Application Security Lead

The Lead Application Security position is responsible for providing technical leadership in securing software applications across the organization. This role involves implementing security policies, conducting security assessments, and working closely with development teams to ensure applications are designed and maintained with robust security measures. The Lead Application Security works with development teams to integrate security best practices throughout the software development lifecycle, helping to mitigate risks and protect organizational data and systems.

Key Accountabilities

- Lead the technical implementation of application security initiatives, ensuring alignment with organizational security strategy
- Design and implement security controls throughout the software development lifecycle (SDLC)
- Conduct detailed threat modeling and risk assessments for critical applications
- Perform advanced code reviews, penetration testing, and vulnerability assessments
- Lead the remediation of security vulnerabilities and track resolution progress
- Deliver application security training and mentor junior team members
- Monitor emerging threats and vulnerabilities, recommending appropriate security measures
- Collaborate with development and operations teams to embed security in the SDLC
- Provide technical guidance and mentorship to application security team members
- Implement and maintain container security policies and best practices
- Assess and enhance security measures for containerized applications
- Review and secure cloud-native application architectures

Required Education & Certifications

- Bachelor's degree in computer science, Information Security, or related field
- Industry certifications such as:
    - CISSP (Certified Information Systems Security Professional)
    - CSSLP (Certified Secure Software Lifecycle Professional)
    - GWAPT (GIAC Web Application Penetration Tester)
    - OSCP (Offensive Security Certified Professional)
    - CKS (Certified Kubernetes Security Specialist) preferred
    - Cloud Security certifications (AWS Security, Azure Security, or GCP Security) preferred

Experience

- 7+ years' experience in information technology or related field
- 5+ years' specific experience in application security
- 2+ years' experience leading technical teams or projects
- 3+ years' experience with container technologies (Docker, Kubernetes)
- 3+ years' experience with major cloud platforms (AWS, Azure, or GCP)
- Demonstrated experience securing containerized applications and microservices architectures

Technical Skills & Knowledge

- Secure Coding: Expert knowledge of secure coding practices and techniques to prevent common vulnerabilities
- Security Testing: Advanced experience with SAST, DAST, and IAST methodologies
- Threat Modeling: Strong capability in identifying threats and developing mitigation strategies
- Vulnerability Management: Expertise in managing and remediating security vulnerabilities
- Cloud Security: Strong understanding of cloud security principles and architectures (IaaS, PaaS, SaaS)
- Container Security: Expert knowledge of:
    - Container security best practices and hardening techniques
    - Container image scanning and vulnerability management
    - Kubernetes security controls and policies
    - Runtime container security monitoring
    - Container networking security
- Cloud Technologies: Proficiency in:
    - Cloud-native security controls and services
    - Infrastructure as Code (IaC) security
    - Serverless security
    - Cloud security posture management
- DevSecOps: Experience integrating security into CI/CD pipelines
- Security Frameworks: In-depth knowledge of OWASP, NIST, and ISO 27001
- Programming: Proficiency in relevant programming languages (Python, Java, JavaScript)

Technical Competencies

- Application Security Architecture
- Access Controls
- Cloud Security
- Container Security Architecture
- Cyber Resilience
- Communications Security
- DevSecOps Implementation
- Security Testing & Assessment
- Cloud-Native Security Controls
- Container Orchestration Security

Behavioral Competencies

- Technical Leadership: Ability to guide and mentor security team members
- Communication: Strong written and verbal communication skills for technical and non-technical audiences
- Collaboration: Effective partnership with development teams and stakeholders
- Problem Solving: Advanced analytical and troubleshooting capabilities
- Adaptability: Flexibility to respond to evolving security threats and technologies

Key Success Factors

- Successful implementation of application security programs
- Reduction in security vulnerabilities and incident rates
- Effective collaboration with development teams
- Positive team mentorship and knowledge sharing
- Timely completion of security assessments and remediation
- Successful implementation of container security controls
- Effective security management of cloud-native applications