【SOC・CSIRT/業務委託】暗号資産×金融システムのセキュリティ運用｜六本木・フレックス

24/365一次対応は専門チームが担当、インシデント対応・リスク管理に携わる

Job Information

Hiring Company
MONEY PARTNERS CO.,LTD.

Job ID
1615986

Division
システム運用部

Industry
Other (Banking and Financial Services)

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

Job Type
Freelance

Location
Tokyo - 23 Wards, Minato-ku

Salary
Negotiable, based on experience ~ 10 million yen

Work Hours
フレックス制

Holidays
会社の規定に準ずる

Refreshed
November 9th, 2026 00:00

General Requirements

Minimum Experience Level
Over 1 year

Career Level
Mid Career

Minimum English Level
Daily Conversation Level

Minimum Japanese Level
Native Level

Minimum Education Level
High-School

Visa Status
Permission to work in Japan required

Job Description

金融サービスのセキュリティ運用経験を、暗号資産という新たな金融領域へ

創業16年の実績を持つマネーパートナーズでは、暗号資産交換業（現物取引・販売所モデル）の本番運用開始に向け、セキュリティ運用体制の構築を進めています。

本案件では、SOC / CSIRT等で培ったセキュリティ運用の専門性を活かし、SIEMやAWS等を活用したインシデント対応、ログ分析、証跡・リスク管理などを支援いただきます。

なお、24時間365日の監視・一次対応は専門チームが担当。本案件では専門チームからエスカレーションされた案件の調査・対応や、関係者との連携、セキュリティ運用・リスク管理に携わっていただきます。

金融システムに求められるガバナンスを前提に、暗号資産という新しい金融領域のセキュリティ運用に専門人材として関われる案件です。

具体的な業務内容

1．セキュリティ監視

- SIEM、WAF、IDS/IPS、EDR等のアラート監視
- AWSセキュリティサービスの監視
- 不正アクセス、不正ログイン、不審通信の検知
- セキュリティイベントのトリアージ
- 専門チームからエスカレーションされた事象の確認・対応

2．インシデント対応

- セキュリティインシデントの初動対応
- 影響範囲の調査
- ログ分析および原因調査
- 関係者へのエスカレーション・連携
- インシデント管理票の作成・更新

3．セキュリティ運用

- アクセス権限管理の確認
- 脆弱性情報の収集および影響分析
- パッチ適用状況の確認
- セキュリティ設定レビュー
- 証跡管理

4．レポーティング・リスク管理

- 日次・週次・月次報告
- セキュリティレポート作成
- 監査対応資料作成支援
- システムリスク管理資料作成支援

※暗号資産交換業に係るシステムとして、日本金融庁、JVCEA、監査法人対応を前提とした運用体制の構築を進めています。一般的なSOC業務に加え、システムリスク管理、インシデント管理、証跡管理、委託先管理等の運用プロセスにも関与いただきます。

※稼働率：100%（応相談）

【雇用形態】
正社員

【給与】
経験考慮の上、応相談

【就業時間】
フレックス制

【勤務地】
東京都港区六本木
※基本的には出社（フレックス制）
※リモートは応相談

【休日休暇】

- 完全週休2日制（土日祝）
- 有給休暇（最大20日）
- 連続休暇5日間
- 慶弔休暇
- 年末年始休暇
- 介護育児休暇及び生理休暇
- 特別休暇（会社が認める日数）
- 育児休業

【待遇・福利厚生】

- 社会保険完備（雇用保険・労災保険・厚生年金・健康保険）
- 交通費全額支給（非課税限度額まで）

- 住宅補助手当（一定基準を満たした方）
- 服装自由
- 健康診断/インフルエンザ予防接種　費用負担
- リフレッシュルームあり
- 個人ロッカー・キャビネット貸与
- 女性はトイレロッカー貸与

- ウォーターサーバー、冷蔵庫、電子レンジ
- ビルラウンジ使用可

【選考について】

- 募集人数：1～2名
- 開始時期：応相談
- 書類選考→一次面接（COO）→最終面接→内定
  ※スピーディーな選考を実施しています。

Required Skills

【必須要件】

- セキュリティ運用（SOC、CSIRT、セキュリティ運用部門など）の実務経験
- セキュリティインシデントへの対応を、検知から復旧・再発防止まで、主担当として経験していること
- インシデントを関係者へ報告・連携した経験
- 技術的な内容（状況・自分の判断・相手への依頼事項）を正確に伝えられること

【歓迎要件】・SIEM、EDR、IDS / IPSのいずれかの運用経験

- AWSのログ・権限の仕組み（CloudTrail、IAM、Security Groupなど）を理解し、調査に使った経
- 験
- 暗号資産交換業、ホットウォレット運用、オンチェーン取引の追跡に関する実務経験
- 暗号資産の取引所システム、入出金、ウォレット運用の仕組みを、自分の言葉で説明できること（実務経験は問いません）
- 金融機関・決済事業者でのセキュリティ運用、またはシステムリスク管理の経験
- 委託先（ベンダー）管理、委託先の運用品質を検証した経験
- 指示を受けずに、自らセキュリティ上の課題を見つけて改善した経験
- Pythonなどによるログ分析・運用の自動化の経験
- 資格：情報処理安全確保支援士、CISSP、GIAC、CEH、AWS認定（Security - Specialty）、CCNA

【求める人物像】

- 「アラートが出たので報告した」で終わらず、自分で調べ判断し報告まで完結できる方
- 指示を待たず、課題を自ら発見して解決に動ける方
- 一人で抱え込まず、必要な場面では早めに関係者と連携できる方
- 委託先の結論も鵜呑みにせず、根拠を確かめる姿勢を持つ方
- 新しい攻撃手口や技術を学び続ける意欲のある方

Company Description