SOC Level 1

Junior Security Analyst Intro

Task 1:

Answer the questions below

What will be your role as a Junior Security Analyst?

Triage Specialist	✓ Correct Answer

Task 2:

No need to submit

Task 3:

Answer the questions below

Click on the green View Site button in this task to open the Static Site Lab and navigate to the security monitoring tool on the right panel to try to identify the suspicious activity.

🗔 View Site

No answer needed	✓ Correct Answer

What was the malicious IP address in the alerts?

221.181.185.159	✓ Correct Answer	♀ Hint

To whom did you escalate the event associated with the malicious IP address?

Will Griffin	◁ Submit

After blocking the malicious IP address on the firewall, what message did the malicious actor leave for you?

THM{UNTIL-WE-MEET-AGAIN}	✓ Correct Answer