

Marcus Reed

Cybersecurity Analyst | SOC & Threat Detection

Arlington, VA
(703) 555-0129
marcus.reed@email.com
linkedin.com/in/marcusreed-sec

> PROFESSIONAL SUMMARY

Cybersecurity Analyst with 3.5 years of experience in security operations, incident response, vulnerability management, and threat hunting. Monitored environments of 8,000+ endpoints, reduced mean time to respond by 55%, and closed 95% of critical vulnerabilities within SLA. Skilled in SIEM, EDR, MITRE ATT&CK, and NIST/ISO-aligned security controls.

> CORE COMPETENCIES

SIEM / EDR: Splunk, Microsoft Sentinel, CrowdStrike Falcon, Defender for Endpoint, QRadar
Vulnerability Mgmt: Nessus, Qualys, Rapid7, Burp Suite, OWASP Top 10, Nmap, Metasploit (basics)
Network & Cloud: Palo Alto, Wireshark, IDS/IPS, Zscaler, AWS Security Hub, Azure Security Center, IAM
Frameworks: NIST CSF, NIST 800-53, MITRE ATT&CK, ISO 27001, CIS Controls, SOC 2, HIPAA
Scripting: Python, PowerShell, Bash, SQL, KQL, SPL

> PROFESSIONAL EXPERIENCE

Cybersecurity Analyst (Tier 2 SOC)

May 2024 – Present

Sentinel Defense Solutions — Arlington, VA

- Triage and investigate 80+ security alerts daily in Splunk and CrowdStrike; escalated and contained 120+ confirmed incidents.
- Reduced mean time to respond (MTTR) from 4.2 hours to 1.9 hours (55%) by building playbooks and automating enrichment in Python.
- Authored 60+ Splunk detection rules mapped to MITRE ATT&CK, increasing true-positive rate by 30% and cutting false positives by 38%.
- Led phishing response program: analyzed 2,500+ reported emails and ran simulations that lowered click rate from 18% to 6%.
- Produced executive incident reports and root-cause analyses for leadership and external auditors.

Information Security Analyst

Jul 2022 – Apr 2024

Atlas Health Systems — Richmond, VA

- Ran weekly Nessus and Qualys scans across 8,000+ endpoints; drove remediation of 95% of critical findings within SLA.
- Supported HIPAA and SOC 2 audits by gathering evidence and remediating control gaps, achieving zero major findings.
- Hardened Windows and Linux servers to CIS benchmarks and tightened IAM and MFA policy, reducing privileged accounts by 35%.
- Conducted threat hunts and log analysis with Wireshark and Sentinel, identifying 3 persistent threats missed by automated tools.

> PROJECTS & LABS

- **Home SOC Lab:** Built a virtual lab with Splunk, Security Onion, and Kali to simulate attacks and tune detections; documented 25 use cases.
- **CTF Competitor:** Top 5% in national Cyber Defense Competition (2024); web exploitation and forensics.

> EDUCATION

B.S. in Cybersecurity

2022

George Mason University — Fairfax, VA | GPA 3.6/4.0

> CERTIFICATIONS

CompTIA Security+ (2022) | CompTIA CySA+ (2023) | GIAC GCIH (2024) | Microsoft SC-200 (2024)