DARRIAN BALDRIC, PMP

Chantilly, VA | 551-227-1645 | Email: darrianbaldric@gmail.com

INFORMATION SYSTEMS SECURITY ENGINEER| INCIDENT RESPONSE | TS/SCI CLEARED | CI POLYGRAPH

Cybersecurity Officer with 5 years of experience working in the DoD industry as a US Army Soldier and Civilian, including the Intelligence Community, supporting critical and mission essential programs. My strengths include incident response, vulnerability management and research, continuous monitoring, planning, and implementing robust security controls to mitigate risk while ensuring compliance with DISA, FISMA, ICD, and DoD standards, in support of assessment and authorization of security systems and enterprise applications. Foundational technical knowledge of bash, Red Hat CLI, network security, protocols, services, and cloud computing services. Graduating with a Bachelor of Science in Cybersecurity in December 2025. Looking to expand my knowledge in the industry by joining a team of professionals to counter cyber threats and improve.

CERTIFICATIONS and ACCREDITATIONS:
• CompTIA SecurityX (CASP+) ce
• CompTIA Security+ ce
• Red Hat Certified System Administrator (Linux) *In progress*
• Project Management Professional (PMP) – PMI
• Professional Scrum Master™ (PSM I)
• Certified Insider Threat – Proof Point

SKILLS:
Vulnerability & Threat Management: ACAS/Tenable Nessus, SCAP, Vulnerability Research, Exploitable Database.
Security Documentation & Authorization: Policy and Procedures, Security Plan, Coding Practices, Risk Assessment Report
Continuous Monitoring & Incident Response: Security Audits, Incident Investigation Processing, Insider Threat Investigation
Network Security & System Hardening: Identity and Account Management, Patch Management, DISA STIGs
Cloud & SaaS Security: AWS AMI, AWS EC2, ServiceNow, Salesforce Application Programs,
Cybersecurity Frameworks & Standards: DoD, NIST, ICD, CNSSI 1253, DoD 8140 Level III
Risk Management & Compliance: SAP, JSIG, RMF, NIST 800-53/37/60, FIPS 199, FISMA, FedRAMP, eMASS

SPECIALIZED EXPERIENCE:
V2X | RDSA, Pentagon, Washington, DC
Incident Response | Cybersecurity Officer | April 2025 – Present
• Collect, investigate, and respond to weekly Cyber Network Defense alerts and provide written remediation to the automated cycle.
• Analyzed Splunk and Security Center data to identify anomalous activity and contributed to the development of improved security monitoring rules to drive insider threat detection capabilities.
• Validate users' authorization and encryption on hardware appliances and essential software applications for deployment.
• Ensure all Information Systems assets, firewalls, switches, SSDs, and computers are sanitized for decommissioning.
• Approve or disapprove data transfers based on users' privileges, permissions, and correct security groups alignment.
• Research vulnerability reports on the collected plugins and CVEs, as well as the exploitable database, and analyze the results to develop a robust patch management plan.
• Conduct open-source intelligence on requested software to detect and analyze threats to the production and test environment

Defense Threat Reduction Agency | TekSynap, Fort Belvoir, VA
Information Assurance Engineer (ISSO) | Feb 2025 – April 2025 (contract realignment)
• Collected information on WAN and LAN to select and deselect over 50 security controls.
• Performed risk assessments and provided recommendations to POAMs to remediate based on security assessment reports.
• Analyze raw ACAS scans (CSV), categorize vulnerabilities by severity: Critical, High, and Low.
• Review and Analyze Servers' Security Technical Implementation Guides (STIGS) based on the identified configuration baseline.
• Collaborate with IT staff to resolve vulnerabilities associated with central servers and applications.
• Provide security recommendations based on documented organization artifacts and other Body of Evidence (BOE)

National Ground Intelligence Center, Charlottesville, VA
Information System Security Officer (ISSO) /Vulnerability Assessment Analyst | January 2024 – March 2025
• Implemented RMF security controls and security policies for SIPR, NIPR, and JWICS classified intelligence environments.
• Conducted risk assessments and vulnerability research analysis, ensuring continuous monitoring and security compliance.
• Assisted in managing Authorization to Operate (ATO) processes, preparing, and submitting security packages via eMASS
• Performed ACAS vulnerability scans review, application, security, and development STIG reviews, and system hardening to reduce attack surface.
• Provided security guidance and best practices to systems engineers and system administrators in the creation of the concept of operations (ConOps).
• Assessed and recommended security tool implementations to enhance incident detection, response, and automation capabilities, ensuring that Code Scans are checked and submitted, including adherence to coding best practices.
• Ensure that all end-of-life media, hardware, and software are correctly destroyed and documented, serving as the alternate destructive media program manager.

Federal Deposit Insurance Corporation, Washington, DC
Information Technology Specialist (Application Platform) | September 2023 – January 2024
• Assessed and enhanced security for Salesforce SaaS applications and ServiceNow workflows, ensuring compliance with Zero Trust Architecture principles by gathering users' onboarding access procedures.
• Assisted in conducting system security audits and continuous monitoring, confirming the effectiveness of implemented security controls and documenting findings in a centralized database.
• Performed tasks in a DevSecOps cross-functional environment along with technical systems engineers to execute patch management strategies, preventing security gaps and compliance violations early in the System Development Lifecycle (SDLC).
• Reviewed and updated security configurations documentation to align with NIST 800-53, FISMA, and FedRAMP requirements.

Defense Media Activity, Fort Meade, MD
Information Technology Specialist (Cyber) June 2022 – September 2023
• Performed security control assessments, analyzing vulnerability scans from Database, Operating Systems, Linux, Windows, and Servers, security technical and implementation guidelines.
• Collaborated and reviewed the current enterprise state to complete Privacy and Impact assessment and Continuity of Operation documentation.
• Developed risk assessment reports and compliance documentation for security authorization and audit readiness.
• Ensure all Vulnerability findings are communicated and captured through daily scrum events.
• Automated compliance reporting, reducing manual efforts and improving remediation timeline, leveraging MS 365 SharePoint functionalities.
• Assisted with SCAP scanning, importing, and exporting STIG checklist for Windows operating system benchmarks.

ADDITIONAL EXPERIENCE:
U.S. Army, 82nd Airborne Division, Fort Bragg, NC
Enterprise Resource Processing Specialist | December 2020 – August 2022
• Secured assets valued at over $ 800,000 using the Global Combat Support System, a specialized DoD-Army software, to ensure operational readiness and adherence to security protocols.
• Assisted in operations for 200 personnel, ensuring efficient deployment, training, inventory, and equipment control, as well as adherence to military security standards.
• Developed and executed risk mitigation strategies during high-pressure operations to maintain mission-critical security and continuity.
• Streamlined interdepartmental communication to optimize the distribution of weapons and vehicle systems, resolving logistical challenges.

EDUCATION & TRAINING: Bachelor of Science in Cybersecurity, American Military University, West Virginia | Graduation December 2025

Sandbox and Testing Environment:
Security Log Aggregator
Configure and deploy an AWS EC2 instance in a network security group, allowing SSH traffic to the server over port 22
Create an S3 bucket to collect and store security logs, ensuring the bucket has the correct permissions.
Configure Syslog to collect authentication logs (failed logon attempts).
Modify shell scripts to run automatically on a regular schedule.