Cybersecurity

Project 3: Interview and Resume Guidance

Congratulations on completing your third project!

- This project covered a wide range of topics, including:
  - Information security continuous monitoring (ISCM)
  - Log types and how they are used for monitoring
  - Log aggregation and correlation
  - Baselining
  - SIEMS
  - Splunk:
    - Splunk Processing Language (SPL)
    - Reporting
    - Alerting
    - Dashboards
    - Add-on applications

- When networking and talking to potential employers, you should be able to reference the work done on this project to answer specific interview questions or demonstrate your skills within a specific domain.

- The following guide will assist you in adding this project to your resume and preparing you for interview questions about your project.

Resume Guidance

Many IT and cybersecurity professionals showcase their projects by adding them to their resume. Follow the instructions below to add your project to your resume:

- List your project under the “work experience” or “accomplishments” section of your resume. Include the following information:

Project 3: Defensive Security
Technologies Used: Splunk: (Reporting, Alerting, Dashboards)

- Developed and designed a custom monitoring solution using Splunk to report and alert on suspicious activity from Windows Events and Apache logs.
- Created dashboards with multiple visualizations to provide in-depth analysis of attack signatures.

Interview Guidance

As a reminder, good interview responses do the following:

1. Restate the problem.
2. Provide a concrete example scenario.
3. Explain the solution requirements.
4. Explain the solution details.
5. Identify advantages and disadvantages of the solution.

Including each of these components will help demonstrate competency in the subject matter and critical thinking.

Interview Questions

1. **Describe your project.**

I used Splunk to design a custom monitoring environment to protect a fictional organization. I created custom reports, alerts, dashboards, and add-on apps to protect our mock company. Then I experienced a simulated attack and analyzed the results to determine the effectiveness of my monitoring solutions. I completed the project by showcasing my defensive solution in a class presentation.

2. **What were your project requirements?**

Our requirements included:

- *Loading Windows and Apache logs into our Splunk environment.*
- *Analyzing the logs to determine baselines and thresholds.*
- *Creating reports, alerts, and dashboards for specific criteria.*
- *Loading Windows and Apache logs that contained a simulated "attack."*
- *Analyzing the attack logs with our Splunk environment to determine its effectiveness.*
- *Presenting our monitoring environment, attack analysis, and future mitigation recommendations to the class.*

3. **How did you determine baselines and thresholds for your alerts?**

I analyzed the mock company's "regular" historical activity to determine its normal range. I then created an alert threshold outside of this normal range (provide percent if you like) to prevent any false positives.

4. **After experiencing the simulated attack, did you determine that your thresholds needed modification?**

(This answer will vary based on your specific findings.)

5. **What future mitigations would you recommend based on your findings?**

(This answer will vary based on your specific findings.)