DENISE JOYNER

Atlanta, GA | MsDeniseJoyner@gmail.com | linkedin.com/in/denise-joyner-218173118 | github.com/denisejoyner09

PROFESSIONAL SUMMARY

Cybersecurity Analyst with hands-on experience in IAM, Security Operations, SIEM monitoring, log analysis, and cloud security. Skilled in MFA enforcement, access control, vulnerability assessment, network traffic analysis, and documenting security artifacts for audits and compliance. Strong troubleshooting and system analysis background supporting enterprise environments aligned with NIST and FISMA. Currently pursuing Okta Professional Certification to deepen IAM expertise.

CORE SKILLS

IAM • MFA Enforcement • SIEM Monitoring (Splunk) • Threat Detection • Incident Triage • Log Analysis (Sysmon, Event Logs) • GCP Security Concepts • DevSecOps Support • Vulnerability Management • Wireshark / Tcpdump • Audit Readiness • Low-Code App Security • Data Governance • Threat Modeling & Risk Assessment

TECHNICAL SKILLS

Security Tools: Splunk, Splunk SOAR, Sysmon, PowerShell, OSINT

Network Analysis: Wireshark, Tcpdump, packet capture analysis

Vulnerability Tools: Kali Linux, Nmap, Metasploit, sandbox testing

Cloud / DevSecOps: Secure configuration, pipeline hardening, GCP fundamentals

Programming: Python (security analysis & automation)

Compliance: Audit artifacts, documentation, security plans, policy adherence

EXPERIENCE

SOC Analyst Intern — 2026 – Present

- Support SOC operations including alert triage, log review, and threat detection.
- Analyze authentication events, network traffic, and host activity to identify suspicious behavior.
- Assist with incident documentation, IOC research, and escalation workflows.
- Use Splunk and Sysmon logs to investigate anomalies and validate security events.

Help Desk Analyst — Randstad 2020 – 2025

- Supported secure user access, authentication troubleshooting, and permissions management.
- Performed system audits, updates, and maintenance aligned with security policies.
- Created documentation and training materials to reduce access-related incidents.
- Troubleshot hardware, software, and network issues across enterprise environments.
- Promoted three times for performance, technical skill, and customer service excellence.

PROJECTS

Hydroficient — Cybersecurity Extern | Extern — 2026 (In Progress)

Cybersecurity, Threat Modeling & Risk Assessment

- Conducting cybersecurity threat modeling and risk assessments for IoT environments, identifying potential attack vectors, vulnerabilities, and associated security risks.
- Applying network security principles to evaluate potential threats and develop risk mitigation recommendations.
- Using Python to support cybersecurity analysis, automation, and security-focused problem solving.
- Documenting security findings and communicating risk-based recommendations aligned with cybersecurity best practices.

EDUCATION & CERTIFICATIONS

Per Scholas Cybersecurity Program — 2026

Laney College — Computer Science Coursework — 2023

Certifications: CompTIA Security+ (2026) • Splunk Core Certified User (2026) • Google Foundations of Cybersecurity (2024) • Okta Professional Certification (In Progress)