Zyquier Brownridge

Resume

Skills

- Python
- Splunk
- Data Analysis
- Machine Learning
- Linux
- SQL
- Communication
- Critical Thinking
- PowerShell/Bash/Putty
- Automation

Education:

Bachelor's Degree :

Computer Science

2017-2021 WSSU

Experience:

Cyber Analyst PamUnix - TIAA (June 2023 - Present)

4th Rotation: PamUnix Team:

Security Engineer - TIAA (Jan/2023 - June/2023)

3rd Rotation: SecOps (Security Operations/Security Logging):

- Docker Container + Linux and Python
- Created Splunk dashboards to visualize and analyze security data effectively.
- Implemented SPL searches to extract relevant information from the Splunk platform.
- Fine-tuned existing use cases and searches to improve their efficiency and accuracy.
- Merged existing dashboards to consolidate information and provide a comprehensive view of the security landscape.
- Configured Splunk alerts, reports, and saved searches to proactively monitor and detect security incidents. Gained knowledge of the collaboration between the Detective Team and Response Team within the Security Operations Center (SOC).
- Utilized CI/CD (Continuous Integration/Continuous Deployment) practices for managing and deploying Splunk use cases using Linux and tools like PuTTY.
- Employed Linux for deploying Splunk use cases.
- Collaborated and communicated with various teams to troubleshoot and resolve issues within the Splunk infrastructure.
- Developed a Python script that extracts data from SDW (presumably a database) using SQL for automation purposes, integrating it with Splunk. Utilized Python in conjunction with Splunk for automation tasks.
- Participated in Kanban Agile Standup Daily meetings to facilitate efficient project management and communication.
- **Volunteer Experience:** Volunteered at a local high school (Westmeck) to educate younger individuals on the importance of cybersecurity, the necessary skills for entering the field, and the recommended career pathways.

SOC Analyst - TIAA (June/2022 - Dec/2022)

2nd Rotation: Data Loss Prevention (DLP):

- Utilized the Symantec Endpoint Protection Tool for data loss prevention activities.
- Focused on Data in Motion (DIM), specifically monitoring data transfers such as emails.
- Analyzed both internal and external users, paying attention to specific domain names.
- Concentrated efforts on identifying and preventing the unauthorized transmission of classified data from internal users.
- Acquired knowledge about DLP policies and their purpose. Learned how policies are configured and the specific rules and detections they employ
- Developed a scripting tool using Python to automate certain DLP tasks.
- Created automation scripts in Python to streamline and enhance DLP processes.
- Worked with the Symantec REST API using Python to interact with DLP functionalities.

Security Engineer - TIAA (Jan/2022 - June/2022)

Vulnerability Management (Application Security)

1st Rotation - Application Security Vulnerability Management:

- Analyzed weekly vulnerabilities, both internal and external scans, using Tableau dashboards.
- Utilized the Remediation Dashboard in Tableau to compare and validate upcoming tasks for the next week and current month. This information was then organized within an Excel file.
- Managed metrics for top vulnerabilities, categorizing them as Medium, High, or Very High. Also tracked the number of applications without scans, both for internet-facing and internal applications.
- Automated controls by leveraging Python scripting
- Utilized Python to interact with the Veracode REST API for in-scope applications. Extracted relevant data from the API responses in JSON format and processed it for validation purposes and automation. This involved generating Excel files to store the data.

Cloud Security Intern | Lenovo *(May/2021 - July/2021)*

Mooresville, North Carolina, United States

- Conducted Vulnerability Analysis to identify potential security weaknesses.
- Acquired proficiency in various penetration testing tools, including Burp Suite.
- Utilized Jira to discover security findings and conduct security reviews.
- Created a dashboard in Jira to track and manage Vulnerability Findings.

Skills and Knowledge:

- Demonstrated proficiency in cloud technologies, specifically Azure.
- Familiarity with the OSI model for network communication.
- In-depth understanding of HTTP/HTTPS protocols.
- Knowledgeable about different types of vulnerabilities and their mitigation strategies.

Software Engineer Intern | SGCI *(May/2020 - August/2020)*

Science Gateways Community Institute · Internship

- Completed certifications in High-Performance Computing using Python and Responsible Conduct of ----Research Investigators and Key Personnel at a competitive coding institute.
- Proficient in HTML web development.

Skills and Accomplishments:

- Acquired knowledge and hands-on experience with science gateways such as Apache Airavata, Hub Zero, and Tapis.
- Actively participated in PEARC20 and PEARC20 Hackathons.
- Engaged in cross-functional team-building activities.
- Enhanced proficiency in JavaScript and HTML coding.
- Familiarity with Agile Development methodologies.
- Proficient in MySQL.

Contact

 linkedin.com/in/Zyquier
 https://github.com/Zyquier