WILLIAM ROBERTS
Cybersecurity Analyst | SOC Analyst | Security Engineer
Birmingham, AL | (251) 888-2076 | williamrobertsIT@proton.me
LinkedIn: linkedin.com/in/williambroberts23 | GitHub: github.com/ikalasy | Portfolio: whois.itskalasy.com

PROFESSIONAL SUMMARY

Cybersecurity practitioner with hands-on security operations experience across SIEM administration, detection engineering, incident response, and network defense. Operates a self-managed, internet-exposed security environment running Wazuh SIEM, pfSense with Suricata IDS/IPS, and segmented VLANs, where custom detection rules are authored, tuned, and validated against live hostile traffic. Backed by corporate network support experience at a regional telecom, including ServiceNow and Jira Service Management incident workflows. Completing a B.S. in Cybersecurity and Information Assurance (December 2026) with CompTIA Security+ and Network+ built into the program.

TECHNICAL SKILLS

Security Operations and SIEM: Wazuh SIEM 4.14, Wazuh Indexer and Dashboard (OpenSearch, forked from Elasticsearch and Kibana), Filebeat log shipping, index management, SIEM administration, log analysis, log aggregation and correlation, syslog, alert triage, threat hunting, security monitoring, security operations center (SOC) workflows
Detection Engineering: custom detection rule authoring (XML), MITRE ATT&CK mapping, multi-event correlation, false positive tuning, detection latency reduction, file integrity monitoring (FIM), realtime FIM with inotify, rule severity design
Threat Detection and Incident Response: indicators of compromise (IOC), phishing analysis, social engineering identification, command and control (C2) detection, brute force and privilege escalation detection, persistence detection, root cause analysis, packet capture, tcpdump, Wireshark, incident triage, incident documentation, evidence preservation, chain of custody, containment, escalation procedures, malware removal procedure
Web and Edge Security: NGINX reverse proxy, Nginx Proxy Manager, TLS termination, TLS/SSL certificate lifecycle, Let's Encrypt and ACME automation, HTTP security headers, Content Security Policy, attack surface reduction
Network Security: pfSense firewall, Suricata IDS/IPS, intrusion detection and prevention, stateful packet inspection, firewall rule management, VLAN and subnet segmentation, network access control (NAC), WireGuard VPN, IPsec, DNSSEC, DNS sinkholing, Pi-hole, Unbound, network traffic analysis
Compliance and Frameworks: MITRE ATT&CK, NIST 800-53, CIS Benchmark hardening standards, security configuration assessment (SCA), PCI DSS, HIPAA technical safeguards, GDPR, vulnerability assessment, vulnerability management, security hardening, DISA STIG concepts
Systems and Identity: Windows 10/11, Windows Server 2025, Active Directory Domain Services (AD DS), Microsoft Entra ID, Microsoft Intune, role-based access control (RBAC), Group Policy (GPO), NTFS permissions, least privilege, Linux (Debian, Ubuntu), bash, Python automation, SSH key based authentication
Platforms and Tooling: ServiceNow, Jira Service Management, Docker, Docker Compose, Proxmox VE, TrueNAS SCALE, ZFS, Git, REST APIs, PostgreSQL

PROFESSIONAL EXPERIENCE

Creator and Security Engineer | ScanForge (scanforge.net) | 2025 to Present | Birmingham, AL
- Built a multi-tenant external attack surface assessment platform that managed service providers resell to their clients, delivering automated security posture assessments across tiered service plans.
- Engineered the assessment engine performing passive, non-intrusive, read-only evaluation of external attack surface: SPF, DKIM, and DMARC email authentication, TLS and HTTPS configuration, HTTP security headers, and domain and WHOIS exposure, mapping each finding to a prioritized remediation.
- Developed an AI analysis layer converting raw scan output into a 0 to 100 posture score with risk-ranked findings and plain-language remediation guidance, producing client-ready security reports.
- Enforced security by design across the platform: strictly non-intrusive scanning methodology, Content Security Policy, per-tenant data isolation, and authenticated access control.
- Delivered the full stack in Next.js, TypeScript, and PostgreSQL with a Dockerized deployment pipeline.

Data Support Technician | C Spire | February 2026 to July 2026 | Birmingham, AL
- Monitored customer network connectivity, routing devices, and traffic flows for anomalies, outages, and service degradation across a regional telecom customer base.
- Triaged, documented, and tracked network incidents in both ServiceNow and Jira Service Management, managing tickets against SLA and escalation targets.

- Supported the complete service path from the fiber line at the optical network terminal (ONT) through customer edge equipment to the firewall, covering OSI Layers 1 through 4.
- Configured and troubleshot Cisco Meraki and Ubiquiti routers, switches, and firewalls, including VLAN tagging, subnet allocation, static IP assignment, interface configuration, and routed IP range delegation.
- Isolated root causes of DNS resolution, subnet mask, VLAN tagging, and routing faults using structured OSI-model methodology and packet-level analysis with tcpdump.
- Partnered with Tier 2 engineering to diagnose escalated infrastructure faults, verifying findings before dispatching field technicians and confirming resolution with customers post-repair.

Creator and Lead Developer | Red Whistle (joinredwhistle.com) | July 2026 to Present | Birmingham, AL
- Designed RWP-1, a cryptographically signed mesh relay protocol delivering authenticated alert messages across LoRa radio without cellular infrastructure, implementing message signing and replay protection in embedded C on the nRF52840 platform.

KEY PROJECTS

Security Operations Center, Self-Managed | Wazuh SIEM, Detection Engineering | Ongoing
- Administer a Wazuh 4.14 SIEM deployment across manager, indexer, and dashboard tiers with Filebeat shipping events into the search cluster, aggregating endpoint, file integrity, configuration, and authentication telemetry from managed Linux hosts, with alerts automatically mapped to MITRE ATT&CK tactics and techniques.
- Authored custom detection rules in XML covering brute force, privilege escalation, persistence, container security, and attacks against the monitoring infrastructure itself, including multi-event correlation identifying successful authentication following failed attempts from the same source.
- Validated detection efficacy against live traffic: an authored rule detected unauthorized SSH authorized_keys creation, the primary Linux persistence technique (MITRE T1098.004), within seconds of the event.
- Reduced detection latency on credential and configuration paths from a 12 hour scheduled scan interval to sub-second realtime monitoring by migrating critical directories to inotify-based file integrity monitoring, measured and documented before and after.
- Eliminated recurring false positives through targeted rule exclusions and root cause analysis rather than broad suppression, preserving detection coverage on DNS configuration tampering while removing application-generated noise.
- Run Security Configuration Assessment against the CIS Debian Benchmark, tracking control pass and fail counts as a measurable hardening baseline.

Network Defense and Perimeter Security | pfSense, Suricata IDS/IPS | Ongoing
- Operate a pfSense firewall virtualized on a Proxmox VE Type 1 hypervisor with Suricata intrusion detection and prevention inline at the perimeter; the ISP gateway is bridged so that all north-south traffic transits a single inspected control point rather than bypassing inspection.
- Designed VLAN and subnet segmentation isolating infrastructure, service, and client networks, with inter-VLAN routing policies enforcing least privilege between segments and WPA3 wireless clients placed into a restricted segment by default.
- Secured DNS resolution with Pi-hole and Unbound performing DNSSEC-validating recursive resolution, analyzing query logs for anomalous lookups and command and control callback patterns.
- Operate an NGINX reverse proxy as the sole internet-facing ingress point, terminating TLS at the edge with automated Let's Encrypt certificate issuance and renewal, and mapping public hostnames to internal service endpoints so that no backend service is directly exposed.
- Treat the edge proxy as a monitored attack surface: published services receive continuous unsolicited scanning, credential stuffing, and content enumeration, providing live adversary traffic against which detection rules are validated rather than simulated.
- Deployed WireGuard VPN with per-peer preshared keys layered over public key authentication for remote access.

Identity and Access Management Lab | Windows Server 2025, Active Directory, Microsoft Intune | December 2025 to January 2026
- Built a Windows Server 2025 domain controller running Active Directory Domain Services, implementing role-based access control with least-privilege permissions enforced per role through Group Policy Objects.
- Managed endpoint compliance and configuration policy through Microsoft Intune, and operated an incident workflow in Jira Service Management with written incident reports on closure.

Phishing Incident Analysis and Reporting | Documented Investigation | 2026

- Identified, analyzed, and reported a credential-harvesting phishing campaign impersonating university faculty, documenting sender domain mismatch, social engineering pressure techniques, and the fraudulent-instrument objective.
- Produced a formal incident report including indicators of compromise, MITRE ATT&CK technique mapping, assessed attack chain, impact analysis, and detection recommendations, and reported the campaign to the institution for broader notification.

EDUCATION

Western Governors University | Bachelor of Science, Cybersecurity and Information Assurance | Expected December 2026

CERTIFICATIONS

CompTIA A+ Core 1, passed
CompTIA A+ Core 2, in progress
CompTIA Network+, in progress
CompTIA Security+, in progress
Microsoft Office Specialist