Paul Brown

CYBER SECURITY SPECIALIST

Summary

Experienced Cyber Security professional with expertise in network security, vulnerability management, security engineering, and identity management. Skilled in guiding system administrators and network specialists to secure systems and networks from advanced cyber threats and address misconfigurations. Proficient in security analysis, revising compliance policies, implementing zero-trust configurations, and providing comprehensive IT department support. Dedicated to protecting US infrastructure from advanced persistent threats, with a passion for safeguarding individual identities within cyberspace.

Work Experience

Cyber Security Analyst | Virginia Railway Express

37.5hrs/week, September 2024 - Present

Cyber Security Analyst | PowerSolv, Inc

Responsible for identifying and mitigating security risks, conducting threat assessments, and implementing security measures to protect the organization's data, systems, and network. I also worked closely with a Managed Detection and Response team to investigate security incidents, maintaining a secure environment.

- Reviewed and optimized policies aligned with the NIST Cybersecurity Framework (CSF) to ensure a robust security program.
- Maintained compliance with TSA SD 1582, adhering to industry regulations and standards.
- Advocated security best practices in Microsoft Azure to enhance cloud infrastructure resilience.
- Developed a zero-trust project plan based on Cisco's SAFE model to reduce attack escalation.
- Collaborated with industry experts to modernize IT security configurations for enhanced cyber resilience.
- Managed devices through Microsoft Intune, ensuring a secure endpoint infrastructure.
- Supported Meraki VPN, contributing to secure and reliable remote access.
- Conducted incident response and threat hunting in Microsoft Defender.
- Assisted in procuring a Managed Detection and Response (MDR) solution to improve IT and security workflows.
- Led vulnerability management initiatives, effectively reducing exposure scores in Microsoft Defender.
- Utilized tools including Microsoft P2 Licensed Azure Stack (Defender, Purview, Sentinel, Entra ID, Intune), Mimecast Email Security, Cisco Meraki Firewalls/Switches/Access Points, ReliaQuest GreyMatter, and Qualys VMDR.

Cyber Security Analyst | Summit Human Capital

As a Cyber Security Analyst, I was responsible for monitoring and analyzing the security of the organization's networks and systems. I identified potential security risks, recommended and implemented security measures, and responded to security incidents. I also conducted regular security audits and provided training to improve security awareness among employees. This position is a contracted role to support a passenger rail organization.

- Conducted regular security assessments to identify and mitigate potential vulnerabilities in systems.
- Monitored network traffic and system logs to detect and respond to security incidents.
- Investigated security breaches and provided recommendations for improving systems and processes.
- Reviewed policies aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), checking for accuracy and contextualizing for a Critical Infrastructure (CI) organization.
- Developed plans for progressing towards a Zero Trust Architecture (ZTA) including high-level strategic documents as well as step- by-step implementation guides.
- Leveraged existing guidance from NIST, Cybersecurity and Infrastructure Agency (CISA), National Security Agency (NSA), Defense Information Systems Agency (DISA), and Center for Internet Security (CIS) to elevate a security baseline.
- Assisted with the procurement of new third-party vendor provided products and services to enhance the technological security stack

Cross-Functional Planning & Coordination Intern | Cybersecurity and Infrastructure Security Agency

40hrs/week, July 2022 - October 2022

As a Cross-Functional Planning & Coordination Intern, I assisted in the development and improvement of CISA Vulnerability Management (VM) products, assisted cross-functional activities such as involvement in focus studies for VM product feedback, and supported project management efforts.

- Assisted in developing cross-functional workflows to ensure smooth coordination between teams.
- Helped facilitate communication between different VM Insights sections for collaborative planning.
- Supported veteran federal agents in analyzing data and identifying areas for improvement in cross-functional coordination.
- Learned about large-scale issues faced by Critical Infrastructure owners and operators across the United States.
- Developed a globally-aware strategic mindset to approaching security control implementation at lower cyber resourced critical organizations.

Information Security and Technology Intern | Virginia Railway Express

~30hrs/week, February 2019 - January 2022

As an Information Security and Technology Intern, responsibilities included assisting with security assessment of user workstations, performing daily help-desk duties, and contributing to projects to improve the IT environment.

- Uncovered and eliminated potential inefficiencies by scheduling periodic maintenance sessions, while documenting all repairs and fixes for future reference.
- Utilized proven response strategies to analyze complex security incidents and resolve technological issues in a timely manner.
- Provided contextual information to users during troubleshooting technical issues to alleviate future frustrations.
- Assisted with invoices and additional duties beyond the scope of Information Technology.

Education

Master of Science Cybersecurity | Old Dominion University, Norfolk

2021 - 2023

Bachelor of Science Cybersecurity | Old Dominion University, Norfolk

2020 - 2021

Skills

Network security | Windows, Mac, Linux | Vulnerability Management | Incident response and management | Threat intelligence analysis | Threat hunting | Microsoft Defender | Microsoft Sentinel | Qualys VMDR | Mimecast Email Security | Security information and event management (SIEM) | Penetration testing | CIS Benchmarks, DISA STIGs, NIST CSF, CISA SCuBA | Writing user-friendly documentation | Learning new programming tools and techniques | Working with open source solutions | Microsoft Azure Cloud Services

Soft skills

Critical thinking | Problem-solving | Attention to detail | Adaptability | Emotional Intelligence | Customer Service

Social networks

LinkedIn

linkedin.com/in/paul-b-58016a61/