Post-Incident Analysis

1. Objective

This report contains the details of the task includes Root Cause Analysis, Fishbone Diagram, and Metrics Calculation. The goal of this task is to:

- Master post-incident analysis to drive continuous improvement in SOC operations.

2. Introduction

Post-incident analysis is a crucial phase of incident response that focuses on understanding how an attack occurred and how defenses can be improved. Rather than closing a case once containment is complete, the SOC reviews evidence, identifies root causes, documents lessons learned, and measures performance using metrics such as MTTD and MTTR. This structured reflection strengthens processes, enhances technology configurations, and reinforces user awareness so future incidents are detected faster and handled more effectively.

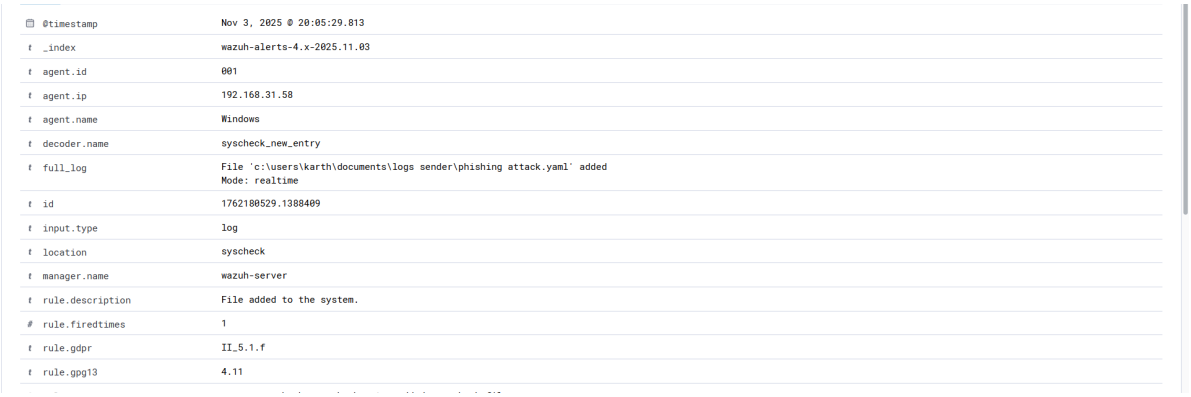
3. Tools

- Google Sheets
  https://docs.google.com/document/
- Draw.io
  https://app.diagrams.net/

4. Root Cause Analysis

Root cause analysis means identifying where actually the problem started or the vulnerability is. Using 5 Whys method for a mock phishing incident. These 5 Whys are very important in-order to perform root cause analysis.

4.1 Mock Phishing Incident



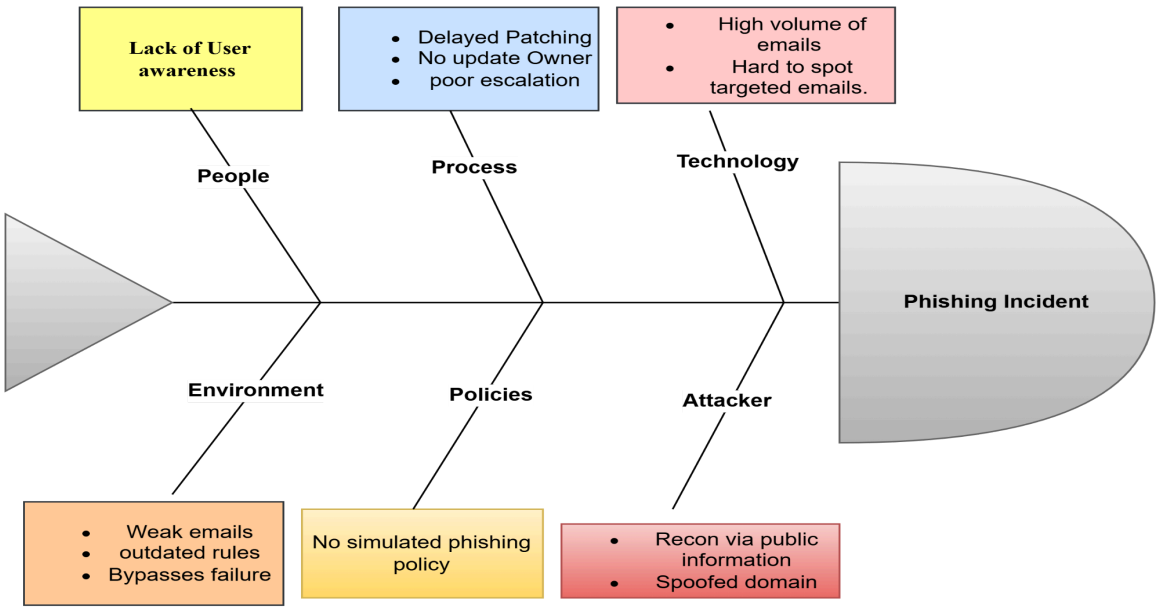
@timestamp	Nov 3, 2025 @ 20:05:29.813
_index	wazuh-alerts-4.x-2025.11.03
agent.id	001
agent.ip	192.168.31.58
agent.name	Windows
decoder.name	syscheck_new_entry
full_log	File 'c:\users\karth\documents\logs sender\phishing attack.yaml' added Mode: realtime
id	1762180529.1388409
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	File added to the system.
rule.firedtimes	1
rule.gdpr	II_5.1.f
rule.gpg13	4.11

Documenting the mock phishing incident and that document includes questions and answers. The 5 Why questions need to be included in the documentation along with answers.

Question	Answer
Why was the email opened?	The user clicked a malicious link.
Why was the link clicked?	The email looked legitimate and bypassed suspicion.
Why did the email look legitimate?	Email filtering rules failed to detect phishing indicators(e.g., IP, Hash file).
Why did filtering fail?	Outdated signature detection.
Why were they outdated?	There was no automated updation process.

5 Fishbone Diagram

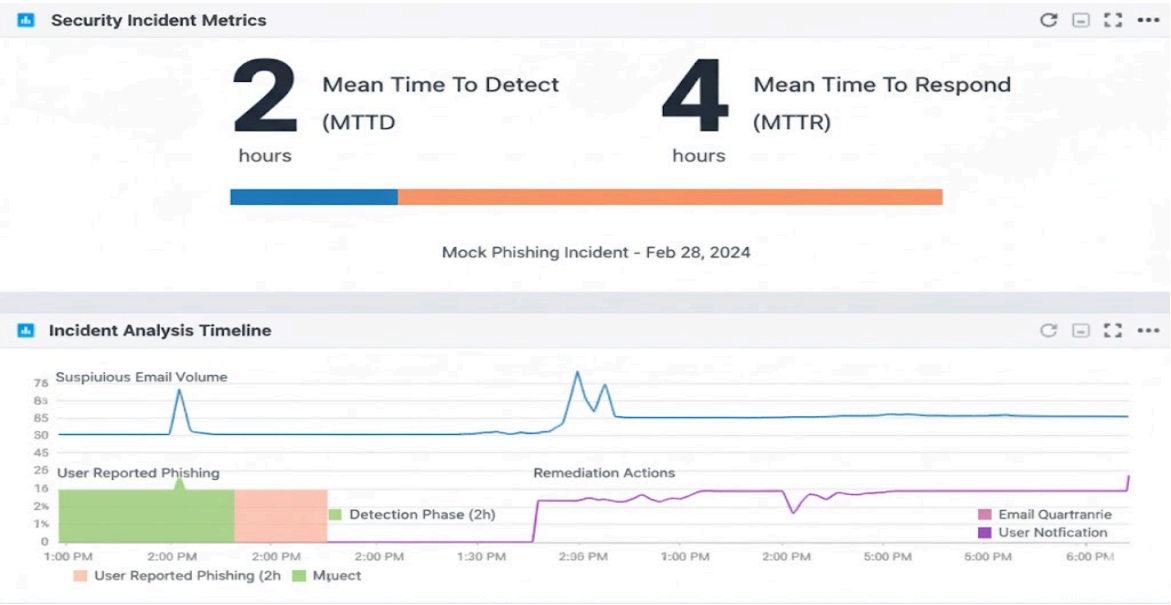
Fishbone diagram includes the mock phishing incident details. In this below diagram it showing The 5 Whys answers are People, Process, Technology, Environment, Policies, and Attacker. This diagram is very important because it gives details of area of improvement.



6. Metrics Calculation

Calculated MTTD (Mean Time To Detect) and MMTR (Mean Time To Respond) for a mock phishing incident (e.g., Detection: 2 hours, Response: 4 hours). I calculated both MMTD and MMTR for this phishing incident and I found detection time as one and half hour and response time as four hours total incident duration is five and half hours.

Mean Time To Detect = 1 ½ hr.
Mean Time To Respond = 4 hrs.
Total incident duration = 5 ½ hrs.



6.1 Summary of Metrics Calculation

The phishing incident was detected within one and half hour and fully contained within four hours, resulting in a total exposure time of five and half hours. The event involved a single user account. Response time could be further improved by enhancing alert fidelity, expanding automated containment, and tightening user awareness training to prevent initial compromise.