Cybersecurity Manager (Threat Management Focus) | N2

A Global insurance services provider

募集職種

人材紹介会社
スキルハウス・スタッフィング・ソリューションズ 株式会社

求人ID
1579526

業種
生命保険・損害保険

会社の種類
大手企業 (300名を超える従業員数)

雇用形態
正社員

勤務地
東京都 23区

給与
750万円 ~ 1500万円

勤務時間
9:00 - 18:00（Mon - Fri）

休日・休暇
Saturday, Sunday, and National Holidays, etc

更新日
2026年02月20日 14:23

応募必要条件

職務経験
3年以上

キャリアレベル
中途経験者レベル

英語レベル
ビジネス会話レベル

日本語レベル
ビジネス会話レベル

English OR Japanese speakers welcome! 英語力不問！

最終学歴
専門学校卒

現在のビザ
日本での就労許可が必要です

募集要項

A Global insurance services provider—one of the largest in the world—is seeking a **Cybersecurity Specialist / Manager** to strengthen, mature, and operate the enterprise cybersecurity environment in Japan.

Responsibilities:
- Lead and improve all ITSM processes in Japan (Incident Management, Problem Management, Change Management, Service Request Management)
- Oversee major incident management, ensuring rapid service restoration and appropriate internal and external communications
- Develop, improve, and maintain enterprise-wide disaster recovery strategies, technical recovery procedures, and resilience methodologies
- Establish and operate robust backup and recovery standards to ensure data availability, integrity, and compliance
- Act as a core leader of the Cyber Incident Response Team (CIRT), driving fast, structured, and effective incident response
- Coordinate incident management with internal stakeholders in Japan (PR, Legal, Compliance, IT teams) and global organizations (Global CIRT, Asia Cyber Team)
- Continuously improve incident response frameworks, playbooks, checklists, and escalation procedures
- Conduct post-incident reviews, identify gaps, and develop improvement plans with business and IT teams
- Plan, design, and execute cyber incident exercises for internal stakeholders and executive management
- Create advanced cyber scenarios, facilitate simulations, and promote cross-functional participation
- Strengthen organizational response capabilities through tabletop exercises and recovery validation
- Improve cyber playbooks, communication templates, and technical recovery procedures
- Oversee daily security operations (monitoring, threat response coordination, operational improvements)
- Manage Data Loss Prevention (DLP) operations: alert review, policy improvement, and incident response
- Approve and supervise security-related change requests, ensuring alignment with global and local standards
- Drive security engineering projects such as infrastructure deployment, tool upgrades, and architecture improvements
- Ensure governance, risk management, and alignment with global security standards

Why should you apply:
- Opportunity to work with global teams and great Work-Life-Balance
- Great team dynamics and learning opportunity
- Opportunities to work with World’s leading insurance company (fortune 500 company)

Company Details:
A US based world’s leading insurance providers, offering a broad range of life, health, and retirement solutions to individuals, families, and businesses. The company is heavily invested in digital transformation, utilizing advanced technologies like cloud computing, data analytics, AI, and cybersecurity to enhance customer experience and streamline operations. As part of its values, it has a strong focus on creating a diverse environment, and in particular on the appointment of women in high-level position.

Working Hours: 9:00 - 18:00 (Mon-Fri)
Working Style: 3 days’ work in office, and 2 days’ work from home
Holidays: Saturday, Sunday, National Holidays, Year-end and New Year Holidays, Paid Holidays
Services/Benefits: Transportation expenses up to 20,000 yen per month, plus Paid leave, plus social insurance (health insurance, welfare pension, and work-related accident insurance), Periodic health examination, and Employment insurance

スキル・資格

- 3–5+ years of hands-on experience in IT (security or operations preferred)
- 3+ years of practical experience in information security (including incident response or security operations)
- Experience leading cyber incident exercises (domestic and international, involving multiple stakeholders)
- Strong understanding of security operations, incident response workflows, and enterprise security technologies
- Experience with monitoring, DLP operations, and reviewing/approving security change requests
- Ability to create clear and accurate reports and presentations for both technical and non-technical stakeholders

会社説明