Author: P. Rajeev Date: 04-11-2025

Response Documentation

1. Incident Response Template

An incident response template provides a structured format to document and manage security incidents effectively. It ensures all key details—detection, analysis, impact, and remediation—are recorded systematically for better response and future prevention.

1.1 Executive Summary

Incident Title / Name: Phishing Incident

Date & Time Detected: 04/11/2025

Reported By / Detection Source: User (Jack)

Analyst Assigned: SOC Analyst

Incident Category: Phishing

Severity Level: High

1.2 Timeline

Date / Time	**Event Description**
04-11-2025 10:00:00 UTC	Phishing email delivered to the user account
04-11-2025 10:15:00 UTC	User clicked the link and entered credentials
04-11-2025 12:00:00 UTC	SIEM alert triggered on suspicious login from external source
04-11-2025 12:05:00 UTC	Account disabled by SOC Analyst

1.3 Impact Analysis

The impact was contained to one user account. Although credentials were stolen, the incident was contained before any lateral movement or data breach occurred. The financial impact was minimal.

1.4 Remediation Steps

1. User account locked and password reset.

2. Suspicious external IP blocked at the firewall.
3. Endpoint cleaned and verified for any malware indicators.

1.5 Lessons Learned & Recommendations

Identified positive detection on suspicious logins, showing effective alert mechanisms.

Improvement: Increase employee awareness about phishing and malicious links.

Prevention: Enforce Two-Factor or Multi-Factor Authentication to prevent future credential compromises.

2. Investigation Steps

Investigation steps are part of the incident response lifecycle, focused on detecting, analyzing, and recovering from security incidents.

Below are the logged actions for a mock phishing incident**:**

Timestamp	**Action**
2025-11-04 13:27:00	Isolated affected user’s device from the network
2025-11-04 13:44:15	Suspicious login session terminated on the mail server
2025-11-04 14:03:04	Collected memory dump from the isolated device for forensic analysis using Velociraptor
2025-11-04 14:30:25	Verified no mail forwarding rules were created on the compromised user account

3. Phishing Checklist

A phishing checklist created in **Google Docs** helps ensure consistency and reduce human error during response operations.

Initial Assessment

[ ] Confirm email headers.

[ ] Check link reputation via VirusTotal/URLScan.

[ ] Check file hash via VirusTotal.

[ ] Identify affected users.

Containment & Eradication

[ ] Force password reset for compromised users.

[ ] Block malicious IP at firewall.

[ ] Delete malicious emails from inboxes.

Post-Incident

[ ] Notify affected users and conduct security awareness.

[ ] Prepare and submit Incident Response Report.

4. Post-Mortem

Post-Mortem is an analysis of a security incident or simulated attack to identify the root cause and evaluate the effectiveness of the response. It helps in improving future detection and mitigation strategies.

Simulated Scenario: A ransomware attack simulated within the network led to temporary file encryption due to delayed detection by the monitoring system.

Lesson Learned: The delay in alert generation allowed limited data encryption. It was observed that log correlation rules need enhancement for faster detection. The primary process improvement is implementing real-time monitoring and automated alerting to ensure immediate analyst response in similar future incidents.