Salman Hersi

CLOUD SECURITY ENGINEER — AWS CSPM, SECURE DELIVERY & AI SECURITY

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

SUMMARY

Reduced high-severity AWS Security Hub findings by more than 50% across 60+ accounts, shortened security-finding closure from nine days to under four hours, and eliminated stored credentials from 40+ CI/CD pipelines. Cloud Security Consultant with 5+ years embedding AWS guardrails, Infrastructure-as-Code controls, and remediation automation into engineering workflows. CISSP-certified; hands-on with AWS IAM, Organizations and SCPs, GuardDuty, Security Hub, Terraform, OIDC federation, and Python/Lambda remediation automation.

SKILLS

Posture & AWS security: AWS Organizations, Control Tower, SCPs, GuardDuty, Security Hub, Config, IAM, cloud security posture management, signal-to-noise prioritization, Terraform & Infrastructure-as-Code

Secure delivery & remediation: CI/CD security, OIDC federation, stored-secret removal, finding-remediation workflows, Python & Lambda, developer enablement, incident runbooks, SSO, MFA, RBAC, NIST CSF, CIS Benchmarks

EXPERIENCE

Cloud Security Consultant — Miipe Quality Solutions — Sept 2023 – Present

- Reduced open high-severity AWS Security Hub findings by more than 50% in six months by operationalizing cloud security posture management across 60+ AWS accounts through SCP guardrails, centralized GuardDuty and Security Hub management, and standardized logging to prioritize actionable findings.
- 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.
- 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.
- 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.

Security Advisor — Mosaic North America — May 2022 – Aug 2023

- Architected and enforced IAM standards including SSO (SAML, OIDC), MFA, and RBAC for a high-volume e-commerce portfolio processing $5M+ annually, securing 250+ client web assets in alignment with the OWASP Top 10.
- Reduced identity-governance gaps by partnering with client engineering teams to embed least-privilege security into onboarding, role changes, offboarding, and access reviews for complex authorization cases.
- Turned architecture assessments for B2B clients into risk-ranked remediation roadmaps and countermeasures, giving senior stakeholders an actionable path to reduce security risk.
- Cut security-related operational overhead 40% across 50+ external e-commerce teams by leading governance workshops and building secure-access playbooks.

IT Coordinator — NPower — Jan 2021 – Dec 2021

- Improved runbook quality and incident response readiness by managing the incident response lifecycle in Jira, documenting detailed case notes, and developing SOPs that established clear alert escalation pathways.

PROJECTS

Enterprise Hybrid Security Platform — Proxmox, AWS, Terraform, Ansible, Wazuh, Splunk, Keycloak — Personal project

- Built an enterprise-style hybrid security platform to test IAM, detection, and response controls across 10+ VMs spanning Proxmox and AWS; connected sites with WireGuard and managed infrastructure with Terraform and Ansible.
- Centralized telemetry from Windows, Linux, AWS CloudTrail, Sysmon, and network devices in Wazuh and Splunk, then authored MITRE ATT&CK-aligned detections, threat-hunting workflows, and incident-response playbooks.
- Prioritized vulnerability remediation across Windows, Linux, and cloud workloads through continuous scanning, configuration hardening, and fix validation.
- Secured a private Qwen 3.5 AI workload on Apple Silicon using Ollama, evaluating prompt-injection failure modes and enforcing audit logging, network segmentation, vulnerability scanning, and SIEM monitoring.

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**