English Speaking Senior Security Engineer

No Japanese language skill

募集職種

人材紹介会社
株式会社PROGRE

採用企業名
Company wiht platforms automateing customer acquisition

求人ID
1619034

業種
インターネット・Webサービス

会社の種類
中小企業 (従業員300名以下)

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, 中央区

給与
700万円 ~ 1100万円

勤務時間
Flextime system; core hours 11:00–16:00

更新日
2026年11月06日 00:00

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
ビジネス会話レベル (英語使用比率: 常時英語)

日本語レベル
基礎会話レベル

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

As a Senior Security Engineer at Meetsmore, you will join the SRE team and lead security initiatives across the company. The role covers four key areas: penetration testing of our products; application security embedded in the software development lifecycle; AI security for both LLM-powered product features and AI-assisted development; and the technical

implementation of security compliance, including control implementation, automated evidence collection, and responses to engineering-related questions in audits and customer security reviews.

You will help build the security function and work closely with an SRE/DevOps team that prioritizes automation. Internal communication is primarily in English, with some Japanese and translation-tool support.

Key Responsibilities

- Lead and improve product security, including penetration testing, vulnerability assessment, remediation tracking, and verification of fixes.
- Integrate security into the software development lifecycle through threat modeling, design reviews, and automated security checks in CI/CD.
- Strengthen cloud and infrastructure security across AWS, application hosting, access controls, networking, and deployment pipelines.
- Implement and operate automated attack detection and protection, including security rules, monitoring, alerting, and incident response.
- Assess and mitigate security risks in LLM-powered features and AI-assisted engineering workflows.
- Implement technical security controls, automate audit-evidence collection, and support certification audits and customer security assessments.
- Collaborate with engineering and SRE/DevOps teams to make security practical, measurable, and automated.

Technology Stack

The following is a representative list, not an exhaustive inventory:

- Languages and application frameworks: TypeScript, Node.js, React
- Cloud and infrastructure: AWS (including ECS, CloudFront, S3, SQS, and Lambda), Vercel
- Data and caching: MongoDB, Redis
- Security technologies relevant to the role: SAST, DAST, dependency scanning, WAF, IDS/IPS, runtime application security, and SIEM

スキル・資格

Required Qualifications

- Hands-on experience building or improving security in a software development process, including threat modeling, design reviews, and CI/CD security tools such as SAST, DAST, and dependency scanning.
- Experience identifying and remediating cloud infrastructure security issues, including AWS IAM and network configuration, Kubernetes RBAC/network policies/workload permissions, and CI/CD pipeline security such as secrets management and software supply-chain protection.
- Experience implementing and operating automated attack detection and protection using technologies such as WAF, IDS/IPS, runtime application security, or SIEM. This includes rule tuning, monitoring, alerting, and responding to attacks such as SQL injection and cross-site scripting (XSS).
- Experience securing Node.js-based applications. Python or Go experience for security tooling is acceptable; TypeScript is preferred.
- Conversational Japanese proficiency or a genuine willingness to learn Japanese. Support is available.
- Currently based in Japan or willing to relocate to Japan. Relocation support is available.

Preferred Qualifications

- Experience testing or securing LLM-based features, including prompt injection, jailbreaks, data leakage, or agent-tool permissions.
- Experience leading a full penetration test from scoping through testing and reporting to verification of remediation, covering web applications, mobile applications, and APIs.
- Experience leading a full certification audit, such as ISO 27001/ISMS, ideally at a Japanese company, including control implementation, evidence collection, and direct coordination with auditors.
- Offensive security certifications such as OSCP or OSWE, or practical bug bounty/CTF experience.

会社説明