ELIE NZWEME

Information Security Analyst | IAM | SOC | Microsoft Security

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

PROFESSIONAL SUMMARY

Cybersecurity professional with hands-on experience across Identity & Access Management (IAM), Security Operations (SOC), Active Directory, Microsoft Entra ID, Splunk SIEM, and PowerShell automation. Skilled at securing identities, monitoring for threats, and hardening enterprise endpoints in Microsoft-centric environments.

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

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

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

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

PROFESSIONAL EXPERIENCE

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

- Administer Microsoft 365, Active Directory, Entra ID, and Intune for enterprise endpoint and identity operations.
- Resolve Windows 10/11, VPN connectivity, Microsoft Teams, and Outlook issues; manage printer deployments and TPM troubleshooting.
- Own endpoint support, hardware lifecycle management, and user account administration end-to-end.

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

- Executed identity provisioning, Conditional Access policy configuration, and Privileged Identity Management (PIM) workflows.
- Processed IAM service requests and change tickets through ServiceNow in a regulated, high-volume environment.

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

- Led a team of IT interns supporting device deployment and end-user technical support.

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

- Provided technical and customer support, resolving hardware/software issues and escalations via ticketing systems.

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

- Delivered desktop and endpoint support across a distributed user base.

FEATURED PROJECTS

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.

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.

Enterprise Identity & Endpoint Management Lab

Active Directory | GPO | Windows LAPS | Microsoft Defender | File Server Permissions

- Designed Active Directory OU structure, Group Policy Objects, and Windows LAPS deployment for a simulated enterprise domain.
- Hardened endpoint security with Microsoft Defender configuration and centralized file server permission auditing.
- Implemented least-privilege access controls across shared network resources.

CERTIFICATIONS

CompTIA Security+ • CompTIA CySA+ • Microsoft SC-200 • Microsoft SC-300 • Splunk Core Certified Power User • CompTIA Network+ • Microsoft AZ-104 • CompTIA CSAP (Stackable) • 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*