Post-Incident Analysis Report

Introduction

This document presents a structured post-incident analysis of a mock phishing attack scenario. It highlights the steps taken to perform a Root Cause Analysis (RCA), visual representation using a Fishbone Diagram, and calculation of key Security Operations Center (SOC) metrics such as Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). The purpose of this report is to document lessons learned and provide actionable improvements to strengthen defenses against future incidents.

Mock Incident Analysis

Overview

Incident Type: Phishing attack

Impact: User clicked on a malicious link received via email

Objective of Analysis: Identify underlying causes, document findings, and evaluate SOC performance metrics.

Root Cause Analysis (RCA) – 5 Whys Method

The 5 Whys method was applied to identify the underlying cause of the phishing incident.

Question	Answer
Why was email opened?	User clicked malicious link.
Why was link clicked?	Weak email filtering.
Why was email filter weak?	Outdated filtering rules.
Why were rules outdated?	No regular updates.
Why no updates?	Lack of clear process ownership.

Key Finding: The incident was not just a user awareness issue but a systemic problem with outdated filtering rules and unclear ownership of the update process.

Fishbone Diagram (Cause and Effect)

A Fishbone Diagram was created in Draw.io to visualize potential contributing factors.

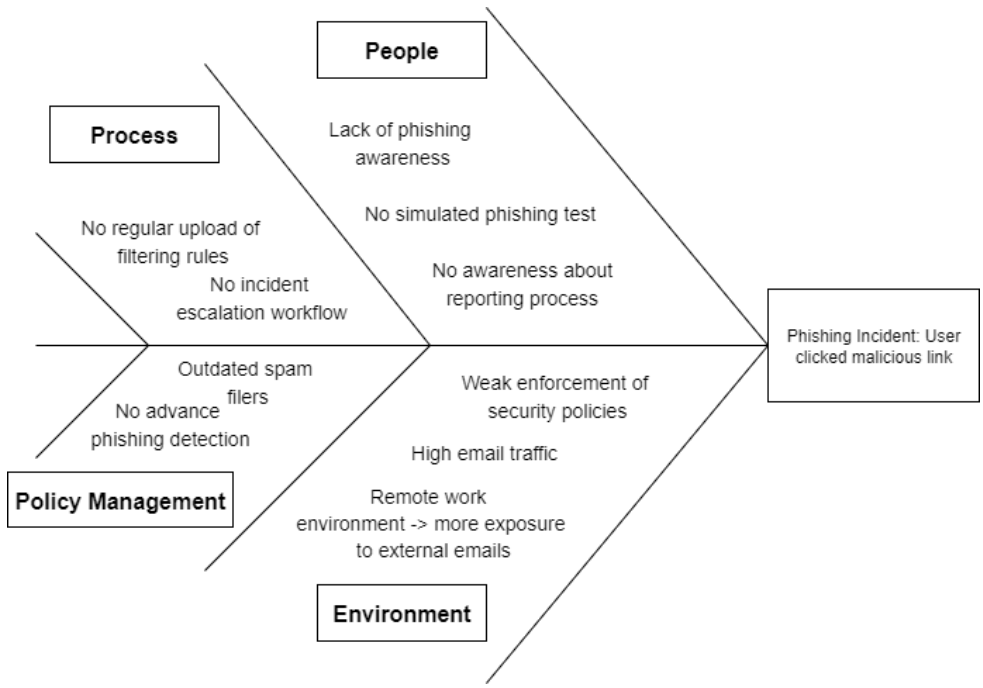
Categories of Causes Identified:

Process: No defined update process, inadequate training sessions.

Technology: Weak spam filter, absence of advanced phishing detection tools.

People: Limited awareness, no phishing simulation exercises.

Policy/Management: Lack of ownership for email security, insufficient incident response procedures.



1: Fishbone Diagram

SOC Metrics Calculation

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

Summary (50 words):

The phishing incident was detected within two hours (MTTD) and contained in four hours (MTTR). The root cause was traced to weak email filtering and outdated rules. Improvements such as stronger filtering, dedicated process ownership, and enhanced user awareness training will reduce detection and response times in the future.

Conclusion

The analysis revealed that while user awareness is a factor, systemic weaknesses in filtering rules and process ownership were the primary causes of the incident. Going forward, the SOC should:

- Implement regular updates for email filtering rules.
- Assign clear ownership for email security processes.
- Conduct periodic phishing awareness and simulation training.

By addressing these gaps, the SOC can reduce incident occurrence, improve detection times, and accelerate responses.

References

- Google Sheets – Used for documenting Root Cause Analysis and SOC metrics.
- Draw.io – Used to create the Fishbone Diagram.
- NIST Cybersecurity Framework – Guidance for incident detection and response best practices.