Chase A. Reber

chasereber@gmail.com | (484) 784-8313 | chasingsecurity.com

EDUCATION

The Pennsylvania State University — **University Park, PA**
College of Information Sciences and Technology — May 2021
Bachelor of Science in Security and Risk Analysis — 3.71 GPA
***Certifications**:* CompTIA Security+, Preparing for ISC2 CAP

WORK EXPERIENCE

Universal Health Services — **King of Prussia, PA**
Security Risk Analyst I — October 2021 - Current

- Presented results of process improvements to C-Suite executives, presidents, vice presidents, and managers
- Facilitated the completion of 270+ facility risk assessments, increasing YoY completion from 61 to 97 percent
- Saved $223,00 over one year by creating script to allow analysts to identify underutilized medical licenses
- Identified and prioritized policies requiring revision to align with compliance for applicable regulations
- Analysis of risks in vendor provided reports, including SOC 2, security white papers, and pen test summaries

Associate Security Risk Analyst

- Developed third party risk process, increasing accuracy of responses and response rates by 60 percent
- Resolved critical security alerts and high severity account issues while on a bi-monthly on call schedule
- Documented third party and first party risk assessment processes for reference by other security analysts
- Utilized Nessus vulnerability scans and endpoint sensor data cross referenced with the NIST vulnerability database to prioritize and remediate security vulnerabilities based on criticality across technical departments

Fidelity Investments — **Merrimack, NH**
Software Development Intern — June 2020 – August 2020

- Consolidated documentation for Ansible and AWX features for automation teams to reference in day to day tasks
- Developed in an agile environment with daily stand ups and bi-weekly scrums while reinforcing self learning
- Increased security of applications developed by providing unit tests to ensure secure coding practices
- Co-Developed internal site displaying storage info for Data Center Ops teams to reference in day to day tasks

SKILLS

Technical Skills

- Familiarity with analysis in common risk and vulnerability tools, including OneTrust, BitSight, and Crowdstrike
- Experience using cyber security frameworks, standards, guidelines including NIST, HIPAA, and ISO publications
- Strong applied knowledge of Linux OS and tools such as NMap, Nessus, Wireshark and Metasploit Framework
- Utilized various IDS/IPS to monitor systems for malicious activity including file, registry and account changes
- Proficient in analyzing SIEM system logs to monitor security across workstations, access points and firewalls
- Networking experience with commonly used protocols, public key infrastructure, switches, routers, firewalls, and proxy servers and the overall OSI and TCP/IP models and their respective layers
- Development of scripts in various languages including Python, Bash, Javas, Powershell and R

Soft Skills

- Collaborated effectively with various teams on projects across software development, information security, first and third party risk assessment, multi-factor authentication deployment, and policy development projects
- Effectively communicated with internal and external business contacts to facilitate regular business functions

PROJECTS

- Stood up an active directory server with several windows hosts on VMware and then attacked the active directory server utilizing Kali Linux and Metasploit to bypass active directory security and access user credentials
- Built a home networking and infrastructure lab running ProxMox hypervisor for TrueNAS, several linux systems, DNS server and a reverse proxy server to access the network and services running on the home lab
- Identified, researched, and exploited insecure protocols utilizing NMap for reconnaissance and Metasploit framework for exploitation of vulnerabilities in order to gain administrative access to the server