Delilah Crenshaw

[Delilah.l.crenshaw@usace.army.mil](mailto:Delilah.l.crenshaw@usace.army.mil)

[Delilahlcrenshaw@gmail.com](mailto:Delilahlcrenshaw@gmail.com)

[https://www.linkedin.com/in/delilahcrenshaw](https://www.linkedin.com/public-profile/settings)

**Objective**

Signal Operations Specialist experienced in managing essential communications systems and ensuring effective collaboration with military partners in mission environments. Skilled in network setup, cybersecurity protocols, and incident response. Knowledgeable in RMF, eMASS, POA&Ms, ACAS, and Vulnerability Management.

**Professional Experience**

United States Army,

2d Multi-Domain Task Force

Signal Company

USAG Wiesbaden

Signal Operations Specialist 2021-2023

* Established secure communication, handling Communication Security (COMSEC).
* Monitored wavelengths and frequencies for anomalies and potential security threats .
* Configured, installed, and tested routers, firewalls, and servers using hypervisor technology, significantly enhancing network security and functionality.
* Resolved and mitigated network errors to restore communication in high-pressure situations, maintaining operational integrity.
* Reengineered software and routers to support mobile tactical command communication systems and ensure reliability in dynamic environments.
* Conducted evaluations of network systems for Local Area Networks (LAN) and Wide Area Networks (WAN).
* Managed radio communication systems, including Ultra-High Frequency (UHF), Very High Frequency (VHF), MUOS, and SINCGARS, ensuring seamless operational communication.

United States Army

2d Multi-Domain Task Force

CEMA Company

USAG Wiesbaden

Signal Cyber Operations Specialist 2023-2025

* Sustained critical signal support and communication systems while ensuring command and troop movement during military operations.
* Collaborated with foreign national militaries and NATO partners to establish secure communication frequencies and deliver comprehensive technical support for their computer systems.
* Managed and optimized local area networks (LAN), terminal devices, and satellite communications in challenging and hostile environments.
* Installed, troubleshot, and maintained computer and network hardware, IP networking systems, and automated signal support systems, enhancing overall operational efficiency.
* Led a high-performing team to achieve 87% accuracy in delivering uninterrupted network services in remote areas, directly driving mission success and operational effectiveness.

U.S. Army Corps of Engineers

NAD-IM

Cybersecurity

Information Management 2024-2025

* Conducted security audits and vulnerability assessments to ensure rigorous compliance with industry regulations and enhance organizational security posture.
* Monitored network traffic to detect and respond to potential threats, ensuring timely incident resolution and system integrity.
* Collaborated on penetration testing and ethical hacking initiatives to rigorously evaluate and strengthen security measures, significantly reducing vulnerabilities.
* Developed security awareness training programs focusing on phishing, social engineering, and password management for employees.
* Supported data encryption and backup protocols to safeguard sensitive information.
* Implement vulnerability and patch management for systems with identified vulnerabilities, enhancing overall security and resilience against threats.
* Conduct DoD Assessment and Authorization (A&A) activities utilizing the DIACAP and RMF processes.
* Analyze the CS architecture of Range systems for compliance with DoD policies; develop and execute security test plans; and use security tools such as ACAS/Nessus, SCAP, and execution of STIGs.
* Conduct vulnerability assessment for information systems, implement risk mitigation strategies, and develop and track the plan of action and milestones (POA&M); comprehend and apply mitigation techniques and methods.
* Research policies, procedures, standards, and guidance are applied under specific conditions to protect information and information systems.

**Education**

Master of Science in Cyber Security – Management and Policy

The University of Maryland Global Campus Europe

Bachelor of Arts in Psychology - Childhood and Adolescent Development

Southern New Hampshire University, Manchester, NH | Cum Laude

National Society of Leadership and Success (NSLS) | 2023

**Certifications**

* CompTIA Security+: Validated foundational knowledge in cybersecurity, risk management, and threat analysis.
* CompTIA Advanced Security Practitioner (CASP+): Demonstrated advanced proficiency in enterprise security, risk management, and advanced security solutions.
* ACAS/Tenable Certified: Expertise in continuous monitoring and vulnerability management to enhance organizational security posture.
* Trellix Certified: Proficient in utilizing Trellix security solutions for threat detection and incident response.
* Top Secret – Sensitive Compartmented Information (TS/SCI): Hold a high-level security clearance, enabling access to classified information and operations.
* IAT Level III Certified: Advanced knowledge in information assurance, focusing on security and risk management principles.