Role: Senior Manager/Chief Manager – Application security & DevSecOps

About GeM

Government eMarketplace is a unified digital platform that facilitates end-to-end procurement of goods and services by various government departments, organizations, and public sector undertakings (PSUs). Our Honourable Prime Minister's concerted efforts to harness the power of digital platforms to achieve 'Minimum Government, Maximum Governance' led to the genesis of GeM in 2016.

GeM provides a paperless, cashless and contactless ecosystem for government buyers to directly purchase products and services from pan-India sellers and service providers through an online platform. GeM covers the entire gamut of procurement process, right from vendor registration and item selection by buyers to receipt of goods and facilitation of timely payments. GeM has envisioned to utilise the agility and speed that come along with a digital platform created with a strategic intent to reinvigorate public procurement systems and bring about a lasting change for the underserved as well as the nation.

Built on the pillars of Efficiency, Transparency and Inclusivity, GeM has emerged as a digital tool in nation's interest, aimed at catalyzing excellence in public procurement. To know more about us, please visit- https://gem.gov.in/

You may also follow us on-:

Twitter LinkedIn Koo App YouTube Facebook

What is it like to work at GeM?

- Opportunity to work with a team of highly passionate professionals from Private and Government sector.
- Unbounded space for creativity and innovation.
- Agile and collaborative work environment
- Highly transparent and open work culture
- Work- Life balance
- Various kinds of health covers (Insurance) for individual and family
- A great opportunity to apply, learn and hone your skills.

Compensation: GeM offers competitive salary and other additional benefits

Location: This position is based in New Delhi

A broad overview of the nature of the role can be garnered from the broad outline of the primary responsibilities shared below:

Job Summary: We are seeking an experienced Senior Manager or Chief Manager for Application security & DevSecOps with a minimum of 9 years of experience in Application Security to drive building the security controls during SDLC, Vulnerability Management and Container Deployment and implementing controls across Cloud services like IaaS, SaaS & PaaS and Public cloud deployments. The ideal candidate will have a strong background in managing application security services such as DevSecOPs, Vulnerability Management, Container Security, Software composition analysis using COTS/ OSS solutions in either On-Prem or cloud high-performance environments, ensuring the efficiency, efficacy, and effectiveness of deployed security technologies either cloud native or third party. The candidate will also work on design and develop cloud platform-specific security policies, standards, and procedures for management group and account/subscription management and configuration.
You will help to utilize public cloud infra securely in conjunction with our on-premises infrastructure and develop strategic and tactical security remediation recommendations / cyber risk roadmap to address identified security gaps. Additional responsibilities will include to define & monitor security KPIs/KRAs/SLAs internal & external.

Key Responsibilities:

- Own and perform application security vulnerability management.
- Facilitate and support the preparation of security releases.
- Providing the required visibility of current state of existing vulnerabilities for complete GeM Infra and Applications universe.
- Building the required controls during IaaC deployments including image security, hardening and benchmarking.
- Liaising with product and development teams in application security and help the organization evolve its application security functions and services.
- Provide expertise in security tools for vulnerability assessment, penetration testing & application security.
- Perform vulnerability risk profiling and prioritization of vulnerabilities.
- Identifying, researching, validating, and exploiting various known and unknown security vulnerabilities on server and client side
- Develop capability to conduct Mobile Application Testing. Responsible for API testing, Application Testing.
- Oversee the development, implementation, and maintenance of vendor standard operating procedures/ run book in line with GeM policies & standards.
- Work closely with cross-functional teams while carrying out daily tasks.
- Providing communications across the organization, interfacing with stakeholders on vulnerability remediation & driving security hardening best practices
- Implementing security controls for container services such as EKS, ECS in AWS based deployments.
- Familiarity with compliance regulations and CSA (cloud security alliance) / CIS Critical Security Controls /NIST frameworks and standards.
- Candidate should have excellent troubleshooting capabilities and be experienced in diagnostic/tracing tools.
- Any other responsibility as may be assigned from time to time.

Education Qualifications

Essential: Bachelor of engineering (B.E.) or Bachelor of Technology (B.Tech.) or Master of Computer Application (MCA) from a recognized University

Professional Experience

Essential skillsets

- Minimum of 11 years of experience in Enterprise Security and Cloud Security.
- At least 3 years of experience in DevSecOps and Application Security for cloud security technologies.
- Lead application vulnerability scanning and penetration testing remediation, discover security exposures and develop mitigation plans.
- Responsible for Driving Secure by design initiatives in the organization & mentor delivery teams with right security controls to protect customer data.
- Responsible for application security reviews including Threat modelling, Code review and manual, Static & dynamic testing, code reviews across all Platforms.
- Automating the security controls during CI/CD Pipeline gaining visibility into security threats applicable by scanning images / registries, flag vulnerabilities, identify / prevent lateral movement in Container environment.
- Shall be able to identify the drifts during container deployment.
- Define data security controls for On-Prem / Cloud & Container deployments (on Open source /Off the shelf). Have detailed experience of handling SSL, PKI based encryption of data at rest, in motion and in use.
- Experience in building cloud security controls in open-source Container Environment (such as Kubernetes) either deployed in On-prem or public cloud. Strong knowledge of CI/CD Pipeline deployments.
- Responsible for development of automated security testing to validate that secure coding best practices are being used.
- Understand and implement best practices for base lining / hardening the heterogeneous environment (such as servers / VM's / Micro services).
- Manage integration with vulnerability check tools such as Static Code Analysis, Dynamic Code Analysis and Software Composition Analysis tools.
- Monitor vendor SLAs, perform regular review with vendor management and report to GeM leadership.
- Maintaining current knowledge and understanding of the threat landscape and emerging security threats and vulnerabilities.

Desirable skillsets

- Excellent analytical and problem-solving abilities.
- Effective communication and interpersonal skills.
- Familiarity with industry-standard tools and technologies.
- Proven experience in building and maintaining CI/CD pipelines for efficient software releases.

- CI/CD delivery using configuration management tools such as GitHub, VSTS, Ansible, Puppet, Chef, Salt, Jenkins, Maven, etc.
- Rich experience in Micro services Architecture, experience in designing, deploying and maintaining micro services architecture in AWS.
- Understanding of Cloud Security technologies and experience in e-commerce domain will be an added advantage.
- Vendor / contract management of IT partners through SLAs, KPIs.
- Knowledge of security and compliance requirements.
- Exposure to agile methodologies and strong understanding of Project Management processes.
- Having good understanding of Procurement processes
- Ensure to share and update the Change Request documentation.
- Strong analytical and problem-solving skills, with the ability to evaluate complex systems and make data-driven decisions.
- Experience with Dash boarding and reporting Management
- Good Communication skills.

Application for Senior Manager/Chief Manager – Application security & DevSecOps Position at Government eMarketplace, GeM

Please answer the below mentioned questions as a process to apply for your candidature and share it along with your updated resume on resume.gem@gem.gov.in.

- Your total experience:
- Your annual current CTC :
- Your annual expected CTC :
- Do you have minimum of 11 years of experience in Enterprise Security and Cloud Security?
- Do you at least 3 years of experience in DevSecOps and Application Security for cloud security Technologies?
- Do you have experience in Lead application vulnerability scanning and penetration testing remediation, discover security exposures and develop mitigation plans?
- Do you have experience in Driving Secure by design initiatives in the organization & mentor delivery teams with right security controls to protect customer data?
- Do you have experience for application security reviews including Threat modelling, Code review and manual, Static & dynamic testing, code reviews across all Platforms?
- Do you have expertise in automating the security controls during CI/CD Pipeline gaining visibility into security threats applicable by scanning images / registries, flag vulnerabilities, identify/prevent lateral movement in Container environment?
- Do you meet essential skillset requirement as specified in job description?
- Are you Open to work in Delhi?
- Do you know anyone in Government eMarketplace (GeM), If Yes, please mention the Name & Employee's current designation and Phone number.