ZION BOGGAN

Security Engineer · SOC Analyst · Detection Engineer · Security Researcher

Memphis, TN · zionboggan0@gmail.com · U.S. Citizen · Open to Relocation

zionboggan.com · linkedin.com/in/zion-boggan · oversightprotocol.dev

> **Clearance & Eligibility:** U.S. Citizen. Eligible for a security clearance. DoD 8140 / 8570 IAT Level II baseline (Security+). Experience aligned to NIST SP 800-171, NIST SP 800-53, CMMC, and DFARS 252.204-7012.

SOC analyst and detection engineer with two years of security operations experience supporting federal control baselines. I run SIEM operations on Splunk and Microsoft Sentinel, lead incident response and forensic investigations, and manage vulnerability remediation aligned to NIST SP 800-171 and DFARS 252.204-7012. I also build the detections I run: detection-as-code pipelines, purple-team validation against MITRE ATT&CK, and secure CI/CD with software supply-chain signing. On my own time I run coordinated vulnerability disclosure and maintain an open-source post-quantum cryptographic protocol in Rust. I am comfortable across detection engineering, incident response, vulnerability management, and cloud security.

CERTIFICATIONS

- CompTIA Security+ (SY0-701), DoD 8140 / 8570 IAT Level II baseline
- Microsoft Certified: Security Operations Analyst Associate (SC-200)
- Microsoft Certified: Azure Administrator Associate (AZ-104)
- Microsoft Certified: Azure Fundamentals (AZ-900)
- SentinelOne Incident Responder Certification
- CompTIA CySA+, exam scheduled June 2026

CORE TECHNICAL SKILLS

SIEM & Detection Engineering: Splunk, Microsoft Sentinel, SentinelOne, Stellar Cyber, Wazuh, Elastic Stack, KQL, Sigma, detection-as-code, correlation-rule tuning, alert triage, MITRE ATT&CK mapping.

Purple Team & Adversary Emulation: Atomic Red Team, MITRE Caldera, detection validation, coverage analysis, file integrity monitoring, auditd.

Incident Response & Forensics: Ransomware investigation (Cactus, BlackByte), forensic timeline analysis, memory forensics (Volatility 3), IOC documentation, evidence packaging, cyber-insurance claim support.

Vulnerability Management & Research: Qualys VMDR, Nessus, OpenVAS, source-code review, proof-of-concept development, coordinated disclosure (Bugcrowd, HackerOne), remediation tracking.

Secure SDLC / DevSecOps: GitHub Actions security pipelines, Semgrep (SAST), gitleaks, pip-audit, Sigstore / Cosign keyless signing, SBOM (syft), grype, Kyverno admission policy.

Endpoint & Identity: CrowdStrike Falcon, Microsoft Defender for Endpoint, Microsoft 365 Defender, Tanium, Okta, Mimecast.

Windows: Windows 10/11, Windows Server, Active Directory, Group Policy, PowerShell, endpoint hardening, Sysmon.

Linux: Debian, Ubuntu, RHEL-family, systemd, Bash, package management, log analysis, OS hardening.

Cloud: Microsoft Azure (administration, Microsoft Sentinel, Defender for Cloud), identity and access management, cloud detection.

Networking: TCP/IP, DNS, routing, firewalling, VLANs, Wireshark, WireGuard, pfSense, Palo Alto, Fortinet FortiGate.

Compliance & Risk: NIST SP 800-171, NIST SP 800-53, CMMC, DFARS 252.204-7012, STIG hardening, control-gap assessment, policy and SOP authoring, audit-trail documentation.

Scripting & Languages: Python, PowerShell, Bash, KQL, Rust, FastAPI, REST API integration, Git.

PROFESSIONAL EXPERIENCE

SOC Analyst I, **Cyber Guards**, Memphis, TN — July 2024 to Present

- Monitor and triage 150 to 300 alerts per shift across Splunk, Microsoft Sentinel, SentinelOne, and Stellar Cyber at an MSSP, supporting compliance against documented client security policies and federal control baselines.
- Investigated Cactus and BlackByte ransomware intrusions, producing timeline analysis, IOC documentation, and evidence packaging that supported a successful cyber-insurance claim resolution.
- Perform vulnerability analysis on Windows and Linux endpoints, validate findings, map them to MITRE ATT&CK and NIST controls, and author remediation guidance for client tenants.
- Track and validate more than 100 vulnerability remediation actions, sustaining a 90 percent or better on-time patching rate with audit-ready evidence of control effectiveness.
- Reduced false-positive escalations by roughly 35 percent through detection-rule tuning and parameterized KQL notebook workflows in Microsoft Sentinel.
- Author incident reports, remediation playbooks, and policy-to-control mappings aligned with NIST SP 800-171, and maintain full SOP compliance across incident documentation.

Independent Security Researcher, **Self-Employed**, Memphis, TN — April 2026 to Present

- Conduct coordinated vulnerability disclosure on Bugcrowd and HackerOne across managed bug-bounty programs.
- Submitted research to programs including Aiven Managed Services (PostgreSQL, MySQL, ClickHouse, Valkey, Kafka), Fireblocks MPC, Electroneum, Cloudinary, AXIS OS, Mattermost, GitLab, Databricks, The Trade Desk, New Relic, Automattic / WordPress,

Snapchat, Vimeo, and Airtable.

- Work from source-code analysis, protocol-level review, and reproducible proof-of-concept development across cryptographic MPC libraries, database engine internals, blockchain consensus, and OAuth / MCP authorization-bypass chains.
- Built an autonomous, multi-agent vulnerability-research platform that reproduced proof-backed findings across more than 20 open-source projects under a strict reproduce-before-report standard, spanning access-control, SSRF, path traversal, injection, and memory-safety classes.

Relationship Banker, **Bank of America**, Memphis, TN June 2023 to June 2024

- Performed daily digital security and compliance checks, verified transactions, and authenticated customer identities with multi-factor procedures, sustaining full compliance with operational and security policies.

SECURITY PROJECTS & RESEARCH

Oversight Protocol (lead maintainer). Open-source cryptographic data-provenance system. A 12-crate Rust workspace (about 10,300 lines) plus a Python reference implementation (about 13,400 lines) with bit-identical cross-language conformance. Hybrid classical and post-quantum cryptography: NIST FIPS 203 (ML-KEM-768) and FIPS 204 (ML-DSA-65), X25519, Ed25519, XChaCha20-Poly1305, Sigstore Rekor v2 transparency, and RFC 3161 timestamping. 141 tests. (oversightprotocol.dev)

GEMINI Malware-Analysis Lab. A sealed, air-gapped lab for static triage and live DFIR. Detonated real ransomware in isolation, captured a 4.1 GB live memory image, recovered AES key schedules from memory with a custom scanner, and reconstructed the encryption timeline in Volatility 3. Every claim is evidence-gated.

Flywheel. An autonomous, multi-agent security-research platform built for authorized testing. A staged decision graph maps a target, forms hypotheses, drafts a proof of concept, and only reports a finding once a deterministic validator reproduces it.

Detection-as-Code. Sigma detections mapped to MITRE ATT&CK, linted and tested in CI, and compiled to Splunk SPL, Microsoft Sentinel KQL, and Elastic from a single source.

Purple-Team Lab. Atomic Red Team and MITRE Caldera techniques run against an instrumented endpoint, with custom Wazuh rules and an ATT&CK coverage matrix confirming each technique fires at the correct severity.

SOC Automation & CTI. Wazuh into Shuffle SOAR into TheHive case management with automated enrichment, plus a CTI pipeline that ingests live threat-intel feeds, extracts ATT&CK techniques, generates Wazuh rules, and routes them through an analyst approval gate before deployment.

CI/CD Supply-Chain Security. Keyless Cosign image signing, signed SBOM attestation, grype scanning, and a Kyverno admission policy that enforces verified provenance.

PERSONAL INFRASTRUCTURE LAB

- Operate a self-hosted Proxmox VE cluster with NVIDIA RTX 3060 GPU passthrough, running 14 or more LXC containers and VMs across Debian, Ubuntu, and RHEL-family guests, hosting WireGuard VPN, a DNS sinkhole, Proxmox Backup Server, a full Wazuh SIEM stack, and automated security workloads.
- Hands-on with hypervisor administration, LXC and KVM orchestration, GPU passthrough, VLAN segmentation, pfSense firewall policy, automated backups, headless Linux deployment, and systemd service management.

EDUCATION

High School Diploma, Memphis, TN, 2021. Self-directed study in security engineering, applied cryptography, and detection engineering.