Post-Incident Analysis Report

1. Root Cause Analysis (5 Whys Method)

Question	Answer
Why was the phishing email opened?	The user clicked on a malicious email link
Why did the user click the link?	The email appeared legitimate and urgent
Why did it appear legitimate?	Email security filters failed to detect the phishing email
Why did email filtering fail?	Spam detection rules were outdated
Why were rules outdated?	Lack of regular email security review and updates

Root Cause Summary

The primary root cause of the incident was inadequate maintenance of email security controls combined with insufficient user awareness training, allowing a phishing email to bypass defenses and be acted upon by the user.

2. Fishbone (Ishikawa) Analysis

Problem Statement:
➡️ Successful Phishing Incident

Contributing Factors

People

- Lack of phishing awareness training
- Users unable to identify suspicious emails

Process

- No scheduled email security audits
- Weak incident response preparedness

Technology

- Outdated spam and phishing filters
- Absence of advanced email threat detection

Policy

- No mandatory cybersecurity awareness policy
- Missing enforcement of email verification procedures

3. SOC Metrics Calculation

Incident Timeline

- **Detection Time:** 2 hours
- **Response Time:** 4 hours

Calculated Metrics

- **MTTD (Mean Time To Detect):** 2 hours
- **MTTR (Mean Time To Respond):** 4 hours

4. Metrics Summary (50 Words)

The phishing incident was detected within two hours, demonstrating moderate monitoring effectiveness. Response actions were completed in four hours, indicating acceptable containment efficiency. Enhancing email filtering, updating security policies, and conducting regular user awareness training can significantly reduce future detection and response times.