



## Cybersecurity Manager (Threat Management Focus) | N2

A global automotive manufacturer

### 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

1579529

#### 業種

自動車・自動車部品

#### 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

500万円 ~ 1000万円

#### 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04月17日 09:01

### 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 automotive manufacturer is seeking a highly experienced **Cyber Security Expert** to lead and mature its Security Operations Center (SOC) function within a complex, global enterprise environment.

This is a manager-level leadership position requiring deep SOC, incident response, and security operations experience. You will oversee day-to-day SOC activities, lead security analysts and responders, optimize security tooling, and work closely with IT, risk, and cybersecurity stakeholders to safeguard the confidentiality, integrity, and availability of enterprise systems and data. The position is ideally suited for professionals comfortable operating in high-responsibility, high-visibility security environments.

**Responsibilities:**

- Lead and manage a 24/7 SOC (Tier 1–3 analysts and incident responders)
- Ensure continuous enterprise-wide monitoring, detection, and incident response
- Oversee the full incident lifecycle, including escalation, containment, recovery, and root cause analysis
- Establish and maintain SOC governance frameworks, playbooks, SLAs, KPIs, and performance metrics
- Coordinate cross-functional response efforts and ensure effective incident communication
- Manage and optimize SOC tooling (SIEM, SOAR, EDR, NDR, threat intelligence integrations)
- Drive automation and operational efficiency through process and technology improvements
- Lead proactive threat hunting and translate intelligence into enhanced detection capabilities
- Provide technical oversight on log analysis and security monitoring across key systems and networks
- Mentor, develop, and build high-performing SOC teams while fostering a resilient security culture

**Why should you apply:**

- Long term work opportunity, plus WFH available
- Great team dynamics and learning opportunity
- Opportunities to learn/brush-up English/Japanese language

**Company Details:**

A large global automobile manufacturer based in Germany. This company is Japan's leading brand, known for its high customer satisfaction performance.

**Working Hours:** 9:00 - 18:00 (Mon-Fri)

**Working Style:** Hybrid

**Holidays:** Saturday, Sunday, and 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**

- 10+ years of experience in information security or cybersecurity domains
- Minimum 5 years of leadership experience within a Security Operations Center (SOC) environment
- Strong expertise in SOC operations, incident response, and threat management practices
- Hands-on experience with SIEM, SOAR, EDR, NDR, and threat intelligence integrations
- Practical experience with Azure Sentinel or equivalent enterprise SIEM platforms
- Strong understanding of cyberattack techniques, detection strategies, and response methodologies
- Familiarity with security frameworks such as MITRE ATT&CK and Cyber Kill Chain
- Ability to interpret and analyze network and application logs (HTTP, SMTP, network telemetry)
- Strong leadership, stakeholder coordination, and decision-making capabilities

---

**会社説明**