Derrick Joseph Horton

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

SUMMARY

Cybersecurity analyst with expertise in SIEM technologies such as Microsoft Sentinel and Splunk for incident response and threat detection. Experienced in vulnerability management and log analysis using tools like Microsoft Defender and PowerShell scripting. Proven ability to accurately identify, triage, and mitigate threats while collaborating with SOC teams. Adept at applying MITRE ATT&CK and NIST guidelines to enhance overall security posture.

EDUCATION

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

EXPERIENCE

Abnormal AI | *Security Analyst* **Feb 2025 - Present**

- Detected and reported phishing threats and compromised vendor accounts, leveraging SIEM tools to support prompt incident response and threat analysis.
- Investigated suspicious login attempts to analyze and mitigate potential malicious account takeovers, incorporating advanced threat hunting techniques.
- Developed automation rules using scripting languages to enhance AI-based threat detection and streamline incident response workflows.

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

- Handled high-volume calls under pressure while triaging issues effectively and ensuring data confidentiality.
- Followed protocols for safeguarding all sensitive customer information.

PROJECTS

Implementing a SOC and Honeynet in Azure

- Source: https://github.com/derrickhorton/CyberRange
- Platforms & Technologies: Azure virtual machines, Azure Sentinel (SIEM), Log Analytics, MITRE ATT&CK Framework

Vulnerability Management Program Implementation

- Source: https://github.com/derrickhorton/vulnerability-management-program
- Platforms & Technologies: Tenable vulnerability scans, Azure virtual machines, Windows 10, Ubuntu

Programmatic Vulnerability Remediations

- Source: 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

- Source: https://github.com/derrickhorton/threat-hunting-scenario-tor
- 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, PCAP Analysis, Malware Analysis, Digital Forensics
- **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

- **CySA+**: CompTIA 2024 – 2030
- **Security+**: CompTIA 2023 – 2030
- **SSCP**: ISC2 2025 – 2028
- **AZ-900 (Azure Fundamentals)**: Microsoft 2025 – 2026
- **Google Cybersecurity Professional**: Coursera 2023 – Life
- **PenTest+**: CompTIA 2024 – 2027
- **CCSP Associate**: ISC2 2024 – 2025
- **Network+**: CompTIA 2023 – 2030
- **Linux Essentials**: Linux Professional Institute 2024 – Life