ELIE NZWEME

SOC Analyst | Threat Detection & Incident Response

Phoenix, Arizona | elie.nzweme@email.com | (801) 842-4374 | LinkedIn | GitHub | elienzweme.com

PROFESSIONAL SUMMARY

Security operations professional experienced with Splunk SIEM, Windows Event Log and Sysmon telemetry, and MITRE ATT&CK-mapped detection engineering. Built an enterprise SOC threat detection lab and vulnerability remediation program, and combines that with production endpoint and identity administration experience.

TECHNICAL SKILLS

Security: Splunk Enterprise • Microsoft Defender • Sysmon • Windows Event Logs • Vulnerability Mgmt • Incident Response • Threat Hunting • Endpoint Protection

Systems: Windows Server • Windows 10/11 • Linux • VMware • Hyper-V • DNS • DHCP • File Services • PowerShell • Bash

Cloud: Azure • Microsoft 365 • AWS • Identity Federation (SAML/OIDC/OAuth)

Identity & Access Mgmt: Active Directory • Entra ID • RBAC • MFA • SSO • JML • LDAP • Kerberos • Group Policy • LAPS • SailPoint (learning)

Networking: TCP/IP • VLANs • VPN • DNS • DHCP • SMB • AD Sites & Services

PROFESSIONAL EXPERIENCE

Technical Support Specialist — Kahala Management (MTY Food Group), Scottsdale, AZ *May 2026 – Present*

- Monitor and troubleshoot endpoint, identity, and network issues across Microsoft 365, Active Directory, Entra ID, and Intune.
- Investigate and resolve Windows 10/11, VPN, and endpoint security issues, escalating anomalies as needed.

Implementation Specialist – IAM & Identity Operations — Paychex, Remote *Nov 2025 – May 2026*

- Supported identity operations including Conditional Access and PIM, reinforcing least-privilege and access-monitoring practices.

IT Intern / Team Lead — TechCharities, Salt Lake City, UT *Apr 2025 – Aug 2025*

- Led an IT intern team, coordinating device support and incident triage for program operations.

IT & Customer Support — Movate (Sony account), Remote *Mar 2024 – Aug 2025*

- Triaged and resolved technical support tickets, documenting root cause and resolution steps.

Technical Support Specialist — Willman Services, Kinshasa, DRC *Oct 2019 – Dec 2022*

- Provided desktop support and issue escalation across a distributed user base.

FEATURED PROJECTS

Enterprise SOC Threat Detection Lab

Splunk Enterprise | Sysmon | Windows Event Logs | MITRE ATT&CK | PowerShell Logging

- Deployed a Splunk Enterprise SIEM pipeline ingesting Windows Event Logs and Sysmon telemetry across a multi-host Windows Server 2025 lab.
- Built and validated detection use cases mapped to MITRE ATT&CK techniques for privilege escalation, lateral movement, and persistence.
- Tuned PowerShell script-block logging and correlation searches to reduce false positives and surface high-fidelity alerts.

Enterprise Endpoint Vulnerability Remediation Lab

Nessus | Patch Management | Credentialed Scanning | Risk Analysis | Executive Reporting

- Ran credentialed Nessus vulnerability scans across a simulated enterprise endpoint fleet and prioritized findings by CVSS and business risk.
- Coordinated patch management remediation cycles and tracked closure rates against SLA targets.
- Translated scan data into executive-level risk dashboards for remediation prioritization.

Active Directory Identity Lifecycle & Access Management Automation Toolkit

PowerShell | Active Directory | RBAC | Group Policy | LAPS | Splunk | Jira

- Built a PowerShell-based IAM automation toolkit for Active Directory covering user provisioning, deprovisioning, account recovery, and end-to-end Joiner-Mover-Leaver lifecycle workflows.
- Automated OU management, RBAC group assignment, and bulk identity operations to reduce manual identity administration effort.
- Implemented inactive account detection, password compliance reporting, and duplicate identity detection with integrated Splunk monitoring and Jira ticketing, plus file server access auditing.

CySA+ Practice Exam App

HTML | CSS | JavaScript

- Developed an interactive web app with 1,000+ practice questions, flashcards, and full exam-simulation mode to support CySA+ certification study.

CERTIFICATIONS

CompTIA CySA+ • Microsoft SC-200 • Splunk Core Certified Power User • CompTIA Security+ • CompTIA CSAP (Stackable) • CompTIA Network+ • Microsoft SC-300 • Microsoft AZ-104 • Microsoft AZ-900 • Microsoft AI-900 • AWS Certified Cloud Practitioner

EDUCATION

Bachelor of Applied Science, Information Technology (Systems Administration) — Ensign College *Feb 2026*

Associate of Applied Science, Information Technology *Aug 2025*