ELIE NZWEME

Identity & Access Management (IAM) Specialist

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

PROFESSIONAL SUMMARY

IAM-focused cybersecurity professional with production experience administering Active Directory, Microsoft Entra ID, Conditional Access, and PIM, plus a self-built PowerShell IAM automation toolkit covering full Joiner-Mover-Leaver lifecycle management. Studied identity federation (SAML 2.0, OIDC, OAuth 2.0) for Entra ID and Okta integration.

TECHNICAL SKILLS

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

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

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

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*

- Manage Active Directory, Entra ID, and Intune identity and device lifecycle for a multi-site enterprise environment.
- Administer user account provisioning/deprovisioning, group membership, and access requests via Microsoft 365 admin tools.

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

- Executed identity provisioning, Conditional Access policy configuration, and Privileged Identity Management (PIM) assignments for enterprise clients.
- Processed IAM service requests and access changes through ServiceNow, ensuring accurate identity governance records.
- Supported Joiner-Mover-Leaver (JML) identity lifecycle operations across client Active Directory and Entra ID tenants.

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

- Led IT interns on device provisioning and account setup for program participants.

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

- Handled account and access-related support tickets for enterprise customers.

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 IAM Audit & Compliance Lab

Active Directory | Access Reviews | Compliance Reporting | RBAC

- Ran periodic access reviews and entitlement audits against Active Directory groups to identify over-permissioned and stale accounts.
- Produced compliance reporting artifacts documenting access certification and remediation actions.

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