Security Incident Plan

Developed by Shield Wall IT for Valhalla Systems

Table of Contents

---

1. Purpose

The purpose of this SOP is to define the procedures for testing security controls and monitoring solutions to ensure they effectively detect and respond to security incidents within Valhalla Systems.

---

2. Scope

This SOP applies to all security controls and monitoring solutions implemented within Valhalla Systems' IT infrastructure. It covers the detailed testing procedures, expected outcomes, and the workflow for responding to detected security incidents.

---

3. Responsibilities

- **IT Security Team:** Responsible for conducting the tests, monitoring the results, and updating the security controls and monitoring solutions as necessary.
- **Incident Response Team (IRT):** Responsible for responding to and mitigating security incidents detected during the tests.
- **System Administrators:** Assist with the implementation and testing of security controls and monitoring solutions.

---

4. Security Controls Testing Procedures

1. **Access Control Testing:**
    - Verify that all access controls (e.g., user permissions, MFA) are properly configured and functioning.
    - Test access restrictions by attempting to log in with unauthorized accounts and ensure access is denied.
2. **Firewall and Network Security Testing:**
    - Conduct penetration testing to assess the effectiveness of firewall rules and network segmentation.
    - Use network scanning tools to identify open ports and vulnerabilities.
3. **Endpoint Security Testing:**
    - Deploy and test antivirus and anti-malware solutions on all endpoints.
    - Simulate malware attacks to evaluate the detection and response capabilities.
4. **Data Encryption Testing:**
    - Verify that data at rest and data in transit are encrypted using approved encryption methods.
    - Attempt to access encrypted data without proper decryption keys to test encryption strength.

---

5. Monitoring Solutions Testing Procedures

1. **SIEM (Security Information and Event Management) Testing:**
    - Configure SIEM to collect and analyze logs from various sources (e.g., firewalls, IDS/IPS, servers).
    - Simulate security incidents (e.g., brute force attacks, data exfiltration) and verify that SIEM detects and generates alerts.
2. **Intrusion Detection and Prevention Systems (IDS/IPS) Testing:**
    - Conduct attack simulations (e.g., SQL injection, cross-site scripting) to test IDS/IPS effectiveness.
    - Verify that IDS/IPS alerts are generated, and actions are taken to block or mitigate attacks.
3. **Log Management Testing:**
    - Ensure that logs from critical systems are being collected, stored, and analyzed.
    - Test log correlation and alerting mechanisms by simulating security incidents.

---

6. Expected Outcomes

- **Successful Detection:** All simulated attacks and security incidents should be detected by the respective security controls and monitoring solutions.
- **Alert Generation:** Appropriate alerts should be generated for each detected incident, with details logged for further analysis.

- **Incident Response:** The Incident Response Team should receive alerts and respond according to the incident response plan.
- **Reporting and Documentation:** Detailed reports of the test results should be generated and reviewed to identify areas for improvement.

---

7. Incident Response Workflow Diagram

Below is a simplified diagram illustrating the expected events when an attack triggers the monitoring tools:

```
1. Attack Initiation:
   - An attacker initiates an attack (e.g., brute force, malware).

2. Detection by Security Controls:
   - Security controls (e.g., firewall, IDS/IPS) detect suspicious activity.
   - Logs are generated and sent to the SIEM.

3. SIEM Analysis:
   - SIEM correlates logs and identifies potential security incidents.
   - Alerts are generated and sent to the Incident Response Team (IRT).

4. Incident Response:
   - IRT receives alerts and begins investigation.
   - IRT takes appropriate actions to mitigate the attack (e.g., blocking
IPs, isolating affected systems).

5. Documentation and Reporting:
   - IRT documents the incident details and response actions.
   - A detailed report is generated for review and future reference.
```

---

8. Review and Revision

This SOP will be reviewed annually or as needed based on changes in security best practices or organizational requirements. All revisions will be documented in the revision history section below.

Revision History

Date	Version	Description	Author
5/28/2024	1.0	Initial Version	Gilbert Collado

Approval: I have read and understand the terms and conditions of this Security Incident Plan SOP.

Employee Name (Print): _____

Employee Signature: _____

Date: _____