Darrian Baldric, TS/SCI Clearance CI Polygraph | Cybersecurity Analyst |Cybersecurity Engineer

551-227-1645

darrianbaldric@gmail.com

https://github.com/darrianbaldric

linkedin.com/in/darrianbaldric

EDUCATION

B.S. Cybersecurity | American Military University

CERTIFICATIONS

CASP+

Security+

PMP®

PSM I

RHCSA (In Progress)

Proofpoint Insider Threat

EXPERIENCE

V2X | RDSA – Pentagon, Washington, DC
Cybersecurity| ISSO (Incident Response) Apr 2025 – Present

- Build an effective ServiceNow dashboard with Splunk engineers to capture and investigate Cyber Network Defense alerts, documenting findings in accordance with SAP/JSIG guidelines, and provide visibility on weekly metrics.
- Analyze Splunk and ACAS logs to detect insider threats involving downloaded software applications and unauthorized access, and verify applications' RBAC matrix for access across all mission systems, including cross-domain solution systems
- Guide out-of-cycle patch management, zero-day detection, on multiple standalone mission systems, to continuously monitor security controls that decrease monthly vulnerability findings by 20% and to reassess current POAMs for review and closure.

Defense Threat Reduction Agency | TekSynap – Fort Belvoir, VA
Information Assurance Engineer (ISSO) Feb 2025 – Apr 2025

- Conducted analysis of ACAS scan results of all enterprise-grade systems to remove all outdated software libraries and components.
- Ensure all STIG checklists are validated using the DISA STIG Viewer and remain within the baseline configuration, and provide support for eMASS updates that enable ATO package development.
- Managed the review and closure of several non-compliant security controls by grouping and testing the provided Body of Evidence.

National Ground Intelligence Center – Charlottesville, VA
ISSO / Vulnerability Assessment Analyst Jan 2024 – Mar 2025

- Implemented and validated RMF controls for SIPR/NIPR/JWICS networks; updated ConOps and POA&M documentation that streamlined the ATO submission process of multiple eMASS packages, including migrated systems to AWS cloud services.
- Collaborated with system engineers and system admins to incorporate Zero-Trust and DevSecOps best practices by verifying and validating privileged users' access and security clearances across the enterprise, along with reporting non-compliant access agreements and NDA.

Federal Deposit Insurance Corporation – Washington, DC
IT Specialist (Application Platform) Sep 2023 – Jan 2024

- Hardened ServiceNow and Salesforce applications under a Zero-Trust architecture framework in collaboration with developers, deploying security in each sprint iteration, and reducing post-deployment vulnerability detection by 15%.
- Supported FedRAMP and FISMA audit preparation through SSP, Data flow diagrams, and ATO documentation, and reviewed open POAMs, assisting the application system owner on findings below 89% threshold for critical financial applications.

Defense Media Activity – Fort Meade, MD
IT Specialist (Cyber) Jun 2022 – Sep 2023

- Conducted monthly assessments on nine critical security controls that continuously bolster the content management system.
- Automated reporting workflows via SharePoint for audit readiness and made manual updates to all DoD customers' dashboards.
- Analyze SCAP scans and import XCCDF files to Stig Viewer to create and validate OS and other software security configurations.

PROJECTS

Technical Cloud Projects – AWS Platform Engineering Lab

- **AWS Lightsail Deployment:** Configured a Linux Nginx web server to host a static website; implemented SSL/TLS and SSH hardening, HTML, hosting code changes on GitHub, and established proper version control of a CI/CD pipeline.
- **S3 Storage Configuration:** Created and managed versioned S3 buckets to store lab data and automated logs with restricted access policies.
- **IAM Access Control:** Built IAM user groups, roles, and custom policies to implement least-privilege security principles.
- **Container Security Testing:** Deployed Podman containers and ran Trivy scans for CVE detection and remediation documentation.

ADDITIONAL SKILLS AND TECHNOLOGIES

Security-Frameworks: RMF NIST 800-53/37 • FedRAMP • DISA STIGs • FISMA • ICD 503 • CNSSI 1253

Tools: ACAS/Nessus • GitHub • Bash • Syslog • S3 • IAM • EC2 • CI/CD Config • Nginx • STIG Viewer • SCAP

Domains: DAAPM • Cloud Security • Linux Administration • DevSecOps • Continuous Monitoring • Vulnerability Management • Incident Response • Security Automation • Documentation (SSP, POA&M, RAR, SAR) • Intelligence Community