Kaden Zobel
Information Security Analyst | Cedar City, UT | kaden@thezobels.com | kadenzobel.com

PROFESSIONAL SUMMARY

Mission-driven Information Security Analyst and proven technical leader, currently serving as President of the SUU Cybersecurity Club and CCDC Team Captain. Backed by two consecutive years of DOE CyberForce competition experience, delivering hands-on proficiency in SOC operations, incident response, and advanced threat hunting. Currently defending enterprise networks by engineering a Kubernetes-based Elastic stack and executing thorough incident analysis across CrowdStrike, Windows Defender for Enterprise, and Palo Alto firewall telemetry. Adept at architecting resilient, secure infrastructure, demonstrated by designing a high-availability Proxmox and Kubernetes homelab driven by a strict GitOps workflow.

TECHNICAL SKILLS

- **Security Tools:** Elastic Security (SIEM), Splunk, Wazuh, CrowdStrike Falcon, Microsoft Defender for Endpoint, Proofpoint, CrowdSec, Nmap.
- **Frameworks & Methodologies:** MITRE ATT&CK, NIST Cybersecurity Framework, Incident Response Lifecycle.
- **Windows/Active Directory:** GPO Management, Kerberos Hardening, AD Certificate Services, Azure AD/Entra ID.
- **Linux/Infrastructure:** RHEL, Debian, Arch Linux, Proxmox VE, Docker, ZFS, Kubernetes Cluster, Git Version Control.
- **Networking:** OPNsense, VLANs, TCP/IP Traffic Analysis, SSH Hardening, DNS/DHCP, Nginx Reverse Proxies.
- **Scripting & Data Structures:** Bash, Python, YAML, PowerShell.

PROFESSIONAL EXPERIENCE

Information Security Analyst | Southern Utah University August 2025 – Present

- **Incident Handling & Containment:** Lead initial response efforts for security alerts generated by CrowdStrike Falcon and Microsoft Defender across 12,000+ endpoints; execute immediate host isolation and conduct root cause analysis to neutralize active threats.
- **Threat Detection & Triage:** Leverage Elastic SIEM to analyze logs and correlate security events; utilize custom dashboards and detection rules mapped to MITRE ATT&CK and NIST frameworks to identify, investigate, and validate anomalous network behavior.
- **Email Threat Mitigation:** Investigate and neutralize targeted phishing and Business Email Compromise (BEC) campaigns using Proofpoint, ensuring malicious payloads and links are quarantined before delivery.

IT Help Desk Technician | Southern Utah University May 2025 – August 2025

- **Automation:** Developed custom PowerShell and Bash scripts to automate user account migrations, reducing manual processing time by 50%.
- **Technical Support:** Consistently resolved over 75 Jira tickets weekly, delivering Tier 1 & 2 support for faculty and staff; diagnosed and mitigated complex campus network connectivity disruptions and managed DHCP reservations.

LEADERSHIP, COMPETITIONS & ENGINEERING PROJECTS

Team Captain & Regional Finalist | Collegiate Cyber Defense Competition (CCDC)

January 2026 – Present

- **Leadership & Threat Detection:** Led the 8-person competition team as the primary Windows AD Administrator and SIEM Engineer, successfully guiding the team to the Regional Finals.
- **Infrastructure Defense:** Hardened Domain Controllers against "Golden Ticket" and privilege escalation attacks with zero downtime; deployed Splunk in a mixed OS environment to detect Red Team lateral movement in real-time.

Blue Team Competitor | DOE CyberForce Competition

2024 – 2025

- **Critical Infrastructure Defense:** Defended simulated energy sector infrastructure against active, live-fire Red Team adversaries while ensuring the continuous operation of critical services and responding to dynamic administrative injects.

President | SUU Cybersecurity Club May 2025 - Present

- **Event Organization:** Spearheaded large-scale events, including a statewide CTF Capstone project for high school students, "ScopeCreep."
- **Club Management:** Managed the club budget, coordinated guest speakers, and led weekly technical workshops for 30+ active members.

Enterprise Security Engineering Lab | Personal Infrastructure

- **Virtualization & Systems Admin:** Designed a highly available Kubernetes cluster using GitOps; managed ZFS storage arrays and self-hosted services via Docker behind Traefik and Authelia utilizing custom YAML configurations.
- **Security Monitoring:** Deployed Elastic for centralized log ingestion, writing and tuning custom detection rules for SSH brute-force and privilege escalation attempts.

EDUCATION

B.S. Cybersecurity | Southern Utah University Expected Graduation: Summer 2026

- **Relevant Coursework:** Advanced Linux Systems, Network Defense, Cryptography, Digital Forensics.
- **Capstone Project:** Infrastructure Design & Management for a Statewide High School CTF Competition.