NOAH SHAFFER

Tallahassee, FL | NoahWilliamShaffer@gmail.com | (941) 451-9208
linkedin.com/in/noahwilliamshaffer | github.com/noahwilliamshaffer | noahwilliamshaffer.com

PROFESSIONAL SUMMARY

CISSP-certified Cybersecurity Engineer with hands-on experience securing AWS-native SaaS platforms, regulated financial systems, and ML pipelines processing 2M+ events per day. Founding Cybersecurity Engineer at Aurepath, Founder of Lockridge Cybersecurity LLC, and Security Engineer at Curvature Securities, with proven delivery across SIEM, EDR/XDR, vulnerability management, secure SDLC, DevSecOps, IAM, and Zero Trust architecture. Deep expertise mapping technical controls to NIST CSF, NIST 800-53/171, SOC 2 Type II, PCI-DSS, FedRAMP, SEC Reg SCI, and FINRA Rule 4370. Currently pursuing an M.S. in Cybersecurity Engineering at the University of San Diego (NSA/CAE-accredited), applying threat modeling, incident response, and AI/ML automation to harden cloud workloads against modern adversaries.

CORE COMPETENCIES

CISSP Security Domains: Security & Risk Management · Asset Security · Security Architecture & Engineering · Communication & Network Security · Identity & Access Management (IAM) · Security Assessment & Testing · Security Operations · Software Development Security

Frameworks & Compliance: NIST CSF · NIST 800-53 · NIST 800-171 · ISO 27001 · SOC 2 Type II · PCI-DSS · HIPAA · GDPR · CCPA · FedRAMP · MITRE ATT&CK · OWASP Top 10 · CIS Controls · SEC Regulation SCI · FINRA Rule 4370 · CSA CCM

Security Tools & Platforms: Splunk · Elastic SIEM · CrowdStrike · SentinelOne · Microsoft Defender (EDR/XDR) · Snort/Suricata (IDS/IPS) · Palo Alto / Fortinet NGFW · Nessus · Qualys · Burp Suite · Wireshark · Metasploit · Nmap · OWASP ZAP · Semgrep · Snyk · Trivy

Cloud & Infrastructure: AWS (IAM, GuardDuty, Security Hub, KMS, CloudTrail, WAF, Macie, Inspector) · Azure AD / Entra ID · GCP IAM · Docker · Kubernetes · Terraform · GitHub Actions · CI/CD Pipelines · Linux (RHEL, Ubuntu) · Windows Server

Engineering & Practices: Threat Modeling (STRIDE, PASTA) · DevSecOps · Secure SDLC · Cryptography & PKI · Zero Trust Architecture · Incident Response & Forensics · Vulnerability Management · Penetration Testing · Red/Blue Team · AI/ML Security · API Security · Data Loss Prevention

Languages & ML: Python · Bash · C / C++ · SQL · JavaScript / TypeScript · Go (intermediate) · PyTorch · TensorFlow · scikit-learn · Pandas · REST / GraphQL API design

PROFESSIONAL EXPERIENCE

Aurepath — Remote*February 2026 – Present*
Co-Founder & Founding Cybersecurity Engineer

- Lead security architecture for an AWS-native AI SaaS platform, embedding **Zero Trust** controls across **IAM, secrets management, KMS-backed encryption, and VPC network segmentation** from day one; secured $2.5K pre-seed funding and signed first enterprise design partner.
- Built a **secure SDLC and DevSecOps pipeline** (CI/CD with GitHub Actions, SAST via Semgrep, DAST, Snyk dependency scanning, Trivy container scanning, Terraform IaC review), reducing mean time to remediate critical vulnerabilities by **40%**.
- Designed and deployed REST APIs handling **10K+ daily calls** with TLS 1.3, OAuth 2.0 / OIDC, rate limiting, and structured logging into a centralized SIEM, achieving sub-100ms p95 latency on core prioritization services.
- Authored security policies, risk register, and control mappings aligned to **SOC 2 Type II, NIST CSF, and ISO 27001** to accelerate enterprise pilot conversations and audit readiness.
- Conducted threat modeling (STRIDE) and tabletop incident response exercises across the platform, producing prioritized remediation roadmaps tied to **MITRE ATT&CK** coverage gaps.

ApexShield LLC — Capstone Engagement*January 2026 – May 2026*
Software Engineer (Sole Engineer, ShieldAudit Platform)

- Sole engineer designing and building **ShieldAudit**, a SaaS platform that automates annual **CCPA cybersecurity audits** required under Cal. Code Regs. tit. 11, §§ 7120–7124 (effective January 1, 2026).
- Architected a **multi-tenant Next.js 16 / PostgreSQL** application with Clerk authentication, Drizzle ORM, and Neon serverless DB; implemented an **immutable audit trail enforced at the database trigger level** to satisfy regulator evidentiary requirements.
- Built an **18-component, 40-question assessment engine** with risk-weighted scoring aligned to **NIST CSF**, producing automated PDF/DOCX reports formatted for regulatory submission.
- Implemented a Stripe per-assessment billing system with white-label reseller tier; productized engagements at **$9,500 direct** and **$300–$500 reseller** price points for California covered businesses.
- Hardened the application with row-level tenancy isolation, encrypted PII at rest (AES-256) and in transit (TLS 1.3), CSP/HSTS headers, OWASP Top 10 mitigations, and continuous dependency scanning.

Lockridge Cybersecurity LLC — Tallahassee, FL*December 2025 – April 2026*
Founder & Lead Security / ML Engineer

- Founded a security practice focused on **ML-driven threat intelligence**; deployed production PyTorch and TensorFlow models for phishing detection and malware classification across a pipeline processing **2M+ emails per day**.
- Built supervised and unsupervised **anomaly detection systems** delivering real-time detection at customer security gateways, achieving **95%+ validated accuracy** against business email compromise (BEC), credential phishing, and malicious attachments.
- Scaled MLOps infrastructure on AWS using Docker, Kubernetes (EKS), and Argo Workflows, enabling **10x traffic** with automated retraining, drift monitoring, model versioning, and end-to-end observability via OpenTelemetry.
- Mapped detection coverage to **MITRE ATT&CK** (Initial Access, Defense Evasion) and authored runbooks for SOC analysts integrating outputs into Splunk and downstream SOAR playbooks.

Curvature Securities — Financial Services*August 2023 – Present*
Security Engineer

- Monitor and secure access to sensitive **fixed-income market data** — including real-time CUSIP-level pricing (BVAL, discount, and dollar prices), Treasury yield curves, OAS/repo spreads, and hedge calculations — across trading and analytics systems.
- Apply data integrity and access control standards aligned with **SEC Regulation SCI, FINRA Rule 4370, PCI-DSS, and SOC 2** to ensure confidentiality, integrity, and availability of proprietary trading data.
- Operate and tune **SIEM detections, EDR alerts, and DLP policies** for insider-threat and market-data exfiltration scenarios; triage and remediate incidents in line with documented Reg SCI escalation procedures.
- Lead quarterly **vulnerability management and patch cadence** across Windows and Linux trading infrastructure, partnering with infrastructure engineering on resilient, compliant remediation windows.
- Contribute to business continuity / disaster recovery testing required under FINRA 4370, including failover validation, tabletop exercises, and post-incident reporting.

CERTIFICATIONS

- **CISSP — Certified Information Systems Security Professional, (ISC)²**
- CC — Certified in Cybersecurity, (ISC)²
- AWS Certified Security – Specialty (in progress)
- AI Security Certificate (in progress)

EDUCATION

University of San Diego — M.S., Cybersecurity Engineering*Expected August 2026*
NSA/CAE-accredited program. Coursework: Secure Systems Architecture, Applied Cryptography, Cyber Threat Intelligence, Incident Response & Forensics, Governance Risk & Compliance.

Florida State University — B.S., Computer Science*2024*
Minors: Business, Mathematics · Leadership: Vice President, FSU student organization