DAVIYON DANIELS

Cybersecurity Analyst | Security Operations, Risk & Governance | CISSP, SSCP
Oklahoma City, OK | daviyon.daniels@gmail.com | linkedin.com/in/daviyondaniels

PROFESSIONAL SUMMARY

Cybersecurity professional with 4+ years of experience across security operations, vulnerability management, third-party risk, governance and compliance, and AI security. Currently the sole dedicated security professional for an NBA organization, owning the cybersecurity risk register, detection engineering, vulnerability management, and third-party risk management end to end. Builds custom security tooling in Python using AI-assisted and agentic coding tools, including an autonomous third-party risk platform with an adversarial LLM review loop and an AI governance reporting pipeline. Works across NIST CSF, NIST SP 800-53/800-63B, PCI DSS, ISO/IEC 27001, SOC 2, CIS Controls and Benchmarks, HIPAA, and GDPR. Founder of an AI security and governance consulting practice, and an active bug bounty researcher. CISSP, SSCP, SecurityX (CASP+), Security+, GSEC, CySA+, PenTest+.

CORE COMPETENCIES

Security Operations: SIEM administration (Sumo Logic Cloud SIEM), network detection and response (Darktrace), EDR (CrowdStrike Falcon), incident investigation and response, playbooks and runbooks, security awareness and phishing simulation (Adaptive Security, KnowBe4)

Vulnerability & Risk Management: Vulnerability management (Rapid7 InsightVM, Qualys, Nessus, Greenbone/OpenVAS), penetration testing and assessment (Metasploit, Nmap, Burp Suite, Wireshark), risk register ownership, risk assessment and prioritization, third-party risk management (TPRM)

Governance, Risk & Compliance: Security policy and standards authoring, compliance framework management (NIST CSF, NIST SP 800-53/800-63B, PCI DSS, ISO/IEC 27001, SOC 2, CIS Controls, CIS Benchmarks, HIPAA, GDPR), audit evidence collection and documentation, AI governance (NIST AI RMF)

Identity, Network & Cloud: Zero Trust/ZTNA (Fortinet), identity and access control (RBAC, IAM, Microsoft Entra ID, Duo), authentication technologies (OAuth, YubiKey, Passkeys), cloud platforms (AWS, GCP, Azure)

Automation & Development: Python, Java, SQL, JavaScript/TypeScript, Bash, C++; AI-assisted and agentic coding tools (Claude Code, Cursor, GitHub Copilot), LLM/AI-assisted automation, API integration (Microsoft Graph Security API), Docker, Linux, Git

PROFESSIONAL EXPERIENCE

Oklahoma City Thunder (NBA) **Aug. 2024 – Present**
Cybersecurity Analyst *Oklahoma City, OK*

- Serve as the organization's sole dedicated security professional, owning security operations across risk management, third-party risk, vulnerability management, detection engineering, and compliance end to end.
- Own and maintain the organization's cybersecurity risk register; perform risk assessments and contribute to data protection strategy and security policies and standards; support compliance initiatives through technical enforcement and documentation.
- Designed and built an autonomous third-party risk management (TPRM) platform against a 60-item conformance specification, with an adversarial LLM review loop replacing manual vendor risk assessment and evidence review with AI-assisted, code-defined automation.
- Develop custom security tooling using AI-assisted and agentic coding tools (Claude Code, Cursor, GitHub Copilot, Python), including an LLM-backed TPRM command-line tool, an InsightVM assistant with verified knowledge files, and a ChatGPT usage analytics pipeline integrated with Sumo Logic for AI governance reporting.
- Administer Rapid7 InsightVM for enterprise vulnerability management, including scan template design, asset group scoping, remediation prioritization, and SQL-based reporting across on-prem and multi-cloud assets in a hybrid environment.
- Build and maintain the organization's Sumo Logic Cloud SIEM environment, including log ingestion architecture, detection content, and dashboards across endpoint, network, identity, and cloud sources.
- Operate Darktrace network detection and response and CrowdStrike Falcon EDR; triage and investigate alerts and respond to security incidents.
- Enforce Zero Trust access to internal applications with Fortinet ZTNA, replacing broad VPN trust with identity- and device-posture-based policies.
- Apply CIS Benchmarks and secure configuration standards when reviewing infrastructure and cloud changes for alignment with security requirements.
- Deliver the organization-wide security awareness training and phishing simulation program (Adaptive Security); author playbooks, runbooks, and operational procedures for security operations.
- Continuously evaluate emerging threats, including AI-specific risks, and recommend proactive security measures to leadership.

Ayliea LLC **May 2023 – Present**

Founder & Principal Consultant, Cybersecurity and AI Governance *Oklahoma City, OK (Remote)*

- Deliver fixed-scope AI Governance Foundations engagements covering risk assessment, policy and standards development, and control implementation aligned to NIST AI RMF and NIST CSF.
- Built Ayliea Assess, a self-assessment platform that maps organizational AI security and governance controls to defined requirements.
- Evaluated the data practices and privacy/security posture of 15 AI products, publishing findings as a CC0-licensed open-source specification to support third-party AI vendor risk and data protection reviews.
- Serve as capstone advisor to university students studying AI governance, providing technical review and presentation feedback.

Client Engagement: IT Security Consultant, Confidential Financial Services Client *Dec. 2023 – May 2024*

- Developed and executed an IT security remediation strategy for findings from a comprehensive vulnerability assessment.
- Hardened authentication and password policies to NIST SP 800-63B and PCI DSS requirements, reducing unauthorized access risk by an estimated 40%.
- Led migration to behavior-based IDS/IPS, improving threat detection rates by 35% and accelerating response times.
- Implemented and maintained data loss prevention (DLP) controls with Microsoft Purview, reducing data leakage incidents by 30% and supporting GDPR and HIPAA compliance.

Delaware Nation Industries (DoD Contractor) **Aug. 2022 – Aug. 2024**

Systems Analyst I *Oklahoma City, OK*

- Managed access control, authentication, and authorization systems for government IT environments; implemented a role-based access control (RBAC) framework that strengthened data security and reduced unauthorized access incidents.
- Streamlined user provisioning and de-provisioning processes, reducing manual overhead and error rates while enforcing least-privilege access.
- Managed government IT assets with security-focused inventory control; authored technical documentation and process improvements that reduced customer support issues by 25% and raised satisfaction ratings by 20%.
- Collaborated with cross-functional IT teams to restore services during outages and resolve complex technical problems.

American Fidelity Assurance Company **Sep. 2021 – Jul. 2022**

Data Science Intern *Oklahoma City, OK*

- Designed and implemented an end-to-end SQL ETL pipeline and built analytics dashboards in Tableau and Power BI, presenting findings to internal stakeholders.

EDUCATION

Western Governors University **2024**

M.S., Cybersecurity and Information Assurance *Salt Lake City, UT*

Western Governors University **2023**

B.S., Cybersecurity and Information Assurance *Salt Lake City, UT*

CERTIFICATIONS

CISSP (ISC2) | SSCP (ISC2) | CompTIA SecurityX (CASP+) | CompTIA Security+ | GIAC GSEC | CompTIA CySA+ | CompTIA PenTest+ | Microsoft AZ-900 Azure Fundamentals

OPEN SOURCE, RESEARCH & COMMUNITY

- Open-source contributions: CC0-licensed AI data practices specification; homelab security tooling (Greenbone, Docker, Tailscale) documented publicly.
- Offensive security researcher (bug bounty) on HackerOne and Bugcrowd, focused on API and access-control vulnerabilities; active in CTFs, Hack The Box, TryHackMe, and LetsDefend blue-team labs.
- DEF CON attendee.