

Cybersecurity Portfolio

Skye Stubbins | Security operations and infrastructure

contact@owzo.xyz | owzo.xyz | linkedin.com/in/skye-s-23b25192

Experience and focus

My background combines enterprise desktop support at Dart Container, technical support for Barracuda security products, and current cyber defense studies at Baker College. I focus on monitoring, infrastructure security, and troubleshooting that produces clear, usable documentation.

Personal security homelab

Independent project | Personal lab environment

The lab provides a place to explore the operational relationship between compute infrastructure, monitoring, access controls, and secrets management. It is a learning and development environment, separate from my professional support experience.

Infrastructure and visibility

- Linux and Docker workloads across virtualization and storage platforms including Proxmox, TrueNAS, and Unraid.
- Wazuh and CrowdSec for host security visibility and security controls; Prometheus, Grafana, Loki, and Alertmanager for metrics, logs, and alerts.
- VLAN segmentation, Tailscale, and Cloudflare Zero Trust for network separation and remote access; Authentik for single sign-on and HashiCorp Vault for secrets management.

Technical discussion

This environment gives me practical context for discussing how log collection differs from detection, how identity controls interact with network access, and why service dependencies matter during troubleshooting. Centralized visibility makes investigation easier, but collection health and meaningful alerts still require attention.

Scope and evidence

This overview describes my personal infrastructure and learning focus. It does not claim enterprise SOC ownership, a measured detection rate, or audited compliance. The accompanying resume summarizes the technologies and professional roles that support this work.

Related foundation

Baker College cyber defense studies are in progress. Completed Spring 2026 courses include Python, Linux II, Hardening Systems, Introduction to Information Security, Legal and Ethical Issues, and Project Management. I also participated on Baker's state-champion Cyber Defense Team in 2013-2014, which advanced to regional competition.

Network Security Architecture

Academic case study | Baker College | March 2026

Introduction to Information Security | Design and operations proposal

Problem

Design a secure small-business network and explain how a team with limited staffing could maintain it over time. The project connected architecture decisions to recurring maintenance, visibility, and incident handling.

Design approach

The architecture separated network functions through VLAN segmentation, a DMZ, and isolated guest wireless. The design included centralized logging and passive intrusion detection to support investigation without placing the IDS directly in the forwarding path.

Operational plan

- Prioritize exposed systems for patching, retain configuration backups, and document changes. The proposal set a seven-day target for security-critical patches where feasible and a monthly window for routine updates.
- Review vulnerabilities by severity, exploitability, and business impact. Review firewall rules and remote-access permissions on a recurring schedule.
- Centralize firewall, server, authentication, VPN, and wireless logs. Define alerts for repeated failed logins, unauthorized administrative access, and firewall configuration changes.
- Isolate backup systems, keep encrypted local and off-site copies, and test restoration. Assign incident-response responsibilities and document post-incident improvements.

Deliverables

A network architecture diagram, a written design rationale, and a maintenance and monitoring proposal. The proposal also identified measures such as patch compliance, remediation time, backup success, and incident-response time as ways to evaluate ongoing operations.

Tradeoffs and limits

The design balanced stronger separation and visibility against limited operational resources. Passive detection reduced the risk of interrupting traffic, but did not itself block attacks. Scheduled reviews created an achievable operating cadence, while urgent findings would still need attention outside that schedule.

This was an academic design exercise. Patch targets, review schedules, and proposed metrics describe the plan; they are not measured results from a deployed customer network.

What this demonstrates

Network security reasoning, operational planning, technical writing, and the ability to connect preventive controls with monitoring and recovery. The useful outcome is a documented approach that explains both what to implement and how to keep it functioning.