Phone: (540) 424-0974
Email: paul.brown@6browns.org

PAUL BROWN
CYBER SECURITY SPECIALIST

Summary

Experienced Cyber Security professional with a strong background in network security, vulnerability management, security engineering, and identity management. Adept at guiding system administrators and network specialists in securing systems and networks against advanced cyber threats while addressing misconfigurations. Proficient in security analysis, policy compliance, zero-trust architecture implementation, and comprehensive IT department support. Passionate about protecting critical infrastructure from persistent cyber threats and safeguarding digital identities within cyberspace.

Work Experience

Cyber Security Analyst | Virginia Railway Express

September 2023 - Present (37.5 hrs/week)

Cyber Security Analyst | PowerSolv, Inc

- Overseeing and enhancing the organization's cybersecurity posture through proactive threat mitigation.
- Managing endpoint security and threat response strategies.
- Identified and mitigated security risks, conducted threat assessments, and implemented robust security measures.
- Collaborated with a Managed Detection and Response (MDR) team to investigate security incidents and strengthen defensive measures.
- Optimized security policies in alignment with the NIST Cybersecurity Framework (CSF) and ensured compliance with TSA SD 1582 regulations.
- Developed and executed a zero-trust project plan based on Cisco’s SAFE model to enhance cybersecurity resilience.
- Managed devices using Microsoft Intune and supported Meraki VPN for secure remote access.
- Conducted incident response and threat-hunting activities within Microsoft Defender.
- Led vulnerability management initiatives, effectively reducing exposure risks.
- Utilized enterprise security tools, including Microsoft P2 Licensed Azure Stack, Mimecast Email Security, Cisco Meraki, ReliaQuest GreyMatter, and Qualys VMDR.

Cyber Security Analyst | Summit Human Capital

Previous Role

- Monitored and analyzed network security, identifying and mitigating potential risks.
- Responded to security incidents, conducted audits, and provided actionable recommendations.
- Reviewed policies based on NIST CSF and contextualized them for a Critical Infrastructure (CI) organization.
- Developed Zero Trust Architecture (ZTA) implementation plans, including strategic roadmaps and step-by-step execution guides.

- Leveraged security guidance from NIST, CISA, NSA, DISA, and CIS to strengthen baseline security.
- Assisted in evaluating and procuring third-party security solutions to enhance the security stack.

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

July 2022 - October 2022 (40 hrs/week)

- Assisted in developing and refining CISA Vulnerability Management (VM) products.
- Facilitated cross-functional collaboration and streamlined vulnerability management workflows.
- Provided data-driven insights to support veteran federal agents in enhancing cybersecurity initiatives.
- Developed a strategic mindset for implementing security controls at resource-limited critical infrastructure organizations.

Information Security and Technology Intern | Virginia Railway Express

February 2019 - January 2022 (~30 hrs/week)

- Conducted security assessments and assisted with daily IT help-desk operations.
- Implemented periodic maintenance schedules to improve system efficiency.
- Analyzed security incidents and developed resolutions to address technological vulnerabilities.
- Provided user training and contextual troubleshooting support to enhance IT security awareness.
- Assisted with financial documentation and other administrative duties beyond IT scope.

Education

Master of Science, Cybersecurity | Old Dominion University, Norfolk *(2021 - 2023)*
Bachelor of Science, Cybersecurity | Old Dominion University, Norfolk *(2020 - 2021)*

Skills

- **Technical Skills:** Network Security, Windows/Mac/Linux Administration, Vulnerability Management, Incident Response, Threat Intelligence Analysis, Threat Hunting, Microsoft Defender, Microsoft Sentinel, Qualys VMDR, Mimecast Email Security, SIEM Operations, Penetration Testing, CIS Benchmarks, DISA STIGs, NIST CSF, CISA Guidelines, Cloud Security, Microsoft Azure Cloud Services.
- **Soft Skills:** Critical Thinking, Problem-Solving, Attention to Detail, Adaptability, Emotional Intelligence, Customer Service, Cross-Team Collaboration.

Network

LinkedIn Profile
Website
Github