Security Operations Manager | SIEM & Service Delivery 独占求人

Lead security delivery, stay hands-on

募集職種

人材紹介会社
フロムホーム合同会社

求人ID
1623107

部署名
Cloud Security

業種
その他 (IT・インターネット・ゲーム)

会社の種類
大手企業 (300名を超える従業員数) - 外資系企業

外国人の割合
外国人 少数

雇用形態
正社員

勤務地
東京都 23区

最寄駅
山手線駅

給与
900万円 ~ 1400万円

勤務時間
flexible, hybrid

休日・休暇
15 days paid leave/year+

更新日
2026年11月13日 12:57

応募必要条件

職務経験
6年以上

キャリアレベル
中途経験者レベル

英語レベル
流暢レベル (英語使用比率: 75%程度)

日本語レベル
ビジネス会話レベル

最終学歴
大学卒： 学士号

現在のビザ
日本での就労許可が必要です

募集要項

We are seeking an experienced Security Operations Manager to lead the delivery and continuous improvement of enterprise security monitoring services.

This is an opportunity for a security professional who combines strong technical knowledge with proven team leadership and service delivery experience.

The role involves managing security operations initiatives, coordinating technical teams and working with stakeholders across different business functions and international locations.

Importantly, this is not a purely administrative management position. The successful candidate will remain close to the technology, providing practical guidance and occasionally becoming directly involved in resolving complex technical challenges.

Key Responsibilities

Security Operations & Service Delivery

- Lead and coordinate a team involved in delivering security monitoring and related operational services.
- Manage priorities, resources, service quality and delivery schedules.
- Coordinate the integration of new systems and security data sources into existing monitoring platforms.
- Work with internal technical teams and business stakeholders to understand requirements and resolve implementation challenges.
- Establish and monitor operational KPIs, service performance and improvement initiatives.
- Manage operational escalations and ensure service delivery commitments are met.

Technical Leadership

- Provide technical guidance on SIEM platforms, security log collection and monitoring processes.
- Support the integration of security data from cloud, on-premises and SaaS environments.
- Assist with complex troubleshooting involving log ingestion, data formatting, field mapping and monitoring accuracy.
- Review security data and monitoring results to identify opportunities for improved detection and operational efficiency.
- Work alongside engineers to resolve technical challenges and maintain reliable monitoring services.

Process Improvement & Collaboration

- Identify opportunities to improve operational efficiency through automation, standardisation and improved workflows.
- Develop and refine operational procedures, documentation and technical runbooks.
- Collaborate with security engineering, infrastructure and incident response teams.
- Support continuous improvement initiatives covering security monitoring, service quality and incident readiness.
- Communicate progress, operational issues and recommendations to stakeholders in Japan and overseas.

スキル・資格

Security Operations & Technical Knowledge

- Solid professional experience in cybersecurity, security operations, SOC environments or related technical security services.
- Practical experience working with SIEM platforms and security log management.
- Understanding of how security logs are collected, processed and used for threat detection and investigation.
- Experience integrating or troubleshooting security monitoring data from enterprise IT systems.
- Ability to investigate technical issues and communicate effectively with security engineers.

Leadership & Service Delivery

- Demonstrated experience managing people within IT operations, cybersecurity, SOC or security service delivery environments.
- Experience coordinating technical projects or services involving multiple teams and stakeholders.
- Understanding of operational service management, performance monitoring, escalation processes and continuous improvement.
- Ability to balance people management and planning responsibilities with hands-on technical involvement.
- Strong communication, organisational and problem-solving skills.

Language Requirements

- **English:** Fluent / Full professional proficiency. Comfortable conducting meetings, discussing technical issues and communicating with international stakeholders.
- **Japanese:** Conversational to business level. Able to communicate with colleagues and stakeholders in a Japanese working environment.

Particularly Relevant Experience

Candidates with experience in several of the following areas would be especially interesting:

- SIEM platforms such as Splunk, Microsoft Sentinel, QRadar or Elastic.
- Security log onboarding, data parsing, normalisation and field mapping.
- Log analysis and querying using SPL, KQL or similar languages.
- Security monitoring involving EDR, firewalls, identity systems, Windows/Linux servers and cloud services.
- AWS, Azure or hybrid enterprise infrastructure.
- SOC operations, incident response or managed security services.
- Security automation, SOAR, scripting or API integrations.
- IT service management platforms such as Jira or ServiceNow.
- Development of operational dashboards, reporting frameworks, KPIs and technical documentation.

Experience across all these technologies is **not expected**. We are particularly interested in candidates who have developed a strong technical foundation and successfully progressed into leadership or service delivery management.

Who Would Suit This Position?

This opportunity could be particularly attractive to an experienced SOC Manager, Security Operations Lead, SIEM Team Lead or Security Service Delivery Manager who enjoys both leading people and remaining involved in technical work.

You may currently work for an IT services company, systems integrator, cybersecurity provider or in an internal corporate security team.

We welcome applications from candidates with different professional backgrounds who can demonstrate a combination of practical security operations experience, team leadership and stakeholder management.

Interested in Learning More?

For further information or a confidential discussion, please apply directly through CareerCross or contact me personally at: craig@fromhome.jp

---

会社説明