STAR Responses Worksheet

Experiences that demonstrate my skills: Over the course of the Google Cybersecurity Professional Certification course, I have had several opportunities to take example events and use the skills taught to approach and handle how I might solve the issues presented in a professional environment. These experiences include identifying and determining asset priority, risk assessment, using SIEM tools such as Suricata, Chronicle, and Splunk, writing incident reports, using playbooks, and many other activities taught throughout the course of the program.

Question 1: Describe an experience in which you implemented a security solution. What was your solution, how did you help with implementation, and what were the results?	
Situation	A suspended account was suspected of being compromised due to a login notification.
Task	Go through logs and determine when the login notification occurred and compare the user credentials with the list of active users.
Action	The account was suspended due to the original owner of the account no longer being with the company. The account was then deleted and the principle of least privilege and proper data handling policies were updated to reduce privileges of inactive user accounts.
Result	Inactive user accounts have their privileges suspended and employees now have access to only data and resources they need to complete their day to day responsibilities.

Question 2: Describe an experience in which you used your cybersecurity skills effectively. How did you analyze variables and identify anomalies to improve security and productivity for your company?

Situation	A Phishing email had been sent and opened by an employee.
Task	Use tools such as VirusTotal to investigate the email and attachments provided alongside to identify any malicious intent.
Action	The file hash from the email, when run through VirusTotal, proved to be a known malicious file.
Result	The incident was escalated due to the potential risk of the recipient opening the malicious file on their workstation so proper actions can be taken to contain and recover the workstation to no further harm is done and the employee can resume normal business operations.

Common Behavioral Interview Questions for Cybersecurity Analysts

1. Describe an experience advising and working with internal business units on security related issues. How did you meet with teams, address questions, encourage compliance, and help ensure optimal productivity?
2. Describe an experience in which you implemented a security solution. What was your solution, how did you help with implementation, and what were the results?
3. Describe an experience in which you used your cybersecurity skills effectively. How did you analyze variables and identify anomalies to improve security and productivity for your company?
4. Tell me about a time when an update in the field of information security, cybersecurity, or regulatory compliance took you by surprise. What was this update and how did you learn of it? What do you do today to stay up-to-date on relevant information?
5. Describe an experience in which you used technical security tools as part of issue resolution. How did you assess the issues and reach the conclusion that these tools represented the optimal solution? What was the outcome?
6. Describe an experience in which you had to plan, develop, execute, and/or maintain documentation related to security processes and procedures.
7. Tell me about a time you had to work across various internal teams on security tasks. How did you plan and arrange appropriate times to meet and mutually acceptable timelines across these teams? What was the outcome?
8. Describe an experience in which a security leak or other issue called for immediate response, analysis, and action. How did you organize and execute this while prioritizing and dealing with other duties disrupted by this event? What was the outcome?
9. Tell me about a time you had to speak to higher management in your role as a cybersecurity analyst about complex technical issues and solutions. How did

you express highly technical information in a way that could be understood and responded to effectively?

10. Tell me about a time you experienced reluctance on the part of some members of higher management with regard to a security or regulatory issue. How did you go about gaining support for your opinions, whom did you speak with, and what was the outcome?