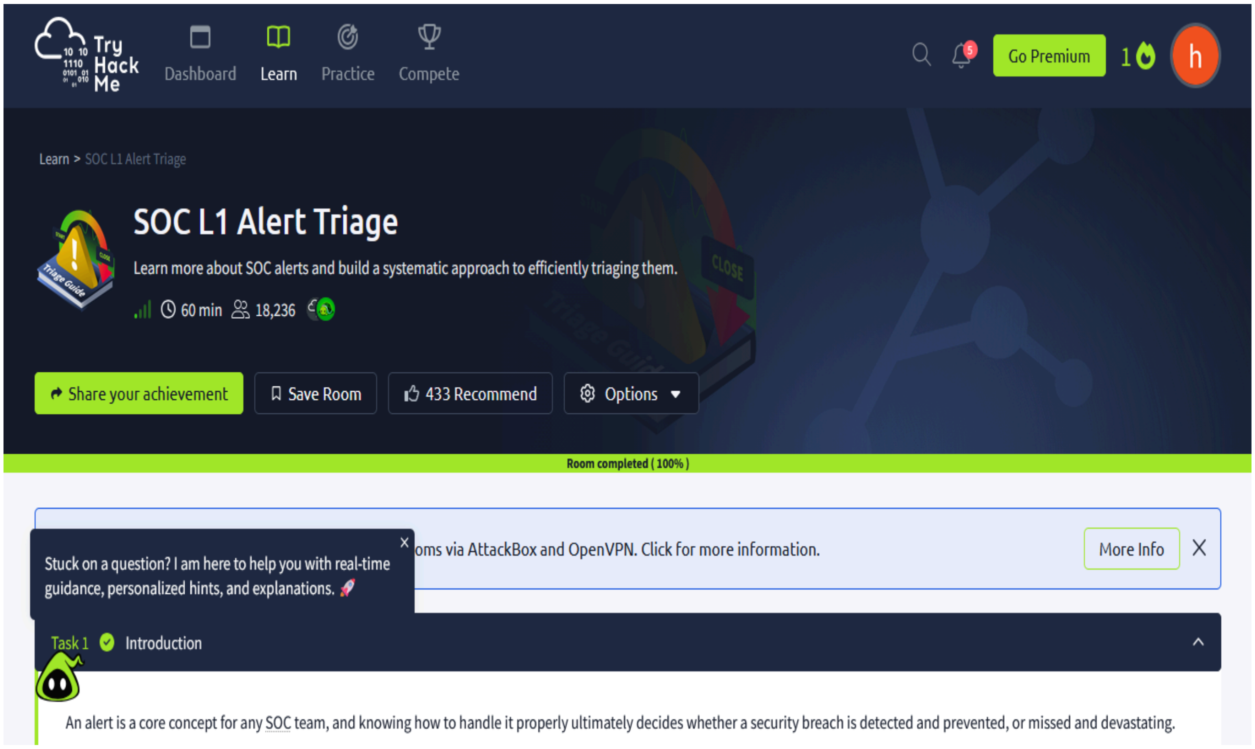
SOC L1 Alert Triage



SOC L1 Alert Triage

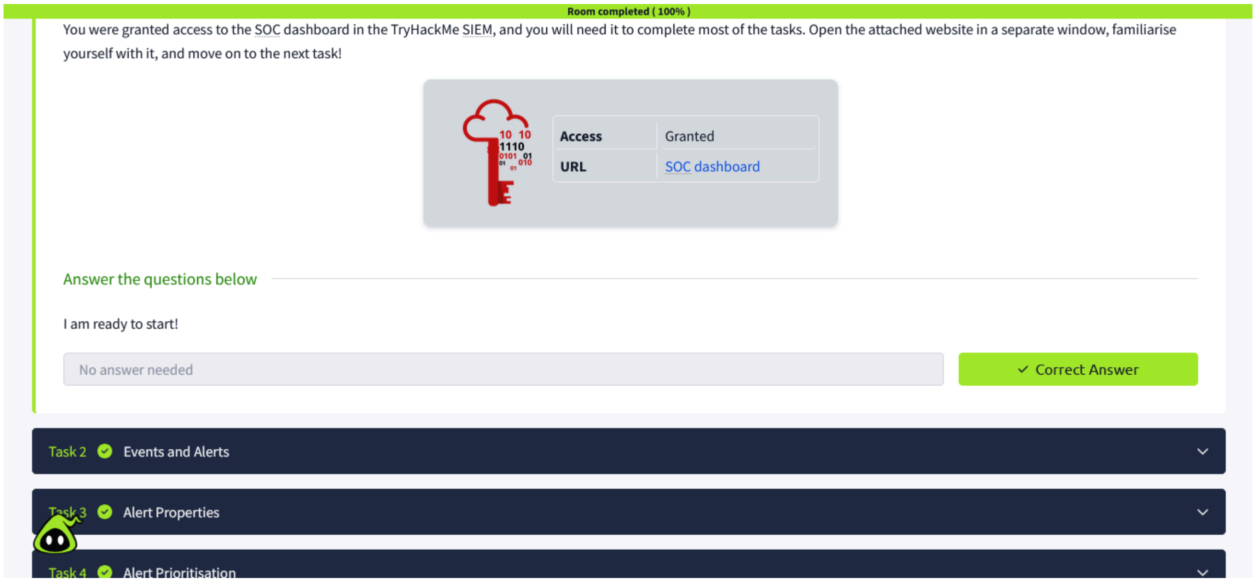
Learn more about SOC alerts and build a systematic approach to efficiently triaging them.

...oms via AttackBox and OpenVPN. Click for more information.

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

Task 1 Introduction

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.



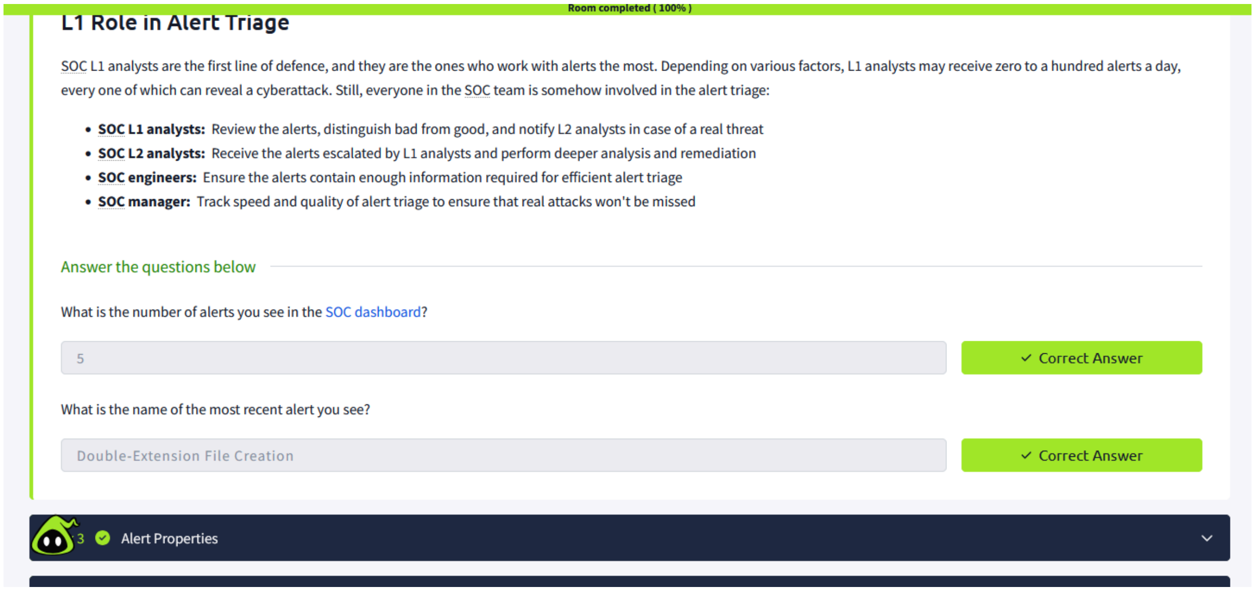
You were granted access to the SOC dashboard in the TryHackMe SIEM, and you will need it to complete most of the tasks. Open the attached website in a separate window, familiarise yourself with it, and move on to the next task!

Access	Granted
URL	SOC dashboard

Answer the questions below

I am ready to start!

No answer needed



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

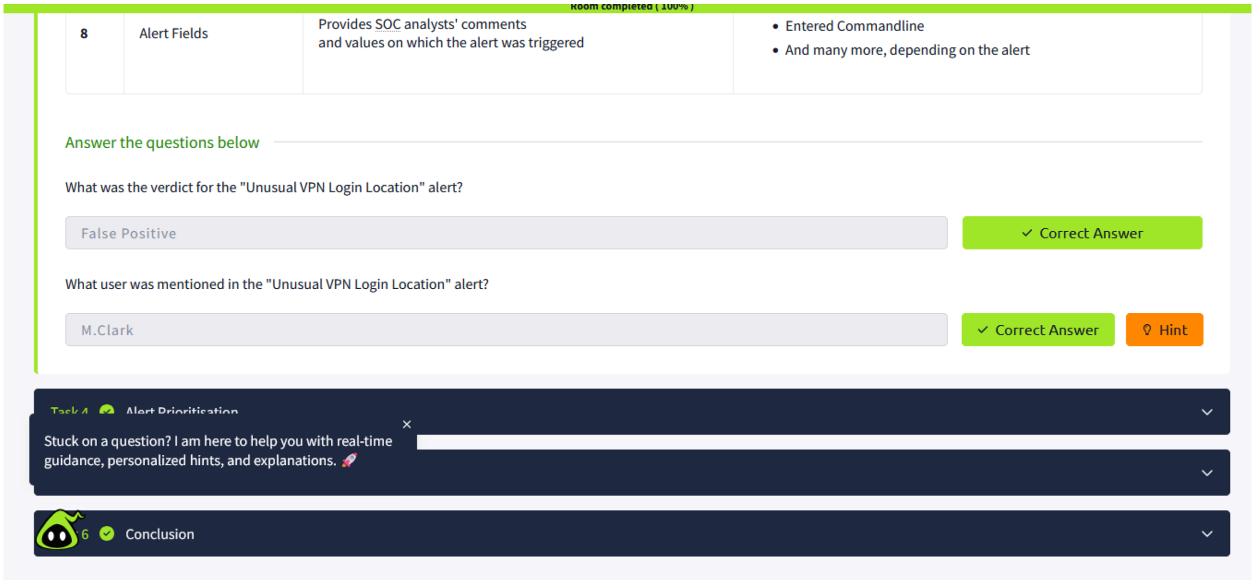
Answer the questions below

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

5

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

Double-Extension File Creation



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

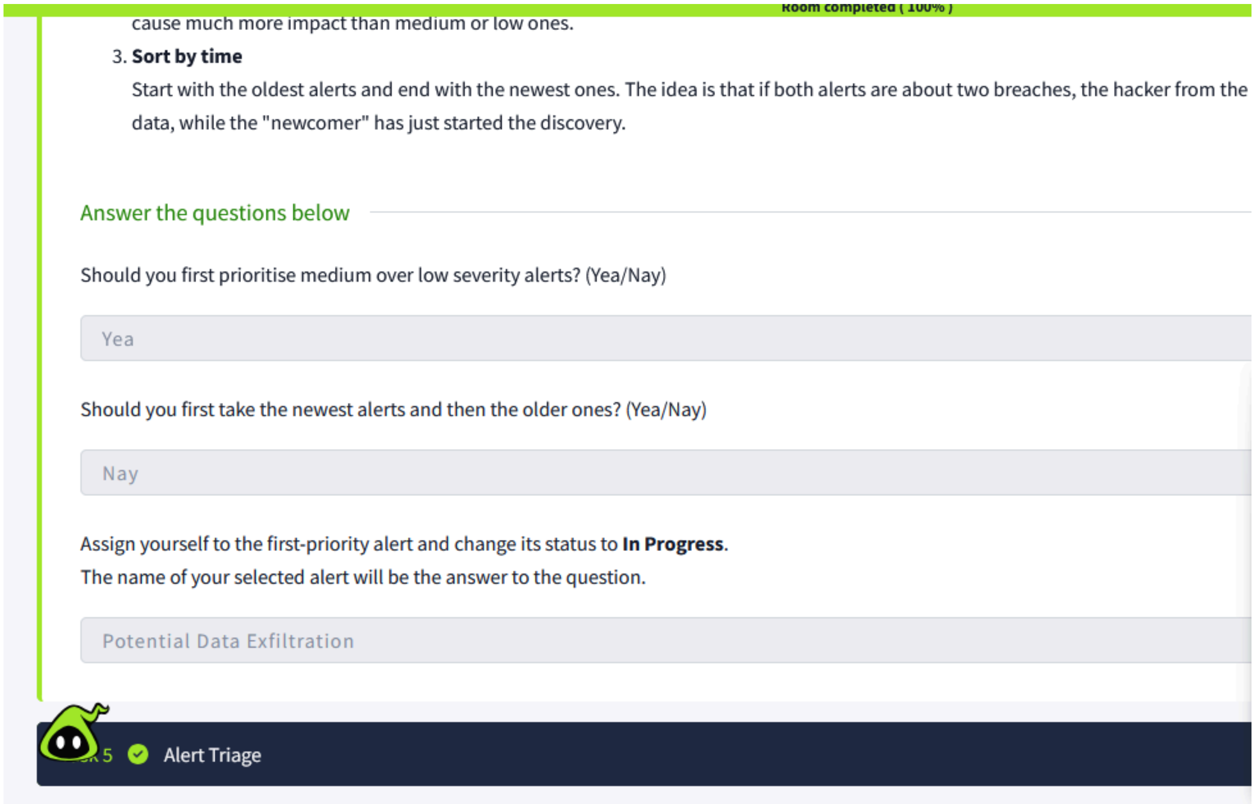
What was the verdict for the "Unusual VPN Login Location" alert?

False Positive

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

M.Clark

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



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)

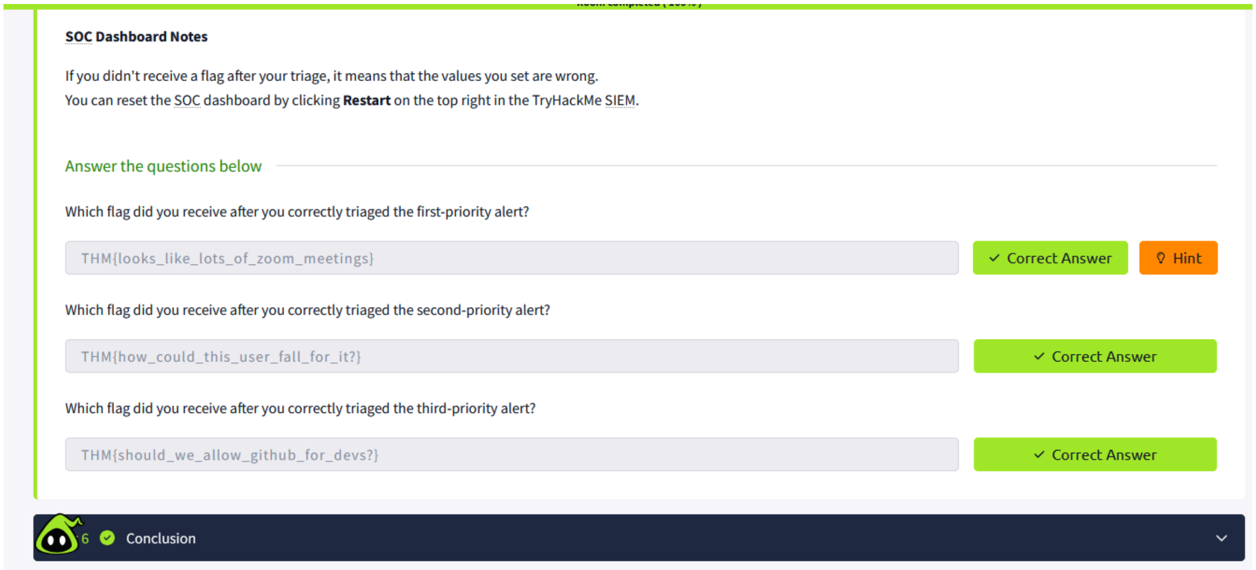
Yea

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?

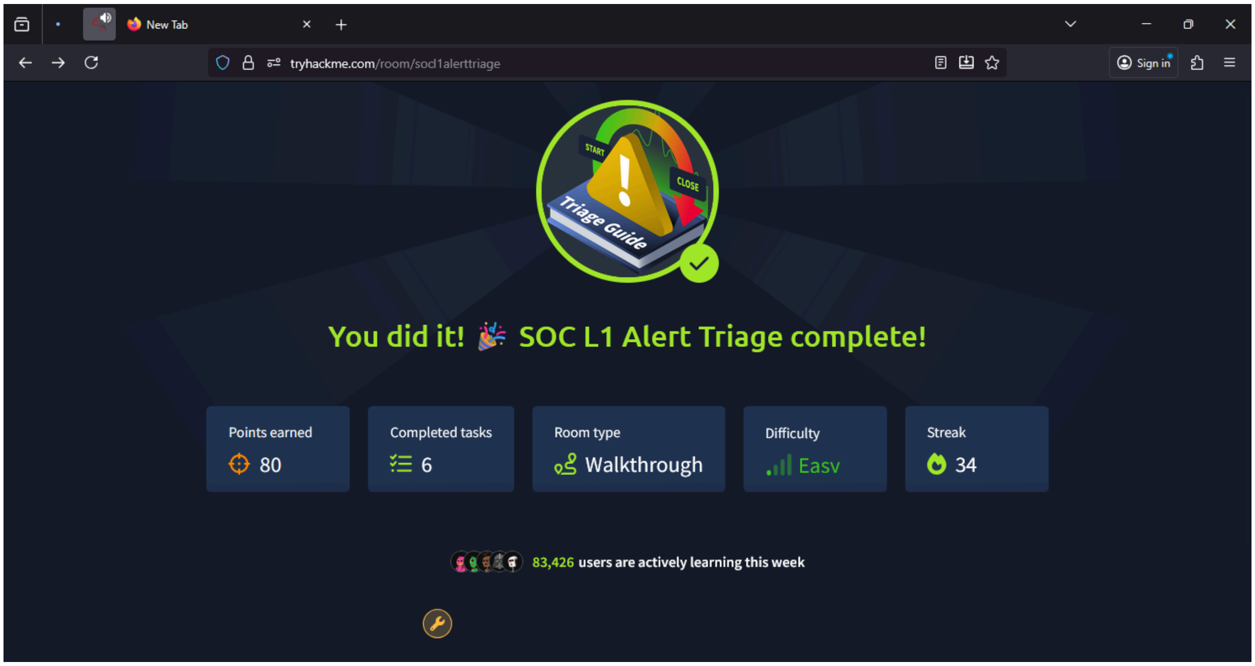
THM{looks_like_lots_of_zoom_meetings}

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

THM{how_could_this_user_fall_for_it?}

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

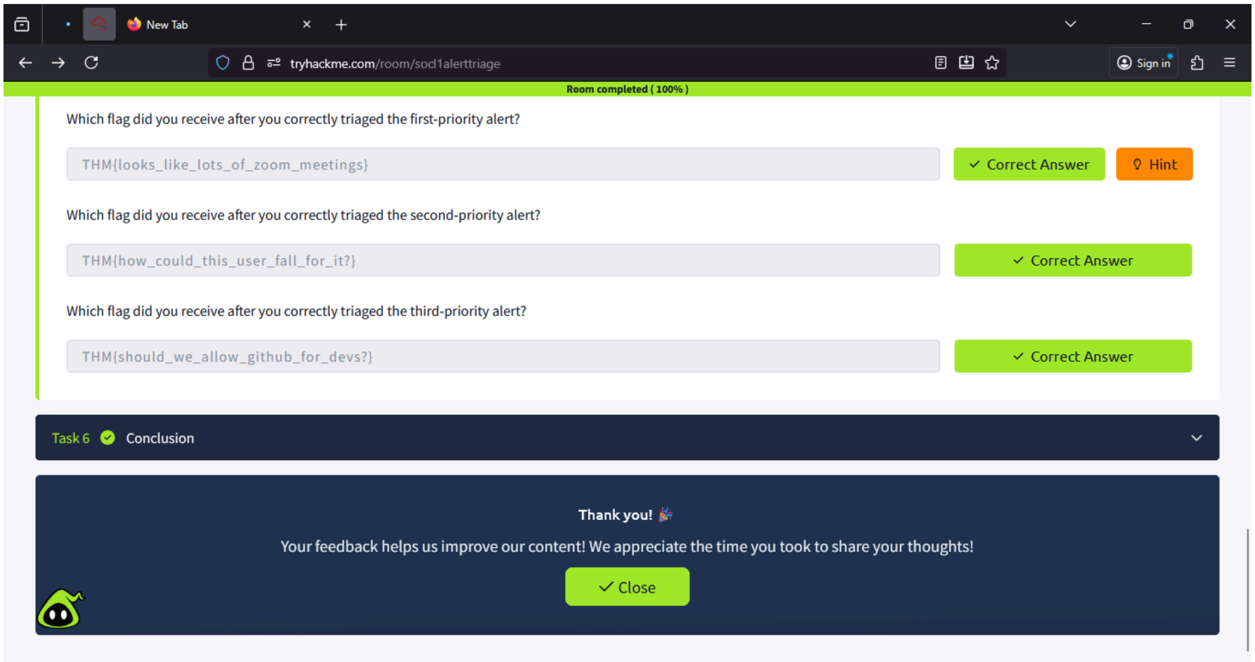
THM{should_we_allow_github_for_devs?}



You did it! 🎉 SOC L1 Alert Triage complete!

Points earned	Completed tasks	Room type	Difficulty	Streak
80	6	Walkthrough	Easy	34

83,426 users are actively learning this week



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

Task 6 ✓ Conclusion

Thank you! 🎉

Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!

✓ Close