CODY BRISENO

IT support and networking professional building toward cybersecurity

cyberbriseno.dev	linkedin.com/in/codybriseno	github.com/cyberbriseno

PROFESSIONAL SUMMARY

IT support, networking, systems troubleshooting, and operations-leadership experience paired with a B.S. in Cybersecurity and Information Assurance in progress and continued cybersecurity study.

EXPERIENCE

IT Support and Networking

Professional experience

Endpoint support, production IT operations, field troubleshooting, and networking in high-availability environments.

Technical Systems Support

Professional experience

Systems support and technical troubleshooting in structured operational environments.

Operations Leadership

Leadership experience

Operations leadership and team management in a high-volume environment.

SELECTED WORK AND DIRECTION

Network Infrastructure Notes | Active

Networking

Structured, confidentiality-safe notes covering subnetting, VLANs, routing, packet analysis, and production troubleshooting. Documentation remains in progress.

Home SIEM Lab | Planned

Defensive security homelab

Designed as a segmented environment for log ingestion, alerting, and triage practice. Hardware procurement and deployment are not complete.

Malware Analysis Foundations | Planned

Long-term research track

A future safe-analysis study track after stronger SOC and lab foundations. No current professional malware-analysis experience is claimed.

EDUCATION

Western Governors University

B.S. Cybersecurity and Information Assurance | In progress | Expected 2027

Formal cybersecurity study alongside technical certifications, field experience, and planned lab work.

OWNER-CONFIRMED EARNED CREDENTIALS

- CompTIA A+
- CompTIA Network+
- CompTIA Security+

Credential dates and current validity are not published.

IN-PROGRESS STUDY

- CompTIA Project+
- CompTIA CySA+
- CompTIA PenTest+

EVIDENCE-BASED STRENGTHS

DEMONSTRATED

IT support; networking; endpoint troubleshooting; production IT operations.

WORKING / FAMILIAR

Windows and Linux administration foundations; completed Linux foundations coursework; Wireshark; PowerShell; Python; Docker fundamentals.

LEARNING / PLANNED

Defensive and offensive security foundations; home SIEM; malware analysis; reverse engineering; AI security.

OPERATING PRINCIPLES

- Keep claims proportional to evidence.
- Work only in owned, isolated, or explicitly authorized environments.
- Document limitations and protect confidential information.