Incident Response Documentation

1. Executive Summary

On **2025-08-21**, a phishing simulation was detected when a user clicked a suspicious link. The Wazuh SIEM generated an alert based on a custom rule. The incident was contained quickly, with minimal impact.

2. Timeline

Timestamp (UTC)	Action Taken
2025-08-21 21:44:29	Wazuh alert triggered: PHISHING-CLICK
2025-08-21 21:46:00	Analyst validated phishing log
2025-08-21 21:47:30	Affected endpoint isolated (mock)
2025-08-21 21:48:00	Memory dump collected (simulated)
2025-08-21 21:55:00	Users warned of phishing attempt
2025-08-21 22:10:00	Incident closed & post-mortem drafted

3. Impact Analysis

- **Scope**: 1 test endpoint (simulated user).
- **Impact**: No real compromise; phishing simulation only.
- **Severity**: Low (educational exercise).

4. Remediation Steps

1. Validated phishing detection rule in Wazuh.
2. Simulated isolating the affected endpoint.
3. Collected mock forensic data (logs, memory dump placeholder).
4. Updated awareness checklist to strengthen phishing detection.

5. Lessons Learned (Post-Mortem, 50 words)

This exercise showed the effectiveness of custom detection rules in Wazuh. Rapid response reduced potential damage. Future improvements include automating phishing detection workflows, better integration with ticketing (TheHive), and refining playbooks. Awareness training remains essential to prevent user clicks on malicious links.