【日系テック大手】ITセキュリティエンジニア｜サイバー犯罪対策（派遣）

大規模なデジタルサービスとユーザーを守り、経験値を高められるポジションです

Job Information

Recruiter
Morgan McKinley

Job ID
1616312

Industry
Bank, Trust Bank

Job Type
Contract

Location
Tokyo - 23 Wards

Salary
Negotiable, based on experience

Refreshed
November 3rd, 2026 19:00

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

大手日系IT企業にて、フィッシング、不正アクセス、オンライン詐欺などのサイバー犯罪から大規模なデジタルサービスとユーザーを守るITセキュリティエンジニアを募集しています。

セキュリティエンジニアリング、脅威インテリジェンス、インシデントレスポンス、ソフトウェア開発を組み合わせて、実際に発生するサイバー犯罪を分析・調査し、自動化された対策を構築。

サイバーセキュリティ防衛に特化したチームの一員として、専門性をさらに高められるポジションです。

主な職務内容

- 社内セキュリティチームや外部関係者と連携し、サイバー犯罪・オンライン詐欺への対策を設計、開発、継続的改善を進めていただきます。
- フィッシングや不正キャンペーンを検知・無効化する自動分析ツールやアプリケーションの開発・運用

- OSINT、ダークウェブ、クローズドメディアのリサーチ；新たなサイバー脅威、攻撃手法、不正行為のトレンドの分析
- フィッシングサイト、不正キャンペーン、その他のセキュリティインシデントに対するCSIRT・インシデントレスポンスの実行
- 不審なアクティビティの特定やサイバー犯罪調査支援（複雑なデータソースの分析など）
- その他、セキュリティエンジニアリング、脅威分析、防御技術の専門知識を活かしてサイバー犯罪対策部門の活動に貢献すること

Join a global technology and e-commerce leader in Tokyo as an **IT Security Engineer**, helping protect a large-scale digital ecosystem and millions of users from phishing, fraud, and emerging cyber threats.

Working within a specialised **Cyber Security Defense and Anti-Cyber Crime team** , you will combine cybersecurity engineering, threat intelligence, incident response, and software development to identify malicious activity and build automated countermeasures.

This role offers hands-on exposure to **Python, SQL, OSINT, threat intelligence, CSIRT operations, phishing analysis, and security automation**. You will investigate real-world cybercrime, analyse complex datasets, research emerging threats across the open and dark web, and develop tools that strengthen anti-fraud capabilities in Japan and globally.

Key Responsibilities

- Design, develop, and continuously improve **anti-fraud and cybercrime countermeasures** through collaboration with internal security teams and external partners.
- Build and maintain automated analysis tools and security applications using **Python and data-driven techniques** to identify and disrupt phishing and fraudulent campaigns.
- Conduct **OSINT, dark web, and closed-media research** to identify emerging cyber threats, attack techniques, and fraud trends.
- Perform **CSIRT incident response** for active phishing websites, fraudulent campaigns, and other cybersecurity incidents.
- Analyse complex datasets using SQL and investigative techniques to identify malicious activity and support cybercrime investigations.
- Apply knowledge of **HTTP, TLS, SMTP, and DNS** to investigate network and web-based fraud techniques.
- Support collaboration with relevant external organisations and provide technical analysis that can contribute to law enforcement actions and criminal investigations.
- Contribute cybersecurity engineering, threat research, and defensive expertise to the dedicated Anti-Cyber Crime function.
- Identify opportunities to automate repetitive investigation and response processes, improving the speed and effectiveness of cyber defence.

Required Skills

必須条件 経験・資格：

- サイバーセキュリティ、サイバー犯罪対策、セキュリティエンジニアリングまたは関連領域での技術・エンジニアリング経験3年以上
- Pythonのプログラミング経験3年以上
- SQL上級（データ分析や調査クエリなど）
- サイバー攻撃やオンライン詐欺で利用されるネットワーク・Webプロトコルの知識（HTTP、TLS、SMTP、DNSなど）

ソフトスキル：

- 顧客・ユーザーファーストの視点で、チーム体制でサイバー防衛に取り組む姿勢
- セキュリティ施策やプロジェクトを推進するリーダーシップ
- 常によりよいものを目指す、継続的改善意欲
- Code of Ethicsを遵守する倫理意識

語学力：

- **日本語：**ビジネスレベル以上（チーム内の連携や技術コミュニケーションができるレベル。母国語でない場合、JLPT N1〜N2目安）
- **英語：**ビジネスレベル

歓迎条件

- Java、C/C++、C#、Go、Ruby、Perl、Bash、PowerShellなど、Python以外のプログラミング言語の経験
- オブジェクト指向プログラミング（OOP）の実務経験
- CSIRT、SOC、セキュリティインシデントレスポンスまたはB2C/B2B環境でのセキュリティ対応経験
- サイバー犯罪、不正アクセスなどに関連する日本の法律・規制に関する知識

採用企業について
大手日系IT企業。

数億人規模のユーザーが利用するデジタルサービスを展開しています。

大規模なデジタルプラットフォームを安全に運営するため、サイバーセキュリティは重要な事業領域となっています。

大規模なデータと最新のセキュリティ技術を活用しながら、グローバルチームと協働してサイバー犯罪対策の専門性を高められる環境です。

この求人がおすすめの理由
- 大規模なデジタルサービスとユーザーをリアルなサイバー犯罪から守る経験を積める
- 現代的なインテリジェンスツールや自動化フレームワークに携われる
- CSIRT・犯罪対策のプロが集まったチームで専門性を高められる
- テックドリブンな企業文化で働きやすい

転職のご相談もお気軽にどうぞ。 Required Skills and Qualifications **Experience:**
- **3+ years of technical or engineering experience in cybersecurity, cybercrime defence, security engineering, or a related field**.
- **3+ years of hands-on Python programming experience** , including development of tools, applications, or automation.
- Strong SQL skills for data analysis, investigative queries, and working with complex datasets.
- Strong understanding of network and web protocols commonly associated with cyber threats and fraud, including **HTTP, TLS, SMTP, and DNS**.
- Practical understanding of cybersecurity investigations, threat analysis, anti-fraud activities, or incident response.
- Ability to combine software engineering and cybersecurity knowledge to develop practical defensive solutions.
- Bachelor's degree or equivalent qualification.

Soft Skills:
- Strong team orientation with a **customer-first mindset** and the ability to collaborate effectively across technical and non-technical teams.
- Leadership potential and the ability to take ownership of security initiatives and project activities.
- Analytical and investigative mindset with a strong interest in understanding complex cyber threats.
- Passion for continuous improvement, technical innovation, and ongoing learning.
- Strong professional integrity and commitment to maintaining a rigorous **Code of Ethics**.
- Proactive problem-solving approach with the ability to investigate unfamiliar threats and develop practical countermeasures.

Language Requirements:
- **Japanese:** Intermediate to business-level proficiency required, ideally **JLPT N1-N2**, for team collaboration and technical communication.
- **English:** Intermediate to business-level proficiency for communication within an international technology and cybersecurity environment.

Preferred Skills & Qualifications
- Programming experience with additional languages such as **Java, C/C++, C#, Go, Ruby, Perl, Bash, or PowerShell**.
- Practical experience with object-oriented programming (OOP).
- Hands-on experience in **CSIRT, cybersecurity incident response, or B2C/B2B security operations** .
- Knowledge of Japanese laws and regulations relating to cybercrime, cybersecurity, and unauthorised system access.
- Experience developing security automation, threat analysis, or investigative tools.
- Familiarity with OSINT methodologies, threat intelligence platforms, or dark web research.
- Experience investigating phishing, online fraud, account abuse, or other cybercrime activity.

About the Company
Our client is a **global technology and e-commerce leader** operating an extensive ecosystem of digital services used by millions of customers.

With large-scale digital platforms and continuously evolving technology, protecting users and services from sophisticated cyber threats is a critical business priority. Its dedicated Cyber Security Defense function combines **security engineering, threat intelligence, incident response, automation, and anti-fraud expertise** to address real-world cybercrime.

You will join a technically focused environment where cybersecurity professionals work with large datasets, modern security technologies, and international teams to strengthen the organisation's global cyber defence capabilities.

Why You'll Love Working Here
- Take on a **high-impact cybersecurity role** directly protecting millions of users and a large-scale digital ecosystem from real-world cybercrime.
- Work with **Python, SQL, OSINT, threat intelligence, CSIRT, and security automation** in a hands-on engineering environment.
- Join a specialised anti-fraud and Cyber Security Defense team focused on phishing, fraud, and emerging cyber threats.
- Work with large-scale datasets, modern threat intelligence capabilities, and automated security frameworks.
- Gain opportunities to lead high-visibility cybersecurity initiatives and collaborate with international security teams.
- Build specialist expertise spanning **cybercrime investigation, incident response, software engineering, and threat intelligence**.
- Work in a technology culture focused on engineering excellence, continuous learning, and innovation.
- Benefit from **flex time, minimal overtime, and casual clothing** .

Don't Miss Out - Apply Now!

Company Description

Morgan McKinleyは国際的な人材コンサルティング会社として、さまざまな業界・分野をリードする採用企業様と、スペシャリストとしてのスキルを有する人材とを結びつけるお手伝いをしています。1988年の創立以来、Morgan McKinleyの名は、「卓越した質のサービス」「市場知識の豊富さ」「No.1企業であり続けようとする強い意志」、そして何よりも「実績」を体現する会社として知られています。

リクルーティング スペシャリストである弊社コンサルタントまでお気軽にお問い合わせください。