LOGAN McKINLEY

Cyber Security Event Analyst | BS - Network Admin & Security

logan.mck4@gmail.com | 801-472-5260 | loganmckinley.com

Related Experience

University of Utah | Salt Lake City, UT
Cyber Security Event Analyst
01/2025 - Current
Full-Time

- Monitored and analyzed security alerts using Qradar to identify and respond to threats in real-time for over 100,000 endpoints org-wide.
- Investigated phishing and malware incidents across faculty, staff, student accounts, and healthcare facilities, ensuring timely containment and remediation.
- Assisted in regular vulnerability scans with Qualys, tracked remediation progress, and supported patch management efforts.
- Supported compliance with FERPA, and HIPAA by enforcing security controls and conducting periodic risk assessments.
- Implemented and maintained multi-factor authentication (MFA) for staff and faculty accounts, reducing unauthorized access risks.
- Assisted in phishing awareness campaigns and delivered cybersecurity training to promote safe computing practices campus-wide.
- Automated security workflows using PowerShell/Python to streamline alert triage and incident documentation.
- Maintained up-to-date security documentation including playbooks, response procedures, and user guidance.

doTERRA International LLC | Pleasant Grove, UT
Technical Support Engineer II
06/2023 - 01/2025
Full-Time

- Appointed as the primary network liaison within the help desk team, entrusted with addressing, triaging, and resolving network-related inquiries and security issues.
- Configured and administered firewall policies for Palo Alto firewalls in both corporate and data center environments.
- Organized, set up, and managed Azure AD/Entra ID, and Intune.
- Ran and analyzed scans within Rapid7, Tenable, and Sentinel One to patch known vulnerabilities company-wide for PCI compliance.
- Addressed network connectivity problems such as router configurations, IP addressing, and DHCP server setup.
- Restructuring of our Active Directory system to accurately organize assets.
- Ensured accuracy and currency of all documentation within our knowledge base through regular updates and verification processes.

doTERRA International LLC | Pleasant Grove, UT
Help Desk Technician
02/2021 - 06/2023
Full-Time

- Created new accounts, reset passwords, and configured access to servers and file management software for users.
- Collaborated with cross-functional teams to escalate complex technical issues and coordinate problem resolution.
- Devised incisive workarounds and resolutions for IT-related problems.
- Provided customer and end-user help desk support in a company of over 2,000 employees in a Windows and Mac environment.

Skills

Core Security Skills
Incident Response · Vulnerability Management · Threat Hunting · Log Analysis · SIEM Monitoring · EDR Management

Tools & Technologies
Qradar · Rapid7 · ServiceNow · HaloITSM · Okta · Cisco Duo · Javascript · HTML · Python · Powershell scripting

Systems & Networking
Windows · MacOS · Linux Active Directory · Azure AD/ Entra ID · DHCP · TCP/IP · Palo Alto Next-Gen Firewalls

Education & Training

Utah Valley University | UT
Bachelor of Science · IT Network Administration and Security **(Aug 2019- April 2024)**

Utah Valley University | UT
Associate in Science · Information Systems & Technology **(Aug 2019- April 2024)**

Mountain View High School | UT
High School Diploma (2017)

Tryhackme.com
8 Hour average per week / Top 8% of users · Jr Pen Tester and Intro to Cyber Security (Skills learned: Burp suite, Nmap, Nessus, Splunk, Metasploit, and XSS)

Hobbies

Projects
Established a virtual environment tailored for local penetration testing, employing industry-standard tools and techniques to simulate real-world security scenarios. Implemented security protocols to ensure accurate assessment of system vulnerabilities.

Developing a custom EDR solution in Python, designed to help small and mid-sized businesses improve their security posture without the high cost of enterprise tools. The goal is to create an all-in-one platform that simplifies compliance by providing actionable insights and guidance, enabling employees at any level to identify, patch, and resolve issues efficiently.

Developed an iOS application leveraging ChatGPT API to dynamically generate stories based on user input. Integrated user authentication to ensure personalized experiences and utilized Firebase for cloud-based database management.

Personal Life
Served a two-year mission with The Church of Jesus Christ of Latter-day Saints, which led to the acquisition of skills in the areas of Cultural Sensitivity and Awareness, Adaptability, Problem-Solving, Communication, Leadership and Teamwork, Emotional Resilience, Project Management, Networking and Collaboration, which are highly transferable to professional and personal life.

I enjoy spending time outdoors through walking, running, swimming, and fly fishing whenever I get the chance.

References upon request