David Brooks Cox

Sarasota, FL | david@cloudpuncher.dev | linkedin.com/in/davidbrookscox | github.com/siestakeydbc | cloudpuncher.dev

Summary

Security operations professional with 10+ years in regulated enterprise environments and active hands-on SOC experience using production-grade tooling. Combines a rare foundation in healthcare compliance, access control, and incident response with current internship work in threat detection, vulnerability management, and cloud security. Targeting SOC Analyst roles with a long-term focus on cloud-native security operations, detection engineering, and AI-augmented threat analysis.

Core Competencies

- SIEM Alert Triage & Tuning
- Incident Response & Playbook Development
- Threat Hunting & Behavioral Analysis
- Vulnerability Assessment & Prioritization
- MITRE ATT&CK Framework
- IOC Analysis & Malware Triage
- AWS Security (GuardDuty, CloudTrail)
- IAM & Least Privilege
- Azure & Microsoft Sentinel
- Splunk · Wazuh · Elastic/ELK
- Nessus · OpenVAS · BloodHound
- PowerShell · Python · Bash

Experience

Security Analyst Intern — Threat Intelligence & Vulnerability Management **Jul 2025 – Present**
LOG(N) Pacific *Remote*

- Conduct cloud-focused vulnerability assessments across 50+ systems per cycle, validating and prioritizing 15–20 findings using Tenable Nessus and OpenVAS
- Investigate and triage 25–40 SIEM alerts weekly in Splunk and Wazuh, contributing to measurable improvement in detection quality and reduced MTTR
- Build AWS detection labs using CloudTrail, GuardDuty, and Wazuh to simulate IAM misconfigurations, excessive permissions, and privilege escalation scenarios
- Analyze identity-based attack paths using BloodHound and SharpHound to identify escalation risk and improve identity visibility across enterprise environments
- Automate vulnerability triage summaries using local LLM workflows (Ollama, GPT4All), reducing manual reporting effort by ∼50% — one of few analysts integrating AI tooling into detection workflows
- Develop executive dashboards highlighting aging high-severity vulnerabilities to support remediation prioritization and leadership reporting

Clinical Systems Information Specialist **Jul 2023 – Present**
AdventHealth West Florida *Sarasota, FL (Hybrid)*

- Maintain mission-critical clinical systems across teaching hospitals with 99.9% uptime, supporting availability requirements equivalent to SOC SLA standards
- Partner with cybersecurity, IT, and compliance teams to support HIPAA, NIST, and HITRUST readiness, contributing to 30+ audits with zero critical findings
- Lead access control reviews and configuration assessments reinforcing least-privilege principles across enterprise clinical platforms
- Respond to system incidents and downtime events, coordinating rapid escalation and recovery — directly applicable to SOC Tier 1/2 incident handling workflows
- Authored incident response and downtime playbooks later adopted as system-wide best practices

Cybersecurity Analyst Intern — Threat Detection & SIEM Operations **Jun 2023 – Sep 2023**
JPMorgan Chase & Co. *Remote*

- Analyzed 500+ security event datasets weekly to identify fraud and potential data exfiltration, reducing false positives by 18%
- Built and tuned SIEM correlation rules and dashboards in Splunk and ELK, improving triage efficiency by 25%
- Supported incident response simulations and phishing-resilience testing, improving MTTC by 30%

Cyber Security Consultant Intern **Mar 2023 – Jun 2023**
PwC Switzerland *Remote*

- Conducted cloud security risk assessments across AWS, Azure, and GCP, identifying misconfigurations and reducing overall cloud exposure by 20%+

- Supported IAM audits and access reviews, resolving excessive privilege issues across 200+ accounts
- Led threat-modeling workshops mapping client environments to MITRE ATT&CK and CIS Controls
- Deployed automated vulnerability scanning pipelines, reducing manual validation time by 30%

Cybersecurity Specialist Intern — Blue Team & Cloud Defense **Jan 2023 – Mar 2023**
ANZ Worldline Payment Solutions *Remote*

- Monitored and triaged enterprise SIEM alerts across financial systems, supporting 24/7 SOC operations
- Participated in incident response investigations, analyzing IOCs and supporting containment and recovery
- Updated and refined SOC runbooks and response playbooks, improving alert consistency and reducing analyst handling time

Cybersecurity Specialist Intern — SOC & Threat Operations **Oct 2022 – Jan 2023**
Telstra GmbH *Remote*

- Analyzed enterprise network traffic and security events to detect anomalous behavior and potential intrusion attempts
- Supported IDS/IPS monitoring and alert analysis, assisting in identification and escalation of network-based threats

Healthcare IT & Quality Systems Consultant **Jul 2015 – Jan 2023**
AMN Healthcare Leadership Solutions *United States*

- Supported enterprise clinical systems in regulated environments, ensuring availability, integrity, and secure access to mission-critical platforms
- Managed user access provisioning and troubleshooting, reinforcing least-privilege principles and access control consistency
- Responded to system incidents and outages, coordinating with engineering teams to restore services in time-sensitive scenarios

Projects & Portfolio

Phishing IR Playbook | *Incident Response, MITRE ATT&CK, CLI Documentation*

- Full 5-phase incident response playbook with CLI examples, MITRE mapping, and evidence log templates — View on GitHub

SOC Analyst Portfolio | *IR Playbooks, Detection Rules, Threat Hunt Documentation*

- Public GitHub portfolio documenting SOC workflows, detection engineering, and threat hunt write-ups — View on GitHub

Education

The George Washington University **Washington, D.C.**
Master of Professional Studies — Cybersecurity | GPA: 3.9 *Graduated January 2019*

Certifications & Training

- **ISC2 Certified in Cybersecurity (CC)** — 2025
- **INE Certified Cloud Associate (ICCA)** — 2025
- **CompTIA Security+** — In Progress, Expected July 2026
- **Josh Madakor SOC Internship** — LOG(N) Pacific (2025–Present)
- **TCM Security Academy** (2024–Present)