CareerCross by JAC Recruitment

【1000～1400万円】Technical Security Assurance Manager（L1） Secruity

外資系生命保険会社での募集です。 金融システムのご経験のある方は歓迎です。

Job Information

Recruiter
JAC Recruitment Co., Ltd.

Hiring Company
外資系生命保険会社

Job ID
1500223

Industry
Insurance

Company Type
International Company

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
10 million yen ~ 14 million yen

Work Hours
09:00 ～ 17:00

Holidays
【有給休暇】初年度 20日 7か月目から 【休日】完全週休二日制 土 日 祝日 GW 夏季休暇 年末年始 ※詳細に関してはオフ…

Refreshed
March 13th, 2025 05:00

General Requirements

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Native

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

【求人No NJB2173962】
We are seeking an experienced and highly skilled Technical Security Assurance Manager to join our organization. As an Technical Security Assurance Manager you will be responsible for ensuring the security and integrity of our applications systems and networks. You will lead a team of security professionals and collaborate with cross functional teams to develop and implement robust security measures. Your expertise in application security will be crucial in identifying vulnerabilities assessing risks and designing and implementing appropriate security controls for our B2C and B2B applications. This is a

challenging and rewarding role that requires strong leadership technical proficiency and a deep understanding of application security best practices.

■Major Responsibilities Include:
1.Lead and manage a team of application security professionals providing guidance mentoring and support in the execution of their responsibilities.

2.Develop and implement a comprehensive application security strategy and roadmap to protect our applications systems and networks.

3.Conduct regular security assessments and penetration testing of applications identifying vulnerabilities and potential risks.

4.Collaborate with development teams to integrate secure coding practices and security controls into the software development life cycle （SDLC）.

5.Perform code reviews and security testing to identify and remediate security vulnerabilities in applications.

6.Stay up to date with the latest industry trends emerging threats and best practices in application security and recommend appropriate security solutions and enhancements.

7.Support to develop and deliver application security training and awareness programs to promote a security conscious culture within the organization.

8.Collaborate with stakeholders across the organization including developers system administrators and project managers to ensure the effective implementation of security controls.

9.Develop and maintain security policies standards and procedures related to application security.

10.Support to manage vendor relationships and assess the security posture of third party applications and services.

11.Participate in application architecture review workshops and provide review comments.

12.Review and approve application security review requests for network application exceptions and risks.

13.Support to monitor and investigate security incidents and coordinate incident response activities as necessary.

14.Prepare and present regular reports and metrics on the state of application security to senior management and stakeholders.

Required Skills

1.Bachelor's degree in Computer Science Information Security or a related field. A master's degree is a plus.

2.Proven experience （X years） in application security including hands on experience with secure coding vulnerability assessments and penetration testing.

3.Strong knowledge of web application security vulnerabilities （OWASP Top 10） and associated mitigation techniques.

4.In depth understanding of application security best practices industry standards and regulatory requirements （e.g. PCI DSS HIPAA GDPR）.

5.Experience in leading and managing a team of security professionals providing guidance and support in a dynamic environment.

6.Proficiency in security assessment tools and techniques such as static analysis dynamic analysis and manual code reviews.

7.Familiarity with secure coding practices frameworks （e.g. SDL BSIMM） and secure development methodologies （e.g. DevSecOps）.

8.Strong knowledge of network protocols web technologies and common application architectures.

9.Excellent problem solving and analytical skills with the ability to assess complex situations and provide effective solutions.

10.Strong communication and interpersonal skills with the ability to communicate complex security concepts to technical and non technical stakeholders.

11.Relevant certifications such as　CISA CISSP CSSLP CEH or OSCP are highly desirable.

12.Experience in cloud security mobile application security or secure coding training is a plus.

13.Business level English and Japanese.

Company Description

ご紹介時にご案内いたします