Alec Eckmann

alec@aleckmann.com
https://aleckmann.com • @aleckmann • @aleckmann

Professional Experience

Azoff Music Company

Information Security Specialist *Apr 2021 – Present*

- Led the company's cybersecurity program, prioritizing improvements based on data-driven risk assessments, industry specific attack patterns, and the NIST Cybersecurity Framework. Reduced IT spending while improving overall security posture.
- Led the design and development of a Bicep-based IaC framework to codify a hub-and-spoke topology and migrate legacy infrastructure to the new model. Implemented a Role Based Just-in-Time permissions model for all cloud resources.
- Enforced biometric sign in requirements and synced local hardware security tokens with Entra ID, enabling passwordless logins from compliant endpoints to all corporate resources. Deployed FIDO2 hardware tokens to a smaller group of highly privileged users. Achieved a 95% device compliance rate within 1 month of policy rollout.
- Fully automated the user onboarding process with Azure DevOps, PowerShell, and app-specific API integrations to streamline provisioning, reducing onboarding turnaround time by 80%.
- Developed highly customized Conditional Access Policy solutions for all identities, employee or otherwise. Maintained an average Identity Secure Score of 90%.
- Transitioned 99% of managed corporate applications to SAML/OIDC Single Sign-On (SSO).
- Served as the primary Intune and Jamf administrator, managing 400+ Windows, MacOS, iOS, and Android endpoints. Enforced hardened device configurations based on CIS Benchmark recommendations. Fully automated app provisioning and patch management across all endpoints.
- Deployed and managed Microsoft's Defender Suite to unify vulnerability reporting across all IT and Development infrastructure. Integrated Microsoft and third-party services into Azure Sentinel with automated playbooks to streamline incident response.
- Designed and led a new hire security training program. Administered new phishing awareness and security training platforms with an emphasis on industry-specific attack patterns.
- Redesigned corporate office network, implementing port-based access controls across several VLANs.
- Deployed Azure Arc to all on-prem servers. Built unified monitoring and patching solutions with Azure Monitor and Update Manager.
- Worked cross departmentally on standardizing and updating company IT and Security policies. Formalized a company wide vendor management process.
- Administered a cloud CA and RADIUS Server (EZCA and EZRadius), enabling Entra ID Wi-Fi authentication for corporate networks.

Cartwheel IT (now Altourage)

Security Analyst *Feb 2018 – Apr 2021*

- Sole developer; designed, developed, and deployed an internal automation suite in Python that monitored, audited, and reported on over a thousand endpoints daily.
- Worked daily to investigate and remediate security alerts through SentinelOne, Office365 Cloud App Security Portal, and ArcticWolf, Cyberhawk Vulnerability Management platforms
- Responsible for the maintenance, management, and continuous improvement of 25+ clients' security programs.
- Routinely configured and hardened common SaaS products (Box, Dropbox, Google Drive, Sharepoint), network security products (Cisco Umbrella, Cisco Secure Internet Gateway), and IdPs (Azure AD and GSuite)
- Enforced industry standard compliance for HIPAA, FINRA, PCI, GDPR, and CCPA requirements.

Project Highlights

Infrastructure as Code Migration
Bicep-based IaC Framework

- Developed a system to migrate existing infrastructure to a modern hub-and-spoke topology
- Wrote modular and parameterized Bicep templates to deploy different development environments across teams, subsidiaries, and regions
- Created an IaC sandbox environment to automate the testing of resource deployment and network restrictions before updating production workloads
- Aligned with Microsoft's Well-Architected framework to centralize network security and monitoring across a multi-spoke, multi-region cloud environment

Geofencing Form
Simple Web Form for Traveling Employees

- Access restricted to employees and requires SSO login; allows submission on behalf of another valid user (useful for assistants)
- Takes travel dates and destination region as input, exempts users from Conditional Access Policies specific to their destination region only for duration of their trip
- "Risky" regions require approval from manager and security team (risk calculated based on current threat model)
- Every step of process is logged through ticketing system, sending email notifications to relevant parties

Onboarding Form
Automated User Provisioning with Advanced Logic and Built-in Approvals

- Access restricted to hiring managers only, requires SSO login
- Takes user metadata and access package as input (no sensitive information) and creates relevant accounts, licenses, and group assignments
- Unique behavior based on access package, department, employement type, and subsidiary
- Built-in approval process for managers, application administrators, and security team depending on requested access
- Every step of process is logged through ticketing system, sending email notifications to relevant parties

Technical Skills

Infrastructure as Code:	Azure DevOps, Bicep, Terraform, Python, PowerShell
Endpoint Administration:	Microsoft Entra ID, Defender for Endpoint, Intune, Jamf
IAM Administration:	SSO, Conditional Access, PAM, Azure KeyVault, 1Password
Network Administration:	DHCP, DNS, VLANs, RADIUS, Meraki
Cloud Networking:	Azure VPN, Azure Firewall, Private Endpoints, PLS, AFD, Azure Policy
Email Security:	Sendgrid, SPF, DKIM, DMARC, Defender for Office 365

Academic Background

New York University
Bachelor, Computer Science *Sep 2013 – May 2017*

Spoken Languages

English: Native or Bilingual Proficiency

Spanish: Limited Working Proficiency

Italian: Elementary Proficiency