Jake Richard Meyers - Identity & Access / Identity Security Architect - Identity & Access / Identity Security Architect

Profile

Background

Education

The University of Michigan, Ann Arbor, MI

- College of Literature, Science, and the Arts (LSA) | Biochemistry, Economics, and Data Science
- School of Music, Theatre, and Dance (SMTD) | Design & Production, Stage Management, Lighting Design & Electrics, Sound Engineering, and Music Production

Detroit Country Day School, Beverly Hills, MI

- High School Diploma | College Preparatory Curriculum

Skills

*Identity, Access & Authorization Control Plane**

Microsoft Entra ID / Azure AD, Entra ID Governance patterns, custom roles, access reviews, entitlement packages, lifecycle workflows, Privileged Identity Management, Azure resource PIM, Just-in-Time access, Conditional Access, passwordless deployment programs, FIDO / MFA, workload identities, managed identities, service principals at scale, service-principal lifecycle governance, RBAC, least-privilege design, Just Enough Administration, PAW/SAW and Tier 0 operating models, Microsoft Graph and Azure Management API identity automation, Active Directory Domain Services, Active Directory Certificate Services, Active Directory Federation Services, schema-level Active Directory work, customer identity and access management, Entra B2B/B2C, external identity, delegated MSP/CSP privileged access, SCIM-preferred provisioning, and automated lifecycle provisioning.

*Privileged Access, Cryptography & Secrets**

Standing-privilege elimination, break-glass controls, M-of-N approvals, CyberArk privileged-access integration governance, HYOK, BYOK, Azure Key Vault, secrets-management patterns, ephemeral-token and check-in/check-out patterns, certificate-based authentication, PKI, certificate lifecycle management, privileged-account discovery, privileged-access monitoring, lateral-movement containment, leaked-privilege remediation, and non-human identity accountability.

*Microsoft Purview, DLP & Information Protection**

Microsoft Purview Data Loss Prevention across Microsoft 365 and endpoints, Exchange / SharePoint / OneDrive / Teams DLP, sensitivity labels, auto-labeling, retention labels and policies, Insider Risk Management, eDiscovery, content explorer, data classification, sensitive-data discovery and mapping, DLP policy authoring, alert investigation, remediation workflows, and AD RMS to AIP/MIP/Purview modernization.

*Security Architecture, Detection & Operations**

Zero Trust, Microsoft Defender, Defender for Cloud Apps, Microsoft Sentinel analytics rules, hunting, UEBA, KQL, SIEM, SOAR, SASE, XDR, vulnerability management, Attack Surface Reduction, Windows Defender Application Control, AppLocker, endpoint protection, incident response, post-incident remediation, continuous red-team / blue-team operations, shadow IT discovery, threat modeling, change-integrated security scanning, and ServiceNow GRC/change integration.

*Federation, Hybrid Identity & PKI**

Ping Federate, SAML, OIDC, OAuth, RADIUS, Kerberos, hybrid identity, tenant onboarding, Azure AD / Entra tenant consolidation, Microsoft 365 identity migration, multi-forest Active Directory consolidation,

Enterprise PKI, HSM-backed offline root patterns, AD CS administrative RBAC, certificate templates, RADIUS certificate enrollment, and certificate-based authentication.

*Cloud, DevOps, Governance & Compliance**

Azure Landing Zones, Azure Policy, Azure RBAC, Azure Arc, Virtual WAN, Azure Stack, hybrid cloud, private cloud, Azure Private Link, Application Gateway, Front Door, Azure Firewall Premium, Web Application Firewall, Network Security Groups, Application Security Groups, Azure Well-Architected Framework, Terraform, HashiCorp Vault exposure and provider-agnostic secrets-management support, ARM Templates, Bicep, PowerShell, GitHub, Azure DevOps, GitHub Advanced Security, CodeQL, Dependabot, CI/CD pipelines, Policy as Code, drift detection, NIST CSF 2.0, CJIS, HIPAA, PCI, CUI, PII, financial and health data protection, FIPS, FINRA, SEC, continuous control monitoring, audit automation, enterprise architecture review boards, SDLC policy enforcement, secure architecture review, control evidence, and reporting.