Comprehensive SOC Incident Response Report

1. Executive Summary

On 25 December 2025, a security incident involving unauthorized remote access was detected on a legacy Linux system running an outdated Samba service. The attacker exploited a known vulnerability in the Samba usermap_script functionality, resulting in unauthenticated command execution with elevated privileges. The activity originated from IP address 10.0.2.23. Security monitoring controls successfully detected the anomalous behavior, enabling timely investigation and containment. Although threat intelligence sources did not classify the source IP as malicious, confirmed exploitation behavior warranted immediate preventive action. The incident was fully contained within approximately 40 minutes, limiting overall impact.

2. Incident Timeline

Timestamp	Event
2025-12-25 15:58:00	Initial interaction with exposed Samba service observed
2025-12-25 16:00:00	Samba usermap_script vulnerability successfully exploited
2025-12-25 16:01:00	Remote command execution achieved with root privileges
2025-12-25 16:09:00	Suspicious Samba daemon activity detected by monitoring controls
2025-12-25 16:10:00	Alert prioritized based on MITRE ATT&CK mapping
2025-12-25 16:14:00	Incident investigation initiated
2025-12-25 16:22:00	Threat intelligence enrichment completed (IP not malicious)
2025-12-25 16:36:00	Preventive containment action applied to source IP
2025-12-25 16:40:00	Network verification confirmed attacker communication blocked
2025-12-25 16:42:00	Incident stabilized and transitioned to post-incident analysis

Table 1: Timeline

Timestamp	Source IP	Description	MITRE
2025-12-25 16:09:42	10.0.2.23	Samba exploit detected	T1210

Table 2: Alert

3. Impact Analysis

The attacker achieved temporary root-level access to the affected system, allowing execution of arbitrary commands. No evidence of lateral movement, data exfiltration, or persistence was identified. The impact was limited to a single legacy host, and no production systems were affected. Prompt detection and containment significantly reduced attacker dwell time and potential business impact.

4. Root Cause Analysis

- System compromised - Vulnerable Samba service
- Vulnerability existed - Outdated software version
- Software outdated - Patches not applied
- Patches missing - System excluded from patch management
- Exclusion - Incomplete asset inventory and ownership

Root cause identified as a process and governance failure, not a tooling gap.

5. Metrics & Reporting

Using **Elastic Security**, the following metrics were calculated:

Metric	Value
MTTD	9 minutes
MTTR	30 minutes
Dwell Time	40 minutes

Table 3:Metrics

6. Remediation Steps

- Blocked the source IP responsible for exploitation
- Isolated the affected system from the network
- Identified and documented the vulnerable service
- Planned patching or decommissioning of the legacy Samba service
- Updated detection logic for improved visibility into remote service exploitation

7. Lessons Learned

This incident highlighted the risks posed by unmanaged legacy systems and exposed services. While detection and response capabilities functioned effectively, gaps in asset inventory and patch management allowed a known vulnerability to remain exploitable. Future improvements will focus on strengthening asset visibility, enforcing patching standards, and reducing reliance on legacy services to prevent similar incidents.

8. Stakeholder Briefing (Non-Technical)

A security incident was identified involving unauthorized access to a legacy system through a vulnerable network service. Monitoring systems detected the activity within 10 minutes, and containment actions were completed within 40 minutes, limiting potential impact. Although the source was not flagged as malicious by threat intelligence, the observed behavior confirmed unauthorized access and justified immediate blocking.

The investigation determined that the root cause was an outdated service that had not been patched due to gaps in asset tracking and maintenance processes. Improvements are being implemented to strengthen asset visibility, enforce timely patching, and expand automated response capabilities. Overall, the incident demonstrated effective detection and response while highlighting opportunities to reduce future risk and response time.