Jordan Slack

608-636-3886 | Slack.Jordan@outlook.com | TryHackMe: https://tryhackme.com/p/Xenosapian

Objective

- To leverage my school and Collegiate Cyber Defense Competition experiences in to bring a fresh perspective to your organization. With goals to continue to bring a security first focus to the field to catch vulnerabilities and poor security practices within a public or private network. Utilizing an expertise in hackathons and cyber defense competition to improve the security posture of an organization.

Education

CYBERSECURITY SPECIALIST ASSCOCIATES | 5/2022 | MADISON COLLEGE

- Related coursework: Threat Hunting and Incident Response, Penetration Testing, Linux Server Security, Security Design, Firewalls and Networking.

DEVLOPMENT OPERATIONS ASSOCIATES | 05/2023 | MADISON COLLEGE

- Related coursework: Amazon Web Services [AWS] and Azure Administration, Development Operations, Advanced Scripting for Cloud, Python Programing.

Experience

CYBERSECURITY ANALYST | SPECTRUM BRANDS | 01/2021 - CURRENT

- Work with our security management team to create a dashboard for visibility.
- Standing up a vulnerability scanner and dashboard for maintaining compliance.
- Created a script in Python to automize reporting.
- Utilizing code repositories for collaboration for development.
- Update and renew certificates for our websites.
- Review security exceptions by reading software documentation to look for potential security risks.
- Troubleshoot authentication issues.
- Provide end user support and trouble shoot a large variety of issues in a fast-paced environment.
- Creating audio files with IBM Watson.
- Create a root cause analysis how we can prevent major incidents from occurrence.

COLLEGIATE CYBER DEFENSE COMPETITION

- Defend and configure network services from working penetration testers in a simulated attack for 8 hours.
- Create and harden firewall rules and policies.
- Respond to injects from management and provide documentation of completion.
- Create reports for detected intrusions.
- Provide updates on incident response.
- Use digital forensics methods to identify threat actors and their activities on the network.