STAR Interview Practice Responses

Experiences That Demonstrate My Skills

1. Suricata Lab & Rule Creation

Created and tested intrusion detection rules using Suricata and analyzed network traffic with fast.log and eve.json. Learned how to detect suspicious activity and create proactive cybersecurity alerts.

2. Python Automation Project

Developed a script to identify and remove unauthorized IP addresses from a log file. Demonstrated knowledge in scripting, file parsing, and incident response automation.

3. Disciplinary Investigations as Grievance Supervisor

Led investigations into employee misconduct within a correctional facility. Applied confidentiality, compliance with policy, and analytical documentation.

Question 1: Tell me about a time when you identified a potential security threat. How

SITUATION:

During my cybersecurity training, I completed a hands-on lab using Suricata, an intrusion detection system. While analyzing packet capture data, I noticed repeated attempts from the same external IP targeting port 22, commonly used for SSH access.

TASK:

My task was to investigate the traffic, determine whether it was malicious, and take appropriate action based on my findings.

ACTION:

STAR Interview Practice Responses

I created a custom Suricata rule to alert on multiple SSH attempts from the same IP within a short time frame. I then reviewed the fast.log and eve.json files to validate that the alert was triggered accurately. I documented my findings and suggested a recommendation to block the IP at the firewall level if this were a real environment.

RESULT:

The rule successfully identified a brute-force attempt pattern, and my documentation clearly outlined the next steps. My instructor noted my attention to detail and how I applied real-world thinking to the exercise. This experience built my confidence in using IDS tools and interpreting log data to make informed decisions.

Question 2: Describe a situation when you used a script or automation to solve a pro

SITUATION:

As part of my cybersecurity portfolio project, I worked on a Python script to parse a server log and remove unauthorized IP addresses attempting to access restricted areas.

TASK:

My task was to write a script that could automatically detect and clean up a list of unauthorized IPs based on predefined rules, and then save the updated list in a secure file.

ACTION:

I used the with statement to open and read the file safely, parsed the data using loops and string functions, and created conditions to identify unauthorized IPs. I then wrote a clean version of the log with only valid entries, ensuring accuracy and minimal disruption to existing systems.

STAR Interview Practice Responses

RESULT:

The final script ran successfully and reduced the manual workload of reviewing logs by at least 70%. This project was added to my GitHub portfolio and helped me demonstrate my automation skills to recruiters and hiring managers.