PAUL CHRISTIAN-BROWN, CISSP

U.S. Citizen • Active Public Trust • linkedin.com/in/paul-christian-brown
Email: pchristianbrown@gmail.com • Phone: 301-257-2006 • Dale City, VA

INCIDENT RESPONSE / CYBER OPERATIONS LEAD — CISSP-certified responder with 10+ years in 24/7 mission-critical operations. Experienced coordinating incident bridges, isolating root cause, validating monitoring alerts, and producing executive-ready updates. Strong documentation discipline (playbooks, SOPs, post-incident reviews) and calm leadership under pressure.

CORE CAPABILITIES (GS-13 Level)

1. Incident Response & Security Operations

- Led incident triage, escalation, and recovery across 24/7 monitored aviation surveillance systems supporting federal stakeholders
- Coordinated cross-functional response actions across engineering, operations, and vendor teams
- Managed high-impact incidents affecting system availability and integrity, improving response consistency and decision clarity

2. Continuous Monitoring & Security Controls (NIST / RMF-aligned)

- Enforced continuous monitoring practices aligned with NIST-style control frameworks, ensuring consistent event handling and documentation
- Produced audit-quality incident documentation, including timelines, root cause analysis, and corrective actions
- Supported system monitoring using SIEM tools (Splunk) for alert validation, escalation, and response tracking

3. Vulnerability Management & Risk Governance

- Coordinated vulnerability remediation efforts across engineering teams, prioritizing based on operational risk and system impact
- Validated remediation effectiveness and supported secure configuration baselines
- Reduced exposure to recurring vulnerabilities through improved coordination and tracking

SELECTED IMPACTS (REPRESENTATIVE)

- Standardized incident documentation and response runbooks to improve consistency, reduce repeat incidents, and support audit readiness.
- Coordinated cross-team remediation for operational and security findings; tracked actions through closure with evidence.
- Delivered executive-ready incident summaries translating technical detail into risk, impact, and next actions.

PROFESSIONAL EXPERIENCE

L3HARRIS TECHNOLOGIES — Herndon, VA | Specialist Network Control (Mission-Critical Aviation Systems NOC) 2019 – Present

Hours per week: 40+

- Lead real-time incident response operations supporting **global aviation surveillance systems across multiple service delivery points and control stations**
- Serve as escalation authority during critical incidents, supporting **high-availability systems with uptime requirements exceeding 99.9%**
- Standardized incident response procedures, improving consistency across shifts and reducing response ambiguity
- Produced **100+ executive-level incident reports annually**, improving audit traceability and post-event analysis
- Enforced continuous monitoring practices aligned to NIST-style controls across operational workflows
- Coordinated vulnerability remediation across teams, supporting risk prioritization and closure tracking
- Supported disaster recovery exercises and operational readiness validation, strengthening system resilience
- Identified recurring system failure patterns and implemented procedural improvements, reducing repeat incidents

HMSHOST INTERNATIONAL — Bethesda, MD | Network Operations Center Engineer 2018 – 2019

Hours per week: 40

- Led incident triage and root cause analysis across enterprise systems supporting multi-location operations
- Standardized escalation workflows, improving response consistency and reducing downtime
- Coordinated remediation across infrastructure teams to resolve service-impacting issues

WILMERHALE LLP — Washington, DC | Network Analyst / IS Operations Technician 2015 – 2017

Hours per week: 40

- Investigated and escalated security-relevant events across enterprise environments
- Supported vulnerability remediation and system hardening efforts
- Maintained audit-ready documentation supporting operational compliance

LOCKHEED MARTIN — Ashburn, VA | Network Operations Center Specialist 2012 – 2015

Hours per week: 40

- Provided Tier 2/3 support within secure infrastructure environments
- Monitored systems and escalated anomalies impacting performance and availability
- Supported early aviation surveillance systems (ADS-B environment)

PRIOR LEADERSHIP (UNDATED)

- Former Assistant Manager roles (Starbucks, Nordstrom) and Manager (SunTrust Bank): escalation management, coaching, and operational discipline.

EDUCATION & CERTIFICATIONS

- CISSP
- CompTIA Security+
- FAA Public Trust (Active)
- B.S. IT Management – Western Governors University (In progress)

TECHNICAL TOOLKIT

- Analysis: Wireshark, tcpdump, log correlation, network telemetry interpretation
- Monitoring/SIEM: Splunk, Microsoft Sentinel (working knowledge), alert triage and reporting
- Networking: TCP/IP, VLANs, DNS, routing concepts (OSPF/BGP familiarity), VPN concepts
- Systems/Automation: Linux, Windows, PowerShell, Python (automation basics)