Singh D

DevSecOps Engineer, 4+ years experience
Mohali, India
https://augmntx.com/profile/devsecops-engineer-singh-d/axo27694

+91 9820045154 | hr@augmntx.com

Results-driven DevSecOps Engineer with expertise in integrating security into cloud and CI/CD environments, hardening AWS systems using STIGs, and securing Infrastructure-as-Code (Terraform) configurations. Adept at vulnerability management, security scanning, and documentation for FedRAMP Moderate compliance. Skilled in aligning processes with NIST 800-53 controls, developing security policies, and proactively addressing risks through testing, patching, and remediation.

INDUSTRIES: IT services

TECHNICAL SKILLS

• Compliance: FedRAMP Moderate NIST 800 53	3 years & 5 months
• IaC Security: Terraform	3 years & 9 months
• Vulnerability Management: Snyk Nessus	3 years & 7 months
• Security Operations: Malware analysis SIEM EDR Splunk	3 years & 9 months
• Networking & Defense: Firewalls Fortinet Cisco	3 years & 2 months

SOFT SKILLS

Soft Skills: Problem-solving, incident response, collaboration

PROJECT DETAILS

• FedRAMP Readiness — January-2022 - November-2022

Project Description: Led the FedRAMP Moderate readiness initiative for a healthcare analytics platform hosted on AWS with a multi-DMZ architecture. Implemented system hardening for AMIs using STIG benchmarks and automated patch management via AWS Systems Manager (SSM). Migrated sensitive secrets to AWS Secrets Manager to enhance credential security. Integrated tfsec into CI/CD pipelines for Terraform scanning and refactored Infrastructure-as-Code into reusable modules to improve maintainability. Managed Fortinet firewalls and AWS VPN to secure network connectivity, and supported vulnerability management efforts using Qualys for continuous risk mitigation

Responsibilities: Led FedRAMP Moderate readiness for a healthcare analytics platform hosted on AWS across multiple DMZs. Hardened AMIs using STIG benchmarks and implemented automated patching with AWS SSM. Migrated sensitive credentials to AWS Secrets Manager for secure storage and rotation. Integrated tfsec into CI/CD pipelines for Terraform code scanning and refactored IaC into reusable modules. Managed Fortinet firewalls and AWS VPN for secure network connectivity. Supported vulnerability management and remediation activities using Qualys.

Technologies: AWS (SSM, Secrets Manager, VPN), FedRAMP Moderate, STIG Benchmarks, Terraform, tfsec, Fortinet Firewall, Qualys, Multi-DMZ Architecture.

Industry: IT services

• SOC 2 & Zero Trust

Project Description: Redesigned the monitoring and alerting framework by leveraging CloudWatch, Prometheus, and Grafana to improve system visibility and incident detection. Supported SOC 2 readiness efforts and implemented Zero Trust security principles across all environments to strengthen access control and reduce attack surfaces. Established quarterly IAM and access reviews to enhance identity hygiene within AWS. Automated alert remediation workflows using SOAR tools, significantly reducing incident response time and improving operational efficiency.
Responsibilities: Enhanced monitoring and alerting by implementing and optimizing CloudWatch, Prometheus, and Grafana. Supported SOC 2 readiness and applied Zero Trust security principles across all environments. Conducted quarterly IAM and access reviews to strengthen identity hygiene in AWS. Automated alert remediation workflows using SOAR tools to reduce incident response time.
Technologies: AWS CloudWatch, Prometheus, Grafana, SOC 2 Framework, Zero Trust Security, AWS IAM, SOAR Tools (Security Orchestration, Automation, and Response)
Industry: IT services

EMPLOYMENT HISTORY

• DevSecOps Engineer

Description: Implement and maintain cloud security controls (AWS) aligned with FedRAMP Moderate & NIST 800-53. Harden systems using STIGs and industry best practices. Secure Infrastructure-as-Code (Terraform) by identifying and fixing misconfigurations. Conduct vulnerability scanning (Snyk, Nessus) and ensure timely patching/remediation. Integrate security automation into CI/CD pipelines. Perform malware analysis, incident response, and security monitoring via SIEM/EDR (Splunk). Develop and maintain security documentation (policies, SOPs, compliance evidence). Coordinate security testing (config reviews, penetration testing). Manage firewall configurations (Fortinet, Cisco) and access controls. Analyze security data and generate reports using Power BI & SQL.

EDUCATION

• Bachelors degree in Computer Science from Punjab University, Patiala 2018 - 2021

LANGUAGES

• English - advanced

END OF DOCUMENT
This PDF is automatically generated by AugmntX on 21 Nov 2026
Profile URL:https://augmntx.com/profile/devsecops-engineer-singh-d/axo27694