Post-Incident Analysis – Phishing Incident

A phishing incident occurred when a user clicked a malicious email link, resulting in credential exposure. The incident was detected within 2 hours and fully contained within 4 hours. A structured post-incident review was conducted to identify root causes, document lessons learned, and evaluate SOC performance metrics.

Root Cause Analysis – 5 Whys

Question	Answer
Why was the email opened?	User clicked malicious link
Why was the link clicked?	Email appeared legitimate
Why did it appear legitimate?	Weak email filtering controls
Why were filters weak?	Outdated email security configuration
Why was configuration outdated?	No periodic security review process

The 5 Whys analysis revealed that outdated email filtering and lack of regular security configuration reviews were the primary contributors to the incident.

Fishbone Analysis Summary

A Fishbone (Ishikawa) diagram was created to categorize contributing factors:

- **People:** Lack of phishing awareness training
- **Process:** No formal email review workflow
- **Technology:** Weak spam filtering, no URL inspection
- **Policy:** No quarterly security audits, no enforced MFA

This structured breakdown helped identify systemic weaknesses beyond the initial user action.

SOC Metrics Calculation

Metric	Value
MTTD (Mean Time to Detect)	2 Hours
MTTR (Mean Time to Respond)	4 Hours

The incident was detected in 2 hours and resolved within 4 hours. While response time was effective, earlier detection mechanisms and stronger email controls could reduce future detection time and prevent recurrence.