KYLE BUTTON, MS, GSEC, GCIH

Marquette, MI | kyle@frequency42.com | LinkedIn

PROFESSIONAL SUMMARY

Information security and network engineer with over 20 years of experience spanning enterprise Zero Trust architecture, security operations, and hands-on software and infrastructure engineering. Serves as full Product Owner for the Zscaler suite (ZIA, ZPA, ZDX, ZCC, DLP) at Mayo Clinic, leading the transformation from legacy VPN and branch-firewall architecture to a cloud-delivered Zero Trust Exchange across a major healthcare enterprise. Builds real tools rather than just operating platforms: internal AI-driven operations software, open network diagnostics utilities, and production SaaS applications with hands-on cryptography, identity, and compliance engineering. Runs an independent security and technology consulting practice continuously since 2009, advising organizations, including regulated financial and healthcare clients, on architecture, vendor selection, and compliance. Holds an MS in Cybersecurity and Information Assurance, GIAC/SANS credentials (GSEC, GCIH), and CompTIA PenTest+.

CORE COMPETENCIES

- **Zero Trust & Zscaler:** ZIA, ZPA, ZDX, ZCC, DLP, Branch Connector, Zero Trust Exchange architecture and strategy; App Connector brokering, micro-segmentation, least-privilege access.
- **Networking:** Routing (BGP, OSPF, static), switching, VLANs, IPsec/GRE tunneling, WireGuard, Policy-Based Routing, SD-WAN concepts, DNS.
- **Security Architecture & Compliance:** Encryption and key management, identity (SAML, LDAP, Entra ID, OAuth), NIST-aligned incident response, PCI-DSS and financial data protection, HIPAA-adjacent healthcare security.
- **Software & AI Engineering:** Python, Bash, PowerShell, JavaScript/Node.js, Flask, REST/GraphQL APIs; GenAI and prompt engineering (Claude, OpenAI, Gemini) integrated into production tooling.
- **Infrastructure:** Red Hat Enterprise Linux, Docker, Proxmox high-availability clustering, AWS, self-hosted production systems.
- **Risk & Incident Response:** SOC incident response (phishing, intrusion, ransomware), forensic and telemetry analysis, vulnerability discovery and remediation.
- **Advisory & Leadership:** Vendor evaluation and technical standards influence, cross-functional stakeholder alignment, technical enablement and mentoring.

PROFESSIONAL EXPERIENCE

Mayo Clinic | Rochester, MN

Senior Engineer, Information Security

Mar 2024 – Present

Network Security & Infrastructure Protection / Security Operations Center

- Serve as full Product Owner for the entire Zscaler suite (ZIA, ZPA, ZDX, ZCC, DLP), owning architecture strategy and driving the organization from legacy VPN and branch-firewall models to a cloud-delivered Zero Trust Exchange architecture.
- Lead technical evaluation, Proof of Value, and renewal decisions for security and network vendors including Zscaler, NetBrain, Voyance, Broadcom, and Cisco, working directly with vendor teams.
- Drive alignment across network, security, and clinical stakeholders on Zero Trust strategy, translating complex architecture for both technical and executive audiences.
- Act as the internal Zscaler subject-matter expert: build support and engineering teams' competency through architecture reviews and reusable documentation, and regularly test beta features, providing structured feedback to Zscaler engineering.
- Designed and built Z Control, a custom internal Zscaler tooling platform (detailed under Projects).
- Administer Red Hat Enterprise Linux 9 infrastructure supporting Zscaler App Connectors, performing routing and tunnel diagnostics and infrastructure hardening.

Engineer, Security Operations Center (SOC)

Mar 2020 – Mar 2024

- Managed incident response, monitoring, and threat mitigation (phishing, intrusion, ransomware); analyzed host forensic and telemetry data using the FireEye suite and SIFT tools.
- Acted as Zscaler SME for the Cyber Security Operations team; aligned the IR framework to the NIST 800 series and standardized SOC documentation.

Senior Network Engineer *Jun 2014 – Mar 2020*

- Administered enterprise routing, switching, and security infrastructure (BlueCoat proxies, Checkpoint firewalls, Cisco); led enterprise deployment and vendor evaluation of Voyance and NetBrain.

PROJECTS

Z Control — Zscaler OneAPI / MCP / GenAI Platform *Mayo Clinic, 2025 – Present*

- Designed and built Z Control, unifying Zscaler OneAPI, the Zscaler MCP server, and the ZDX GraphQL API behind a single Flask-based platform, with Claude integrated as an AI reasoning layer over live operational data, letting teams ask natural-language questions instead of hand-building console queries.
- Presented Z Control in a Zscaler Zenith Live spotlight interview as an example of AI-driven tooling combined with hands-on platform expertise.

ZLookup — Network Diagnostics with ZPA Validation *Mayo Clinic*

- Built ZLookup, a self-hosted diagnostics platform (DNS lookup, ping, traceroute, TCP/UDP checks) with a Zscaler Branch Connector/ZPA mode for validating cross-branch connectivity.

TECHNICAL CONTENT & THOUGHT LEADERSHIP

- **Skill packages and enablement content:** Authored a Zscaler Administration Expert skill and a library of reusable technical skills capturing production lessons, published as standalone enablement material.
- **Security architecture and policy writing:** Produced a full security-architecture and implementation report and a five-policy security suite for a graduate capstone, validated against a live production codebase.

CONSULTING & ADDITIONAL EXPERIENCE

Frequency 42 LLC (2021–Present) / StackTech (2009–2021) | Marquette, MI / Rochester, MN

Owner and Principal Consultant. Operated as StackTech in Rochester, MN from 2009–2021; re-formed as Frequency 42 LLC after relocating to Marquette, MI, continuing the same scope.

- Serve as trusted technology and security advisor to small business owners and leadership, guiding decisions on infrastructure, tooling, and risk on an ongoing basis, and function as vCISO and MSP for SMB clients, deploying edge networking (Firewalla, UniFi), Policy-Based Routing, and secure tunnels.
- Advise accounting, bookkeeping, and financial-services clients on PCI-DSS compliance, payment processing security, and financial data protection.
- Built and operate production SaaS platforms including **RallyText** (Flask/PostgreSQL/Redis/Nginx, Stripe billing) and **SitePunch** (Node.js/PostgreSQL), implementing per-organization encryption, WebAuthn/passkey MFA, RBAC, and SHA-256 hash-chain audit logging.
- Built financial data security directly into both platforms: PCI-DSS scope reduction through tokenized payment processing, encryption at rest for financial and payroll-relevant records, and audit logging of financial transactions.
- Architect and operate WireGuard and Pangolin tunnel deployments across home lab and production; authored Portless, a self-hosted remote-access installer hardened through STRIDE/PASTA-style review.
- Found and remediated real production vulnerabilities through an automated per-commit security review pipeline, including stored XSS, path traversal, authentication/MFA bypass, and privilege escalation.

United States Coast Guard Auxiliary

Branch Chief, Cybersecurity Engineering *Oct 2023 – Present*

- Administer AWS cloud infrastructure for cgauxnet.cc, a phishing simulation platform used to test and train Auxiliary personnel, with logging to track simulation results and activity.

Marquette County Interscholastic Cycling | Marquette, MI

President, Team Director, and Coach *Jan 2024 – Present*

- Provide strategic leadership, manage board operations, and mentor coaching staff for a NICA-affiliated youth cycling organization.

Earlier roles: SCCM Administrator, Rochester Public Schools; Lead Computer Support Technician, Northern Michigan University (helpdesk serving 10,000+ students).

EDUCATION & CERTIFICATIONS

- **M.S. Cybersecurity and Information Assurance** – Western Governors University (Feb–June 2026)
- **B.S. Media Productions and New Technology**; B.S. Political Science, Leadership in Government – Northern Michigan University
- **GIAC Security Essentials (GSEC)** – SANS SEC401; **GIAC Certified Incident Handler (GCIH)** – SANS SEC504; **CompTIA PenTest+**
- **Zscaler Zero Trust Branch (ZTB)** and **Zscaler Administration and Engineering** training – completed (certification exams pending)
- **NetBrain Certified Administrator and SME**