CLEVELAND OLIVER

Senior IAM Engineer | Identity Architecture & Automation | Zero Trust | Entra ID | Okta | OAuth2 / OIDC / SAML
Fayetteville, NC | 502-428-9619 | dolivernetwork@gmail.com | LinkedIn | GitHub: IAM Production Scenarios

PROFESSIONAL SUMMARY

Senior IAM Engineer with 6 years of hands-on ownership over enterprise identity ecosystems at scale — spanning Okta, Microsoft Entra ID, and hybrid Active Directory environments of 10,000–20,000+ users. Deep practitioner across the full IAM stack: federated identity (SAML 2.0, OIDC, OAuth2, SCIM), Zero Trust architecture, Conditional Access, PIM/JIT privileged access, and lifecycle automation via PowerShell, Python, Graph API, and Terraform. Documented history of translating audit findings and executive security mandates into hardened, policy-as-code IAM controls with measurable outcomes — eliminating 40+ hours/month of manual effort, automating reporting pipelines, and reducing HIGH-risk orphaned access findings to zero. Strong SOC 2, HIPAA, and SOX compliance delivery track record. Built and published a public IAM production scenario lab (GitHub) covering MFA bypass remediation, Zero Trust rollout, SCIM provisioning, OAuth2 automation, and orphaned access governance — demonstrating practitioner-level depth beyond certification.

CORE COMPETENCIES

Identity Platforms: Microsoft Entra ID (P1/P2), Okta (SSO, MFA, FastPass, Workflows, IGA), Active Directory DS

Protocols & Federation: SAML 2.0, OIDC, OAuth2 (Client Credentials, Auth Code), SCIM, Basic Auth remediation

Zero Trust & Conditional Access: Phishing-resistant MFA, device compliance, PIM JIT, named locations, risk-based sign-in blocking

PAM & Governance: Azure PIM, least-privilege enforcement, JIT activation, service account lifecycle, access reviews

Automation & IaC: PowerShell (advanced), Python, Microsoft Graph API, Terraform (AzureAD provider), Azure Automation

Identity Lifecycle (JML): Joiner-Mover-Leaver design, HRIS-driven pipelines, SCIM provisioning, orphaned access auditing

Compliance & Audit: SOC 2 Type II, SOX, HIPAA, NIST 800-63, access certifications, audit evidence delivery

SIEM & Detection: Entra sign-in diagnostics, Graph API reporting, identity risk posture automation, SIEM integration

PROFESSIONAL EXPERIENCE

Senior IAM & Infrastructure Engineer

June 2025 – Present

ID Sentinel Solutions (Independent Practice) — Remote

- Sole platform owner for enterprise IAM simulation environment spanning Okta, Microsoft Entra ID P2, and hybrid Active Directory (Entra Connect) — designing and operating production-equivalent identity controls for a 1,100+ user org.
- Designed and enforced a Zero Trust architecture across three workstreams: PIM Just-in-Time privileged access (zero permanent admin assignments), a 4-policy Conditional Access suite (MFA, device compliance, risky sign-in blocking, legacy auth block), and Terraform-as-code deployment for repeatable, version-controlled policy management.
- Identified and closed a critical MFA bypass gap caused by legacy auth protocols (SMTP, IMAP, POP3, Basic Auth); deployed CA policy in report-only mode, validated with What If tool, enforced org-wide — achieving zero unauthorized legacy auth attempts post-enforcement.
- Automated identity risk reporting via Python + Microsoft Graph API (OAuth2 client credentials flow); reduced manual reporting from 4–6 hrs/week to under 5 minutes — detecting 1,096 users without MFA registration and directly informing Zero Trust rollout prioritization.
- Conducted orphaned access audit using Graph API and PowerShell; detected 42 findings (disabled accounts with active memberships, stale guests, ownerless groups, inactive accounts) — remediated all HIGH-risk findings, reducing total findings by 19% with evidence exported for SOC 2 compliance documentation.
- Authored advanced PowerShell automation runbooks for HRIS-driven JML lifecycle workflows, bulk provisioning/deprovisioning, AD group management, and Entra Connect sync operations — eliminating 40+ hours of monthly manual administration effort.

- Published full scenario walkthroughs and scripts to GitHub (IAM Production Scenarios) covering MFA bypass, Zero Trust rollout, SCIM provisioning, OAuth2 API integration, and access governance — demonstrating practitioner-level implementation across the IAM stack.

IAM Engineer — Okta, Entra ID & Lifecycle Automation
May 2024 – June 2025

Moderna | Regulated Healthcare (HIPAA, SOX) | 10,000+ Users

- Primary IAM platform engineer for 10,000+ user Okta environment; served as escalation point for SSO, SAML 2.0, SCIM provisioning, MFA enforcement (Okta FastPass, FIDO2), and lifecycle management issues end-to-end.
- Architected and automated end-to-end Joiner-Mover-Leaver lifecycle driven by HR system data — PowerShell and Graph API pipelines validated identity data from SQL databases, triggering workflows across AD, Okta, and M365; reduced provisioning cycle time by 25%.
- Managed Entra Connect sync rules, attribute mappings, scoping filters, and AD extension attributes across a large-scale hybrid environment; administered OU structures and GPO enforcement.
- Designed and maintained Conditional Access policies enforcing MFA, device compliance, and risk-based access controls; administered Entra PIM role assignments and managed app registrations, service principals, API permissions, and certificate lifecycle governance.
- Authored ServiceNow runbooks and automated workflows for onboarding, offboarding, and account management — patterns directly transferable to Azure Automation and Freshservice environments.
- Contributed to SOX and HIPAA audit readiness through access controls documentation, change management records, and compliance reporting; supported periodic access certifications and audit evidence delivery.

IAM Engineer / Identity Security Analyst
Jan 2023 – May 2024

HCLTech (Client: United States Steel) | Hybrid Enterprise | 20,000+ Users

- Administered IAM operations for 20,000+ user hybrid environment across AD and Entra ID — OU structures, GPO, AD-to-Entra sync, and attribute mappings; served as Tier 2/3 escalation for identity incidents.
- Built and maintained PowerShell and Graph API automation for identity lifecycle workflows, bulk provisioning/deprovisioning, group management, and SQL-based identity data extraction for audit reporting.
- Configured and maintained Okta SSO, SAML, SCIM, and MFA integrations for 20+ enterprise applications; troubleshot authentication failures and Conditional Access evaluation issues using Okta System Log and Entra sign-in diagnostics.
- Established documentation standards for automation scripts, runbooks, and IAM configurations; collaborated with HR, Security, and application owners to align and improve identity lifecycle workflows.

IAM Operations Analyst
June 2021 – Dec 2022

HCLTech (Client: Chubb Insurance) | SOX-Regulated Financial Services

- Delivered end-to-end incident resolution for 400+ monthly issues across Okta MFA, SSO, Active Directory, Conditional Access, and identity lifecycle operations — maintaining strong SLA performance in a SOX-regulated environment.
- Developed operational runbooks and automation scripts; supported JML lifecycle workflows and collaborated with HR and Security to enforce least-privilege access and PAM controls.

CERTIFICATIONS

Microsoft SC-300: Identity & Access Administrator Associate | **CompTIA Security+** | **Okta Certified Professional (Scheduled May 2026)**

IAM PRODUCTION SCENARIOS LAB (GITHUB)

Publicly documented production IAM engineering challenges. Environment: Windows Server 2019 (AD DS), Microsoft Entra ID P2 (M365 Dev Tenant), Okta Developer Edition, hybrid Entra Connect sync. Tools: PowerShell, Terraform, Python, Postman, SAML Tracer.

- Implemented Zero Trust controls with Conditional Access, MFA enforcement, PIM JIT access, and Terraform IaC deployment.
- Automated MFA and identity risk reporting via Python, Postman, and Microsoft Graph API using OAuth2 client credentials flow.
- Conducted orphaned access audits with Graph API and PowerShell, identifying stale accounts, inactive guests, and ownerless groups.
- Built SCIM lifecycle automation workflows in Okta for provisioning/deprovisioning and reduced manual access delays.