

## Security Engineer

Job Information

#### Recruiter

Coto World Inc.

#### **Hiring Company**

Innovation and Digital Strategy Hub

#### Job ID

1564443

#### Industry

IT Consulting

#### **Company Type**

Small/Medium Company (300 employees or less) - International Company

#### Non-Japanese Ratio

About half Japanese

#### Job Type

Permanent Full-time

#### Location

Tokyo - 23 Wards

#### Salary

7 million yen ~ 9 million yen

### Refreshed

November 19th, 2025 00:00

## General Requirements

## **Minimum Experience Level**

Over 3 years

#### Career Level

Mid Career

## Minimum English Level

**Business Level** 

# Minimum Japanese Level

**Daily Conversation** 

## **Minimum Education Level**

Bachelor's Degree

## Visa Status

Permission to work in Japan required

### Job Description

Our client is a digital innovation hub that combines advanced data science, AI, and cloud technologies to create intelligent, scalable solutions for real-world business challenges. Their teams work across industries to turn data into actionable insights that drive smarter decisions and measurable impact.

They are looking for an experienced **Senior Security Engineer** to strengthen security across our cloud-based systems and DevOps environments. You'll play a key role in defining secure development and deployment practices, conducting architecture and code reviews, and driving "shift-left" security initiatives across multiple agile teams. This role offers the opportunity to shape security strategy while remaining hands-on with tools, automation, and architecture.

#### **Key Responsibilities**

- Define and implement secure CI/CD and continuous delivery processes.
- Establish and maintain security requirements for cloud infrastructure and DevOps pipelines.
- · Conduct security architecture reviews, code assessments, and threat modeling.
- · Review and enhance application security controls and configurations.
- Develop and enforce secure coding policies, procedures, and standards.
- Collaborate with engineering teams to integrate security checkpoints into the SDLC.
- Support automation of compliance, monitoring, and alerting systems.
- Contribute to incident response planning, forensic analysis, and security testing.

### Required Skills

#### Qualifications:

- Minimum 4 years of experience in cybersecurity, including areas such as secure engineering, consulting, SOC operations, or DevOps security
- At least 2 years of leadership experience, managing or mentoring security teams and driving key initiatives
- Strong penetration testing expertise; certifications such as OSCP or CEH are a strong plus
- · Hands-on experience with vulnerability management and a deep understanding of secure engineering principles
- Working knowledge of public cloud environments (Azure, AWS, GCP, etc.)
- . Experience using SAST and DAST tools to identify and mitigate security risks
- Solid understanding of vulnerability and compliance management, patch management, anti-malware, APT defense, and identity and access control solutions
- · Skilled in threat modeling and proactive risk assessment
- Familiar with Agile methodologies and comfortable working in fast-paced, collaborative environments
- Excellent communication and interpersonal skills, with the ability to partner across teams
- Business level English (TOEIC 800+) and conversational Japanese (JLPT N3 or above)

#### Certifications:

- CISM, CISSP, CISA, or GIAC (Information Security Management)
- CEH, LPT, CEPT, or GIAC Penetration Tester (Ethical Hacking)
- CCSK, CCSP, or cloud provider certifications (Azure, AWS, GCP)
- OSCP or OSCE (Offensive Security)

#### Company Description