
Gregory Stephens

Fort Worth, TX (Relocating Summer 2026) → Eligible to Work in the U.S.

(825) 365-0695

gregstephens96@gmail.com

GitHub: github.com/gstephens-cyber

LinkedIn: [linkedin.com/in/gregorystephens96](https://www.linkedin.com/in/gregorystephens96)

PROFESSIONAL SUMMARY

Cybersecurity student specializing in SOC operations, network defense, and incident response. Skilled in SIEM log analysis, firewall configuration, VLAN/OSPF networking, Linux administration, and system hardening. Strong focus on protecting organizational assets through methodical investigation, secure configuration, and evidence-based decision-making. Actively developing a professional portfolio demonstrating hands-on technical capability in blue-team workflows.

SKILLS

Security Operations: SIEM monitoring, log analysis, alert triage, IOC identification

Incident Response: Event correlation, evidence collection, containment, escalation

Networking: VLANs, ACLs, OSPF, DHCP, DNS, NAT, subnetting, L2/L3 switching

Security Administration: MFA setup, identity management, endpoint hardening

Tools: IBM QRadar, Splunk, Wireshark, Kali Linux, Linux CLI, Packet Tracer, GitHub

Frameworks: NIST CSF, NIST SP 800-61, ISO 27001 (Foundational)

EXPERIENCE

Cybersecurity & Network Technician

Trinity Systems - Edmonton, AB

Sep 2024 - Present

- Monitor authentication logs and security alerts to identify suspicious activity.
- Perform workstation hardening, patching, and secure configuration.
- Implement MFA, user provisioning, and least-privilege access controls.
- Develop SOPs for onboarding, password policies, and access control.
- Configure firewall rules, including ACLs, NAT, and outbound policies.
- Build VLAN segmentation, trunking, and Layer 3 routing in lab environments.
- Conduct SIEM investigations using QRadar to identify malicious indicators.

-
- Review Windows event logs (4624/4625) and network logs to identify anomalous patterns.
 - Produce incident response playbooks and documentation for operational use.

Cybersecurity Student

NAIT (Northern Alberta Institute of Technology) - Edmonton, AB

Sep 2024 - Present

- Complete hands-on labs covering SOC workflows, incident response, and SIEM analysis.
- Perform Linux system investigation, firewall configuration, and packet inspection.
- Build enterprise network simulations using Cisco environments and CLI tools.

CEO / Digital Operations (Legacy Role)

Trinity Systems - Redmond, WA

May 2018 - Aug 2024

- Managed technical operations, client projects, and system deployments.
- Oversaw design and development work prior to transitioning into cybersecurity.

EDUCATION

Northern Alberta Institute of Technology (NAIT), Edmonton, AB -

Cybersecurity Post-Diploma Certificate

Sep 2024 - Apr 2026

British Columbia Institute of Technology (BCIT), Burnaby, BC - Digital

Design and Development

Sep 2017 - Apr 2019

CERTIFICATIONS

- CompTIA Security+ (SY0-701) — *Expected April 2026*
- Google Cybersecurity Professional Certificate
- IBM Cybersecurity Analyst Professional Certificate — *In Progress*
- Cisco Networking Essentials

PROJECT PORTFOLIO

GitHub Portfolio: github.com/gstephens-cyber

Highlighted Projects:

- **VLAN Segmentation & OSPF Routing Lab** — secure network segmentation and routing
- **Firewall Configuration Lab** — ACLs, NAT, outbound policies
- **QRadar SIEM IOC Analysis** — event correlation and threat identification
- **Linux Hardening Exercises** — permissions, auditing, system controls

ADDITIONAL INFORMATION

- Eligible to work in the United States (no sponsorship required).
- Relocating permanently to Fort Worth, Texas — Summer 2026.
- Career focus: SOC Analyst • Cybersecurity Analyst • Security Operations Technician.