MOHAMMED ALI KHAN

IT Security Administrator | Identity & Access Management | Endpoint Security | SIEM/EDR Operations | AI Automation

Skokie, IL | (847) 877-1980 | ali789059@gmail.com | linkedin.com/in/mohammedalikhan-ai

PROFESSIONAL SUMMARY

IT Security and Infrastructure professional with 4+ years of experience spanning Identity & Access Management (IAM), endpoint security, SIEM/EDR operations, and enterprise systems administration. Proven record securing and supporting 5,000+ users and 815+ endpoints across 120 retail locations - implementing SailPoint IdentityNow IAM, Azure Entra ID SSO/MFA/Conditional Access, and CrowdStrike Falcon EDR, while managing SIEM operations through a transition from Arctic Wolf to Rapid7. Led the migration of 120 retail locations from legacy on-premises hardware servers to a Hyper-V-based Remote Desktop Server Collection (RDSC), mitigating end-of-life security risk while improving system performance by 70%. Hands-on across MECM/SCCM, JAMF Pro, SOTI, SharePoint/Teams/Power Platform, and DSPM-driven data governance, with additional experience building AI automation and CRM integrations using LLM-based conversational agents. Skilled at translating complex technical and security initiatives into clear documentation, measurable KPIs, and cross-functional collaboration with HR, Security, and Network teams.

EDUCATION

Bachelor of Science - Management Information Systems & Finance

DePaul University, Driehaus College of Business | Minor: Accounting

Relevant Coursework: SaaS Systems, Business Analytics, Database Systems Analysis & Design, Applied Networks & Security, Financial Statement Analysis, Web Computing, Microsoft Access

PROFESSIONAL EXPERIENCE

AI Implementation Engineer | *Dealership Accelerator - Remote* **Jan 2026 - Present**

- Increased qualified-lead response rates for automotive dealership clients by architecting end-to-end AI automation workflows integrating CRM platforms (CDK Global, Cox Automotive, Tekion) with GoHighLevel (GHL) and Twilio A2P SMS/voice messaging.
- Built and deployed 10+ automated workflows in GoHighLevel (GHL) - including lead routing, automated follow-up sequencing, and CRM syncing - cutting manual outreach time by 60% and accelerating lead response speed by 45%.
- Extended automation beyond native GHL capabilities by building custom multi-step pipelines in n8n, connecting CRM, inventory, and communication systems to support more complex, client-specific logic.
- Enabled reliable data flow across 12+ CRM, inventory, and communication integrations processing 10,000+ records/month by building and maintaining RESTful API integrations for multiple dealership clients.
- Maintained 100% accuracy on daily user onboarding/offboarding workflows by auditing access changes against corporate SOPs and data-integrity protocols.
- Onboarded and maintained 245 active client accounts at 99.7% data accuracy, contributing to approximately $840,000 in monthly recurring revenue, by building automated validation and reconciliation checks into the AI onboarding workflow.
- Delivered measurable ROI on deployed AI solutions by gathering client requirements, conducting workflow automation analysis, and iterating on prompt engineering and model configuration with LLM-based conversational agents.

IT Security Administrator | *American Signature Inc. - Remote* **Jan 2024 - Jan 2026**

- Strengthened enterprise identity security for 5,000+ users by implementing SailPoint IdentityNow-driven IAM and configuring Azure Entra ID Single Sign-On (SSO), reducing authentication friction while cutting unauthorized-access risk.
- Enforced a Zero Trust access model by deploying Multi-Factor Authentication (MFA) and Conditional Access policies across all corporate and retail accounts, and automating user provisioning/deprovisioning through SailPoint.

- Improved least-privilege compliance across the organization by designing and implementing Organizational Units (OUs) in Azure AD to align user permissions with role-based access requirements.
- Streamlined user lifecycle management across a hybrid identity environment by provisioning and deprovisioning accounts through on-premises Active Directory and the Azure Admin Center, maintaining consistent access controls across both platforms.
- Improved security event visibility and incident triage speed by managing SIEM operations through a strategic transition from Arctic Wolf to Rapid7, expanding continuous monitoring coverage across the environment.
- Upgraded endpoint threat-detection coverage by evaluating and deploying CrowdStrike Falcon EDR across 815+ endpoints for consistent, real-time protection.
- Maintained a 98% security patch compliance rate across all endpoints by administering CrowdStrike Falcon EDR alongside monthly patch and feature-update cycles via MECM/SCCM.
- Reduced unclassified sensitive-data exposure by 70% across 50,000+ data assets by implementing DSPM-driven data classification, retention, and access-governance frameworks with Varonis and Cyera, aligned with Purview-based litigation hold policy.

Infrastructure Specialist & Systems Administrator | *American Signature Inc. - Remote* **Aug 2022 - Jan 2024**

- Reduced endpoint-related incidents by 28% and sustained 99%+ uptime across 815+ Windows/macOS endpoints spanning 120 retail locations by owning full device lifecycle management - provisioning, configuration, patching, and retirement - via MECM/SCCM, JAMF Pro, and SOTI Cloud.
- Unified macOS and Windows compliance reporting into a single source of truth by leading a Jamf-to-Intune coexistence initiative, linking Jamf Smart Groups to Entra Conditional Access for real-time compliance evaluation and automated remediation.
- Enabled secure collaboration for 5,000+ users by administering SharePoint Online and Microsoft Teams - provisioning sites/libraries with metadata and versioning, managing channel access, and aligning Teams membership with SharePoint permissions.
- Improved system performance by 70% and retired end-of-life server risk across 120 retail locations by architecting a Hyper-V-based Remote Desktop Server Collection (RDSC) to replace legacy on-premises infrastructure.
- Maintained zero data-loss incidents and 100% audit-trail compliance over two years by managing Veeam Backup & Replication and Cisco Meraki network monitoring across all retail locations.
- Increased HR team productivity by 50% by gathering requirements and co-building a SailPoint/Power Automate HRIS automation application in partnership with HR, Security, and Network stakeholders.
- Resolved 500+ ServiceNow tickets/month within SLA by administering ITSM incident, change, and service-request processes, and authored runbooks/knowledge articles that cut onboarding time for new IT staff by 25%.

Information Technology Intern | *American Signature Inc. - Remote* **May 2022 - Aug 2022**

- Sustained 99%+ system uptime across 815+ endpoints by monitoring performance via MECM and network tools, proactively flagging 30+ issues/month before store-level impact.
- Reduced end-user downtime by an estimated 20% by diagnosing and resolving hardware/software issues across 50+ endpoints through structured troubleshooting.
- Cut new-IT-staff onboarding time by roughly 25% by creating and maintaining technical documentation for 10+ processes, system configurations, and network diagrams.
- Maintained data integrity across 600+ Active Directory object changes by executing user, market, and OU restructuring updates supporting the company's cloud migration to a Hyper-V RDSC environment.

AI Support Agent | *CyCobra AI - Remote (Part-time)* **Jan 2022 - Jan 2024**

- Reduced AI error rates by 30% and cut QA testing time by 40% by running structured regression testing across 8 model-review cycles.
- Resolved 85%+ of Tier 1 support tickets at first contact (50+ tickets/month) by triaging production AI issues and maintaining a 20+ article knowledge base.

TECHNICAL SKILLS

IAM & Identity Security: SailPoint IdentityNow, Azure AD (Entra ID), Azure Admin Center, Conditional Access, MFA/SSO, Zero Trust, RBAC, On-Prem Active Directory, LDAP, User Provisioning & Deprovisioning

SIEM/EDR & Data Security: CrowdStrike Falcon (EDR), Rapid7 (SIEM), Arctic Wolf (SIEM), DSPM (Varonis, Cyera, Securiti AI), Data Classification & Retention, Purview-Aligned Litigation Hold, GRC

Endpoint & Infrastructure: MECM/SCCM, Microsoft Intune, JAMF Pro, SOTI Cloud, Cisco Meraki, Hyper-V, RDSC, VMware, Windows Autopilot, BitLocker/FileVault, PowerShell Scripting

Microsoft 365 & Collaboration: SharePoint Online, Microsoft Teams Administration, Power Platform (Power Automate, Power Apps), Copilot Studio, Microsoft 365 Global Admin

AI & Automation: AI Implementation, Prompt Engineering, LLM Integration, Conversational AI/Chatbot Development, CRM Automation, GoHighLevel, Twilio A2P, n8n, REST API Integration

ITSM & Analytics: ServiceNow, JIRA, Veeam Backup & Replication, ITIL, Incident/Problem/Change Management, Power BI, KPI Dashboards, Business Intelligence

CERTIFICATIONS & CREDENTIALS

- DSPM Architect - Cyera
- DSPM Fundamentals - Securiti AI
- AI Fluency for Builders
- SaaS Workflows - SailPoint
- Discover Non-Employee Risk Management - SailPoint
- Identity Now Introduction - SailPoint
- Bloomberg Market Concepts (BMC) - Bloomberg
- Fundamentals of Alternative Investments - CAIA Association

LANGUAGES

English (Native) | Urdu (Native) | German (Full Professional) | Arabic (Professional Working) | Spanish (Limited Working)