STAR Responses

Experiences that demonstrate my skills:

1. Helped Nice Touch Healthcare group strengthen their security posture through adherence to industry standard policies and procedures.
2. Maintained effective communications with various teams across the organization to ensure overall alignment on security best practices.
3. Completed the Google Cybersecurity Certificate, demonstrating my eagerness to learn and grow my knowledge and skill set.

Question 1: 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?

Situation	When I was a Cybersecurity Junior Analyst at Nice Touch Healthcare Group, the organization was experiencing a tremendous increase in employees clicking on phishing email links. The security team determined that various department leaders were not educating their employees on the importance of not clicking every link and attachment found in an email.
Task	I was part of a team tasked with identifying which departments were clicking on the most phishing links and communicating those findings to the leaders of those departments.
Action	I went into our organization's work calendar to find available times to meet with more senior-level analysts to discuss the phishing data they gathered. We discussed the impact of the data and the need for me to put that data into a visual presentation. After I created bar charts for the phishing data, I reached out to the assistants of the various department leaders via email to establish the best date and time for my team and those leaders to join a video call to discuss the data. We came up with a plan to minimize the amount of phishing emails being clicked on by launching an employee awareness campaign and set a timeline to complete the plan by end of year.
Result	The organization saw a 20% decrease in the amount of phishing

	links clicked on by employees one month after my team and I met with all of the department leaders.
Question 2: Describe an experience in which you had to create, develop, and/or maintain documentation related to security processes and procedures. How did you plan, execute and maintain these documents?	
Situation	When I first started working at Nice Touch Healthcare Group, the organization was working on establishing its third-party assessment program. The purpose of the program was to properly assess the security of all third-party companies we did business with to ensure those companies did not have major security vulnerabilities that could negatively impact our organization.
Task	After working at Nice Touch for a year, I was put in charge of managing any updates or changes to the third-party assessment program procedures and policies..
Action	I was granted access to a shared drive that contained the third-party assessment policies and procedures. From there, I did an audit of the individuals who currently had access to that shared folder. I found that a few employees who were either no longer working for the company or no longer working with the third-party assessment team still had access to the shared folder. I mentioned this to my direct supervisor and was given permission to remove those individuals' access to the shared folder. From there, I set up weekly meetings with other members of the third-party assessment team to discuss any new changes or adjustments that needed to be made to the policies and procedures. I also periodically added or removed individuals' access to the shared folder as needed.
Result	Executives mentioned the third-party assessment program in the end-of-year functional review meeting. The executives remarked that they appreciated how much more streamlined and collaborative the third-party program had become after I began maintaining the documentation.

Common Behavioral Interview Questions for Cybersecurity Analysts

1. Describe an experience advising and working with internal business units on security related issues. In what way 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. How did you plan, execute and maintain these documents?
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, if any, 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, who did you speak with, and what was the outcome?