Post-Incident Analysis Report

1. Executive Summary

This report presents a detailed post-incident analysis of a phishing incident. A malicious email bypassed email security controls and was opened by a user, who clicked on a malicious link. Although no confirmed data compromise occurred, the incident revealed gaps in email filtering, security awareness, and preventive controls. Root Cause Analysis (RCA) was conducted using the 5 Whys method, and contributing factors were analyzed. SOC performance metrics such as MTTD and MTTR were calculated to assess detection and response efficiency.

2. Root Cause Analysis (5 Whys Method)

Question	Answer
Why was the email opened?	The user trusted the sender and content.
Why was the malicious link clicked?	The message created urgency and looked legitimate.
Why did it look legitimate?	Email filtering failed to detect phishing indicators.
Why did filtering fail?	Email security rules were outdated.
Why were rules outdated?	No periodic review or tuning process existed.

Table 1: 5 Whys Method

The absence of a structured review process for email security configurations resulted in outdated detection rules, allowing phishing emails to bypass controls.

3. SOC Metrics Calculation

Mean Time to Detect (MTTD)

- Detection Time = **2 hours**
- **MTTD = 2 hours**

Mean Time to Respond (MTTR)

- Response Time = **4 hours**
- **MTTR = 4 hours**

4. Impact Assessment

- **User Impact:** Single user affected
- **System Impact:** No system compromise
- **Data Impact:** No data loss detected
- **Business Impact:** Minimal
- **Risk Level:** Medium

5. Lessons Learned

- Email security controls require continuous tuning
- User behavior remains a critical risk factor
- SOC metrics provide valuable insight into response efficiency
- Proactive phishing simulations improve detection readiness

6. Final Conclusion

The phishing incident was detected within two hours, demonstrating reasonable monitoring effectiveness. The response was completed within four hours, indicating acceptable containment capability. However, preventive measures were insufficient. Enhancing email security controls, enforcing regular configuration reviews, and improving user awareness training will significantly reduce phishing risks.