KEVIN LEVERETT

Information Security & Risk Specialist | SOC Operations | Incident Response | Vulnerability Management
Concord, NC | (850) 774-2218 | k.leverett32@gmail.com | linkedin.com/in/kevin-leverett-8b1828128 | kevinleverett.com

CERTIFICATIONS & CREDENTIALS

CompTIA Security+ — CompTIA — *In Progress — 2026*
CompTIA CySA+ — CompTIA — *In Progress — 2026*
SSCP — Systems Security Certified Practitioner — ISC2 — *In Progress — 2026*
CC —Certified in Cybersecurity— ISC2 — *2026*
CPR / BLS — American Heart Association — *2025*
Florida Security License — Class D — Florida Security Training — *2015*

PROFESSIONAL SUMMARY

Security professional with 10+ years protecting high-volume enterprise environments, now transitioning fully into cybersecurity. Hands-on experience with Splunk, Microsoft Sentinel, CrowdStrike Falcon, and OpenVAS. Skilled in MITRE ATT&CK framework mapping, SIEM-based threat detection, IDS/IPS configuration, vulnerability management, and incident response workflows. Leverages AI-augmented workflows — including Claude AI — to accelerate threat research, security documentation, and automation scripting in Python and PowerShell. Military-trained (U.S. Army, Secret Clearance) with a proven record of coordinating large-scale operations under pressure. B.S. in Cybersecurity with active pursuit of Security+, CySA+, and SSCP. Positioned to deliver immediate SOC impact — identifying threats faster, reducing false-positive noise, and improving mean time to respond.

PROFESSIONAL EXPERIENCE

Security Specialist | *Walt Disney World Resort* — Sep 2022 – May 2026 · Orlando, FL

- Triaged and documented 1,000+ security incidents annually across a 50-person security network, synthesizing post-incident data to update response protocols and reduce repeat-incident rates by an estimated 20%.
- Applied MITRE ATT&CK-aligned vulnerability identification across high-traffic resort areas, implementing risk mitigation strategies that reduced unaddressed threat exposure within 24-hour windows.
- Coordinated real-time incident response with law enforcement and fire department partners, cutting average multi-agency response coordination time through streamlined communication protocols.
- Directed daily SOC-equivalent security operations — monitoring, triage, escalation, and documentation — for one of the world's highest-footfall entertainment environments (50M+ annual visitors).
- Produced structured incident reports and trend analyses used by leadership to drive measurable compliance and safety improvements quarter-over-quarter.

Security Officer | *Walt Disney World Resort* — Jul 2015 – Sep 2022 · Orlando, FL

- Managed access control and threat detection operations for a 20-person screening team, achieving a 15% increase in guest satisfaction scores within 6 months as part of the Galaxy's Edge and Disney Springs opening teams.
- Reduced emergency incident response times by refining cross-departmental communication protocols, cutting coordination delays across security, medical, and operations teams.
- Conducted daily security assessments and vulnerability identification across high-traffic zones, applying risk-based prioritization to ensure fastest remediation of critical gaps.
- Coordinated multi-stakeholder security operations involving emergency services and technical resources to maintain facility-wide safety posture across a 580-acre property.

Loss Prevention & Security Officer | *Hilton Inc.* — Feb 2013 – Jul 2015 · Panama City Beach, FL

- Safeguarded assets exceeding $50M across 3 properties through continuous risk assessment, incident monitoring, and coordinated security compliance programs.

- Identified and remediated technical and operational security vulnerabilities in collaboration with IT and facilities teams, maintaining 100% compliance across all sites.
- Led emergency traffic management and control operations, improving emergency services response time through structured incident command protocols.

Fire Support Specialist — Secret Clearance | *U.S. Army National Guard* May 2012 – Jun 2018 · Panama City, FL

- Directed 200+ artillery operations annually, achieving a 25% improvement in team mission success rate through optimized communication workflows across 30+ missions per year.
- Managed communication systems and logistics for 15 large-scale military exercises annually, improving logistical efficiency by 15% through process standardization.
- Coordinated joint fires and real-time targeting operations under live-fire conditions — directly translatable to high-pressure SOC environments requiring rapid, precise decision-making.

TECHNICAL SKILLS

SIEM & Monitoring: Splunk, Microsoft Sentinel, CrowdStrike Falcon EDR

Network & Endpoint Security: IDS/IPS, Next-Gen Firewall Management, Endpoint Protection, Nmap, Wireshark

Vulnerability Management: OpenVAS, Nmap, Nessus (familiar), Risk Assessment, Patch Management

Frameworks & Compliance: MITRE ATT&CK, NIST CSF, ISO 27001 (awareness), SOC Operations, GRC, Security Awareness Training

Scripting & Automation: Python (automation/scripting), PowerShell, Incident Response Automation

Operations: Threat Hunting, Digital Forensics (foundational), Incident Management, Compliance Reporting, Cross-functional Leadership

AI & Productivity Tools: Claude AI, AI-augmented threat research, prompt engineering for security automation, AI-assisted Python/PowerShell Scripting

EDUCATION

Bachelor of Science in Cybersecurity
Southern New Hampshire University 2026 · President's List — 3 Semesters

Associate of Science, Electrical & Computer Engineering
Valencia College, Orlando, FL 2022

Advanced DHS Emergency Preparedness
Gulf Coast State College, Panama City, FL 2015