Nicholas Carter

Roanoke, VA

Phone: (540) 816-2135 | Email: nicholascarter12@icloud.com

LinkedIn

PROFESSIONAL SUMMARY

Operational Technology (OT) cybersecurity analyst with hands-on experience supporting FERC hydropower Cyber Asset Inventory initiatives in SCADA environments. Skilled in PLC/RTU asset validation, cyber/physical asset mapping, governance risk compliance (GRC), and network segmentation documentation with an audit-ready mindset. CompTIA Security+ certified and currently preparing for CySA+. Graduating May 2026 with a B.S. in Cybersecurity, bringing a strong blend of industrial awareness, security operations fundamentals, and regulatory-aligned documentation.

CERTIFICATIONS

- CompTIA Security+ (SY0-701) — 2025
- CompTIA CySA+ — In Progress (Target 2026)
- TryHackMe SOC Level 1 Path — In Progress

CORE COMPETENCIES

- OT / ICS: SCADA environment documentation; PLC/RTU identification; annunciators; asset criticality inputs; legacy PLC constraints
- Cyber Asset Inventory: parent/child device relationships; OSI tag correlation; instrumentation vs. cyber asset classification; traceability
- Network & Security: segmentation and trust boundary identification; basic packet analysis; security control verification support
- Security Operations: log analysis and event correlation; IOC handling; malware hash (SHA256) workflows; sandbox triage
- Governance & Compliance: regulatory-aligned documentation; workshop support; audit readiness and defensibility

TECHNICAL SKILLS

OT / ICS: PLCs, RTUs, SCADA networks, control system components, asset identification & validation

Security Tools: Wireshark; Elastic/SIEM exposure; VirusTotal; AnyRun; CyberChef; Nmap

Platforms: Linux CLI; Windows troubleshooting fundamentals

Framework Exposure: NIST CSF; NIST SP 800-82 (ICS Security); FERC/NERC-aligned documentation workflows

PROFESSIONAL EXPERIENCE

Associate Analyst – OT Cybersecurity Consulting | GFT (Consulting Firm) | Virginia | May 2025–Present

Support large-scale hydropower cybersecurity initiatives aligned with FERC regulatory expectations.

- Conduct on-site validation of control components including RTUs, PLCs, annunciators, and networked devices supporting OT operations.
- Develop and maintain structured Cyber Asset Inventory deliverables aligned to FERC 3A-style guidance and client documentation standards.
- Correlate OSI tag data to parent cyber assets and field instrumentation to improve traceability and defensible asset relationships.
- Review OT network diagrams and configurations to document segmentation, communications paths, and key trust boundaries.
- Assist in workshop preparation by organizing inventory evidence, validating scope accuracy, and supporting risk discussion inputs.
- Coordinate with engineers, field staff, and project managers to clarify asset classification decisions and ensure inventory completeness.
- Contribute to legacy PLC compensating control discussions (monitoring overlays, segmentation, access control considerations).

Impact Highlights:

- Improved consistency of parent-device mapping and asset traceability across site documentation packages by applying repeatable naming and relationship logic.
- Strengthened audit-ready documentation quality by emphasizing evidence-backed asset validation and clear scope rationale.

TECHNICAL PROJECT EXPERIENCE

Legacy PLC Compensating Controls Research Project | Academic (2025)

- Developed an interdisciplinary security strategy for legacy PLC environments within hydropower OT systems.
- Integrated engineering constraints, risk management concepts, and governance objectives to propose realistic control improvements.
- Outlined layered defenses such as segmentation enhancements, monitoring visibility, and controlled remote access approaches.

Security Operations Laboratory Experience | Hands-on Training

- Performed log-driven investigations of brute-force attempts, credential misuse patterns, and suspected lateral movement indicators.
- Validated suspicious files using SHA256 hashing, threat intelligence lookups, and sandbox detonation workflows.
- Used packet capture analysis to trace originating IP activity and evaluate suspicious outbound connections.
- Reviewed email authentication artifacts (SPF/DMARC) and message indicators during training scenarios.

EDUCATION

Old Dominion University | Bachelor of Science in Cybersecurity | Graduation: May 2026

Relevant Coursework: Network Security Essentials; Business Data Networks & Security; Incident Response & Digital Forensics; Risk Analysis & Governance

Virginia Western | Associates of Science in Computer Science | August 2022 – May 2024

Glenvar High School | Advanced High School Diploma | August 2018 – May 2022

ADDITIONAL STRENGTHS

- Detail-oriented, audit-ready documentation and inventory defensibility
- Cross-functional communication (engineering, field operations, and cybersecurity stakeholders)
- Comfortable working in hybrid hands-on/site environments and translating findings into structured deliverables
- Continuous learning with rapid certification progression