Derrick Joseph Horton

Austin, TX | (202) 489-9284 | derrick@derrickhorton.com | LinkedIn | GitHub | Website

SUMMARY

Communicative cybersecurity analyst well-practiced in using Azure Sentinel as a SIEM for threat detection and incident response, Nessus Tenable for vulnerability management, and Microsoft Defender for log analysis. Skilled with KQL queries, MITRE ATT&CK framework, and adhering to NIST guidelines. Adept at identifying and triaging potential threats with high accuracy, collaborating with SOC teams, and improving overall security posture.

EDUCATION

Western Governors University **2024**
Bachelor of Science, Cybersecurity & Information Assurance

EXPERIENCE

Abnormal AI **Feb 2025 - Aug 2025**
Security Analyst *Remote*

- Detected and reported phishing threats and compromised vendor accounts, enhancing overall network security
- Investigated suspicious login attempts to analyze malicious account takeovers, improving incident response efficiency
- Created automation rules using AI to better detect threats that slipped through the cracks, reducing false negatives in threat detection

Leading Edge Connections **Sep 2023 - Jan 2025**
Customer Service Representative *Remote*

- Managed high-pressure situations by quickly triaging calls and serving multiple clients, improving response times and customer satisfaction
- Implemented protocols for safeguarding sensitive customer data using NIST 800-61 guidelines, enhancing data security and compliance

PROJECTS

Implementing a SOC and Honeynet in Azure | https://github.com/derrickhorton/CyberRange **2024**

- Platforms & Technologies: Azure virtual machines, Azure Sentinel (SIEM), Log Analytics, MITRE ATT&CK Framework

Vulnerability Management Program Implementation **2024**
https://github.com/derrickhorton/vulnerability-management-program

- Platforms & Technologies: Tenable vulnerability scans, Azure virtual machines, Windows 10, Ubuntu

Programmatic Vulnerability Remediations **2024**
https://github.com/derrickhorton/programmatic-vulnerability-remediations

- Platforms & Technologies: PowerShell, Windows 10 VM, Bash, Ubuntu VM, Tenable vulnerability scans

Threat Hunt Report: Unauthorized TOR Usage | https://github.com/derrickhorton/threat-hunting-scenario-tor **2024**

- Platforms & Technologies: Azure, Microsoft Defender for Endpoint, Kusto Query Language (KQL)

SKILLS

- **Tools**: Splunk, Microsoft Sentinel, Defender for Endpoint, Log Analytics, SIEM, IDS/IPS
- **Scripting**: Bash, SQL, Python, PowerShell, Linux Command Line, File Permissions
- **Frameworks**: MITRE ATT&CK, NIST 800-61, NIST 800-144
- **Cybersecurity**: Threat Detection, Incident Response, Vulnerability Assessment, Threat Hunting
- **Cloud Security**: AWS, Azure, Google Cloud, Virtual Networks, Access Control Lists
- **Networking**: TCP/IP, DNS, VPNs, Network Troubleshooting, Firewalls, Active Directory
- **Soft Skills**: Communication, Documentation, Collaboration, Analytical Thinking

CERTIFICATIONS

- CompTIA CySA+
- CompTIA PenTest+
- CompTIA Security+
- CCSP (ISC2 Associate)
- ISC2 SSCP
- CompTIA Network+
- Microsoft AZ-900 (Azure Fundamentals)
- Linux Professional Institute Linux Essentials
- Coursera Google Cybersecurity Professional