

SOC L1 Alert Triage

The screenshot shows the TryHackMe platform interface. At the top, there's a navigation bar with icons for Try Hack Me, Dashboard, Learn, Practice, Compete, a search bar, a notification bell with 9 notifications, a 'Go Premium' button, a user icon with '1' and a 'h' inside, and a profile picture.

The main content area is titled 'SOC L1 Alert Triage'. It features a thumbnail image of a book titled 'Triage Guide' with a yellow exclamation mark on it. Below the thumbnail, the title 'SOC L1 Alert Triage' is displayed, along with a description: 'Learn more about SOC alerts and build a systematic approach to efficiently triaging them.' It also shows a duration of '60 min' and '18,236' participants.

Below the title are several buttons: 'Share your achievement', 'Save Room', '433 Recommend', and 'Options'. A progress bar at the bottom indicates 'Room completed (100%)'.

A tooltip message appears in the center: 'Stuck on a question? I am here to help you with real-time guidance, personalized hints, and explanations.' It includes a small green robot icon and a link to 'More Info'.

Under the 'Task 1' heading, there's a sub-section titled 'Introduction' with a green robot icon. The text below states: 'An alert is a core concept for any SOC team, and knowing how to handle it properly ultimately decides whether a security breach is detected and prevented, or missed and devastating.'

Room completed (100%)

You were granted access to the SOC dashboard in the TryHackMe SIEM, and you will need it to complete most of the tasks. Open the attached website in a separate window, familiarise yourself with it, and move on to the next task!



Answer the questions below

I am ready to start!

No answer needed

✓ Correct Answer

Task 2 Events and Alerts

Task 3 Alert Properties

Task 4 Alert Prioritisation

Room completed (100%)

L1 Role in Alert Triage

SOC L1 analysts are the first line of defence, and they are the ones who work with alerts the most. Depending on various factors, L1 analysts may receive zero to a hundred alerts a day, every one of which can reveal a cyberattack. Still, everyone in the SOC team is somehow involved in the alert triage:

- **SOC L1 analysts:** Review the alerts, distinguish bad from good, and notify L2 analysts in case of a real threat
- **SOC L2 analysts:** Receive the alerts escalated by L1 analysts and perform deeper analysis and remediation
- **SOC engineers:** Ensure the alerts contain enough information required for efficient alert triage
- **SOC manager:** Track speed and quality of alert triage to ensure that real attacks won't be missed

Answer the questions below

What is the number of alerts you see in the SOC dashboard?

5

✓ Correct Answer

What is the name of the most recent alert you see?

Double-Extension File Creation

✓ Correct Answer

Task 3 Alert Properties

ROOM COMPLETED (100%)

8	Alert Fields	Provides SOC analysts' comments and values on which the alert was triggered	• Entered Commandline • And many more, depending on the alert
---	--------------	---	--

Answer the questions below

What was the verdict for the "Unusual VPN Login Location" alert?

False Positive ✓ Correct Answer

What user was mentioned in the "Unusual VPN Login Location" alert?

M.Clark ✓ Correct Answer 💡 Hint

Tutor A Alert Prioritization X

Stuck on a question? I am here to help you with real-time guidance, personalized hints, and explanations. 🚀

6 Conclusion ▼

Room completed (100%)

cause much more impact than medium or low ones.

3. Sort by time

Start with the oldest alerts and end with the newest ones. The idea is that if both alerts are about two breaches, the hacker from the data, while the "newcomer" has just started the discovery.

Answer the questions below

Should you first prioritise medium over low severity alerts? (Yea/Nay)

Yea

Should you first take the newest alerts and then the older ones? (Yea/Nay)

Nay

Assign yourself to the first-priority alert and change its status to **In Progress**.

The name of your selected alert will be the answer to the question.

Potential Data Exfiltration



SOC Dashboard Notes

If you didn't receive a flag after your triage, it means that the values you set are wrong.

You can reset the SOC dashboard by clicking **Restart** on the top right in the TryHackMe SIEM.

Answer the questions below

Which flag did you receive after you correctly triaged the first-priority alert?

THM{looks_like_lots_of_zoom_meetings}

✓ Correct Answer

✗ Hint

Which flag did you receive after you correctly triaged the second-priority alert?

THM{how_could_this_user_fall_for_it?}

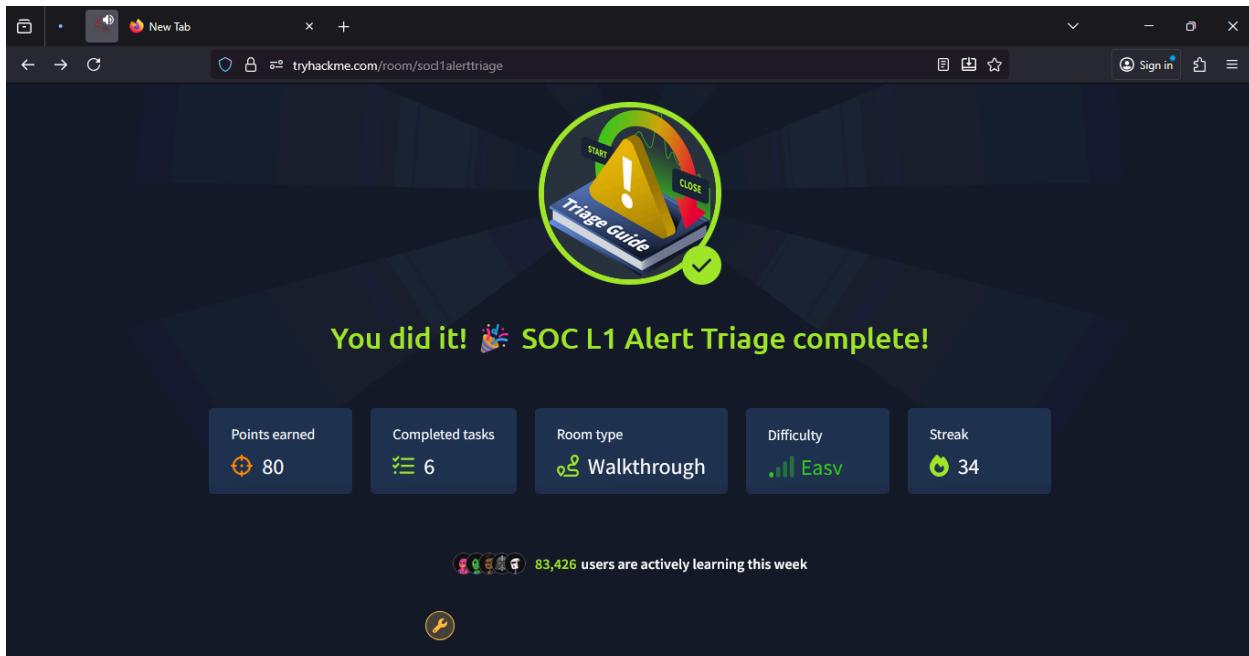
✓ Correct Answer

Which flag did you receive after you correctly triaged the third-priority alert?

THM{should_we_allow_github_for_devs?}

✓ Correct Answer





The screenshot shows the completed room screen for SOC L1 Alert Triage. The top bar displays "Room completed (100%)". Below it, three questions are listed with their answers and correctness status:

- Which flag did you receive after you correctly triaged the first-priority alert?
THM{looks_like_lots_of_zoom_meetings} ✓ Correct Answer ✗ Hint
- Which flag did you receive after you correctly triaged the second-priority alert?
THM{how_could_this_user_fall_for_it?} ✓ Correct Answer
- Which flag did you receive after you correctly triaged the third-priority alert?
THM{should_we_allow_github_for_devs?} ✓ Correct Answer

Below the tasks is a section titled "Task 6" with a "Conclusion" button. At the bottom is a feedback form with a "Thank you! 🎉" message, a "Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!" message, and a "✓ Close" button.