DOMINIC M. HOANG

New York

1 (929) 520-0670, | DominicMH@pm.me
github.com/mikedominic92 | mikedominic-portfolio.netlify.app

PROFESSIONAL SUMMARY

Cybersecurity Engineer with 10+ years in Cybersecurity and Technical Support, specializing in Identity & Access Management. Hands-on experience with AWS IAM, Entra ID, Active Directory, and access governance. Focused on Zero Trust architecture, privileged access management, and cloud identity security. Integrating AI/ML for identity threat detection, anomaly-based risk scoring, and intelligent access analytics.

CORE COMPETENCIES

- **Identity Platforms**: Azure AD/Entra ID, Active Directory, Okta, AWS IAM, GCP IAM, SailPoint IdentityIQ
- **Authentication & Protocols**: SSO, MFA, OAuth 2.0, OpenID Connect (OIDC), SAML 2.0, SCIM, Conditional Access, FIDO2
- **Identity Governance**: Access Reviews, Role Based Access Control (RBAC), Least Privilege, JML Lifecycle, Entitlement Management
- **Privileged Access Management**: CyberArk, HashiCorp Vault, Just in Time Access, Credential Rotation, Session Recording
- **Automation & AI Integration**: Python, Boto3, PowerShell, Terraform, AI Powered Identity Analytics, Anomaly Detection
- **Security & Compliance**: Zero Trust Architecture, NIST 800 53, ISO 27001, SOC 2, Identity Threat Detection (ITDR)

PROFESSIONAL EXPERIENCE

AlgOPro Solutions   Jan 2024 - Present
Threat & Vulnerability Management Engineer

- Enforced Least Privilege access models using SailPoint IdentityIQ and AWS IAM Access Analyzer, resulting in enhanced security by identifying and reducing overly permissive policies across hybrid infrastructure
- Configured Identity Threat Detection and Response (ITDR) rules in CrowdStrike Falcon, improving security posture by effectively detecting compromised credentials, impossible travel anomalies, and lateral movement patterns
- Prioritized vulnerability remediation using Tenable.io and Qualys, enhancing asset security by focusing on assets with privileged access or service accounts, correlated with CVE data and identity exposure
- Investigated access-related incidents using Splunk, successfully performing root cause analysis by correlating CloudTrail logs, Azure AD sign-in logs, and Active Directory event logs, thereby improving incident response and resolution times

AlgOPro Solutions   Jan 2022 - Dec 2023
Cloud Security Engineer

- Built automated user provisioning and deprovisioning workflows using Python and Boto3, integrating with AWS IAM and Azure AD via Microsoft Graph API for JML lifecycle management
- Analyzed IAM policies using AWS IAM Access Analyzer and Policy Simulator to identify cross account trust misconfigurations and excessive wildcard permissions
- Integrated AWS CloudTrail and VPC Flow Logs with Splunk SIEM, building dashboards to monitor IAM role assumptions, access key usage, and privilege escalation attempts
- Implemented infrastructure as code security using Terraform with Checkov policies to enforce IAM guardrails in CI/CD pipelines

Amazon Web Services (AWS)   Jan 2021 - Dec 2021
Cloud Support Engineer

- Resolved cross account role assumption failures using IAM Policy Simulator and CloudTrail, diagnosing trust policy misconfigurations and implicit denies from SCPs in AWS Organizations
- Troubleshot Service Control Policy (SCP) conflicts using AWS Organizations console and CLI, helping enterprise customers implement region restrictions and service guardrails
- Debugged Lambda based credential rotation scripts written in Python/Boto3 that triggered GuardDuty findings, identifying issues with Secrets Manager integration and IAM permissions
- Diagnosed VPC Endpoint and PrivateLink connectivity issues using VPC Flow Logs and CloudWatch, restoring S3 and EC2 access while maintaining Zero Trust network segmentation

Pho House & Hong Thanh   May 2014 - Apr 2020
Technical Lead & Co Owner

- Implemented PCI DSS compliant access controls using Active Directory group policies for POS system authentication and role based permissions for payment processing
- Migrated on premises infrastructure to AWS and GCP, configuring IAM roles, service accounts, and VPC security groups for secure multi cloud operations
- Built custom iOS Point of Sale application using Swift with Python backend APIs, implementing OAuth 2.0 authentication and encrypted credential storage

CERTIFICATIONS

- Microsoft SC 100: Cybersecurity Architect Expert
- Microsoft SC 300: Identity and Access Administrator Associate
- Microsoft AZ 500: Azure Security Engineer Associate
- Google Cloud: Professional Cloud Security Engineer
- AWS: Certified Security Specialty
- CyberArk: Defender PAM
- Okta: Certified Professional
- SailPoint: IdentityIQ Associate
- CompTIA: Security+
- Cisco: CCNA