Hands-On IT & Cybersecurity Training **+ Internships**
https://skool.com/cyber-range/about

FIRST LAST

425-319-xxxx
first.last@email.com
github.com/joshmadakor0
linkedin.com/in/name

EXPERIENCE

Company: Log(N) Pacific 4/1/2023 - Present
Title: Cyber Security Support Analyst (Vulnerability Management & SecOps 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.
- Deep understanding of the "soft" side of Vulnerability Management: rapport, trust, transparency, and business need.

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.

Company: <Company Name> Start Date - End Date
Title: <Title>

- Responsibilities (with metrics if possible)

PROJECTS

Vulnerability Management and Threat Hunting Projects
Source: github.com/username
Platforms and Technology Used: Tenable.io, SIEM (Microsoft Sentinel), EDR (Defender for Endpoint), Azure VMs, KQL

CERTIFICATIONS

CompTIA Security+
CISSP (Expected 3/2024)

EDUCATION

B.S. Information Technology Management Western Governors University, (Expected 2026)

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