Fullstack Academy

Career Preparation Feedback Form

Unit 7: Blue Team

Student Name: Frankie Bruno

Risk Management

Interviewer

Question	**Best Answer**
How do you ensure governance, risk, and compliance in cybersecurity?	I follow the NIST framework and use **Nessus** to perform vulnerability scans. I check systems against compliance standards and document risks for remediation.
How would you describe the use and benefits of the NIST Cybersecurity Framework?	The NIST CSF breaks security into five key areas: Identify, Protect, Detect, Respond, and Recover. It helps guide security decisions and ensures nothing important is missed.
How do you approach intrusion detection in cybersecurity?	I use **Snort** to detect suspicious network traffic. It helps alert me to patterns like port scans, malware activity, or brute force attempts.

Data Analysis and Security

Question	Best Answer
Describe your experience using SIEM tools. What are the benefits to using these tools?	I've used **Splunk** to collect and analyze logs. It makes it easier to detect threats in real time, investigate incidents, and create alerts for specific behaviors. As well as seeing the data parsed out. We ingested static data, parsed/search data using SPL

Digital Forensics

Question	Best Answer
Explain the phases of the digital forensics investigation process.	The phases are: Identification, Preservation, Collection, Analysis, Documentation, and Reporting. I use **Autopsy** for analysis to uncover deleted files, timelines, and suspicious activity.
How is data integrity verified?	I use **SHA-256** hashing to verify integrity. Matching hash values before and after analysis proves the data hasn't been changed.

Incident Management

Question	Best Answer
Explain the phases of the NIST incident response life cycle.	The six phases are: Preparation, Detection, Containment, Eradication, Recovery, and Lessons Learned. I use **CrowdStrike** for endpoint detection and to help with fast response and containment.