ADAM MUKDAD

Chicago, IL | AdamMukdad97@gmail.com | https://linktr.ee/adammukdad | 773 595-0620

PROFESSIONAL SUMMARY

Security-focused IT Support Specialist pursuing advancement into Identity & Access Management (IAM). 5+ years of experience in technical support, user provisioning, endpoint security, and access governance across enterprise and educational environments. Adept at balancing usability with compliance, implementing least-privilege principles, and reinforcing secure authentication and account lifecycle workflows. Currently pursuing Microsoft AZ-900, Okta Certified Professional, and CompTIA Security+ to strengthen IAM readiness.

Core Strengths: Access Control • IAM Fundamentals • Endpoint Security • Log Analysis • Office 365 & Google Workspace Administration • User Provisioning • Policy Documentation • Incident Response Support

CORE COMPETENCIES

Identity & Access Management (IAM) • Active Directory / Azure AD • Authentication & Authorization • User Lifecycle Management • Endpoint Security • Patch Management • Security Awareness Training • Incident Response • Compliance & Governance • Ticket Resolution (JIRA / ServiceNow) • Documentation & SOP Development • ITIL Principles

PROFESSIONAL EXPERIENCE

Financial Services Associate

Walmart | Chicago, IL | July 2024 – Present

- Enforced identity verification and validation procedures in compliance with financial regulations.
- Detected potential fraud via behavioral analysis and transaction pattern recognition, reinforcing compliance vigilance.
- Protected customer data integrity by rejecting expired, invalid, or altered identification.
- Developed strong analytical and regulatory awareness applicable to IAM access auditing and verification functions.
- Administered account-based privileges for tax-exempt entities and warranty validation systems.

IT Support Specialist

The Vazquez Holdings Organization, LLC | Chicago, IL | Feb 2020 – July 2024

- Managed user provisioning, access requests, and account lifecycle workflows, implementing least-privilege and separation-of-duties principles.
- Authored 12+ internal security procedure guides, aligning operations with compliance and audit standards.
- Conducted endpoint hardening, patch management, and vulnerability mitigation across distributed devices.
- Monitored system activity logs (Event Viewer, McAfee, Proofpoint) to identify anomalies and escalate incidents.
- Delivered internal security awareness training, boosting phishing resilience and incident reporting accuracy.
- Supported multi-platform environments (Office 365, Google Workspace, VPNs) ensuring secure collaboration and continuity.

OIT Support Specialist

City Colleges of Chicago – Richard J. Daley College | Chicago, IL | Aug 2017 – Jan 2020

- Resolved 30+ weekly IT tickets related to authentication, hardware, and network issues, maintaining 99.9% uptime.
- Administered onboarding/offboarding for 200+ users, maintaining consistent access control documentation.
- Authored and maintained standard operating procedures (SOPs) for software deployment, security updates, and user access protocols.
- Rolled out new labs using mass OS imaging, software installations, and system lockdown tools (Deep Freeze).
- Troubleshot and replaced defective components, upgraded RAM and SSDs, and performed lifecycle management of end-user assets.
- Collaborated with IT leadership to support patching and endpoint audit readiness efforts.

EDUCATION

Associate of Science in Computer Science
City Colleges of Chicago – Richard J. Daley College

CERTIFICATIONS (In Progress)

• Microsoft Certified: Azure Fundamentals (AZ-900)
• Okta Certified Professional (OCP)
• CompTIA Security+

TECHNICAL TOOLKIT

Active Directory | Azure AD | Office 365 | Google Workspace | VPN Configuration | Endpoint Security Tools | Proofpoint | McAfee | Windows Server | Event Viewer | Imaging / Deep Freeze | PowerShell (basic) | Python (basic scripting) | Ticketing Systems (ServiceNow / JIRA)

BRANDING STATEMENT

"I build secure, efficient access environments where technology and compliance intersect — ensuring every identity is verified, every access is justified, and every endpoint is protected."