

---

# Gregory Stephens

Redmond, WA

(825) 365-0695

[gregstephens96@gmail.com](mailto:gregstephens96@gmail.com)

GitHub: [github.com/gstephens-cyber](https://github.com/gstephens-cyber)

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

## PROFESSIONAL SUMMARY

Security Operations Analyst experienced in log analysis, incident triage, endpoint hardening, and monitoring authentication activity across Windows and Linux environments. Skilled in reviewing security alerts, identifying anomalous behavior, supporting firewall policy updates, and enforcing access control procedures. Known for a structured, analytical approach to investigations, clear documentation, and steady operational discipline in day-to-day SOC workflows.

## EXPERIENCE

### Cybersecurity & Network Analyst

*Trinity Systems - Edmonton, AB*

Sep 2024 - Present

- Monitored authentication activity and reviewed suspicious log patterns across client systems
- Managed user access, MFA enrollment, and secure workstation configurations
- Performed basic investigations into alert activity and escalated potential security issues
- Supported firewall rule updates, endpoint hardening, and access control enforcement
- Applied understanding of AI/ML-assisted alert triage, including false positives, bias, and the need for analyst verification
- Maintained documentation for onboarding/offboarding, permissions, and incident tracking

### Cybersecurity & Network Analyst

*Trinity Systems - Redmond, WA*

May 2015 - Aug 2024

- Monitor authentication logs and investigate suspicious login activity
- Perform workstation hardening and secure configuration updates
- Support firewall rule changes, access control updates, and segmentation planning

- 
- Conduct basic SIEM investigations and document findings

## 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
- Cisco Networking Essentials
- EC-Council — Cybersecurity Attack and Defense Fundamentals (2025)
- Google Cloud AI & ML Foundations (Skill Badge)

## PROJECT PORTFOLIO

GitHub Portfolio: [github.com/gstephens-cyber](https://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
- **Server Hardening** — Linux and Windows

*References will be provided upon request.*