TYLESHA ALEXANDER

GRC Analyst | Cybersecurity Compliance & Continuous Monitoring
Virginia Beach, VA | tyleshashanee@icloud.com | 757-576-8185

PROFESSIONAL SUMMARY

Cybersecurity Analyst with hands-on experience in vulnerability management, continuous monitoring, and compliance operations aligned to NIST 800-53 and FedRAMP standards. Holds CompTIA Security+ (SY0-701) and applies that foundation daily through active work in vulnerability lifecycle management, SIEM-driven alerting, DISA STIG hardening, and security control documentation. Built and operates a FedRAMP-aligned homelab environment that mirrors real-world ISSO responsibilities including POA&M-style risk tracking, SSP-style artifact creation, and audit evidence collection. Proven ability to translate technical security findings into compliance-relevant reporting and to collaborate across teams to operationalize regulatory requirements. Prepared to contribute immediately to GRC operations, FedRAMP continuous monitoring, and audit readiness for a public sector program.

CORE COMPETENCIES

GRC & Compliance: FedRAMP | GovRAMP | NIST 800-53 | NIST 800-171 | Continuous Monitoring | Audit Readiness | Compliance Evidence Collection | POA&M Management | SSP Documentation | Access Reviews
Security Operations: Vulnerability Management Lifecycle | SIEM Monitoring | Threat Detection | Incident Investigation | DISA STIG Hardening | Security Control Validation | Risk Management
Tools & Technologies: Microsoft Sentinel | Tenable (Nessus) | PowerShell | Python | KQL | Windows & Linux
Frameworks & Standards: NIST Cybersecurity Framework | MITRE ATT&CK | ISO 27001 | HIPAA | RBAC | Least Privilege

PROFESSIONAL EXPERIENCE

Cybersecurity Analyst – Vulnerability Management & SecOps *Feb 2026 – April 2026*

Log(N) Pacific

- Drive the full vulnerability management lifecycle across 50+ systems using Tenable — from scan execution and finding triage to remediation tracking, validation, and closure — supporting continuous monitoring obligations aligned to FedRAMP standards.
- Develop and maintain PowerShell automation scripts that accelerate vulnerability remediation workflows, reducing manual tracking effort and improving remediation cycle times.
- Execute system hardening procedures following DISA STIG guidelines, documenting control compliance status to support audit readiness and security authorization activities.
- Monitor security events via Microsoft Sentinel dashboards, investigating suspicious activity and escalating findings with documented evidence — consistent with continuous monitoring and incident response requirements in regulated environments.
- Build and refine Sentinel alerting rules and dashboards that improve threat visibility and reduce mean time to detect (MTTD) across the environment.
- Translate vulnerability findings and security event data into risk-prioritized reporting that supports compliance decisions and communicates exposure to stakeholders.

Export Compliance Specialist *May 2024 – Oct 2025*

Atlantic Container Line (Remote)

- Reviewed and validated documentation for 50+ international shipments weekly, ensuring adherence to global trade regulations — developing a compliance mindset directly applicable to GRC evidence management and audit preparation.
- Identified, escalated, and resolved documentation discrepancies in coordination with vendors and internal teams, mirroring the cross-functional collaboration required in GRC and FedRAMP compliance programs.
- Maintained accurate, audit-ready records supporting regulatory compliance checks — building systematic documentation discipline aligned to evidence collection requirements in security authorization workflows.
- Coordinated across multiple operational teams to sustain process continuity and regulatory adherence under deadline pressure, demonstrating the stakeholder management skills central to GRC analyst roles.

PROJECTS & COMPLIANCE LAB

FedRAMP-Aligned ISSO Homelab Environment *Ongoing*

Personal GRC Practice Environment

- Designed and operate a compliance-focused homelab that simulates ISSO responsibilities in a FedRAMP-style environment, including continuous monitoring, control documentation, and audit evidence workflows.
- Deployed Microsoft Sentinel as the core SIEM platform; configured detection rules, alert logic, and log ingestion pipelines that reflect continuous monitoring requirements under NIST 800-53 CA-7.

- Execute structured vulnerability identification, tracking, remediation, and validation workflows using Tenable maintaining a POA&M-style risk register with finding severity, remediation status, and closure evidence.
- Map all security activities to NIST 800-53 control families (AC, AU, CA, CM, IA, RA, SI) to validate control implementation and identify gaps directly mirroring SSP control narrative documentation.
- Collect and organize audit evidence artifacts including screenshots, log exports, scan reports, and configuration records structured to meet FedRAMP audit readiness standards.
- Validate access control implementations including RBAC configurations and least-privilege principles, documenting access review findings consistent with AC-2 and AC-6 control requirements.
- Produce SSP-style control documentation and risk summary reports to simulate the deliverables required of an ISSO supporting a security authorization package.

AI Security Governance Platform *Personal Project*

- Engineered a web-based tool to automate AI security risk assessments, incorporating risk scoring, compliance reporting, and remediation tracking features demonstrating the automation-first GRC mindset required for scalable compliance programs.
- Automated security validation workflows that reduced manual review overhead, translating directly to efficiency gains applicable in FedRAMP continuous monitoring operations.

Windows Event Log Threat Detector *Personal Project*

- Developed a Python-based detection tool to identify brute-force attack patterns and suspicious authentication activity from Windows event logs simulating SOC and ISSO detection workflows aligned to NIST 800-53 AU and SI control families.
- Documented detection logic and findings in structured reports, reinforcing the evidence collection and audit trail practices central to compliance monitoring programs.

EDUCATION & CERTIFICATIONS

CompTIA Security+ (SY0-701) — Active Certification

Associate of Arts in Sociology

Tidewater Community College