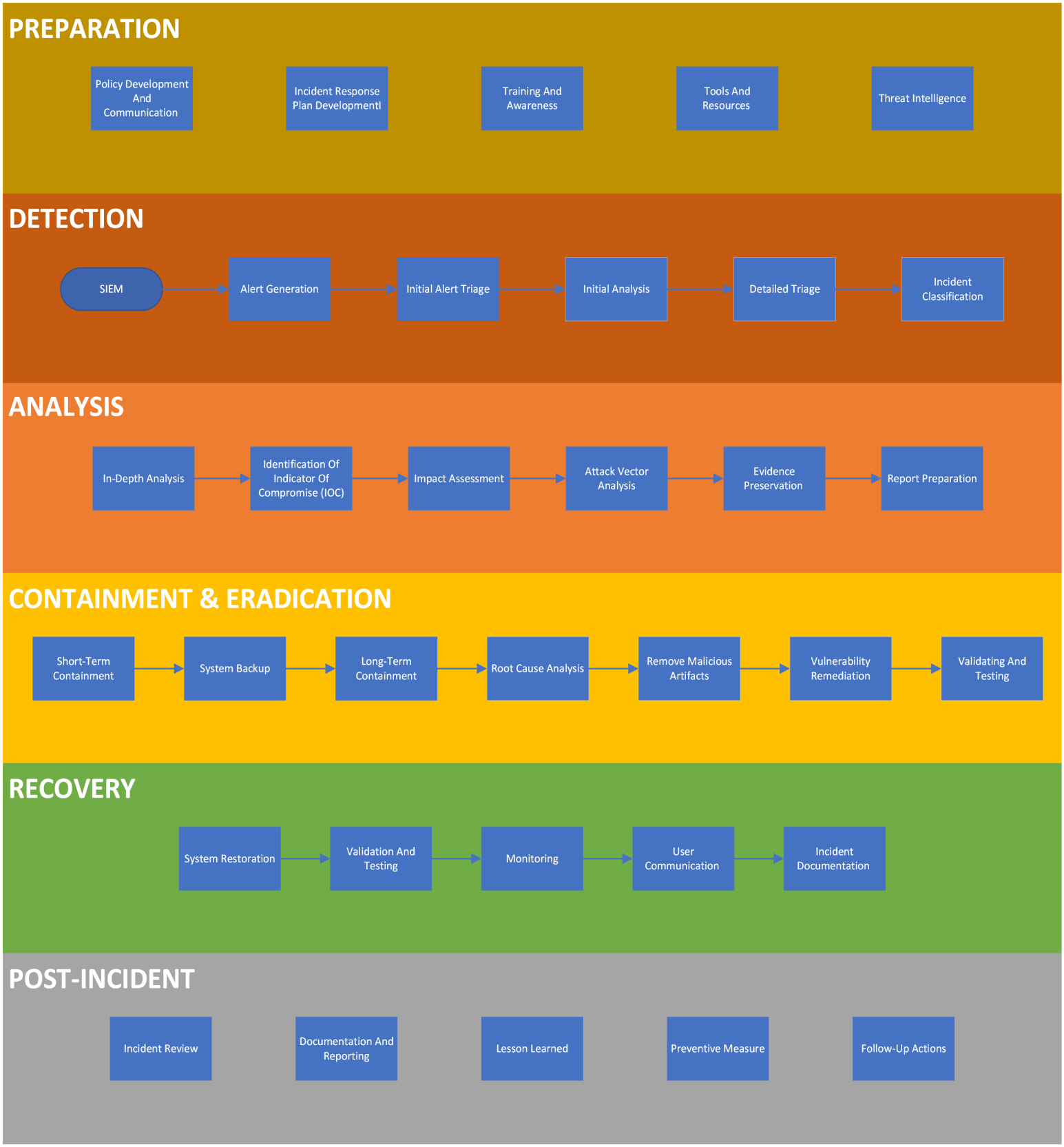
INCIDENT RESPONSE PLAN WORKFLOW WITH EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

INCIDENT RESPONSE WORKFLOW



BREAKDOWN OF INCIDENT RESPONSE WORKFLOW

1. PREPARATION

- **Policy Development and Communication**
  - Define and communicate the incident response policy.
  - Identify and assign roles and responsibilities.
  - Ensure organisational support for incident response activities.
- **Incident Response Plan Development**
  - Develop and maintain an incident response plan.
  - Include contact information for key personnel and external parties.
- **Training and Awareness**
  - Conduct regular training and awareness programs for employees.
  - Simulate incident response scenarios to test readiness.
- **Tools and Resources**
  - Ensure availability of necessary tools and resources (e.g., SIEM systems, forensic tools).
  - Keep an updated inventory of hardware and software.
- **Threat Intelligence**
  - Subscribe to threat intelligence feeds.
  - Integrate threat intelligence into detection mechanisms.

2. DETECTION

SIEM Alert Generation

- **Event Collection**
  - Collect logs and events from various sources (firewalls, IDS/IPS, endpoints, applications, etc.).
  - Ensure logs are timestamped and stored in a centralised location for correlation and analysis.
- **Alert Generation**
  - Correlate events using predefined rules and anomaly detection techniques.
  - Generate an alert when a rule is triggered or an anomaly is detected.

Initial Alert Triage

- **Alert Prioritisation**
  - Assess the severity and priority of the alert based on predefined criteria (e.g., asset value, threat intelligence).
  - Filter out false positives and benign events.
- **Alert Enrichment**
  - Enrich the alert with additional context (e.g., threat intelligence, asset details, user information).
  - Utilize automated tools to gather relevant information.

Initial Analysis

- **Incident Validation**
  - Validate the alert to confirm if it indicates a genuine incident.
  - Investigate the source and nature of the alert.
- **Scope Determination**
  - Determine the scope and impact of the potential incident.
  - Identify affected systems, users, and data.

Detailed Triage

- **Data Collection**
  - Collect additional data from affected systems (e.g., logs, network traffic captures, endpoint data).
  - Use forensic tools to gather evidence.
- **Technical Analysis**
  - Perform a detailed technical analysis to understand the attack vector and tactics used.
  - Identify indicators of compromise (IOCs) and indicators of attack (IOAs).
- **Threat Intelligence Correlation**
  - Correlate findings with threat intelligence to understand the threat actor's tactics, techniques, and procedures (TTPs).
  - Check for known vulnerabilities or exploits associated with the alert.

Incident Classification

- **Severity Assessment**
  - Assess the severity of the incident based on its potential impact and scope.
  - Classify the incident (e.g., low, medium, high severity).
- **Notification**
  - Notify relevant stakeholders (e.g., incident response team, management) based on the incident classification.
  - Follow communication protocols for internal and external notifications.

3. ANALYSIS

In-Depth Analysis

- **Detailed Incident Examination**
  - Conduct a thorough examination of the incident to understand its full scope.
  - Analyse the compromised systems, affected networks, and any involved applications.
- **Malware Analysis (if applicable)**
  - Isolate and analyse any malware discovered.
  - Reverse engineer malware to understand its behaviour and objectives.

- **Network Traffic Analysis**
  - Analyse network traffic to identify abnormal patterns and communications.
  - Use tools like Wireshark to capture and inspect network packets.
- **Log Analysis**
  - Examine system, application, and security logs for signs of compromise.
  - Correlate logs from different sources to trace the attack path.

Identification of Indicators of Compromise (IOCs)

- **IOC Extraction**
  - Identify and extract IOCs such as IP addresses, domain names, file hashes, and registry changes.
  - Use threat intelligence feeds to enrich and validate IOCs.
- **IOC Sharing**
  - Share IOCs with internal and external stakeholders for proactive defence.
  - Update detection mechanisms with newly identified IOCs.

Impact Assessment

- **Data Exfiltration Analysis**
  - Determine if sensitive data was exfiltrated.
  - Identify the volume and types of data affected.
- **Business Impact Analysis**
  - Assess the impact on business operations and processes.
  - Quantify potential financial, reputational, and regulatory impacts.

Attack Vector Analysis

- **Root Cause Identification**
  - Identify the initial attack vector (e.g., phishing email, vulnerability exploitation).
  - Understand how the attacker gained access and moved laterally within the network.
- **Tactics, Techniques, and Procedures (TTPs) Analysis**
  - Analyse the attacker's TTPs to understand their behaviour and goals.
  - Map TTPs to frameworks like MITRE ATT&CK.

Evidence Preservation

- **Forensic Evidence Collection**
  - Collect and preserve digital evidence following legal and organisational procedures.
  - Ensure the integrity and chain of custody of the evidence.
- **Documentation**
  - Document all findings, analysis steps, and evidence collected.
  - Maintain a detailed timeline of the incident and response actions.

Report Preparation

- **Detailed Incident Report**
  - Prepare a comprehensive report detailing the incident, analysis, findings, and recommendations.
  - Include technical details, impact assessment, and remediation steps.
- **Executive Summary**
  - Create an executive summary for senior management, highlighting key points and business impacts.
  - Provide actionable recommendations for improving security posture.

4. CONTAINMENT & ERADICATION

Containment

Short-Term Containment

- **Isolate Affected Systems**
  - Disconnect affected systems from the network to prevent further spread.
  - Apply network segmentation to isolate compromised segments.
- **Block Malicious Traffic**
  - Implement firewall rules and access control lists (ACLs) to block malicious IP addresses and domains.
  - Use intrusion prevention systems (IPS) to block malicious traffic in real-time.
- **Disable Compromised Accounts**
  - Disable user accounts and credentials that have been compromised.
  - Reset passwords for affected accounts and enforce strong password policies.
- **Apply Temporary Fixes**
  - Apply temporary patches or configurations to mitigate the immediate threat.
  - Monitor the effectiveness of these measures.

System Backups

- **Verify Backup Integrity**
  - Ensure backups are recent and not compromised.
  - Validate the integrity of backups before restoration.
- **Create Additional Backups**
  - Take additional backups of affected systems, ensuring they are stored securely.
  - Document the backup process and locations.

Long-Term Containment

- **Implement Long-Term Solutions**

    - Develop and implement more permanent fixes for vulnerabilities and weaknesses.
    - Conduct thorough testing to ensure the effectiveness of long-term solutions.
- **Monitor Affected Systems**
    - Continuously monitor isolated systems for signs of further compromise.
    - Adjust containment measures as necessary based on monitoring results.

Eradication

Root Cause Analysis

- **Identify Root Cause**
    - Conduct a thorough investigation to identify the root cause of the incident.
    - Analyse attack vectors, vulnerabilities exploited, and methods used by the attacker.
- **Forensic Analysis**
    - Perform forensic analysis on affected systems to gather detailed evidence.
    - Use tools and techniques to analyse memory dumps, disk images, and logs.

Remove Malicious Artifacts

- **Malware Removal**
    - Use anti-malware tools to scan and remove any detected malware.
    - Manually remove persistent threats and backdoors that automated tools might miss.
- **System Cleaning**
    - Clean and sanitize affected systems to remove all traces of the attack.
    - Ensure all compromised files and configurations are restored to a known good state.

Vulnerability Remediation

- **Patch Management**
    - Apply security patches and updates to all affected systems.
    - Ensure all software and firmware are up-to-date.
- **Configuration Hardening**
    - Review and harden system configurations to prevent future attacks.
    - Implement security best practices and compliance requirements.
- **Access Control Review**
    - Review and adjust access controls to minimize the risk of unauthorised access.
    - Implement least privilege principles and regularly review permissions.

Validation and Testing

- **System Validation**
  - Validate the integrity and functionality of cleaned systems.
  - Conduct thorough testing to ensure systems are fully operational and secure.
- **Penetration Testing**
  - Perform penetration testing to verify the effectiveness of remediation measures.
  - Identify any remaining vulnerabilities or weaknesses.

5. RECOVERY

System Restoration

- **Restore from Backups**
  - Restore affected systems from verified, clean backups.
  - Ensure that backups used for restoration are up-to-date and uncompromised.
- **System Reinstallation**
  - Reinstall operating systems and applications on affected systems if backups are not available.
  - Configure systems to meet security standards and organisational policies.
- **Configuration Restoration**
  - Restore configurations to a known good state.
  - Apply security hardening measures to prevent future incidents.

Validation and Testing

- **Functional Testing**
  - Test restored systems to ensure they are fully functional.
  - Verify that all business-critical applications and services are operating correctly.
- **Security Testing**
  - Conduct vulnerability scans and penetration tests on restored systems.
  - Ensure that all identified vulnerabilities have been addressed.

Monitoring

- **Enhanced Monitoring**
  - Implement enhanced monitoring on restored systems to detect any signs of residual compromise.
  - Use SIEM tools to continuously monitor logs and events.
- **Anomaly Detection**
  - Configure anomaly detection rules to identify unusual activity.
  - Investigate any suspicious behaviour promptly.

User Communication

- **User Notification**
  - Inform users about the recovery process and any changes that have been made.
  - Provide clear instructions on any actions users need to take.
- **Training and Awareness**
  - Conduct training sessions to educate users about the incident and preventive measures.
  - Emphasize the importance of security best practices.

Incident Documentation

- **Incident Summary Report**
  - Prepare a summary report detailing the incident, response actions, and recovery process.
  - Include key findings, lessons learned, and recommendations.
- **Lessons Learned Review**
  - Conduct a post-incident review to identify areas for improvement.
  - Update incident response plans and procedures based on lessons learned.

6. POST-INCIDENT

Incident Review

- **Debriefing Session**
  - Conduct a debriefing session with the incident response team and relevant stakeholders.
  - Review the incident timeline, response actions, and decision-making processes.
- **Root Cause Analysis Review**
  - Re-examine the root cause analysis to ensure that all contributing factors have been identified.
  - Discuss any gaps or issues that were discovered during the response.

Documentation and Reporting

- **Comprehensive Incident Report**
  - Compile a detailed report that includes the incident summary, impact assessment, root cause analysis, and actions taken.
  - Document all findings, evidence collected, and steps followed during the response.
- **Compliance Reporting**
  - Prepare and submit any necessary reports to regulatory bodies or industry compliance organisations.

    - Ensure that the incident documentation meets any legal or regulatory requirements.

Lessons Learned

- **Identify Lessons Learned**
    - Identify what worked well and what didn't during the incident response.
    - Gather feedback from all participants to understand their perspectives.
- **Update Policies and Procedures**
    - Revise incident response policies, procedures, and playbooks based on lessons learned.
    - Ensure that all changes are documented and communicated to relevant teams.

Preventive Measures

- **Implement Improvements**
    - Implement technical and procedural improvements to address identified weaknesses.
    - Apply additional security measures, such as enhanced monitoring, new security controls, or updated configurations.
- **Employee Training and Awareness**
    - Conduct training sessions for employees to reinforce security best practices.
    - Raise awareness about the incident and preventive measures to avoid future occurrences.

Follow-Up Actions

- **Continuous Monitoring**
    - Monitor the environment for any signs of recurring or related incidents.
    - Ensure that enhanced monitoring tools and processes are in place and functioning correctly.
- **Review of Response Capabilities**
    - Assess the effectiveness of the incident response team and their capabilities.
    - Provide additional training or resources if needed to enhance the team's readiness for future incidents.

EXAMPLES AND SIMULATIONS

Scenario 1: Brute-Force Attack Detected on Web Server

Alert Details:

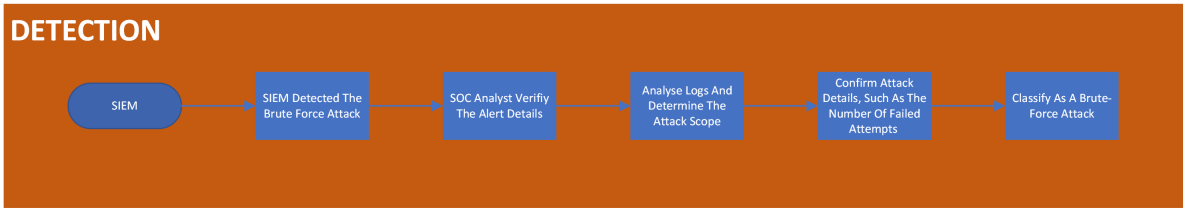
- **Alert Name**: Brute-Force Attack Detected
- **Source**: SIEM (Security Information and Event Management) System
- **Time of Alert**: 7 August 2024, 10:30 AM
- **Affected System**: Web Server (IP: 192.168.1.10)
- **Description**: Multiple failed login attempts detected on the web server.

Incident Response Analysis

1. **Preparation**

- **Policy Development And Communication**
  - Ensure policies for account lockout thresholds and SSH configurations are in place.
- **Incident Response Plan Development**
  - Have a clear plan for handling brute-force attacks.
- **Training And Awareness**
  - Train staff on identifying and responding to brute-force attacks.
- **Tools And Resources**
  - Ensure tools like SIEM and firewall rules are configured and ready.
- **Threat Intelligence**
  - Keep updated on common brute-force attack patterns and sources.

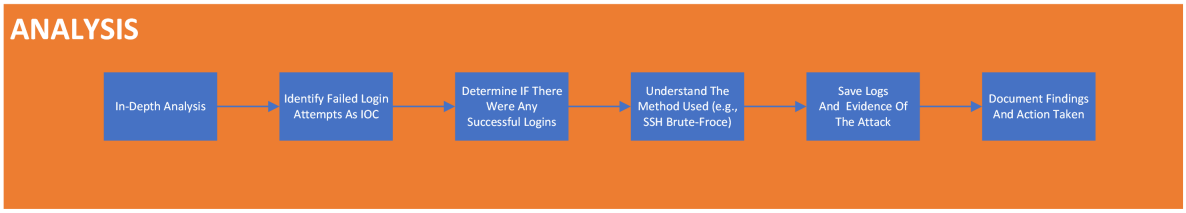
2. **Detection**



Alert Received:

- **Time**: 7 August 2024, 10:30 AM
- **SIEM Alert**: Brute-Force Attack Detected on Web Server (IP: 192.168.1.10)
- **Details**: The SIEM system has detected 1000 failed login attempts in the last 10 minutes from the IP address 203.0.113.50.

3. **Analysis**



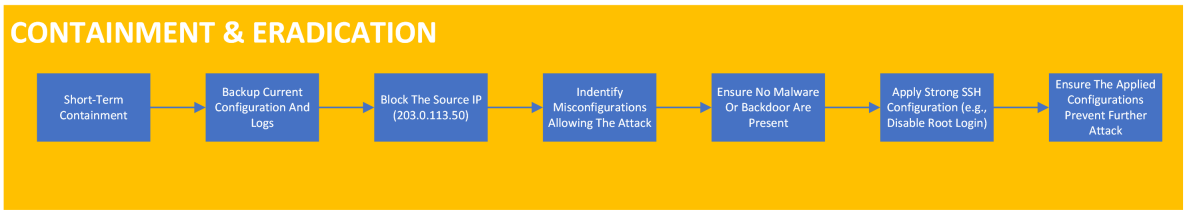
Initial Triage:

- **Analyst**: SOC Analyst
- **Actions**:
    1. **Verify Alert**:
        - Check the logs on the SIEM system to confirm the alert.
        - Verify the number of failed login attempts and the source IP.
    2. **Assess Impact**:
        - Determine if the attack is ongoing.
        - Check if there were any successful login attempts.
    3. **Notify**:
        - Inform the Incident Response (IR) team and relevant stakeholders about the detected brute-force attack.

Log:

Aug 07 10:20:15 webserver sshd[1234]: Failed password for invalid user admin from 203.0.113.50 port 54321 ssh2
Aug 07 10:20:17 webserver sshd[1235]: Failed password for invalid user root from 203.0.113.50 port 54322 ssh2
...
Aug 07 10:30:05 webserver sshd[2234]: Failed password for invalid user test from 203.0.113.50 port 55432 ssh2

4. Containment and Eradication



Short-Term Containment:

- **Actions**:
    1. **Isolate Source IP**:
        - Block the source IP address (203.0.113.50) on the firewall to prevent further attempts.
        - Verify that the block is successfully applied.
    2. **Disable Affected Accounts**:

        - Disable any accounts that showed suspicious activity (e.g., admin, root).
    3. **Enable Rate Limiting**:
        - Apply rate limiting on login attempts to mitigate further brute-force attacks.

Firewall Rule:

iptables -A INPUT -s 203.0.113.50 -j DROP

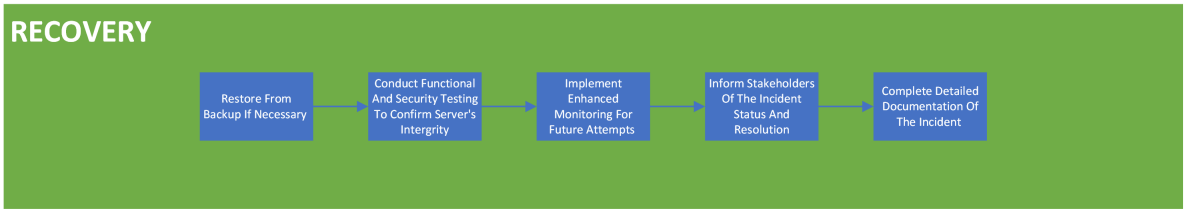
Eradication:

- **Root Cause Analysis**:
    1. **Identify Vulnerabilities**:
        - Check for any misconfigurations or vulnerabilities that allowed the brute-force attack.
        - Ensure that SSH access requires strong, unique passwords or SSH keys.
    2. **Patch and Update**:
        - Apply any necessary patches to the web server software.
        - Update the SSH configuration to enforce stronger security measures.

Configuration Hardening:

PermitRootLogin no
PasswordAuthentication no
AllowUsers specificuser

5. Recovery



System Restoration:

- **Actions**:
    1. **Restore from Backup**:
        - If necessary, restore the web server from a known good backup.
    2. **Revalidate Configurations**:
        - Ensure that all security configurations and hardening measures are applied.
        - Test the functionality of the web server to ensure it is operating correctly.

Validation and Testing:

- **Functional Testing**:
  - Ensure the web server is functioning correctly and that all services are operational.
- **Security Testing**:
  - Conduct vulnerability scans to verify that the brute-force attack vector has been closed.
  - Perform penetration testing to ensure there are no remaining vulnerabilities.

6. Post-Incident Review

Incident Review:

- **Debriefing Session**:
  - Conduct a debriefing session with the incident response team and relevant stakeholders.
  - Review the incident timeline, response actions, and decision-making processes.

Documentation and Reporting:

- **Comprehensive Incident Report**:
  - Prepare a detailed report including:
    - Incident summary and timeline
    - Impact assessment
    - Root cause analysis and attack vector
    - Response actions and remediation steps
    - Findings and evidence collected

Incident Summary Report:

Incident Summary:
- Date: 7 August 2024
- Alert: Brute-Force Attack Detected on Web Server
- Source IP: 203.0.113.50
- Affected System: Web Server (IP: 192.168.1.10)
- Response Actions: Blocked source IP, disabled affected accounts, applied rate limiting, hardened configurations
- Impact: No successful logins detected, no data exfiltration observed

Root Cause Analysis:
- The attacker exploited weak SSH login configurations.
- The web server allowed multiple failed login attempts without rate limiting.

Remediation Steps:

- Blocked the attacking IP address.
- Applied strong SSH configurations.
- Enforced the use of SSH keys for authentication.
- Conducted a full security review of the web server configurations.

Lessons Learned:
- Importance of implementing rate limiting for login attempts.
- Regular review and hardening of SSH configurations.
- Continuous monitoring and alerting for failed login attempts.

Recommendations:
- Regular security training for administrators.
- Implementation of multi-factor authentication for sensitive accounts.
- Periodic vulnerability assessments and penetration testing.

Lessons Learned:

- **Identify Lessons Learned**:
  - Discuss what worked well and what didn't during the incident response.
  - Gather feedback from all participants to understand their perspectives.
- **Update Policies and Procedures**:
  - Revise incident response policies and playbooks based on the lessons learned.
  - Ensure all changes are documented and communicated to relevant teams.

Preventive Measures:

- **Implement Improvements**:
  - Apply technical and procedural improvements to address identified weaknesses.
  - Enhance security measures, such as improved monitoring and new security controls.
- **Employee Training and Awareness**:
  - Conduct training sessions for administrators on secure SSH configurations and best practices.
  - Raise awareness about the importance of monitoring and responding to security alerts.

Follow-Up Actions:

- **Continuous Monitoring**:
  - Implement enhanced monitoring on the web server to detect any signs of recurring attacks.
  - Ensure that the SIEM system is configured to alert on similar activities in the future.
- **Review of Response Capabilities**:

- Assess the effectiveness of the incident response team and their capabilities.
- Provide additional training or resources if needed to enhance the team's readiness for future incidents.

Scenario 2: Data Exfiltration Detected

Alert Details:

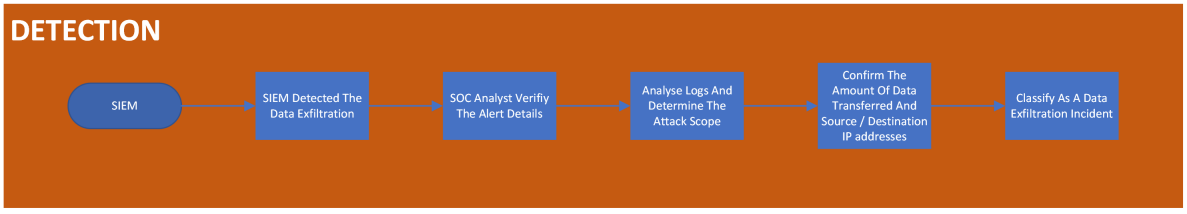
- **Alert Name**: Data Exfiltration Detected
- **Source**: SIEM (Security Information and Event Management) System
- **Time of Alert**: 7 August 2024, 2:45 PM
- **Affected System**: Database Server (IP: 192.168.1.20)
- **Description**: Unusual volume of data transferred to an external IP address.

Incident Response Analysis

1. **Preparation**

- **Policy Development And Communication**
  - Ensure policies for data transfer monitoring and restrictions are in place.
- **Incident Response Plan Development**
  - Have a clear plan for responding to data exfiltration incidents.
- **Training And Awareness**
  - Train staff on detecting and responding to data exfiltration.
- **Tools And Resources**
  - Ensure tools like SIEM, firewalls, and Data Loss Prevention (DLP) solutions are configured and ready.
- **Threat Intelligence**
  - Stay informed about common data exfiltration methods and sources.

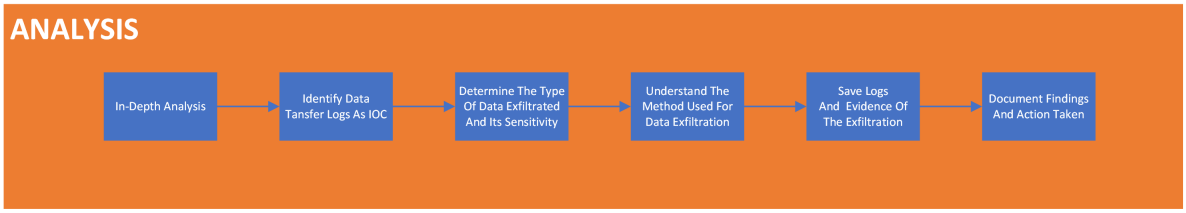
2. **Detection**



Alert Received:

- **Time**: 7 August 2024, 2:45 PM
- **SIEM Alert**: Data Exfiltration Detected on Database Server (IP: 192.168.1.20)
- **Details**: The SIEM system has detected 50 GB of data transferred to the external IP address 198.51.100.100 in the last hour.

3. **Analysis**



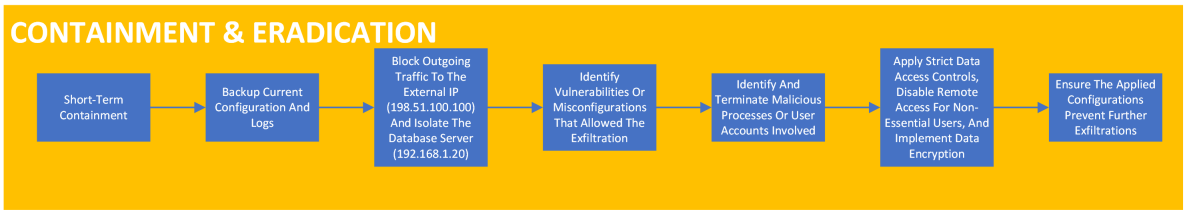
Initial Triage:

- **Analyst**: SOC Analyst
- **Actions**:
    1. **Verify Alert**:
        - Check the logs on the SIEM system to confirm the alert.
        - Verify the amount of data transferred and the source and destination IP addresses.
    2. **Assess Impact**:
        - Determine the type of data that was exfiltrated.
        - Identify the user or process responsible for the data transfer.
    3. **Notify**:
        - Inform the Incident Response (IR) team and relevant stakeholders about the detected data exfiltration.

Log:

Aug 07 14:30:00 dbserver transfer[5678]: 10 GB data transferred to 198.51.100.100
Aug 07 14:35:00 dbserver transfer[5678]: 15 GB data transferred to 198.51.100.100
Aug 07 14:40:00 dbserver transfer[5678]: 25 GB data transferred to 198.51.100.100

4. Containment and Eradication



Short-Term Containment:

- **Actions**:
    1. **Block Data Transfer**:
        - Block outgoing traffic to the external IP address (198.51.100.100) on the firewall.
        - Verify that the block is successfully applied.
    2. **Isolate Affected System**:
        - Isolate the database server (IP: 192.168.1.20) from the network to prevent further data loss.
    3. **Identify and Terminate Malicious Processes**:

- Identify any malicious processes or users responsible for the data transfer.
- Terminate the malicious processes and disable the user accounts involved.

Firewall Rule:

iptables -A OUTPUT -d 198.51.100.100 -j DROP

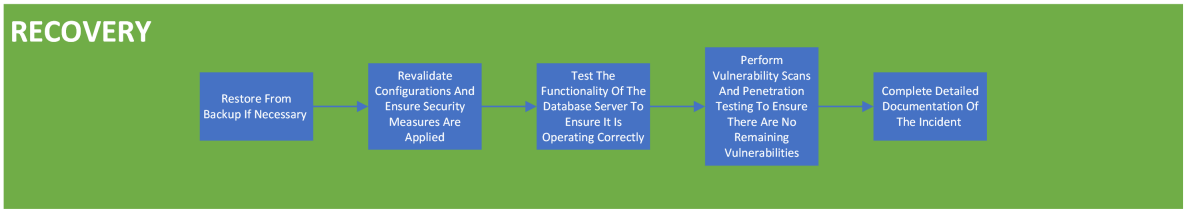
Eradication:

- **Root Cause Analysis**:
  1. **Identify Vulnerabilities**:
     - Check for any vulnerabilities or misconfigurations that allowed the data exfiltration.
     - Ensure that all data access permissions are properly configured.
  2. **Patch and Update**:
     - Apply necessary patches to the database server software.
     - Update the server and application configurations to enforce stronger security measures.

Configuration Hardening:

Disable remote access for non-essential users
Enforce strict data access controls and permissions
Implement data encryption for sensitive information

5. Recovery



System Restoration:

- **Actions**:
  1. **Restore from Backup**:
     - If necessary, restore the database server from a known good backup.
  2. **Revalidate Configurations**:
     - Ensure that all security configurations and hardening measures are applied.
     - Test the functionality of the database server to ensure it is operating correctly.

Validation and Testing:

- **Functional Testing**:
  - Ensure the database server is functioning correctly and that all services are operational.
- **Security Testing**:
  - Conduct vulnerability scans to verify that the data exfiltration vector has been closed.
  - Perform penetration testing to ensure there are no remaining vulnerabilities.

6. Post-Incident Review

Incident Review:

- **Debriefing Session**:
  - Conduct a debriefing session with the incident response team and relevant stakeholders.
  - Review the incident timeline, response actions, and decision-making processes.

Documentation and Reporting:

- **Comprehensive Incident Report**:
  - Prepare a detailed report including:
    - Incident summary and timeline
    - Impact assessment
    - Root cause analysis and attack vector
    - Response actions and remediation steps
    - Findings and evidence collected

Incident Summary Report:

Incident Summary:
- Date: 7 August 2024
- Alert: Data Exfiltration Detected on Database Server
- Source IP: 198.51.100.100
- Affected System: Database Server (IP: 192.168.1.20)
- Response Actions: Blocked outgoing traffic to the external IP, isolated affected system, terminated malicious processes
- Impact: 50 GB of data exfiltrated, sensitive data potentially compromised

Root Cause Analysis:
- The attacker exploited weak data access controls.
- The database server allowed large data transfers without adequate monitoring.

Remediation Steps:

- Blocked the exfiltration IP address.
- Applied strict data access controls and permissions.
- Implemented data encryption for sensitive information.
- Conducted a full security review of the database server configurations.

Lessons Learned:
- Importance of monitoring and alerting for large data transfers.
- Regular review and hardening of data access controls.
- Continuous monitoring and alerting for suspicious data transfer activities.

Recommendations:
- Regular security training for administrators.
- Implementation of data loss prevention (DLP) solutions.
- Periodic vulnerability assessments and penetration testing.

Lessons Learned:

- **Identify Lessons Learned**:
  - Discuss what worked well and what didn't during the incident response.
  - Gather feedback from all participants to understand their perspectives.
- **Update Policies and Procedures**:
  - Revise incident response policies and playbooks based on the lessons learned.
  - Ensure all changes are documented and communicated to relevant teams.

Preventive Measures:

- **Implement Improvements**:
  - Apply technical and procedural improvements to address identified weaknesses.
  - Enhance security measures, such as improved monitoring and new security controls.
- **Employee Training and Awareness**:
  - Conduct training sessions for administrators on secure data handling and best practices.
  - Raise awareness about the importance of monitoring and responding to data exfiltration alerts.

Follow-Up Actions:

- **Continuous Monitoring**:
  - Implement enhanced monitoring on the database server to detect any signs of recurring attacks.
  - Ensure that the SIEM system is configured to alert on similar activities in the future.
- **Review of Response Capabilities**:

- Assess the effectiveness of the incident response team and their capabilities.
- Provide additional training or resources if needed to enhance the team's readiness for future incidents.

Scenario 3: Phishing Email Detected

Alert Details:

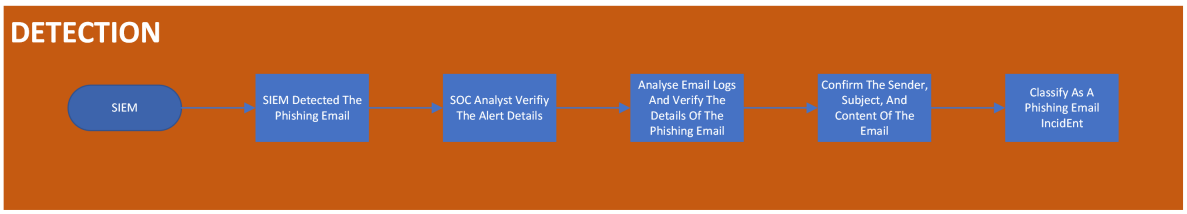
- **Alert Name**: Phishing Email Detected
- **Source**: SIEM (Security Information and Event Management) System
- **Time of Alert**: 7 August 2024, 4:15 PM
- **Affected System**: Employee Workstation (IP: 192.168.1.30)
- **Description**: A phishing email was detected and reported by an employee.

Incident Response Analysis

1. **Preparation**

- **Policy Development And Communication**
  - Establish policies for email security, including phishing detection and response.
- **Incident Response Plan Development**
  - Develop a plan specifically addressing phishing attacks.
- **Training And Awareness**
  - Conduct regular training sessions for employees on identifying and reporting phishing emails.
- **Tools And Resources**
  - Ensure that email filtering tools, web proxies, and SIEM systems are properly configured.
- **Threat Intelligence**
  - Stay updated on common phishing techniques and emerging threats.

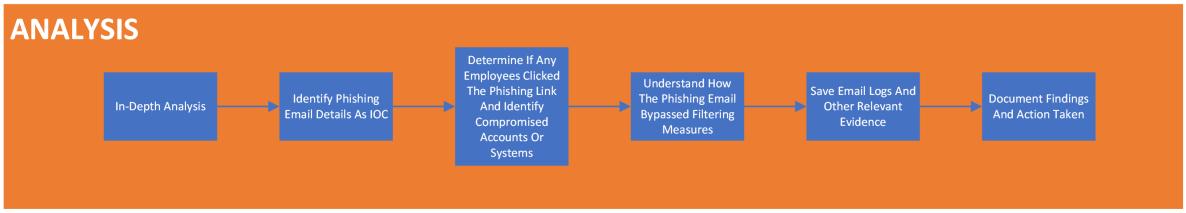
2. **Detection**



Alert Received:

- **Time**: 7 August 2024, 4:15 PM
- **SIEM Alert**: Phishing Email Detected on Employee Workstation (IP: 192.168.1.30)
- **Details**: The SIEM system has detected a phishing email reported by an employee. The email contains a suspicious link to an external website (http://malicious-site.com).

3. **Analysis**



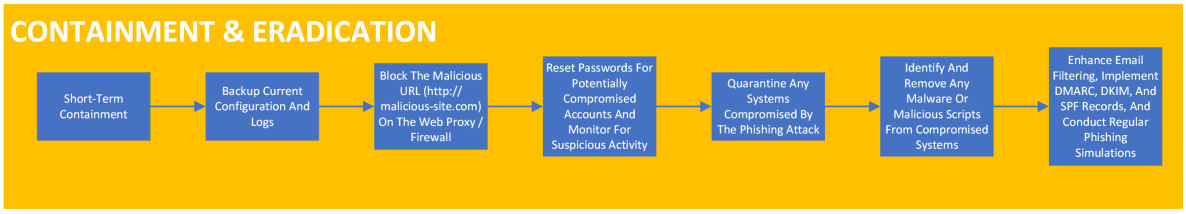
Initial Triage:

- **Analyst**: SOC Analyst
- **Actions**:
    1. **Verify Alert**:
        - Check the email logs on the SIEM system to confirm the alert.
        - Verify the details of the reported phishing email, including the sender, subject, and content.
    2. **Assess Impact**:
        - Determine if any employees have clicked on the phishing link.
        - Identify any compromised accounts or systems.
    3. **Notify**:
        - Inform the Incident Response (IR) team and relevant stakeholders about the detected phishing email.

Email Log:

From: attacker@example.com
To: employee@company.com
Subject: Urgent: Account Verification Required
Body: Please click on the following link to verify your account: http://malicious-site.com

4. Containment and Eradication



Short-Term Containment:

- **Actions**:
    1. **Block Malicious URL**:
        - Block the malicious URL (http://malicious-site.com) on the web proxy/firewall to prevent further access.
        - Verify that the block is successfully applied.
    2. **Isolate Affected Accounts**:

        - Reset passwords for any accounts that may have been compromised.
        - Monitor the affected accounts for any suspicious activity.
    3. **Identify and Quarantine Infected Systems**:
        - Identify any systems that may have been compromised by the phishing attack.
        - Quarantine the infected systems to prevent further spread.

Firewall Rule:

iptables -A OUTPUT -d malicious-site.com -j DROP

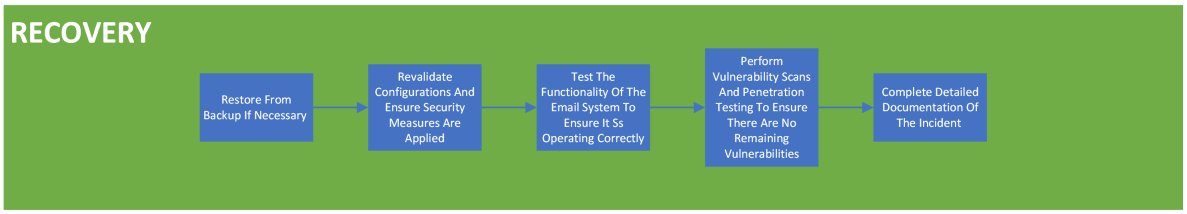
Eradication:

- **Root Cause Analysis**:
    1. **Identify Vulnerabilities**:
        - Check for any vulnerabilities or misconfigurations that allowed the phishing email to reach the employee.
        - Ensure that email filtering and anti-phishing measures are properly configured.
    2. **Patch and Update**:
        - Apply necessary patches to the email filtering system.
        - Update email filtering rules and anti-phishing measures.

Configuration Hardening:

Enable advanced email filtering and anti-phishing measures
Implement DMARC, DKIM, and SPF records for email authentication
Conduct regular phishing simulations and employee training

5. Recovery



System Restoration:

- **Actions**:
    1. **Restore from Backup**:
        - If necessary, restore any compromised systems from a known good backup.
    2. **Revalidate Configurations**:
        - Ensure that all security configurations and hardening measures are applied.

        - Test the functionality of the email system to ensure it is operating correctly.

Validation and Testing:

- **Functional Testing**:
    - Ensure the email system is functioning correctly and that all services are operational.
- **Security Testing**:
    - Conduct vulnerability scans to verify that the phishing attack vector has been closed.
    - Perform penetration testing to ensure there are no remaining vulnerabilities.

6. Post-Incident Review

Incident Review:

- **Debriefing Session**:
    - Conduct a debriefing session with the incident response team and relevant stakeholders.
    - Review the incident timeline, response actions, and decision-making processes.

Documentation and Reporting:

- **Comprehensive Incident Report**:
    - Prepare a detailed report including:
        - Incident summary and timeline
        - Impact assessment
        - Root cause analysis and attack vector
        - Response actions and remediation steps
        - Findings and evidence collected

Incident Summary Report:

Incident Summary:
- Date: 7 August 2024
- Alert: Phishing Email Detected on Employee Workstation
- Source Email: attacker@example.com
- Affected System: Employee Workstation (IP: 192.168.1.30)
- Response Actions: Blocked malicious URL, isolated affected accounts, quarantined infected systems
- Impact: No accounts compromised, potential exposure to phishing

Root Cause Analysis:
- The phishing email bypassed email filtering measures.
- The employee reported the email before any damage was done.

Remediation Steps:
- Blocked the malicious URL.
- Enhanced email filtering and anti-phishing measures.
- Implemented DMARC, DKIM, and SPF records for email authentication.
- Conducted a full security review of the email system configurations.

Lessons Learned:
- Importance of advanced email filtering and anti-phishing measures.
- Regular phishing simulations and employee training.
- Continuous monitoring and alerting for suspicious email activities.

Recommendations:
- Regular security training for employees.
- Implementation of advanced email security measures.
- Periodic vulnerability assessments and penetration testing.

Lessons Learned:

- **Identify Lessons Learned**:
  - Discuss what worked well and what didn't during the incident response.
  - Gather feedback from all participants to understand their perspectives.
- **Update Policies and Procedures**:
  - Revise incident response policies and playbooks based on the lessons learned.
  - Ensure all changes are documented and communicated to relevant teams.

Preventive Measures:

- **Implement Improvements**:
  - Apply technical and procedural improvements to address identified weaknesses.
  - Enhance security measures, such as improved email filtering and new security controls.
- **Employee Training and Awareness**:
  - Conduct training sessions for employees on recognizing phishing emails and best practices.
  - Raise awareness about the importance of reporting suspicious emails promptly.

Follow-Up Actions:

- **Continuous Monitoring**:
  - Implement enhanced monitoring on the email system to detect any signs of recurring attacks.

    - Ensure that the SIEM system is configured to alert on similar activities in the future.
- **Review of Response Capabilities**:
    - Assess the effectiveness of the incident response team and their capabilities.
    - Provide additional training or resources if needed to enhance the team's readiness for future incidents.