Salman Hersi

CLOUD SECURITY ENGINEER — AWS SECURITY, GUARDRAILS & IAM

Toronto, ON · (647) 606-2184 · hersi.salman@gmail.com · linkedin.com/in/salmanhersi · salmanhersi.com

SUMMARY

Senior Cloud Security Engineer with 6+ years reducing AWS risk across enterprise environments. Reduced high-severity Security Hub findings by 50% across 60+ accounts, cut median closure time from nine days to under four hours, eliminated stored credentials from 40+ CI/CD pipelines, and drove secure Terraform adoption across 12 engineering teams. CISSP-certified; hands-on with AWS Organizations, SCPs, GuardDuty, Security Hub, Lambda, OIDC, and Terraform.

SKILLS

Cloud security: AWS Organizations, Control Tower, SCPs, GuardDuty, Security Hub, Config, IAM, CI/CD security & OIDC federation, Terraform & Infrastructure-as-Code

Identity, detection & governance: Okta, Microsoft Entra ID, SSO, MFA, RBAC, Splunk, Microsoft Sentinel, Python & Lambda automation, NIST CSF, ISO 27001, CIS Benchmarks

EXPERIENCE

Senior Cloud Security Engineer — Miipe Quality Solutions — Mar 2024 – Present

- Reduced open high-severity AWS Security Hub findings by 50% in six months by implementing SCP guardrails, centralizing GuardDuty and Security Hub management, and standardizing logging across 60+ AWS accounts.
- Reduced median closure time for 25 recurring AWS security findings from nine days to under four hours by building Python and AWS Lambda remediation workflows with approval gates for potentially disruptive changes.
- Eliminated stored AWS credentials from 40+ CI/CD pipelines by implementing OIDC-federated IAM roles with access restricted by repository, branch, and deployment environment.
- Standardized AWS provisioning across 12 engineering teams by developing reusable Terraform modules and CI security checks that embedded encryption, logging, IAM, tagging, and network controls into deployment workflows.
- Cut average cloud security design approval time from approximately six weeks to three by introducing standardized requirements, acceptance criteria, decision logs, and cross-functional review sessions.

Cyber Security Consultant — PwC — Feb 2023 – Mar 2024

- Reduced cloud-security risk across AWS and Azure by assessing configurations, validating control gaps, and working with system owners to prioritize remediation through closure.
- Strengthened identity governance across SaaS applications by designing SSO, MFA, and RBAC patterns that standardized authentication and authorization controls.
- Automated joiner-mover-leaver processes by integrating Workday with Okta Workflows and SCIM, improving consistency across account provisioning, access changes, and deprovisioning.
- Guided technical and business stakeholders through security findings, architectural trade-offs, and remediation priorities, turning assessment results into practical implementation roadmaps.

Security Analyst — Acosta — Jan 2021 – Sep 2022

- Cut alert-to-triage time from 45 minutes to 12 by building Splunk correlation searches enriched with Microsoft Defender for Endpoint and Entra ID sign-in context, removing manual lookups for a six-person SOC.
- Flagged an offboarding gap after finding three terminated contractors with active VPN access, then built a weekly automated audit reconciling HR records against Active Directory, closing a finding external auditors had

raised twice.

- Rebuilt the 20 noisiest detection rules after a quarter in which 70% of alerts closed as false positives, dropping the rate to 22% and recovering two analyst hours per shift for threat hunting.
- Investigated and documented 150+ incidents annually across phishing, malware, and unauthorized access in Microsoft Defender and Splunk, maintaining SLA compliance and updating 10 incident-response runbooks.

Service Desk Analyst (IAM) — Toronto Community Housing Dec 2018 – Jan 2021

- Supported IT initiatives involving enterprise networking, cloud services, cybersecurity, technology procurement, and infrastructure operations.
- Enabled secure access to business systems by processing user provisioning, password resets, and approved access requests.
- Strengthened identity lifecycle controls by documenting approvals and coordinating access changes during employee onboarding and offboarding.

PROJECTS

Enterprise Cloud Security Lab — AWS Control Tower, SCPs, GuardDuty, Terraform, Python Personal project

- Built a multi-account AWS lab to test how preventive guardrails and centralized detection scale across enterprise boundaries, using Control Tower, Organizations SCPs, GuardDuty, and Security Hub.
- Codified guardrails and detections in Terraform, using the lab to validate the SCP baseline and OIDC-federated pipeline patterns before production rollout at Miipe.

EDUCATION & CERTIFICATIONS

M.S., Cybersecurity (in progress) — Georgia Institute of Technology, Atlanta, GA

Honours B.Com., Information Technology — York University, Toronto, ON

CISSP · **AWS Certified Solutions Architect – Associate** · **CompTIA Security+** · **Okta Certified Professional**