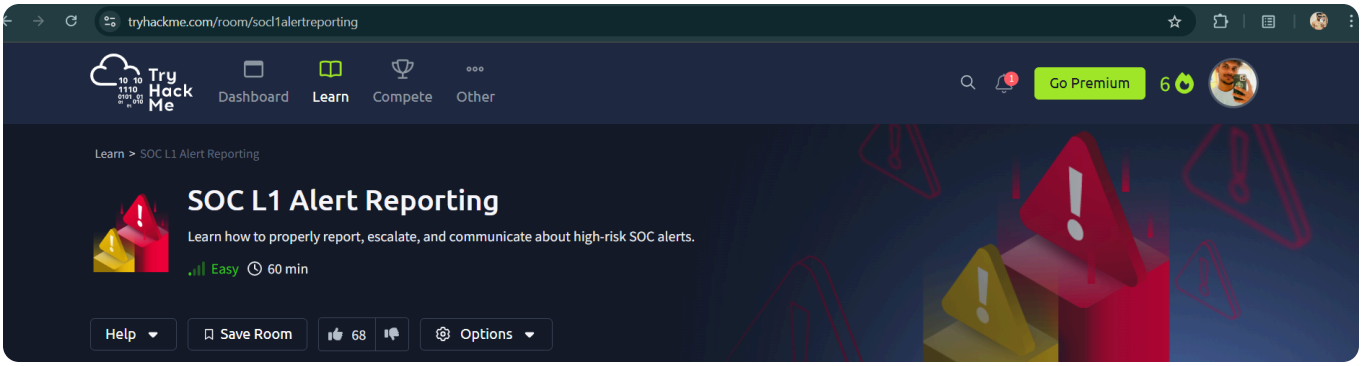
SOC L1 Alert Reporting



Task 1 Introduction

During or after alert triage, L1 analysts may be uncertain about how to classify the alert, requiring senior support or information from the system owner. Also, L1 may deal with real cyberattacks and breaches that need immediate attention and remediation actions. This room covers these cases by introducing three new terms: alert reporting, escalation, and communication.

Learning Objectives

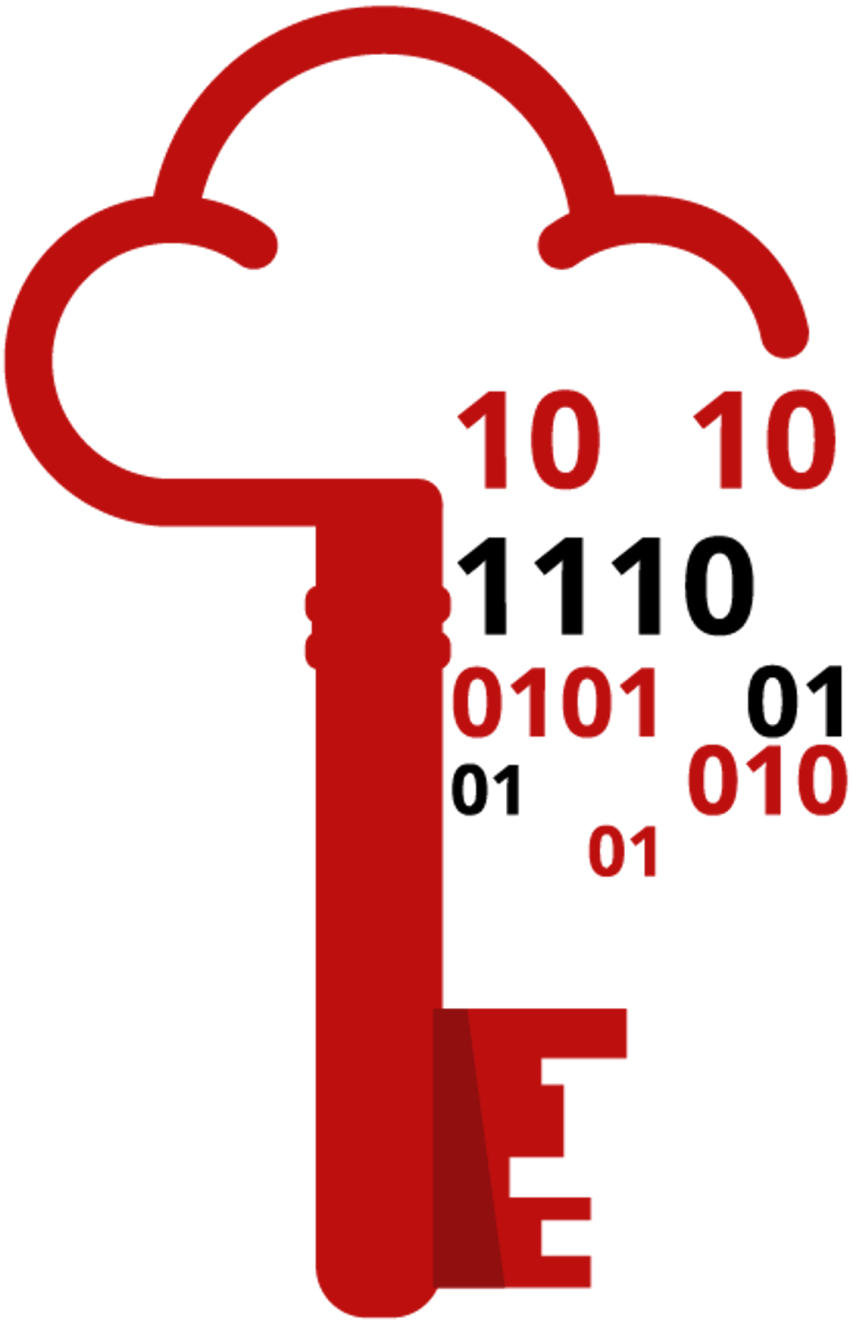
- Understand the need for SOC alert reporting and escalation
- Learn how to write alert comments or case reports properly
- Explore escalation methods and communication best practices
- Apply the knowledge to triage alerts in a simulated environment
- Feel more confident in SOC Simulator and during SAL1 certification

Prerequisites

- Complete the preceding SOC L1 Alert Triage room
- Have a basic understanding of common attacks
- Know the responsibilities of SOC L1 analysts

SOC Dashboard

Continue your journey in the SOC dashboard! This time you will need it to write professional reports and practice in escalating the alerts. Open the attached website in a separate window by clicking on the SOC dashboard link below and move on to the next task!



Access	Granted
URL	SOC dashboard

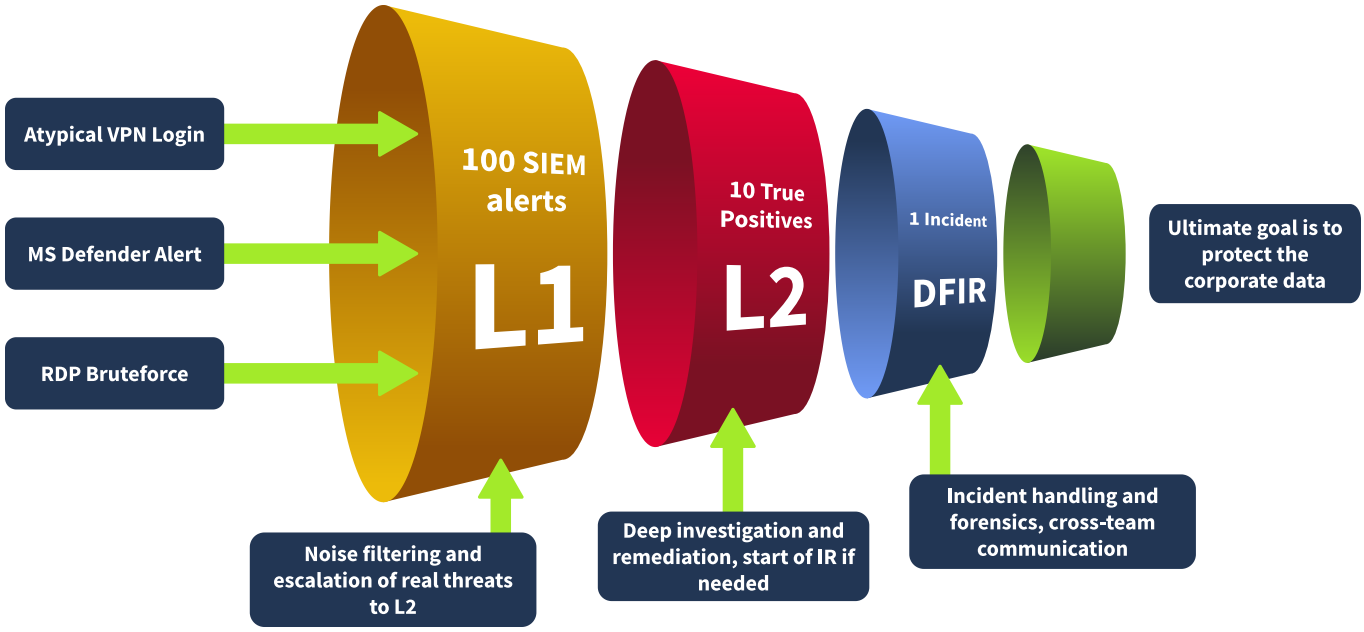
Answer the questions below

I am ready to start

Task 2 Alert Funnel

In the previous room, you learned how to classify and triage the alerts. But you might be curious about what happens next. How does your triage help prevent threats and stop breaches? This is a whole new topic that this room will cover soon, but for now, let's recall the path of the alerts.

First, L1 analysts receive the alerts in a SIEM, EDR, or a ticket management platform. Most of the alerts are closed as False Positives or are handled on L1 level, but complex and threatening ones are sent to L2 that remediate most breaches. And to send the alerts further, you need to learn three new terms: reporting, escalation, and communication.



Alert Reporting

Before closing or passing the alert to L2, you might have to report it. Depending on team standards and alert severity, instead of a short alert comment, you can be required to document your investigation in detail, ensuring all relevant evidence is included. This is especially important for True Positives, which require escalation.

Alert Escalation

If the True Positive alert requires additional actions or deeper investigation, escalate it to the L2 analyst for further review following the agreed procedures. That's where your alert report comes in handy since L2 will use it to get the initial context and spend less on the analysis from scratch.

Communication

You may also need to communicate with other departments during or after the analysis. For example, ask the IT team if they confirm granting administrative privileges to some users or contact HR to get more information about the newly hired employee.

==Answer the questions below

==QES 1 *What is the process of passing suspicious alerts to an L2 analyst for review?

ANS **Alert Escalation

==QES 1 *What is the process of formally describing alert details and findings?

ANS **Alert Reporting

==Task 3Reporting Guide

Before we move on, it is essential to clarify why anyone would want L1 analysts to write reports in addition to marking them as True or False Positives and why this topic can not be underestimated. Having L1 analysts write alert reports serves several key purposes:

Alert Report Purpose	Explanation
Provide context for escalation	- A well-written report saves lots of time for L2 analysts - Also, it helps them quickly understand what happened
Save findings for the records	- Raw SIEM logs are stored for 3-12 months, but alerts are kept indefinitely - As a result, it's better to keep all the context inside the alert, just in case
Improve investigation skills	- If you can't explain it simply, you don't understand it well enough - Report writing is a great way to boost L1 skills by summarising alerts

Report Format

![An example of good, structured report following the 5Ws approach]
Imagine yourself as an L2 analyst, a DFIR team member, or an IT professional who needs to

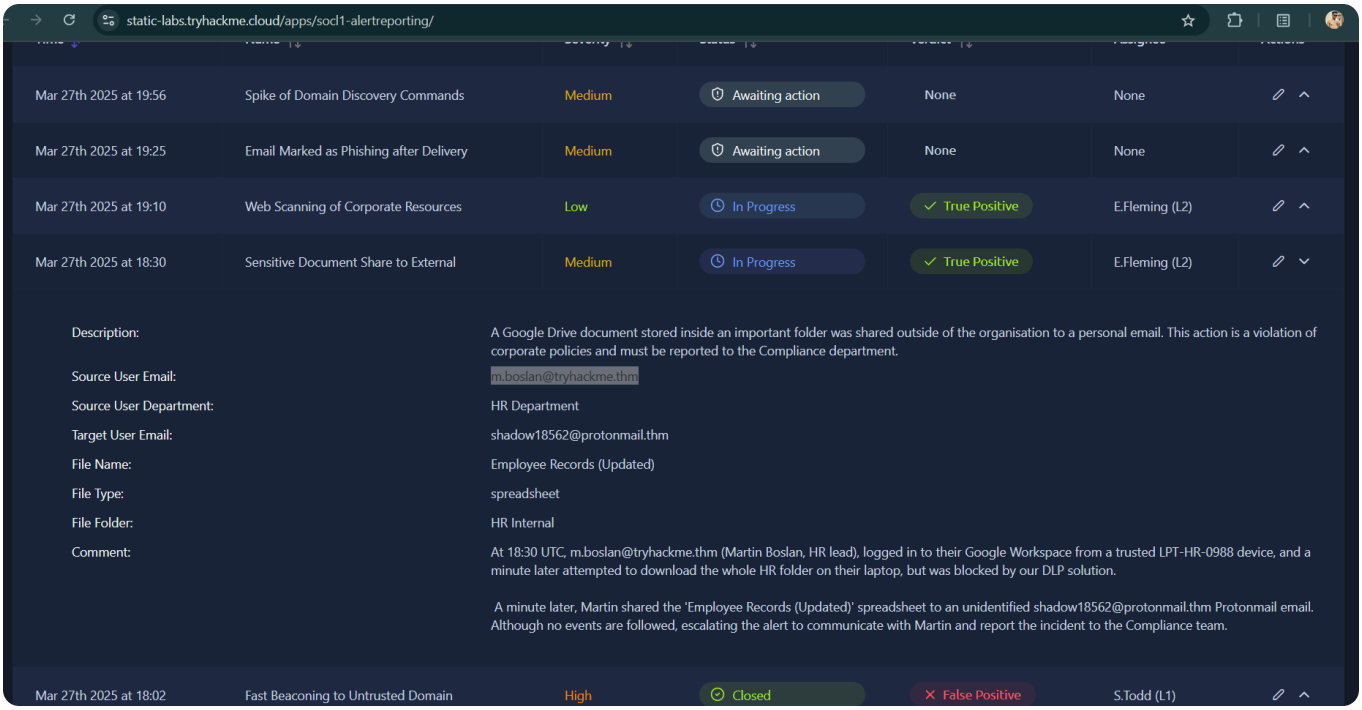
understand the alert. What would you want to see in the report? We recommend you follow the [redacted] approach and include at least these items in the report:

- **Who**: Which user logs in, runs the command, or downloads the file
- **What**: What exact action or event sequence was performed
- **When**: When exactly did the suspicious activity start and ended
- **Where**: Which device, IP, or website was involved in the alert
- **Why**: The most important W, the reasoning for your final verdict

==Answer the questions below

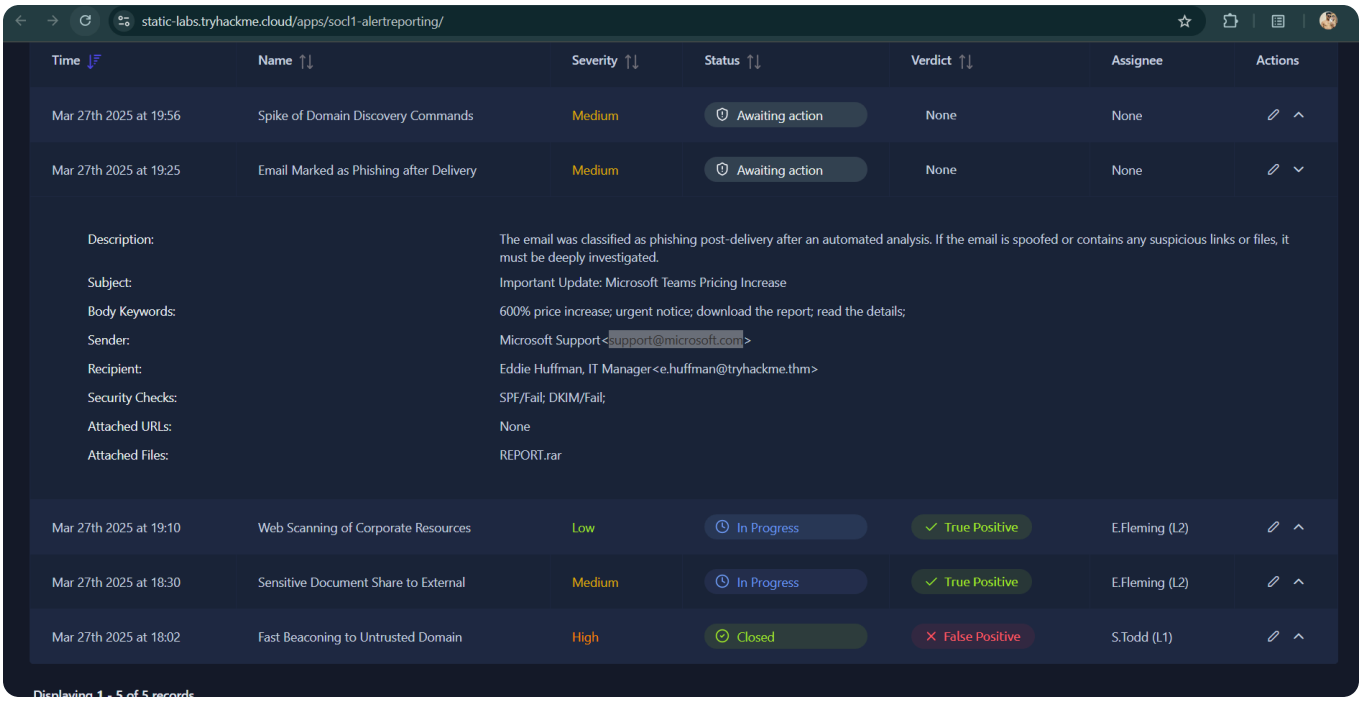
==QES 1 *According to the SOC dashboard, which user email leaked the sensitive document?

ANS m.boslan@tryhackme.thm



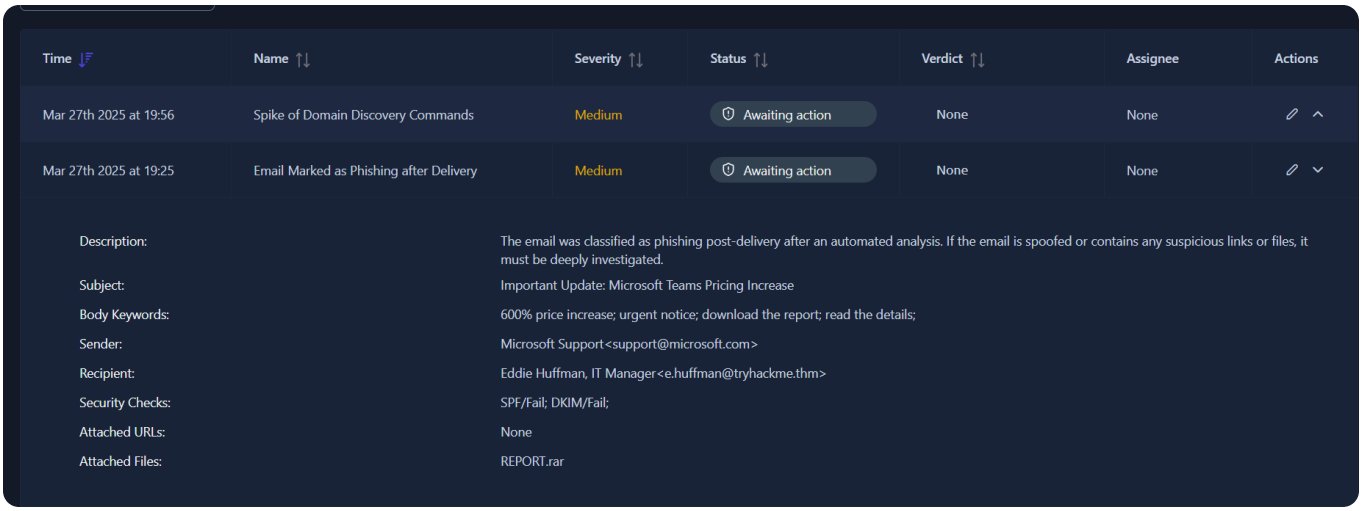
==QES 2 Looking at the new alerts, who is the "sender" of the suspicious, likely phishing email?

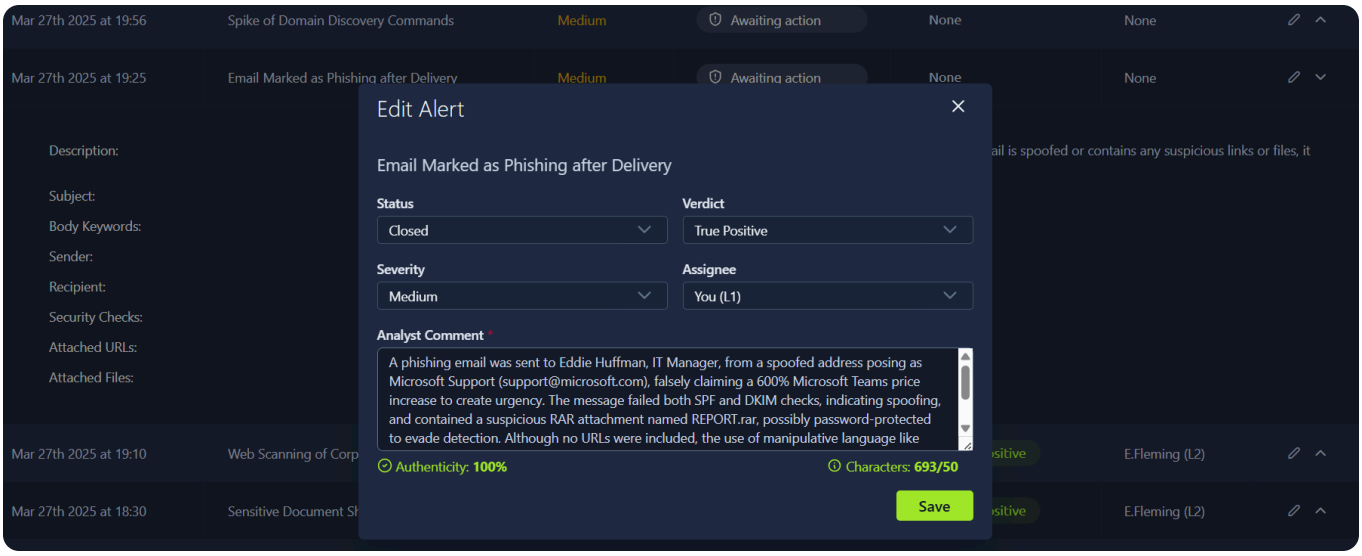
ANS support@microsoft.com

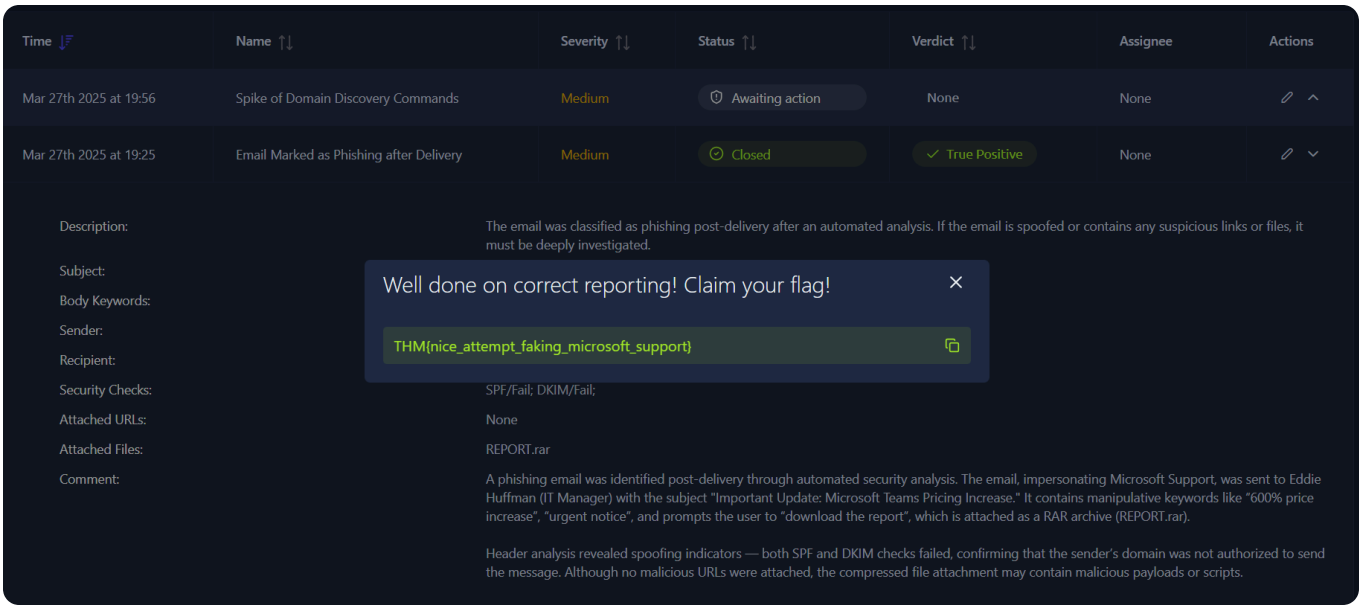


==QES 3 Open the phishing alert, read its details, and try to understand the activity. Using the Five Ws template, what flag did you receive after writing a good report?

ANS **THM{nice_attempt_faking_microsoft_support}







==Task 4 Escalation Guide

After you have made a verdict and written your alert report, you must choose whether to escalate the alert to L2. Again, the answer may differ from team to team, but the following recommendations would generally fit most SOC teams. You should escalate the alerts if:

1. The alert is an indicator of a major cyberattack requiring deeper investigation or DFIR
2. Remediation actions like malware removal, host isolation, or password reset are required
3. Communication with customers, partners, management, or law enforcement agencies is required
4. You just do not fully understand the alert and need some help from more senior analysts

Escalation Steps

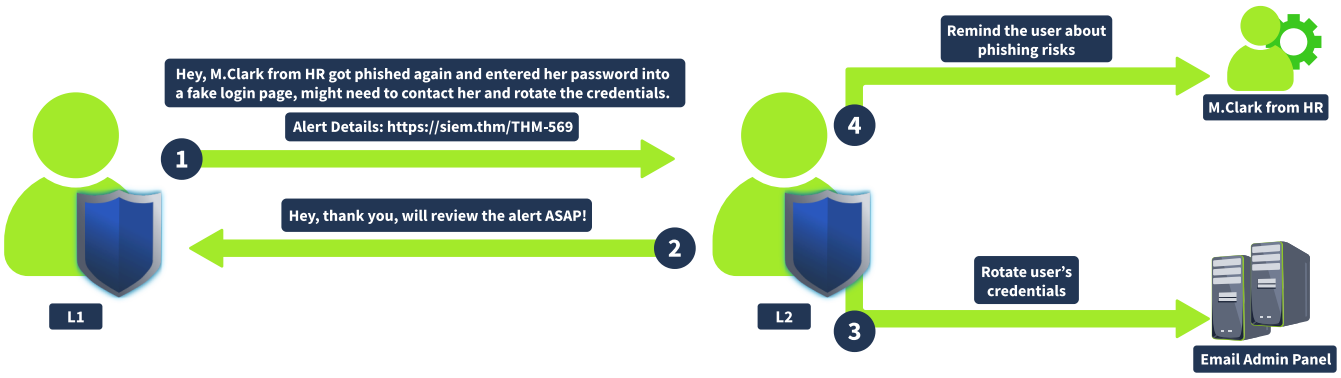
To escalate the alert, in most cases, all you have to do is to reassign the alert to the L2 on shift and ping them in corporate chat or in person. In some teams though, you may be required to create a formal written escalation request with dozens of required fields.

No matter what the agreements are, L2 will eventually receive the ticket from you, read your report, and contact you in case of any questions. Once everything is clear, the L2 analyst will typically research the alert details further, validate if the alert is indeed a True Positive, communicate with other departments if needed, and, for major incidents, start a formal Incident Response process.

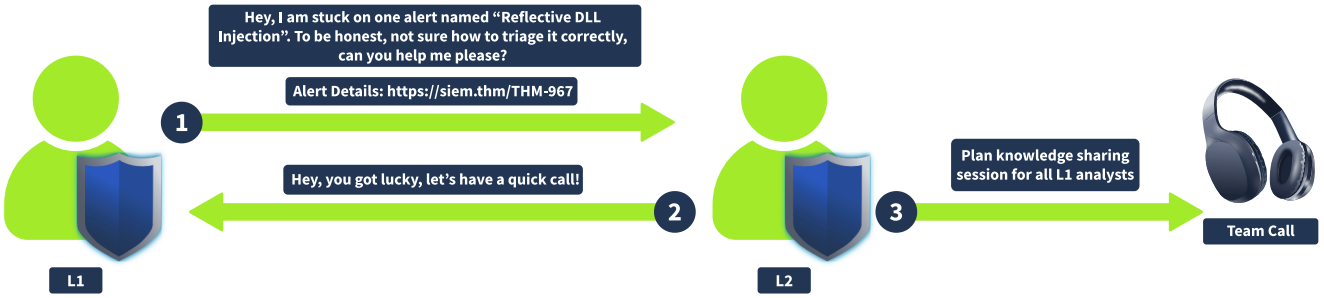
SOC Dashboard Escalation Procedure

1. Write an alert report and provide your verdict; move the alert to In Progress status
2. Assign the alert to your L2 on shift. L2 will receive a notification and start from your report

Escalating Threats to L2



Requesting L2 Support



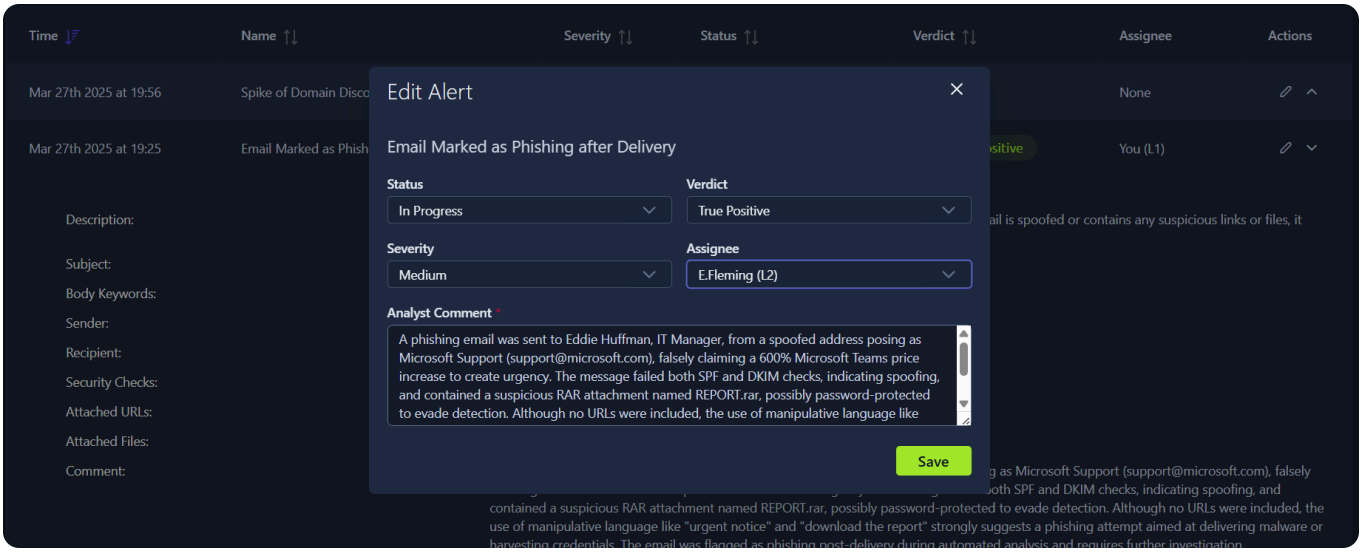
Answer the questions below

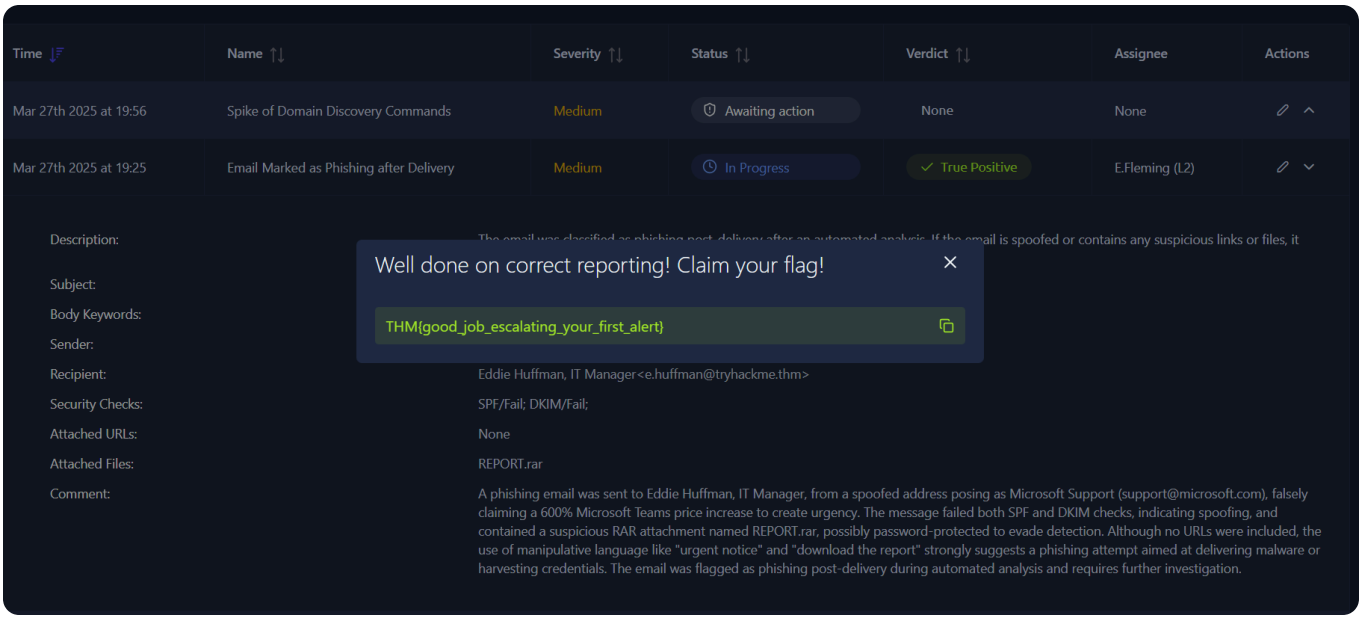
==QES 1 Who is your current L2 in the SOC dashboard that you can assign (escalate) the alerts to?

ANS E.Fleming

==QES 2 What flag did you receive after correctly escalating the alert from the previous task to L2?
Note: If you correctly escalated the alert earlier, just edit the alert and click "Save" again

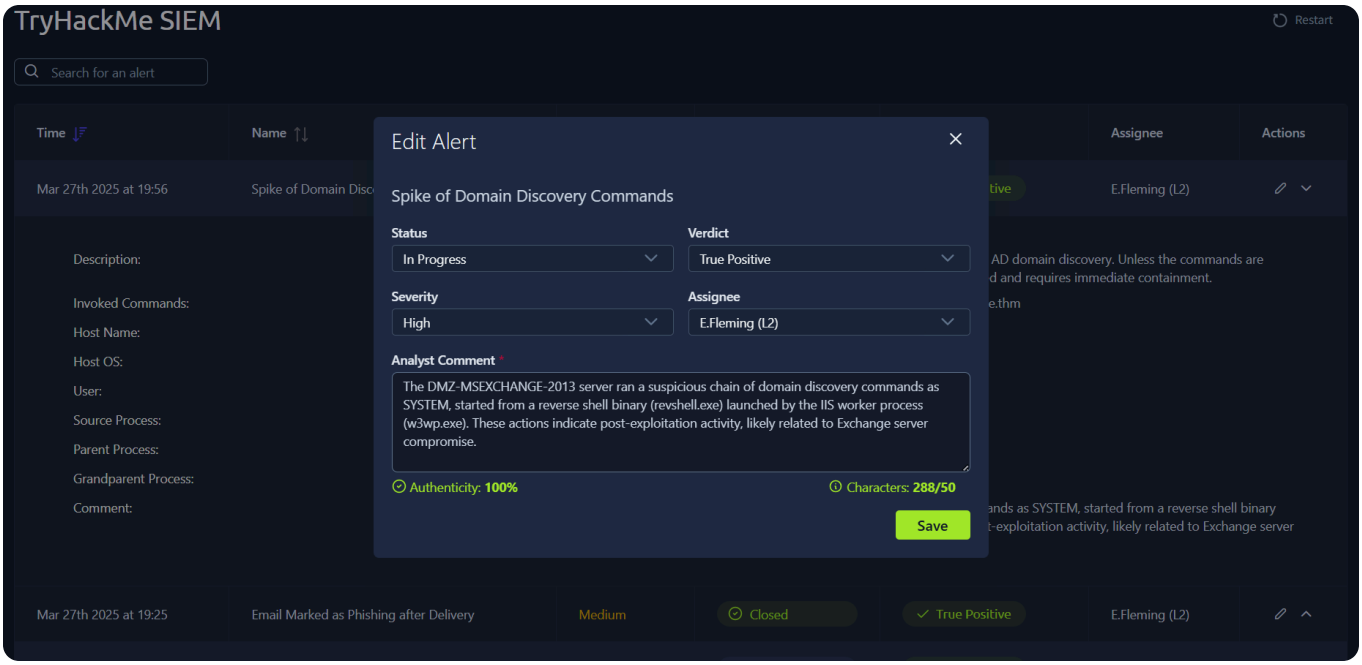
ANS *THM{good_job_escalating_your_first_alert}

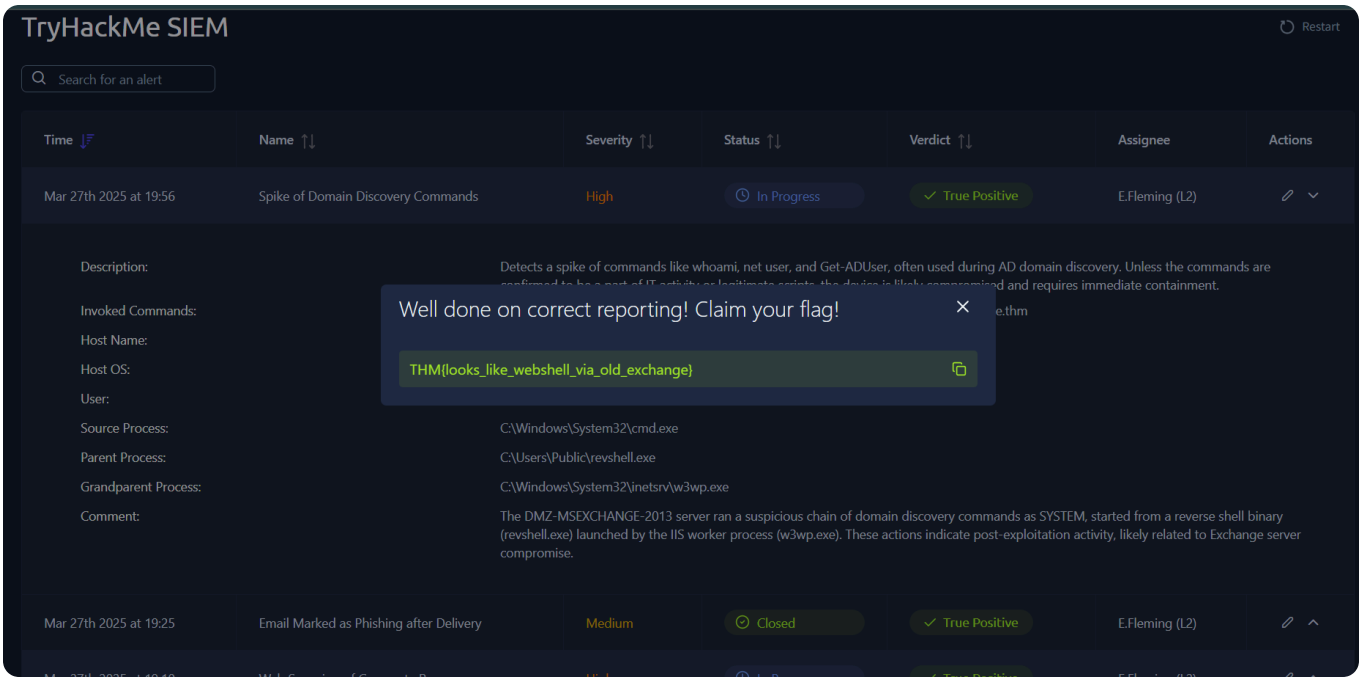




==QES 3 Now, investigate the second new alert in the queue and provide a detailed alert comment.
Then, decide if you need to escalate this alert and move on according to the process.
After you finish your triage, you should receive a flag, which is your answer!

ANS *THM{looks_like_webshell_via_old_exchange}





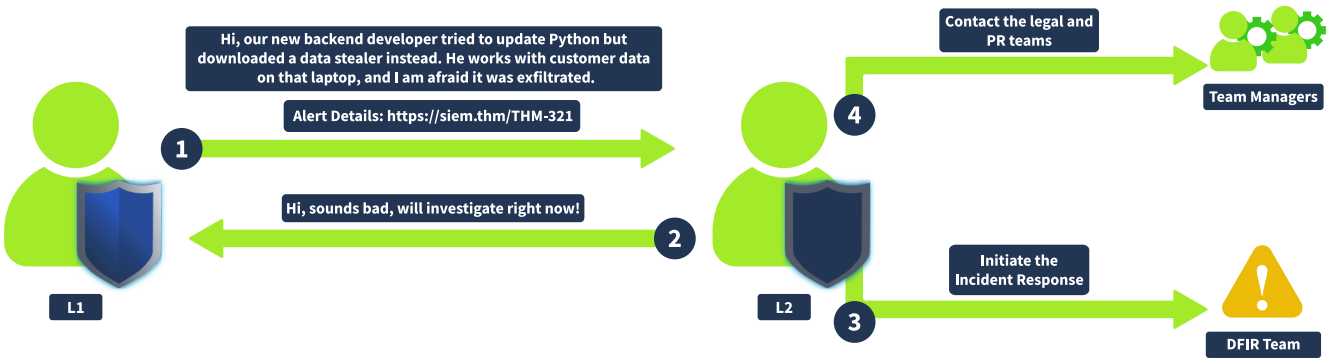
==Task 5 SOC Communication

The escalation and reporting topics should sound straightforward and logical to you. But, as always, it's easier said than done, and you should be prepared for unexpected scenarios and know what to do in critical cases. In the best scenario, the SOC team has its own **Crisis Communication** procedures - the guides and processes to help you and your teammates resolve the issues. If not, you are advised to read the cases below and be prepared to handle them effectively.

Communication Cases

- **You need to escalate an urgent, critical alert, but L2 is unavailable and does not respond for 30 minutes.**
  Ensure you know where to find emergency contacts. First, try to call L2, then L3, and finally your manager.
- **The alert about Slack/Teams account compromise requires you to validate the login with the affected user.**
  Do not contact the user through the breached chat - use alternative contact methods like a phone call.
- **You receive an overwhelming number of alerts during a short period of time, some of which are critical.**
  Prioritise the alerts according to the workflow, but inform your L2 on shift about the situation.
- **After a few days, you realise that you misclassified the alert and likely missed a malicious action.**
  Immediately reach out to your L2 explaining your concerns. Threat actors can be silent for weeks before impact.
- **You can not complete the alert triage since the SIEM logs are not parsed correctly or are not searchable.**
  Do not skip the alert - investigate what you can and report the issue to your L2 on shift or SOC engineer.

Communication By L2



Answer the questions below

==QES 1 Should you first try to contact your manager in case of a critical threat (Yea/Nay)?

ANS *Nay*

QES 2 Should you immediately contact your L2 if you think you missed the attack (Yea/Nay)?
ANS *Yea*

##==Task 6 Conclusion

Great job learning three important SOC skills: alert reporting, escalation, and communication. These skills are essential for any L1 analysts: Alert reporting helps to preserve and provide activity context for L2, escalation ensures threats are remediated in time, and communication makes the coordination between SOC and other departments clear and effective.

Answer the questions below

I am ready to move on!