ELIE NZWEME

Cloud Security Analyst | Azure & Identity Security

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

PROFESSIONAL SUMMARY

Cybersecurity professional building toward cloud security engineering, with Microsoft Azure administration (AZ-104), AWS Cloud Practitioner certification, and hands-on Entra ID identity and Conditional Access experience. Studied identity federation protocols (SAML 2.0, OIDC, OAuth 2.0) and is progressing toward AZ-500 and Terraform Associate.

TECHNICAL SKILLS

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

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

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)

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

PROFESSIONAL EXPERIENCE

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

- Administer Microsoft 365, Entra ID, and Intune for cloud identity and device management across the organization.
- Support VPN connectivity and endpoint security configuration in a hybrid cloud/on-premises environment.

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

- Configured Conditional Access policies and Privileged Identity Management (PIM) for cloud identity governance.
- Supported identity provisioning workflows across client Entra ID tenants.

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

- Led IT interns supporting device and account provisioning.

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

- Provided technical support, including account and access troubleshooting.

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 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.

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 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.

CERTIFICATIONS

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

EDUCATION

Bachelor of Applied Science, Information Technology (Systems Administration) — Ensign College *Feb 2026*
Associate of Applied Science, Information Technology *Aug 2025*