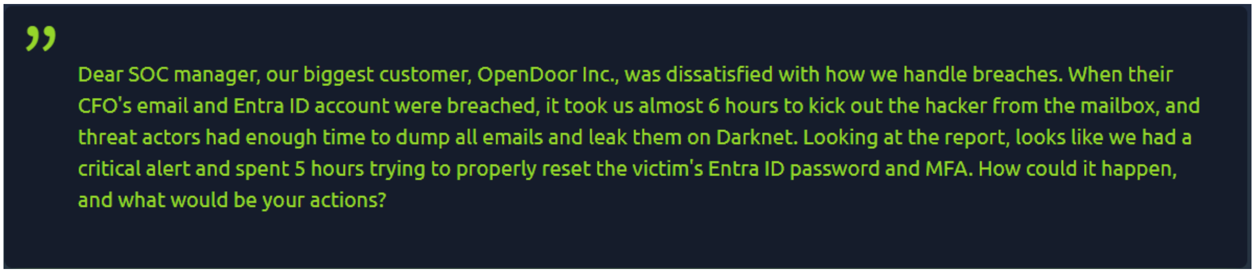
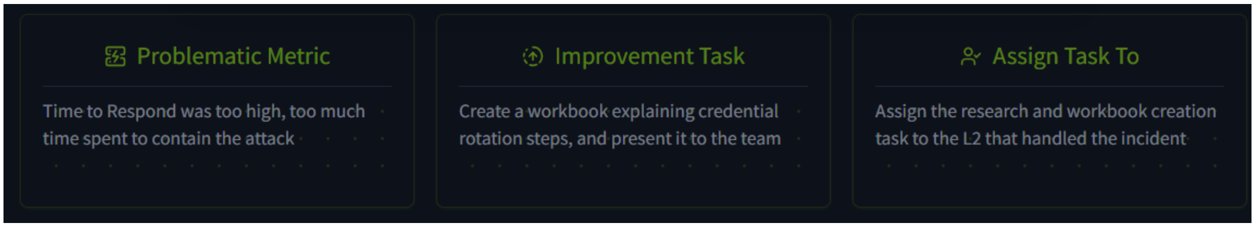
# Improving SOC metrics 2026/01/03

**Objective**: For this lab, I was tasked to imagine myself as a SOC manager receiving different complaints related to the SOC team. Improving SOC metrics across three scenarios by correctly assigning improvement tasks from the list.

### Scenario 1 – Unhappy customer



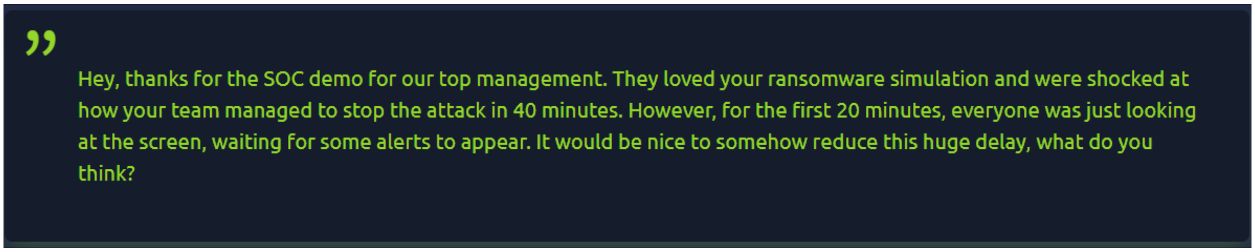
> Dear SOC manager, our biggest customer, OpenDoor Inc., was dissatisfied with how we handle breaches. When their CFO's email and Entra ID account were breached, it took us almost 6 hours to kick out the hacker from the mailbox, and threat actors had enough time to dump all emails and leak them on Darknet. Looking at the report, looks like we had a critical alert and spent 5 hours trying to properly reset the victim's Entra ID password and MFA. How could it happen, and what would be your actions?



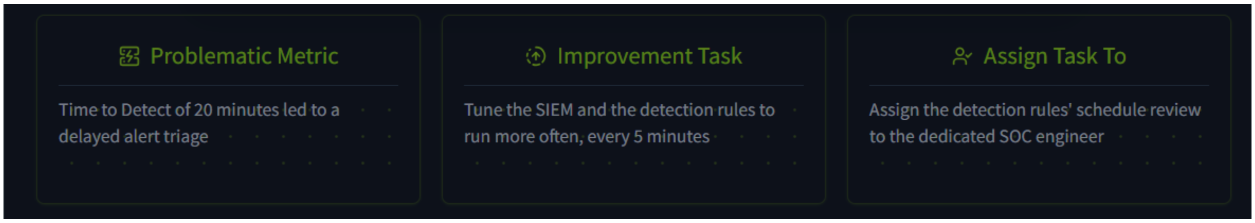
| Problematic Metric | Improvement Task | Assign Task To |
|---|---|---|
| Time to Respond was too high, too much time spent to contain the attack | Create a workbook explaining credential rotation steps, and present it to the team | Assign the research and workbook creation task to the L2 that handled the incident |

The problem here was that the team had a high MTTR. To improve workflow, creating a playbook/runbook would be beneficial to team efficiency. Assigning this task to the L2 that handled the True Positive would be a good idea due to their investigation expertise.

### Scenario 2 – Delayed alert



> Hey, thanks for the SOC demo for our top management. They loved your ransomware simulation and were shocked at how your team managed to stop the attack in 40 minutes. However, for the first 20 minutes, everyone was just looking at the screen, waiting for some alerts to appear. It would be nice to somehow reduce this huge delay, what do you think?



Problematic Metric

Time to Detect of 20 minutes led to a delayed alert triage

Improvement Task

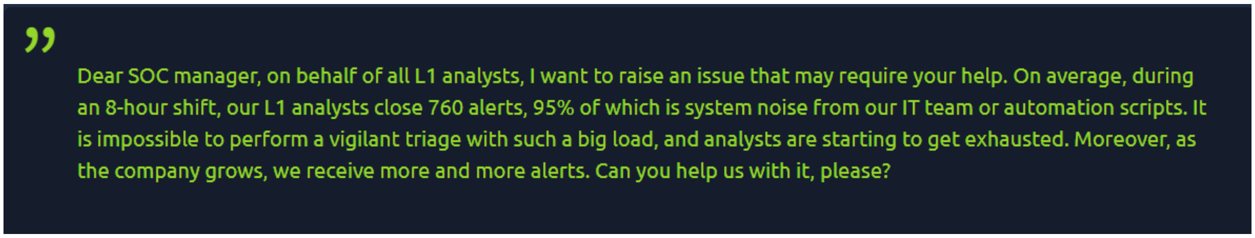
Tune the SIEM and the detection rules to run more often, every 5 minutes

Assign Task To

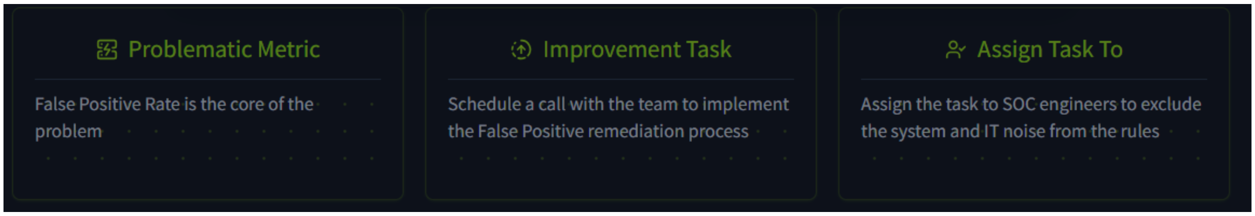
Assign the detection rules' schedule review to the dedicated SOC engineer

The problem here was the MTTD, 20 minutes is too much time spent on detecting an incident and lowering this time would be efficient. To improve this, tuning and running SIEM every 5 minutes would be feasible. Assigning this task to the dedicated SOC engineer would be the right action to take on improving overall detection rate.

**Scenario 3 – Tired analysts**



Dear SOC manager, on behalf of all L1 analysts, I want to raise an issue that may require your help. On average, during an 8-hour shift, our L1 analysts close 760 alerts, 95% of which is system noise from our IT team or automation scripts. It is impossible to perform a vigilant triage with such a big load, and analysts are starting to get exhausted. Moreover, as the company grows, we receive more and more alerts. Can you help us with it, please?



Problematic Metric

False Positive Rate is the core of the problem

Improvement Task

Schedule a call with the team to implement the False Positive remediation process

Assign Task To

Assign the task to SOC engineers to exclude the system and IT noise from the rules

The problem here was the FPR rules. To improve this, scheduling a call with the team to implement a remediation process would be the hammer on the nail. Assigning this task to SOC engineers to exclude the system and IT noise from the rules would certainly help lift weight off of L1 analysts.

**Summary Conclusion**

This lab highlighted how SOC performance can be improved by addressing key operational metrics. By analysing high MTTR, delayed MTTD, and excessive false positives, appropriate corrective actions were identified and assigned to the right roles. Implementing runbooks, tuning SIEM detection frequency, and refining alert rules demonstrated how structured processes and collaboration directly enhance SOC efficiency, accuracy, and analyst effectiveness.