+1 (425) 555-0197
daniel.star@email.com
linkedin.com/in/danielstar
Seattle, Washington, USA
U.S. Citizen

DANIEL STAR

SENIOR CLOUD SECURITY ENGINEER

SUMMARY

Senior Cloud Security Engineer with over 8 years of experience architecting, implementing, and securing AWS and Azure environments. Deep expertise in identity and access management, cloud network security, infrastructure as code (Terraform) hardening, and compliance with frameworks such as SOC 2, ISO 27001, and NIST. Proven record of reducing risk exposure through automation, incident response, and collaboration with DevOps and platform teams. Adept at designing security controls for containerized applications and implementing effective security monitoring across cloud-native platforms.

WORK EXPERIENCE

Senior Cloud Security Engineer | CloudStratus Solutions
May 2021 - Present

Lead engineer responsible for cloud security architecture and operations in multi-cloud (AWS & Azure) environments supporting SaaS and enterprise workloads.

- Designed and implemented least privilege IAM strategies across AWS and Azure, reducing excessive permissions by 60%
- Deployed and managed cloud-native network segmentation and WAF controls, resulting in a 45% improvement in detection and blocking of malicious traffic
- Developed automated CI/CD security checks using Terraform, Sentinel, and custom policy-as-code, accelerating secure deployments by 40%
- Collaborated with DevOps and platform engineering to embed container security in Kubernetes clusters using admission controllers and scanning tools
- Coordinated successful SOC 2 and ISO 27001 audits by leading technical evidence collection and policy reviews
- Led incident response for cloud-focused security events, decreasing mean time-to-remediation by 30%

Cloud Security Engineer | NextGen Fintech
March 2018 - April 2021

Implemented cloud security controls, monitoring, and incident response for AWS-based fintech platforms serving millions of users.

- Developed and maintained IAM policies, SSO integrations, and MFA enforcement, increasing compliance across critical services
- Hardening of VPCs, subnets, and security group configurations leading to measurable reduction in lateral movement risk
- Automated audit and remediation of misconfigured S3 buckets and IAM roles using Lambda and CloudFormation
- Supported regulatory compliance by mapping controls to NIST and SOC 2 requirements
- Monitored and triaged security events using AWS Security Hub and GuardDuty, leading to improved detection and faster response times
- Partnered with software engineering teams to embed secure coding practices and threat modeling into SDLC

Security Engineer | BluePeak Technologies
January 2016 - February 2018

Assisted in cloud migration projects, focusing on security baselining, IaC controls, and incident handling.

- Conducted security assessments of cloud architectures and implemented security best practices during migration
- Created and maintained Terraform templates to enforce infrastructure security baselines
- Configured and managed cloud firewalls and network ACLs to segment resources and control access
- Supported vulnerability management and remediation workflow for cloud-based assets
- Participated in post-incident reviews and root cause analyses for security events

PROJECTS

Automated Cloud IAM & Policy Management Platform
github.com/danielstar/cloud-iam-platform

Developed an automated toolchain for managing and auditing AWS & Azure IAM policies using Terraform, Sentinel, and Python. Achieved zero critical IAM misconfigurations in production by providing continuous policy validation and drift detection.

Kubernetes Security Blueprint for Cloud-Native Applications
github.com/danielstar/k8s-sec-blueprint

Designed and deployed a Kubernetes security framework integrating OPA Gatekeeper policies, network policies, and automated vulnerability scanning to enforce least privilege and separation of environments. Reduced container security incidents by 50%.

CERTIFICATIONS

AWS Certified Security – Specialty | Amazon Web Services
August 2021

Validated advanced technical skills and experience in securing AWS workloads.

Certified Kubernetes Security Specialist (CKS) | The Linux Foundation
April 2020

Demonstrated expertise in securing containerized applications and Kubernetes platforms.

Microsoft Certified: Azure Security Engineer Associate | Microsoft
June 2019

Certification in implementing security controls and threat protection in Azure cloud environments.

EDUCATION

Bachelor of Science Computer Science | University of Washington, Seattle, WA
2011 - 2015

SKILLS

AWS Security (IAM, KMS, VPC, Security Hub, GuardDuty, WAF, S3, CloudFormation) | Azure Security (Azure AD, Key Vault, NSG, Azure Policy, Security Center) | Identity and Access Management (least privilege, RBAC, SSO, MFA) | Network security (cloud-native firewalls, segmentation, private endpoints) | Infrastructure as Code Security (Terraform, Sentinel, Open Policy Agent) | Container and Kubernetes security (OPA/Gatekeeper, admission controllers, image scanning) | Security monitoring and incident response | Compliance frameworks (SOC 2, ISO 27001, NIST) | DevSecOps automation and policy-as-code | Security audits and risk assessments