

Delstun McCray

CYBER SECURITY SPECIALIST

PROFESSIONAL SUMMARY

Proactive Cybersecurity Specialist with hands-on experience in network defense, vulnerability assessment, and system hardening. Proven ability to detect and respond to threats utilizing tools like Security Onion and Splunk. AWS certified with a strong foundation in cloud security, scripting, and log analysis. Eager to contribute to a dynamic SOC or blue team environment, leveraging analytical skills and practical experience to enhance organizational security posture.

Phone:
+1(971) 323-9404

Email:
Delstunmccray@gmail.com

EDUCATION

Certificate of Completion, Cybersecurity
Davis Technical College, August 2024 - April 2025

- Graduated with NTHS honors.
- GPA 3.87
- Relevant Coursework: Network Security Fundamentals, Ethical Hacking & Penetration Testing, Incident Response & Forensics, Security Operations & Analysis, Cloud Security

SKILLS & PROFICIENCIES

Security Tools:

- Wireshark
- Burp Suite
- Nessus
- Splunk
- Nmap

Systems:

- Windows
- Linux (Ubuntu, Kali)
- Mac

Networking:

- TCP/IP
- DNS
- VPNs
- VLANs
- Subnetting

Cloud/DevOps:

- AWS
- Git
- Swift
- Python

Frameworks:

- OWASP Top 10
- MITRE ATT&CK
- Incident Response

WORK EXPERIENCE

iOS Developer (Cybersecurity Focus)
Midwestern, April 2022 - August 2023

- Identified and remediated high-impact software vulnerabilities, including memory leaks and insecure data handling, significantly improving application stability and security posture.
- Conducted comprehensive code reviews and implemented secure coding practices reducing the risk of data exposure across API endpoints.
- Traced root causes of application crashes using Xcode Instruments, crash logs, and memory profilers, cutting crash frequency by 40% and enhancing overall reliability.
- Collaborated effectively with product, QA, and backend teams to rapidly patch critical security bugs and ensure secure application deployments.

CERTIFICATIONS & VOLUNTEER WORK

Certifications

- iOS Development (Issued 02/2022)
- CompTIA ITF+ (Issued 08/2024)
- CompTIA A+ (Issued 12/2024)
- CompTIA Network+ (Issued 02/2025)
- CompTIA Security+ (Issued 03/2025)
- Amazon AWS Cloud Practitioner (Issued 04/2024)

Volunteer Work

Mentor

Davis Technical College

Guided students through practical exercises and real-world cybersecurity scenarios, sharing expertise to develop essential skills.

PROJECTS

SIEM Implementation & Threat Detection Lab

Ongoing

- Designed and deployed a virtualized security lab environment using VirtualBox, integrating Kali Linux and vulnerable Windows/Linux machines.
- Implemented Splunk to collect, parse, and analyze logs from various sources (Syslog, Windows Event Logs).
- Developed custom detection rules and dashboards to monitor for common attack patterns, including brute-force attempts and suspicious network activity.
- Simulated basic attacks (e.g., Nmap scans, login failures) to validate SIEM alerting capabilities and practice log analysis.

Vulnerability Assessment & Reporting

Ongoing

- Utilized Nessus (or OpenVAS) to perform comprehensive vulnerability scans against intentionally vulnerable virtual machines (e.g., Metasploitable).
- Analyzed scan results to prioritize vulnerabilities based on severity and potential impact, adhering to industry best practices.
- Authored detailed remediation reports outlining identified weaknesses, proposed mitigation strategies, and recommended security enhancements.
- Demonstrated understanding of common vulnerabilities (e.g., SQL Injection, XSS) and their real-world implications.

Network Traffic Analysis & Anomaly Detection

Ongoing

- Captured and analyzed network traffic using Wireshark to identify common protocols, anomalous behaviors, and potential security threats.
- Investigated packet captures to identify clear-text credentials, suspicious DNS queries, and unusual data exfiltration attempts.
- Applied knowledge of TCP/IP, DNS, and HTTP protocols to dissect network communications and pinpoint indicators of compromise.
- Documented findings and proposed network segmentation or intrusion detection rules to enhance network security.