

Robert Lynch

SOC Analyst (Tier 1) | Security-Focused IT Support Engineer

Lake City, FL · Open to remote · (386) 205-9612 · r.f.lynch@gmail.com

linkedin.com/in/robertflynch · github.com/RobertLynch21 · robertlynch.dev

Professional Summary

IT Support Engineer with hands-on endpoint, Linux and MSP experience, moving into a Tier 1 SOC Analyst role. I triage issues to separate user error, misconfiguration and hardware failure from security-relevant activity, and I document every case clearly enough to escalate. I write Python to parse logs and automate investigation tasks, backed by seven years of secure web development. Currently earning CompTIA Security+ and a B.S. in Information Technology (Cybersecurity) at Strayer University.

Technical Skills

- **Security operations:** alert triage, log analysis (Windows Event Logs, Linux auth/syslog), phishing analysis, incident documentation and escalation, system hardening, configuration baselines
- **Networking:** TCP/IP, DNS, DHCP, packet capture with Wireshark
- **Systems:** Windows, macOS, Linux (Ubuntu, CLI administration), imaging and deployment, Microsoft 365, Active Directory basics
- **Tools:** NinjaOne RMM, HaloPSA, Hudu, Git/GitHub, Docker, AWS
- **Scripting and development:** Python (log parsing, automation), Bash, JavaScript, Vue.js, React, HTML/CSS, SQL, WordPress/WooCommerce
- **Secure development:** input validation, authentication and session management, role-based access control (RBAC)
- **Practice:** Hack The Box, home security labs

Certifications

- **NinjaOne Certified Technician | MSP** — August 2026 (valid through August 2027)
- **CompTIA Security+** — in progress, target [January 2027]

Professional Experience

Information Technology Support Engineer — AdvanTech

Gainesville, FL (Hybrid) · August 2026 - Present

- Support endpoints for multiple managed clients across Windows, macOS and Linux, isolating hardware, user, configuration and potential security causes.
- Monitor device health and respond to alerts in NinjaOne RMM; work and escalate tickets in HaloPSA.
- Apply hardening controls (permissions, account policies, secure configuration baselines) consistent with MSP standards.
- Maintain client documentation and credentials in Hudu so any technician can pick up a case.

Deskside Support Team Lead — CSX

Jacksonville, FL (On-site) · October 2025 - August 2026

- Led the deskside support team, mentoring technicians on troubleshooting, ticket quality and escalation.
- Performed OS-level troubleshooting across Windows, macOS and Linux, flagging anomalous behavior for security review.
- Investigated endpoint issues to separate hardware failure, user behavior, misconfiguration and possible security events.
- Reviewed system logs during investigations and documented incidents and resolutions to improve escalation workflows.
- Supported deployments, imaging and configuration baselines that kept devices in a secure, consistent state.

Full-Stack Developer — Produced By Deuce, LLC

Remote · February 2018 - October 2025

- Built and maintained WordPress/WooCommerce sites, including custom themes and plugin updates.
- Found and replaced deprecated plugin code to remove stability and security risks.
- Applied secure development practices (input validation, authentication, session management, RBAC) and contributed Python components.

- Improved site performance and SEO through systematic debugging and Git-based development.

Frontend Developer — Premium Peanut

Douglas, GA (Remote) · March 2022 – July 2022

- Added stricter input validation and safer data flows to internal applications, reducing errors and exposure to malicious input.
- Traced logic issues through application logs with backend engineers to find root causes.

Security Projects

Code at github.com/RobertLynch21

- **Phishing Email Analyzer:** Python CLI that triages saved emails: checks SPF/DKIM/DMARC, look-alike domains, deceptive links and risky attachments, then outputs a verdict, defanged IOCs and next steps (github.com/RobertLynch21/phishing-email-analyzer).
- **Windows Event Analyzer (in development):** Python tool that parses Windows Event Logs to surface security-relevant events such as failed logons and account changes.
- **Network Triage Tool (in development):** script that gathers network connection and configuration data from a host for first-pass investigation.
- **Python Log Analysis Scripts:** parsed authentication and system logs, extracted key indicators and produced structured output for investigation.
- **Linux Security Hardening:** applied baseline controls including SSH configuration, file permissions and account policies.

Education

- **B.S. Information Technology, Cybersecurity Concentration** — Strayer University · Expected March 2028
- **Full-Stack Web Development Program** — DevMountain · 2021