LAUREN BURNS

Senior Security & Compliance Consultant

Tyrone, GA • lauren@divin3.io • linkedin.com/in/lburnscissp

PROFESSIONAL SUMMARY

CISSP-certified security operations leader with 13 years of experience across critical infrastructure, federal, healthcare, and SLED environments. Specializes in translating regulatory frameworks into operational reality — including SOC 2 readiness, NIST 800-53 control mapping, and HIPAA. Threat-informed perspective shaped by years on the operations side of security, including a combat deployment as an Army network operator. Available for contract engagements supporting security questionnaire responses, SOC 2 readiness, vendor risk management, and policy writing.

CORE COMPETENCIES

Compliance & GRC: SOC 2 readiness • NIST 800-53 / NIST CSF control mapping • HIPAA / HITECH • ISO 27001 • COBIT • Vendor Risk Management • Security Questionnaire Responses • Policy Writing • Audit Preparation

Security Operations: SIEM Architecture & Administration • Splunk Enterprise / Cloud • Detection Engineering • Incident Response • Threat Detection • Log Onboarding • Vulnerability Management

Technical Background: Splunk Enterprise / Cloud • SIEM administration • Security operations tooling • Python scripting for security automation

Leadership: Team management • Performance coaching • Cross-functional collaboration • Client escalation management • Technical mentorship

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP) — (ISC)², 2016 – Present
- Splunk Certified Administrator — Splunk Inc.

PROFESSIONAL EXPERIENCE

Managed Services Security Team Lead | *NuHarbor Security* May 2023 – Dec 2024

- Led a team of 10 analysts and engineers supporting State, Local Government, and Education (SLED) clients operating under regulatory and compliance requirements.
- Served as senior technical escalation point for clients across a diverse compliance-driven portfolio, translating regulatory requirements into operational detection and response actions.
- Owned detection engineering, incident response, and Splunk Cloud / Enterprise architecture decisions across the client portfolio.
- Partnered with compliance, product, and client-side stakeholders to align managed security services with client requirements.

Managed Services Security Engineer | *NuHarbor Security* Nov 2022 – May 2023

- Delivered managed security services to SLED clients, including detection engineering, incident response, and Splunk administration across regulated environments.
- Promoted to Team Lead within six months in recognition of technical depth and client-facing impact.

Information Security Contractor | *Booz Allen Hamilton*Jun 2022 – Dec 2022

- Federal-sector security engineering contracting work supporting agency clients.
- Led Splunk deployments integrating Tenable, Carbon Black, and Forescout for the Continuous Diagnostics and Mitigation (CDM) program.
- Developed test cases, dashboards, and data analysis reports for L3 testing events.

IT Security Engineer — Lead Splunk Engineer | *Norfolk Southern* Oct 2020 – Feb 2022

- Owned Splunk platform architecture, integrations, data source onboarding, and performance tuning for one of the largest railroad networks in North America — a Class I critical infrastructure environment.
- Built custom Splunk applications to segment data access by team and preserve data privacy across the enterprise.
- Engineered custom log parsers for proprietary applications using regular expressions and automated security processes with Python and Bash.

Senior Information Security Analyst | *Norfolk Southern* Jul 2018 – Oct 2020

- Senior incident response, threat detection, and SIEM operations work at scale in a railroad environment with significant OT / IT convergence considerations.
- Tuned detection content, correlation searches, and Splunk dashboards for application development and operational technology teams.

Information Security Analyst | *Norfolk Southern* Dec 2016 – Jul 2018

- Security operations analyst supporting detection, alert triage, and incident handling in a critical infrastructure environment.

Information Security Contractor | *Anthem, Inc.* Jun 2016 – Dec 2016

Atlanta, GA

- Information security contracting role at a major healthcare insurance organization, supporting HIPAA-aligned security operations for the protection of electronic Protected Health Information (ePHI).
- Conducted ServiceNow workflow pilot to evaluate new operational processes.
- Documented routine maintenance procedures, archiving policies, and ticketing standards.
- Built custom user behavior analytics reports and analyzed ticket metrics to identify trends and tune use cases.

Information Security Co-op | *Norfolk Southern* Jan 2015 – Dec 2015

- Mapped security controls across the NIST Cybersecurity Framework, NIST 800-53, ISO 27000, COBIT, and internal corporate policy.
- Created and ran scheduled and unscheduled vulnerability scans in a railroad enterprise environment.
- Documented configuration and change management procedures and generated patch status reports across the enterprise.

Network Security Administrator | *United States Army* Nov 2009 – Mar 2013

50th Signal Battalion, 35th Signal Brigade, XVIII Airborne Corps — Fort Liberty (formerly Fort Bragg), NC

- Operated the Joint Network Node (JNN), the Army's tactical satellite-based communications and network platform supporting brigade-level operations.
- Deployed to Iraq in support of Operation Iraqi Freedom, maintaining mission-critical network operations in a combat environment under FIPS 200 compliance.

- Executed installation, operation, deployment, and maintenance of IP-based nodal systems, combat net radios, and related COMSEC devices.

EDUCATION

Bachelor of Science, Information Sciences & Technology May 2016

Security and Risk Analysis — The Pennsylvania State University

ADDITIONAL

U.S. Army Veteran — Combat-deployed network operations specialist (OIF)

Active Memberships: (ISC)² CISSP • ISACA