Christopher Danley

773-537-5899
Cartiea88@gmail.com
cartiea88.github.io
www.linkedin.com/in/christopherdanley

EDUCATION

B.S. Business Administration — Northern Illinois University, May 2011

CERTIFICATIONS

CompTIA Security+
CompTIA Network+
Microsoft Azure Fundamentals (AZ-900)
Splunk Core Certified User - Splunk

PROJECTS

Implemented a Hypothetical Vulnerability Management program
Source: https://github.com/Cartiea88/Project-Vulnerability-Management-Program
Platforms and Technology Used: Azure VM, Tenable Nessus, PowerShell

Completed an Threat Hunt to detect unauthorized TOR Browser usage
Source: https://github.com/Cartiea88/threat-hunting-scenario-tor
Platforms and Technology Used: SIEM (Microsoft Sentinel), EDR (Defender for Endpoint), Azure VM, KQL

EXPERIENCE

Company: Log(N) Pacific — 10/14/2025 - Present
Title: Cybersecurity Analyst **(Vulnerability Management Intern)**
Vulnerability Management:

- Conducted vulnerability scans, provided detailed reports, and implemented PowerShell-based remediations, contributing to a 100% reduction in critical, 90% in high, and 76% in medium vulnerabilities for the server team.
- Performed vulnerability assessments and risk prioritization using Tenable across Windows and Linux environments.
- Executed secure configurations and compliance audits (DISA STIG) with Tenable to meet industry standards.
- Automated remediation processes and STIG implementations using PowerShell to address critical vulnerabilities.

Company: Log(N) Pacific **(Security Operations and Incident Response)** — 10/14/2025 - Present
Title: Cybersecurity Analyst (Security Operations Intern)
Security Operations:

- Performed threat hunting with EDR, detecting IoCs from brute force attacks, data exfiltration, and ransomware.
- Designed, tested, and published advanced threat hunting scenarios for incident response tabletop exercises
- Developed custom detection rules in Microsoft Defender for Endpoint to automate isolation and investigation of compromised systems.
- Reduced brute force incidents by 100% by implementing inbound NSG/firewall rules to limit Internet exposure.
- Created Microsoft Sentinel dashboards to monitor logon failures and malicious traffic using threat intelligence.
- Experienced with KQL (similar to SQL/SPL) which I used to query logs within the SIEM and EDR platform.

Aspen Dental **5/10/2023 - Present**

Procurement Specialist

- Monitor, support, and execute the purchasing process for goods for over 900+ dental practices which includes vendor setup, requisition & purchase order creation, order expediting, fulfillment & return.
- Utilized ServiceNow ticketing system to manage and track support requests for over 100+ tickets per month.
- Created and maintained reports and documentation to ensure accurate tracking and compliance with company standards

ADDITIONAL SKILLS AND TECHNOLOGIES

Endpoint Detection and Response, CVE/CWE Management, CVSS Scoring, OWASP Top 10, Risk Prioritization, Vulnerability Remediation, PowerShell Scripting, BASH Scripting, Firewall/NSG Configuration, NIST 800-37: Risk Management Framework, NIST 800-53: Security and Privacy Controls, NIST 800-61: Computer Security Incident Handling Guide, NIST 800-40: Guide to Enterprise Patch Management Planning, NIST Cybersecurity Framework, PCI-DSS, GDPR, HIPAA