Senior Security Operation Centre Engineer

Global Retail

Job Information

Recruiter
Skillhouse Staffing Solutions K.K.

Job ID
1582658

Industry
Retail

Company Type
Large Company (more than 300 employees)

Non-Japanese Ratio
About half Japanese

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience ~ 13 million yen

Work Hours
Flextime

Holidays
weekend, National Holidays, Year-end and New Year Holiday etc

Refreshed
March 18th, 2026 08:23

General Requirements

Minimum Experience Level
Over 3 years

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Business Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

A Global and well-known brand retail is seeking a **Senior SOC Engineer**

Responsibilities:
- Detect, assess and respond to alerts and incidents
- Perform rapid triage to determine severity, validity, and urgency of alerts
- Follow SOC playbooks and SOPs to ensure consistent triage and decision-making
- Creates custom detections aligned to the MITRE ATT&CK Framework
- Review and audit available logging to determine potential gaps in detection capabilities
- Reviews threat intel reports and feeds, makes recommendations for profile or toolset changes based on reviews
- Hunts for new threats and perform data analytics to surface activity not seen within the environment
- Performs in-depth investigations on Windows, Linux, and MacOS hosts
- Write stories for engineers to improve our SOAR environment
- Support the improvement of SOC processes through feedback and operation observations
- Acts as a mentor and escalation point for SOC engineers
- Tune security tool configuration to minimize false positives
- Collaborate with security leadership, engineering, and compliance to execute security strategies
- Assess our current cloud security and propose improvements or solutions
- Serve as a subject matter expert for security tools, applications, and processes

Why should you apply:
- Full remote work is acceptable, but must be flexible to come back to office upon request.
- There is no micromanagement in the company, candidates are free to own their own scope. Colleagues are very nice, one of best HR support system as company values human resources.
- Amazing benefits and salary revision available once a year depending on performance

Company Details:
Join a leading global coffeehouse brand in Japan where technology drives every aspect of the customer experience. As part of the IT team, you'll work on innovative systems supporting retail operations, digital platforms, and data-driven business decisions. The company offers a collaborative, dynamic environment where ideas are valued, continuous learning is encouraged, and career growth is supported through mentorship and exposure to global technology initiatives. Be part of a tech-forward organization where you can make a meaningful impact and shape the future of retail in Japan.

Working Hours: 9:00 - 18:00 (Mon-Fri)
Working Style: Remote work is allowed but candidate needs to have the flexibility to come back to HQ to work in office if required.
Holidays: Weekend, national holidays, etc.
Benefits: Salary revision once a year, bonus twice a year, incentives that may be paid according to company-wide and individual performance, Bean Stock (RSU), remote work assistance allowance, late night work allowance, childcare facility subsidy allowance, various social insurances such as employees' pension, health insurance, employment insurance, and workers' compensation insurance, corporate defined contribution pension plan, property savings system, various loan interest rate preferences, partner discount (employee discount), Partner Bean (coffee beans provided once a week for self-training), CUP Fund (mutual aid in disasters), and Benefit Station (benefits program).
Interview Process：3 rounds of interview

Required Skills

- Strong security operations experience (SOC), at least 5 years' experience focused on security operations
- Deep understanding of modern cybersecurity threat frameworks such as MTTRE ATT&CK with ability to develop detection based on attacker tools & techniques

Company Description