STAR Responses Worksheet

Experiences that demonstrate my skills:

*Earned the Google Cybersecurity Certificate, which contained plenty of hands on labs to put my cybersecurity skills into practice.

*Worked in a team using tools such as Jira and Bitbucket so we could work in the project independently of our time availability.

*Was the team captain of the TXST University. During that time, I developed skills such as leadership and teamwork.

Question 1: 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?	
Situation	An employee received a phishing email and installed malware into his work computer.
Task	Analyzing the incident, determine the appropriated risk level, and decide whether or not to escalate the issue.
Action	I use a playbook for these situations, so first thing I did was checking it. According to its guidelines, the level I should assigned to the incident was medium, so I had to escalate the issue. I immediately reported my supervisor.
Result	The issue ended up resolved without further consequences than a slight delay.

1. **Question 2: 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?**	
Situation	An employee received a suspicious email. They weren't sure whether it was actually important or a phishing attempt.

Task	I was given the task to analyze logs to determine whether a domain name that interacted with an employee was dangerous.
Action	I used the SIEM tool chronicle to perform a detailed inspection of the domain name. I started by checking VirusTotal, which indicated that the account was dangerous. I investigated further and looked for the IP associated to POST messages. After tracking it, I was also able to find another email associated to his account, so I also included it in my report.
Result	No malicious files were installed and the dangerous account was reported.

Common Behavioral Interview Questions for Cybersecurity Analysts

- 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?
- 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?
- 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?
- 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?
- 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?
- Describe an experience in which you had to plan, develop, execute, and/or maintain documentation related to security processes and procedures.
- 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?
- 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?
- 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?

- 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?