CYART

inquiry@cyart.io

www.cyart.io

Full SOC Workflow Simulation Report

1. Executive Summary

A simulated exploitation attempt targeting a vulnerable service was detected through SOC monitoring controls. The alert was triaged, validated using threat intelligence, and contained before any confirmed system compromise or lateral movement occurred. The incident was escalated to Tier 2 for deeper investigation. Preventive recommendations have been provided to strengthen the organization's security posture.

---

2. Incident Overview

- **Incident Type:** Remote Exploitation Attempt
- **Detection Source:** SIEM / Wazuh Alert
- **Affected Asset:** Server-Y
- **Severity:** High
- **MITRE Technique:** T1210 – Exploitation of Remote Services
- **Status:** Contained

---

3. Timeline of Events

Time	Event
14:00	Exploit attempt detected
14:02	Alert triaged by Tier 1
14:05	IOC validation performed
14:10	Host isolated (simulated)
14:15	Escalated to Tier 2
14:30	Incident documented

4. Detection and Triage

The SOC monitoring system detected suspicious activity consistent with a Samba exploitation attempt.

Key Indicators:

- Suspicious connection pattern
- Known exploit behavior
- Intelligence correlation

Source IP: 192.168.1.101
Technique: T1210 – Remote Service Exploitation

Initial triage classified the alert as **High severity** due to exploitation behavior.

---

5. Response and Containment

The following response actions were performed:

- Reviewed affected host logs
- Validated IOC reputation
- Simulated host isolation
- Recommended IP blocking
- Increased monitoring on target asset

No confirmed post-exploitation activity was observed.

---

6. Escalation Summary

The incident was escalated from Tier 1 to Tier 2 due to:

- Exploitation behavior observed
- High-severity classification
- Potential risk to critical asset

Tier 2 was requested to perform deeper forensic review and lateral movement analysis.

---

7. Impact Assessment

- No confirmed system compromise
- No data exfiltration observed
- No service disruption detected

The threat was contained at an early stage.

---

8. Recommendations

- Patch vulnerable services
- Restrict unnecessary network exposure
- Strengthen intrusion detection rules
- Implement continuous threat monitoring
- Conduct periodic vulnerability assessments

---

9. Conclusion

The simulated incident demonstrated effective SOC detection, triage, escalation, and containment workflows. The structured response minimized potential risk and highlighted the importance of integrating threat intelligence and proper escalation procedures within SOC operations.