Mustafa Albassam

Somerville, MA | mustafa.s.albassam@gmail.com | 617-692-0292
LinkedIn: linkedin.com/in/mustafa-albassam
Security Clearance: Active DoD TS/SCI | Citizenship: U.S. Citizen

Professional Summary

Cybersecurity Engineer specializing in Identity and Access Management (IAM) with 10+ years of experience securing cloud and hybrid environments across DoD and commercial sectors. Expert in designing and implementing IAM strategies in AWS and Azure, enforcing Zero Trust, automating access provisioning, and integrating authentication protocols (RADIUS, SAML, OAUTH2, OpenID). Proven ability to reduce risk, streamline audits, and enforce RBAC and least-privilege access through scalable, policy-driven IAM frameworks.

Core Competencies

IAM Platforms & Controls: AWS IAM, Azure AD, Role-based Access Control (RBAC), Conditional Access, MFA, & Identity Federation.

Authentication & Federation: SAML, OAuth2, OpenID Connect, PKI, RADIUS & TACACS.

Cloud & Security Tooling: AWS KMS, GuardDuty, Security Hub, Config, CloudTrail, Macie, CloudWatch, & Control Tower.

IAM Lifecycle Automation: Terraform, CloudFormation, Lambda, & GitHub Actions CI/CD.

Security Practices & Compliance: NIST, FedRAMP, ISO 27001, RMF, GDPR, HIPAA, PCI, MITRE ATT&CK & Cloud Matrix.

Professional Experience

Principal Cybersecurity Engineer

Raytheon Missiles & Defense – Tewksbury, MA – Aug 2023 – Present

- Designed and enforced AWS IAM policy structures across multiple accounts to enable fine-grained access and adhere to RBAC and least-privilege principles.
- Collaborated with internal and external clients to design and maintain a cloud incident response playbook—improving response consistency across teams.
- Integrated AWS GuardDuty alerts, Security Hub, and Config to monitor IAM policy drift and automate incident response.
- Implemented zero-trust architecture across multi-cloud environments, reducing security incidents by 78% and achieving SOC 2 compliance in 6 months.
- Developed and deployed custom AWS Lambda functions for real-time threat detection, improving response time by 92% and saving $150K annually.

Senior Information Systems Security Officer

Charles Stark Draper Laboratory – Cambridge, MA – Aug 2022 – Aug 2023

- Hardened identity and access controls across AWS environments; remediated 200+ vulnerabilities using Inspector and Security Hub.
- Built and automated GuardDuty and CloudTrail dashboards to enable continuous monitoring—improving threat detection capabilities by 75%.
- Partnered with DevOps and security teams to automate IAM policy enforcement in CI/CD workflows.
- Created NIST-aligned contingency plans and tabletop exercises—reducing system recovery time by 60%.
- Supported audit readiness for identity-centric risks and kept key stakeholders informed of the systems' security posture.

System Analyst – Cloud Security & IAM Compliance

U.S. Army Cyber Command – Augusta, GA – Jun 2021 – Jul 2022

- Conducted identity and policy assessments across AWS and Azure environments; enforcing compliance across 50+ virtual systems.

- Deployed and maintained hybrid IAM infrastructure using AWS Direct Connect and federation protocols.
- Streamlined cloud cost and compliance by optimizing AWS resources while adhering to NIST standards.
- Addressed system vulnerabilities and created POAM items for ATO packet submission—eliminating 40% of the residual risks.
- Led hybrid cloud migration using AWS Well-Architected Tool and Direct Connect, cutting time by 30% and ensuring secure on-prem/cloud integration.

Information Security Specialist – Identity & Network Access

U.S. Army – Fort Irwin, CA – Nov 2013 – Aug 2021

- Implemented secure access control for sensitive DoD systems using RSA SecurID MFA, PKI, and role-based provisioning.
- Enforced NIST 800-37 controls across network devices and hardened perimeter defenses using Cisco and InfiniBand hardware.
- Performed IR drills and identity governance reviews to maintain 99.9% compliance with internal SLAs and regulatory frameworks.
- Guided engineering teams on cloud misconfiguration, asset visibility, and patching cadence using cybersecurity best practices.
- Supported the accreditation of cloud and on-prem services through RMF processes and advised executive leadership on NIST audit findings—reducing the security gap by 45%.

Education

- M.S. Information Systems Technology – George Washington University – 2022
- B.A. Middle Eastern Studies – American Military University – 2019

Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Ethical Hacker (CEH)
- CompTIA SecurityX
- CompTIA Security+