

STAR Responses Worksheet

Experiences that demonstrate my skills:

Experience 1: Technology Professional Intern at Los Angeles County Internal Services Department

- **Cybersecurity Tools:** You were involved in a Mobile Application project, which likely included the use of cybersecurity tools and practices to secure data. Discuss any tools or measures you employed.
- **Security Policies and Procedures:** Mention if you were exposed to any security policies and procedures within the organization and how you contributed to their implementation.

Experience 2: Grace Coding (Owner)

- **Vulnerability Assessment and Compliance:** As an owner of a design company, you may have performed vulnerability assessments to secure websites and ensure compliance with security standards.
- **Security Awareness and Training:** If you educated your clients on security best practices, it's worth mentioning in your responses.

Experience 3: Delete The Divide (Digital Aide)

- **Incident Response and Threat Intelligence:** In this role, you could discuss how you handled IT assistance requests and how you stayed informed about the latest threats and incidents.

Question 1: Describe a situation where you demonstrated your cybersecurity skills.

| | |
|------------------|---|
| Situation | I was working as a Technology Professional Intern at Los Angeles County Internal Services Department, handling design duties for the Mentorship section of the Delete The Divide's website. This project involved managing a web page with WordPress for the primary mentorship section, and a subdomain with custom .NET backend code for the database team of a Mobile Application project. The application aimed to assist in the distribution of over 10,000 laptops to disenfranchised residents in LA County via ISD. |
| Task | My responsibilities included the design and maintenance of the web pages, which required knowledge of secure coding practices, as well as ensuring data integrity and availability. Additionally, I was advocating for digital equity in underserved communities, educating users about the ACP program, and offering digital support in public county libraries. |
| Action | I implemented robust security measures for the web pages, including regular updates and security patches, secure coding practices to mitigate potential vulnerabilities, and regular backups to ensure data availability. I also actively engaged with users, addressing their IT concerns and educating them on secure digital practices, contributing to the promotion of digital equity in the community. |
| Result | By successfully handling the security aspects of the web |

| | |
|--|--|
| | <p>pages and providing IT support to users, I ensured the availability of valuable mentorship resources and contributed to the distribution of laptops in LA County. These experiences enhanced my skills and awareness of cybersecurity principles in a practical setting, equipping me with valuable knowledge for addressing future security challenges.</p> |
| <p>Question 2: Describe a time when you responded to a security incident or threat.</p> | |
| <p>Situation</p> | <p>While working as a Field Service Technician for Robert Half, I was involved in providing IT support for the 2022 Los Angeles County Election, which required a heightened focus on security due to the critical nature of the event. I was responsible for ensuring the smooth operation of Vote Centers, troubleshooting Ballot Marking Devices, setting up ePollBooks, and creating incident tickets.</p> |
| <p>Task</p> | <p>My role was to ensure the IT systems related to the election process functioned securely and efficiently, which included verifying the integrity of router connections, UPS machines, and Ballot Devices to prevent potential security breaches.</p> |
| <p>Action</p> | <p>I meticulously examined and validated the security of the IT infrastructure, ensuring that all systems were well-protected from vulnerabilities and potential intrusion attempts. In the event of system issues, I promptly created incident tickets to address and document security concerns.</p> |

| | |
|---------------|---|
| Result | <p>My efforts contributed to the secure and successful operation of the 2022 Los Angeles County Election. Through vigilant security checks, prompt incident reporting, and proactive troubleshooting, I helped maintain the integrity of the election process and ensured that all systems functioned securely. These experiences reinforced the importance of security in critical operations and sharpened my skills in responding to security incidents.</p> |
|---------------|---|

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?