

CAREER SUMMARY:

Solution-oriented and problem solver with 4 years of experience in Cyber Security while using software development skills for solving complex problems as well. Highly skilled in communication, collaboration, and technical documentation.

WORK EXPERIENCE:

CDW | Security Engineer Consultant | JAN 2024 - Present

- Strategize and assist in the development of IAM solutions within SailPoint IIQ.
- Establishes trust with customers in order to become a trusted advisor client for IAM-related services for clients.
- Deploying SailPoint IIQ and adding users following full Identity Life cycle management provision plan.
- Developing custom Beanshell and Java scripts for Rules
- Implementing policies for RBAC
- Developing Custom Workflows for client needs
- Implementing Users with RAPID-7 Joiner , Mover and Leaver Workflows

TIAA|Security Engineer| Jan 2022 - Jan 2024

- Developed custom rules and scripts in Sailpoint IIQ for managing users Access .
- Created Splunk report to notify the team of Service accounts that were still in active/inactive every 30 days from SailPoint IIQ Entitlements.
- Enhanced Splunk 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.
- Managed users on identifying and preventing the unauthorized transmission of classified data from internal users leaving the internal network with Symantec tool from defining policies RBAC,PBAC and ABAC.
- Developed python scripts with the Symantec REST API using Python to interact within DLP Symantec environment.
- Managed Weekly tableau dashboard metrics for top vulnerabilities, categorizing them as Medium, High, or Very High. Tracked the number of applications without scans, both for external and internal applications from Veracode SAST/DAST Scans.
- Utilized Python to interact with the Veracode REST API for in-scope applications. Extracted relevant data from the API responses in JSON format using Pandas and processed it for validation purposes and automation.

Lenovo | Cloud Security Engineer | May 2021 - Oct 2021

- Responsible for supporting the Vulnerability analysis concepts and measures for our global customers, as directed by the Lead Cyber Security Architects and Senior Engineers.
- Training in OWASP Hacking Lab and Various Secure Coding Trainings.
- Monitoring and detecting Web-Applications Vulnerabilities with Burp-Suite.
- Weekly Burp-Suite Training.
- Filed reports, gathered information, and performed research for AZURE CLOUD.
- Build Weekly Vulnerability Dashboard tool for analysis and applied the different risk score for Vulnerability categorization in JIRA.

SGCI |Software Engineer | May 2020 - Oct 2020

- Participated in cross-functional team-building activities.
- Assisted troubleshooting in python environment.
- Web Scraped Covid19 Death rates using python selenium and data analysis on data to compare to death rate of other viruses.
- Configured MYSQL Database for Python Project Backend in Visual Studio Code and HTML webpage with JavaScript configurations.

CODING PROJECTS:

Python Streamlit Azure Storage

<https://github.com/Zyquier/ZOPSDATACENTER>

Machine Learning Intrusion Detection System

https://github.com/Zyquier/CYBER/tree/main/ml_ids

Port Scanner

https://github.com/Zyquier/CYBER/blob/main/PortScanner_excelfile.py

SGCI Python Coding Project

<https://github.com/SGCI-Coding-Institute/project-air>

EDUCATION:

2017-2021 - Winston Salem State University

- Bachelor of Computer Science - Information Security
- Minor in Mathematics

Certifications:

- CompTIA Security+
- Azure 900 Fundamentals

SKILLS:

- Java , Python , Bash , HTML , MYSQL, JavaScript, Active Directory/LDAP, Tomcat
- Azure, Linux , UNIX, Visual Studio Code, Docker, Gitlab, Splunk, Virtual Machines, SailPoint, Burpsuite.
- NIST Framework And OWASP Top 10.
- Application Security, IAM , DLP , SOC.