Security Monitoring and Incident Response Report

1. Introduction

This report demonstrates the implementation of security monitoring and incident response strategies within a cybersecurity context. It includes the setup of a basic security monitoring system using a mock environment, focusing on one use case to illustrate detection rules, alert prioritization, and response procedures. Additionally, it documents one incident response scenario, detailing incident classification, response steps, and lessons learned. All implementations are supported by evidence of functionality (e.g., mock configurations, logs, and screenshots) and clear documentation of processes. Mock data is used to simulate a realistic network environment, inspired by prior vulnerability scan findings (e.g., from "Apply Vulnerability Assessment Techniques.pdf").

The objective is to showcase practical security monitoring and incident response capabilities, ensuring timely detection and mitigation of cyber threats while improving organizational resilience.

2. Security Monitoring Setup

2.1 Environment Overview

- **Network**: A small local network (192.168.1.0/24) with devices including a gateway (192.168.1.1), workstations (e.g., 192.168.1.93, 192.168.1.153), and servers (e.g., 192.168.1.15).
- **Tools**:
    - **SIEM**: Splunk Enterprise (mock deployment) for log aggregation and alerting.
    - **Network Monitoring**: Zeek (mock deployment) for network traffic analysis.
    - **Endpoint Detection**: Microsoft Defender for Endpoint (mock deployment) for host-based monitoring.
- **Monitoring Scope**: Focus on detecting unauthorized access attempts, particularly targeting the previously identified open port 6783/tcp on 192.168.1.93 (unknown service).

2.2 Use Case: Detecting Unauthorized Access to Port 6783/tcp

Detection Rules

- **Objective**: Detect and alert on multiple failed connection attempts to port 6783/tcp on 192.168.1.93, indicating a potential brute-force or reconnaissance attack.
- **Tool**: Splunk Enterprise.
- **Rule Configuration**:
  - **Data Source**: Firewall logs and Zeek network logs.
  - **Search Query**:
    ```
    index=firewall host=192.168.1.93 port=6783 action=denied | stats count by src_ip | where count > 5 | eval alert_severity=if(count > 10, "High", "Medium")
    ```
  - **Logic**:
    - Monitors firewall logs for denied connections to port 6783/tcp.
    - Counts connection attempts by source IP within a 5-minute window.
    - Triggers an alert if more than 5 attempts are detected (threshold for suspicious activity).
    - Assigns severity: "High" for >10 attempts, "Medium" for 6–10 attempts.
  - **Alert Output**:
    - Sends email to security team (security@org.com).
    - Logs alert in Splunk dashboard with details (source IP, attempt count, timestamp).
- **Evidence of Functionality**:
  - **Mock Log Entry**:
    ```
    2025-04-24T10:15:23Z src_ip=203.0.113.10 dst_ip=192.168.1.93 dst_port=6783 action=denied
    ```
  - ```
    2025-04-24T10:15:24Z src_ip=203.0.113.10 dst_ip=192.168.1.93 dst_port=6783 action=denied
    ```
  - ```
    ... (8 more entries within 5 minutes)
    ```
  - **Mock Alert Generated**:
    ```
    Alert: Unauthorized Access Attempt
    ```

    - `Time: 2025-04-24T10:20:00Z`
    - `Source IP: 203.0.113.10`
    - `Destination: 192.168.1.93:6783`
    - `Attempt Count: 10`
    - `Severity: High`
    - `Action: Investigate and block source IP`
    - **Screenshot Description**: A Splunk dashboard displays the alert with a graph of connection attempts over time, highlighting the spike from 203.0.113.10.

Alert Prioritization Process

- **Criteria**:
    - **Severity**: Based on attempt count (High: >10, Medium: 6–10, Low: ≤5).
    - **Asset Criticality**: Host 192.168.1.93 is a potential workstation/server, increasing priority.
    - **Threat Context**: Multiple failed connections suggest brute-force or reconnaissance, warranting immediate attention.
- **Process**:
    - **Triage**:
        - Alerts are routed to the security team via Splunk.
        - High-severity alerts are prioritized for immediate investigation.
    - **Context Enrichment**:
        - Check Zeek logs for additional traffic from the source IP (e.g., other ports targeted).
        - Query Microsoft Defender for endpoint activity on 192.168.1.93 (e.g., process execution).
    - **Prioritization**:
        - High-severity alerts with confirmed malicious intent (e.g., known malicious IP) are escalated to incident response.
        - Medium-severity alerts are monitored for escalation if patterns persist.
        - Low-severity alerts are logged for trend analysis.
    - **Evidence**:

        - **Mock Triage Log**:
          ```
          Alert ID: 20250424-001
          ```
        - `Status: High Priority`
        - `Reason: 10 failed attempts from 203.0.113.10 to 192.168.1.93:6783`
        - `Enrichment: Zeek logs show scans on ports 80, 443 from same IP`
        - `Action: Escalate to incident response`
- **Justification**:
    - Prioritizing based on severity and asset criticality ensures rapid response to high-risk threats. Enrichment with Zeek and Defender data provides context, reducing false positives and focusing efforts on genuine threats.

Response Procedures

- **Objective**: Contain and mitigate unauthorized access attempts to port 6783/tcp.
- **Steps**:
    1. **Containment**:
        - Add source IP (e.g., 203.0.113.10) to firewall blocklist to prevent further connections.
        - Command: iptables -A INPUT -s 203.0.113.10 -j DROP.
    2. **Investigation**:
        - Analyze Zeek logs for other activities from the source IP.
        - Check 192.168.1.93 logs for successful connections or process execution via Microsoft Defender.
        - Identify the service on port 6783 using nmap -sV -p 6783 192.168.1.93 or packet capture.
    3. **Mitigation**:
        - If the service is unnecessary, disable it (e.g., stop service, block port via firewall).
        - If necessary, apply patches or restrict access (e.g., allow only trusted IPs).
    4. **Documentation**:

        - Log incident details (alert ID, actions, findings) in a ticketing system (e.g., ServiceNow).
        - Update Splunk with resolution status.
    5. **Evidence**:
        - **Mock Firewall Rule**:
        - `Chain INPUT (policy ACCEPT)`
        - `target     prot opt source               destination`
        - `DROP       all  --  203.0.113.10         0.0.0.0/0`
        - **Mock Investigation Log**:
        - `Incident ID: INC-20250424-001`
        - `Findings: No successful connections detected. Service on 6783/tcp identified as custom app (unpatched).`
        - `Action: Blocked source IP, restricted port access to 192.168.1.0/24.`
        - `Status: Resolved`
- **Justification**:
    1. Immediate containment prevents further attacks, while investigation identifies the root cause and service vulnerabilities. Mitigation ensures long-term security, and documentation supports compliance and future analysis.

3. Incident Response Scenario

Scenario: Malware Infection on 192.168.1.93

Incident Classification

- **Description**: On 2025-04-24 at 14:00, Microsoft Defender detected a malicious executable (hash: 25624f3554e989cfb58b220c1742a0334766bb42c5b9f555652b83b3b6d2b6d) on 192.168.1.93, matching a known malware IoC (from "Implement Threat Intelligence Principles.pdf"). The executable attempted to connect to a C2 server (198.51.100.20).
- **Classification**:

- **Type**: Malware Infection.
- **Severity**: Critical.
  - **Impact**: Potential data exfiltration, system compromise, or network propagation.
  - **Likelihood**: High, as the executable is actively running and matches a known threat.
- **Asset Criticality**: 192.168.1.93 is a workstation/server, critical to operations.
- **Threat Context**: The hash links to a phishing-delivered Trojan, indicating a targeted attack.

- **Evidence**:
  - **Mock Defender Alert**:
    ```
    Alert: Malware Detected
    ```
  - `Time: 2025-04-24T14:00:00Z`
  - `Host: 192.168.1.93`
  - `File: suspicious.pdf.exe`
  - `Hash: 25624f3554e989cfb58b220c1742a0334766bb42c5b9f555652b83b3b6d2b6d`
  - `C2 Attempt: 198.51.100.20:443`
  - `Severity: Critical`

Response Steps Taken

1. **Isolation**:
   - Disconnected 192.168.1.93 from the network by disabling its network interface.
   - Command: ip link set eth0 down.
   - Blocked C2 server IP (198.51.100.20) on the firewall.
     - Command: iptables -A OUTPUT -d 198.51.100.20 -j DROP.
2. **Investigation**:
   - Analyzed Defender logs to confirm the executable's actions (e.g., process execution, network connections).
   - Identified the infection vector: A phishing email with a malicious PDF attachment.

- Checked Splunk for related alerts (e.g., prior connections to 198.51.100.20).
- Collected forensic evidence (e.g., memory dump, file copy) using a sandboxed environment.

3. **Eradication**:
   - Quarantined and deleted the malicious executable using Defender.
   - Scanned 192.168.1.93 for additional malware or persistence mechanisms (e.g., registry keys).
   - Reimaged the host to ensure no residual threats.
4. **Recovery**:
   - Restored 192.168.1.93 from a clean backup after verifying no further threats.
   - Reconnected the host to the network with restricted access pending monitoring.
   - Updated antivirus signatures and patched the operating system.
5. **Documentation**:
   - Logged incident details in ServiceNow (INC-20250424-002).
   - Updated Splunk with resolution status and lessons learned.

- **Evidence**:
  - **Mock Splunk Log**:
    ```
    Incident ID: INC-20250424-002
    ```
  - Time: 2025-04-24T14:00:00Z
  - Host: 192.168.1.93
  - Action: Isolated, eradicated malware, reimaged host
  - Findings: Phishing email delivered Trojan
  - Status: Resolved
  - **Mock Firewall Rule**:
    ```
    Chain OUTPUT (policy ACCEPT)
    ```
  - ```
    target     prot opt source               destination
    ```
  - ```
    DROP       all  --  0.0.0.0/0            198.51.100.20
    ```

- **Screenshot Description**: A ServiceNow ticket shows the incident timeline, including isolation, eradication, and recovery steps.

Lessons Learned

1. **Phishing Vulnerability**:
   - **Issue**: Users opened a malicious attachment, indicating insufficient awareness.
   - **Action**: Implement mandatory phishing awareness training and simulate campaigns quarterly.
2. **Delayed Detection**:
   - **Issue**: The malware executed before detection, suggesting gaps in real-time monitoring.
   - **Action**: Enhance Defender's behavior-based detection and integrate with Splunk for faster correlation.
3. **Network Visibility**:
   - **Issue**: Prior connections to the C2 server were not flagged earlier.
   - **Action**: Deploy Zeek signatures for known C2 IPs and monitor outbound HTTPS traffic.
4. **Backup Reliability**:
   - **Issue**: Recovery relied on backups, which were fortunately up-to-date.
   - **Action**: Schedule weekly backup tests and automate verification.

- **Evidence**:
  - **Mock Lessons Learned Report**:
    ```
    Incident: INC-20250424-002
    ```
  - ```
    Lessons:
    1. Phishing training required (Action: Q2 2025 training program).
    2. Enhance real-time detection (Action: Update Defender rules by May 2025).
    3. Improve C2 detection (Action: Zeek signatures deployed 2025-04-25).
    ```
    ```

    - `4. Backup testing (Action: Weekly tests starting May 2025).`

4. Documentation of Processes

Security Monitoring Process

- **Setup**:
    - Deploy Splunk, Zeek, and Microsoft Defender to monitor firewall, network, and endpoint activity.
    - Configure data ingestion for firewall logs (index=firewall), Zeek logs (index=network), and Defender alerts (index=endpoint).
- **Detection**:
    - Create rules in Splunk to detect suspicious activities (e.g., multiple failed connections to port 6783/tcp).
    - Test rules with mock data to ensure alerts trigger correctly.
- **Alert Management**:
    - Triage alerts based on severity, asset criticality, and threat context.
    - Enrich alerts with Zeek and Defender data for context.
    - Escalate high-priority alerts to incident response.
- **Response**:
    - Contain threats by blocking IPs or isolating hosts.
    - Investigate using logs, scans, or forensic tools.
    - Mitigate by removing threats and securing assets.
    - Document actions in Splunk and ServiceNow.

Incident Response Process

- **Preparation**:
    - Maintain updated tools (Splunk, Defender, Zeek) and backups.
    - Train staff on incident response roles.

- **Identification**:
    - Classify incidents based on type, severity, and impact.
    - Use SIEM and EDR alerts to detect incidents.
- **Containment**:
    - Isolate affected hosts and block malicious IPs.
    - Apply short-term fixes to limit damage.
- **Eradication**:
    - Remove malware, patch vulnerabilities, or reimage systems.
    - Verify no residual threats.
- **Recovery**:
    - Restore systems from backups.
    - Monitor for recurrence.
- **Lessons Learned**:
    - Document findings and actions.
    - Update policies, training, and tools based on insights.

5. Conclusion

This report demonstrates the practical implementation of security monitoring and incident response through a mock environment. The security monitoring use case effectively detected unauthorized access attempts to port 6783/tcp using Splunk, with clear prioritization and response procedures. The incident response scenario addressed a critical malware infection, showcasing structured containment, eradication, and recovery steps, supported by lessons learned to prevent recurrence. Evidence such as mock logs, alerts, and configurations validates functionality, while detailed documentation ensures transparency and compliance. By integrating tools like Splunk, Zeek, and Microsoft Defender, organizations can enhance threat detection and response, strengthening their cybersecurity posture.

6. References

- NIST SP 800-61: Computer Security Incident Handling Guide.

- Splunk Documentation: https://docs.splunk.com/Documentation/Splunk.
- Zeek Documentation: https://docs.zeek.org/en/stable/.
- Microsoft Defender for Endpoint: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/.
- OWASP Incident Response Guide: https://owasp.org/www-project-incident-response/.