Markus Holmgren Senior Cloud Security Engineer

Bellevue, WA · markus.holmgren@gmail.com · +1 425-555-0148 · linkedin.com/in/markusholmgren

PROFILE SUMMARY

- **Senior Cloud Security Engineer** with **7 years of experience** securing the **AWS and Kubernetes platform** behind a **global identity service**, specializing in **workload identity**, **EKS hardening** and **multi-region network design**.
- Hands-on with **AWS** (IAM, Organizations, KMS), **Amazon EKS** with Kyverno and Falco, **Terraform** with OPA policies, **HashiCorp Vault** for secrets and **Splunk** for detection, scripting in **Go** and Python.
- Deep expertise in **IRSA and short-lived credentials**, **admission policy design**, **FedRAMP High boundary controls** and **key rotation at scale**, built on **NIST 800-53** and the **CIS EKS Benchmark**.
- Works with **SRE**, **platform engineering**, **product security** and the **FedRAMP compliance team**, leading threat models for new services and joining the bridge on any high-severity cloud alert.
- Mentors **3 engineers** on the cloud security team, runs a **quarterly EKS game day**, owns the **Terraform guardrail library** other teams build on, and holds the **CCSP** and **CKS** certifications.

TECHNICAL SKILLS

Cloud Platforms & Frameworks:	AWS, AWS Organizations, NIST 800-53, FedRAMP High, CIS Benchmarks
Identity & Access:	AWS IAM, IRSA, IAM Identity Center, Okta Workforce Identity, SCPs
CSPM & CNAPP:	Prisma Cloud, AWS Security Hub, AWS Config
Containers & Kubernetes:	Amazon EKS, Kyverno, Falco, Trivy, Sigstore Cosign
IaC & Policy-as-Code:	Terraform, OPA/Rego, Conftest, Atlantis
Network & Encryption:	AWS KMS, HashiCorp Vault, Transit Gateway, AWS PrivateLink, AWS Network Firewall
Detection, Logging & Scripting:	Splunk, Amazon GuardDuty, AWS CloudTrail, VPC Flow Logs, Go, Python

EDUCATION

University of Washington — B.S. in Informatics — Seattle, WA · Sep 2015 to Jun 2019

ISC2 and The Linux Foundation — CCSP and CKS certifications — Bellevue, WA · 2023 and 2024

WORK EXPERIENCE

Okta — Senior Cloud Security Engineer — Bellevue, WA · Mar 2022 to Present

- Rolled out **Kyverno** admission policies and Falco runtime rules across **Amazon EKS** clusters in 9 regions, blocking privileged pods and unsigned images, and cut critical runtime alerts by **71%**.
- Replaced static AWS keys in service pods with **IRSA** and short-lived roles, retiring **1,450 long-lived access keys** across production accounts with no customer-facing downtime.
- Led threat models for **22 new services** before launch, writing the account layout and network rules each one had to follow inside the **FedRAMP High** boundary.
- Moved signing and database keys to customer-managed **AWS KMS** keys with automatic rotation and put service secrets in **HashiCorp Vault**, cutting secrets older than a year from **3,200 to 40**.
- Wrote **OPA/Rego** policies that check every **Terraform** plan in Atlantis for public endpoints and wildcard IAM before apply, which stopped **600+ risky changes** in 2025.

Tenable — Cloud Security Engineer — Columbia, MD · Jun 2019 to Feb 2022

- Set up **Prisma Cloud** on 60 AWS and Azure accounts behind the company's SaaS products, and brought high-severity misconfigurations down from **480 to 52** with owner-assigned fix dates.
- Moved internal admin tools off public load balancers and behind **AWS PrivateLink** and an identity-aware proxy, closing **23 internet-facing endpoints** in one quarter.
- Wrote **Splunk** detections on CloudTrail for root logins, disabled logging and unusual AssumeRole chains, cutting the time to spot cloud account misuse from 2 days to **3 hours**.