Steven Walters

TS/SCI

Graniteville, SC 29829

762-333-3153

stevewalters@wolfensixx.tech

Personal Website | LinkedIn

PROFESSIONAL SUMMARY

Cybersecurity professional with over seven (7) years of experience in security engineering and threat analysis. Specialized in threat mitigation, Endpoint Detection and Response (EDR) management, Security Information and Event Management (SIEM) integration, and defensive cyber operations (DCO). Developed modular cyber platforms and Operational Technology/Industrial Control Systems (OT/ICS)-focused solutions, enhancing organization capabilities and decision-making. Passionate about Security Operations Center (SOC) analysis, cyber operations consulting, and teaching/mentoring on-boarding cyber analysts.

PROFESSIONAL EXPERIENCE

Course Instructor – US Army

March 2023 – March 2026

- Led instruction for over 800+ students through hands-on training environments focusing primarily on cloud infrastructure design, network traffic analysis, Digital Forensics and Incident Response (DFIR), and SIEM configuration.
- Developed 4 comprehensive training modules on incident response using Elastic Stack and Arkime, directly aligning and updating course content with evolving cybersecurity threats and industry standards.
- Developed and standardized brigade-wide training content for on-boarding personnel, supporting sustained certification and skills validation for 1,300+ cyber personnel across 3 battalions.
- Dual-hatted as a senior DevOps engineer, building and maintaining version control records for on-prem and cloud-based DDS-M tools, utilizing Ansible and OpenStack across 12 operations, along with 4 joint-force cyberspace exercises. Streamlined CI/CD pipelines and data ingestion process through big data platforms such as Splunk and Apache NiFi.
- Established a hybrid environment of 40+ virtual machines and 19 physical servers, which facilitated the development and testing of innovative methodologies; the infrastructure is now leveraged by 700+ personnel brigade-wide.

Cyber Capabilities Engineer – US Army
June 2021 – May 2023

- Evaluated OT monitoring technologies via operational testing and mock exercises to determine integration eligibility into Deployable Defense System-Modular (DDS-M) kits, assessing IDS/IPS resiliency and addressing key defensive capability gaps for defensive cyber operations (DCO)
- Engineered and modernized curriculum to reflect real-world adversary tactics, enterprise architectures, and defensive operational processes.
- Collaborated with on-site caregivers and stakeholders to ensure smooth IT transitions during expansions and renovations for eleven (11) separate United States Cyber Command (USCYBERCOM) facilities, assessing operational impacts through the change management process.
- Led evaluation of Red Hat and vSphere-based platforms through automated (Terraform/Ansible) deployment testing, addressing critical capability gaps for 930 + user workstations.
- Reverse-engineered network and communication protocols for developing real-time, packet-level threat detection and response tools, improving response effectiveness by 15% for 12 teams.
- Supported the successful execution of five(5) high-level security audits (including CCRIs) by performing hands-on control validation, maintaining documentation, conducting risk analysis, and ensuring audit readiness across multiple enclaves.
- Collaborated with product owners to develop 38 incident response playbooks aligned with the full incident response lifecycle, strengthening response consistency.

Cyber Operations Specialist – US Army
May 2018 – May 2021

- Conducted enterprise-level vulnerability analysis and mitigation across military and private sector networks in support of defensive cyber operations.
- Applied cyber intelligence, surveillance, and defensive/offensive techniques to detect, analyze, and disrupt adversary activity within complex network environments.
- Produced executive-level cyber protection plans and incident reports, translating technical risk into actionable insights for senior leadership.

Cyber Operations Training (JCAC/CCTC) – US Army
June 2016 – May 2018

- Completed intensive, 9-month Joint Cyber Analysis Course acquiring a broad spectrum of skills in network forensics, malware analysis, vulnerability assessment and security system administration across Windows and Linux environments.
- Engineered, simulated, and defended complex virtualized networks during numerous capstone events, demonstrating proficiency in TCP/IP analysis and cyber security operations.

CORE COMPETENCIES

- **Policies & Procedures:** MITRE ATT&CK, RMF, CSF 2.0 (NIST), ATO, Acceptable Use Policy
- **Scripting:** Python (including NumPy and pandas), Powershell, Bash, NodeJS
- **Cloud Infrastructure:** Terraform, Ansible, Azure, AWS, Gabriel Nimbus, Git
- **IAM Design:** MFA, SSO, Zero Trust, AWS IAM, Microsoft EntraID (Azure AD)
- **Platforms:** Linux (Arch, Debian, RHEL), ESXi, vSphere Enterprise, Big Data(Splunk, Apache NiFi)
- **Incident Response:** Kibana, Splunk, Nessus, Security Onion, Nozomi, Tenable, MemProcFS

EDUCATION

- **Bachelor of Arts (BA), Cybersecurity**
  University of Maryland Global Campus | *Expected June 2026*
- **Associate of Applied Science, Computer & Electronics Engineering**
  ITT Technical Institute | August 2001 – January 2004
- **SANS SEC555** – Detection Engineering and SIEM Analytics
- **SANS SEC503** – Network Monitoring and Threat Detection In-Depth
- **SANS SEC401** – Security Essentials – Network, Endpoint, and Cloud
- **SANS FOR508** – Advanced Incident Response, Threat Hunting, and Digital Forensics
- **Joint Cyber Analysis Course**
- **Common Cyber Technical Core**