

NICOLAS A. WELSH

Augusta, GA | 215-873-5896 | nicolas.a.welsh@gmail.com
www.linkedin.com/in/nicolas-welsh | Open to relocation: Washington or Remote

CYBERSECURITY ANALYST | INCIDENT RESPONSE | ELASTIC SECURITY | TS/SCI

SUMMARY

Cybersecurity analyst and U.S. Army Staff Sergeant with 5+ years of experience conducting threat hunting, incident response, and digital forensics in support of U.S. Cyber Command missions. Elastic Certified Analyst with hands-on experience deploying Elastic Stack in segmented DFIR environments, automating forensic artifact ingestion, and building AI-assisted workflows that query Elastic data to accelerate analysis, reporting, and storyboard development. TS/SCI cleared professional with a background in Linux infrastructure, Python automation, and scalable detection workflows.

TECHNICAL SKILLS

Elastic / Security Analytics: Elastic Stack • Elasticsearch • Kibana • Elastic ingest workflows • SIEM workflows • Detection engineering • Forensic artifact ingestion

Cybersecurity Operations: Threat Hunting • Incident Response • Digital Forensics • Host Analysis • Network Forensics • Malware Analysis

DFIR Infrastructure: Ubuntu Server • Linux • FLARE VM • NAS / SMB • Segmented forensic environments • OpenRelik workflows

Forensic Tools: KAPE • Volatility • MemProcFS • Autopsy • Zimmerman's Tools

Systems / Platforms: Linux • Ubuntu Server • Proxmox • VMware ESXi • Docker

Programming / Automation: Python • SQL • Bash • Docker • AI-assisted analysis workflows

SELECTED HIGHLIGHTS

Elastic Security Builder: Deployed Elastic Stack for a segmented DFIR environment ingesting host artifacts to support cyber operations and forensic analysis.

DFIR Automation: Automated forensic artifact processing through OpenRelik workflows feeding directly into Elastic ingest pipelines.

AI-Enabled Analysis: Implemented on-prem AI agents and CUI Codex agents capable of querying Elastic directly to automate analysis, documentation, full reports, and storyboard generation.

Operational Scale: Authored a DFIR kit SOP adopted organization-wide at Cyber National Mission Force (CNMF), standardizing collection, ingestion, and analysis workflows.

Advanced Threats: Identified web shells, lateral movement, and advanced persistent threat (APT) persistence across partner networks.

PROFESSIONAL EXPERIENCE

UNITED STATES ARMY | Fort Eisenhower, GA | Nov 2020 - Present

Cyber Operations Sergeant / Elastic DFIR Mission Lead | Jun 2025 - Present

Lead cyber analysts conducting threat hunting, incident response, and digital forensic operations while building Elastic-based DFIR infrastructure and automation workflows for partner-nation cyber defense missions.

- Deployed Elastic Stack for a segmented DFIR environment ingesting host artifacts from partner-nation forensic collections.
- Automated forensic artifact processing through OpenRelik workflows feeding directly into Elastic ingest, enabling scalable analysis across host images.
- Built and documented a full-stack DFIR kit using Ubuntu Server VMs, Elastic Stack, FLARE VMs, and NAS storage; authored an SOP now used organization-wide at CNMF.
- Implemented on-prem AI agents and CUI Codex agents capable of querying Elastic directly to automate analysis, documentation, full reports, and storyboard generation, increasing analyst throughput by up to 10x in pilot workflows.
- Lead a current mission analyzing forensic host images from a foreign partner network using Linux-based DFIR infrastructure, Elastic analytics, and SIEM workflows.
- Lead and mentor 8 cyber analysts conducting threat hunting, incident response, and forensic analysis across partner-nation enterprise networks.

Platoon Sergeant | Jun 2024 - Jun 2025

Managed readiness, integration, and professional development of a 32-person cyber operations platoon supporting Cyber Protection Brigade missions.

- In-processed and integrated 200+ personnel into Cyber Protection Brigade operational units.
- Migrated administrative infrastructure from legacy shared drives to Microsoft 365 cloud systems, improving operational efficiency 70%.
- Managed 2,000+ personnel and administrative records across Army systems.
- Led training and mentorship for junior cyber personnel while overseeing onboarding and professional development.

UNITED STATES ARMY (CONTINUED) | Fort Eisenhower, GA | Nov 2020 - Present

Cyber Operations Analyst / Senior Host Analyst | Jun 2022 - Jun 2024

Conducted threat hunting, digital forensics, and incident response supporting national-level defensive cyber operations.

- Conducted forward cyber operations in foreign partner countries, deploying EDR solutions across 40+ systems to establish host-level visibility.
- Identified and reported web shell exploitation on a partner network by correlating network telemetry and SIEM data in Elastic, Security Onion, Wireshark, and CyberChef.
- Discovered an advanced persistent threat (APT) backdoor during large-scale forensic analysis of 51 host images in a 96-hour hunt operation using KAPE, Splunk, and custom Python scripts.
- Used Elastic and Security Onion to pivot across logs, network telemetry, and host indicators during partner-nation threat hunting operations.
- Led training for 4+ international cyber operators, improving partner capability and long-term network defense posture.
- Supported persistent hunt operations for partner nation networks, coordinating recurring engagements and remediation efforts.

Cyber Operations Trainee | Nov 2020 - Jun 2022

Completed the U.S. Army Cyber Operations training pipeline, including the Joint Cyber Analysis Course (JCAC) and Cyber Common Technical Core (CCTC). Graduated as an Honor Graduate from JCAC.

APTIV - STUDENT-HIRE PROGRAM | West Lafayette, IN | Oct 2019 - Oct 2020

Software Verification Engineer

Student-hire engineering role completed concurrently with full-time Computer Engineering coursework at Purdue University.

- Supported software verification efforts by developing Python scripts to automate portions of the sensor testing and reporting pipeline.
- Automated detection of sensor data uploads and report generation, reducing manual processing and improving consistency.
- Wrote and ran unit tests to validate automation workflows.
- Assisted in the design and implementation of a SQL-based solution for storing and querying sensor data.
- Built database schemas and CRUD utilities using Python and SQLAlchemy.
- Used Docker to configure and manage MySQL instances for development and testing environments.

EDUCATION

B.S. Cybersecurity Technology: University of Maryland Global Campus | Dec 2025

GPA: 4.0 | President's List | Summa Cum Laude

Coursework toward B.S. Computer Engineering: Purdue University | Aug 2018 - Oct 2020

Full-time coursework completed prior to joining the U.S. Army

High School Diploma: Sheridan High School | May 2018

GPA: 3.98

CERTIFICATIONS

Elastic Certified Analyst: ID: 150875048 | Jun 2025 - Jun 2027

Senior Host Analyst Certification: U.S. Army Cyber Command (ARCYBER) | Mar 2023

Joint Cyber Analysis Course (JCAC): Honor Graduate | Oct 2021

CLEARANCE

Active Top Secret / Sensitive Compartmented Information (TS/SCI) Clearance