サイバーセキュリティ・リード (DFIR) | 世界最大級金融サービス

個性を尊重する環境で、人々の暮らしに貢献しながら成長できる

募集職種

人材紹介会社
スキルハウス・スタッフィング・ソリューションズ 株式会社

求人ID
1616950

業種
銀行・信託銀行・信用金庫

会社の種類
大手企業 (300名を超える従業員数)

外国人の割合
(ほぼ) 全員日本人

雇用形態
正社員

勤務地
東京都 23区

給与
経験考慮の上、応相談 ~ 1300万円

勤務時間
9:00 – 18:00

休日・休暇
Saturday, Sunday, and National Holidays, etc

更新日
2026年11月24日 04:00

応募必要条件

職務経験
10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

日本語レベル
流暢レベル

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

世界最大級金融サービス企業では、**サイバーセキュリティリード**を募集しています。
本ポジションは、Cyber Defense & Response 組織におけるデジタルフォレンジクスおよびインシデントレスポンス (DFIR)領域のマネージャーとして、高度な技術チームを率い、企業全体のサイバーインシデント対応能力を継続的に強化

していく役割です。
インシデント対応においては、シニアレベルの意思決定者としてエスカレーション案件を判断・指揮しつつ、中長期的にはインシデントレスポンスプログラム全体の成熟度向上（プロセス、体制、技術の強化）をリードしていただきます。
また、チームメンバーの技術力とキャリアの成長を重視しており、社内トレーニング、ナレッジ共有、メンタリングなどを通じて、専門性の高い人材を育成することも重要なミッションです。
そのため、深い技術的専門性に加え、状況を俯瞰して整理する力、関係者と合意形成を進めるコミュニケーション力、多様性を尊重したリーダーシップ、そして常に進化する脅威や技術を学び続ける姿勢が不可欠です。

業務詳細
- グループ生命保険各社、情報セキュリティオフィス（ISO）、グローバルテクノロジーチームと連携し、サイバーインシデント対応を統括・調整し、迅速かつビジネス影響を考慮した対応を実現する
- Cyber Security Operations Center（CSOC）や各部門、外部パートナーからエスカレーションされる重大インシデントに対する最終判断・意思決定を担う
- 新しい業務プロセスや技術導入において、インシデントレスポンス能力を組み込むための体制整備・成熟度向上施策を推進する
- 調査案件のライフサイクル全体を管理し、ドキュメント作成、レポーティング、証拠管理（チェーン・オブ・カストディ）などを法規制・監査要件に沿って確実に運用する
- テクノロジー、法務、プライバシー、広報などと連携し、サイバーリスク・業務リスクを含む横断的なリスクマネジメントを主導する
- 事後分析やKPI、脅威インテリジェンスを活用しプロセス改善やレジリエンス向上施策を継続的に実施する
- 新技術や脅威動向に関する専門知識を活かし、調査の方向性を示すとともに、チームの技術的成長を支援・牽引する
- サイバーセキュリティの原則、フレームワーク、業界トレンドに関する知識を維持・発信し、組織としての対応レベルを先進的な水準に保つ

ポジションの魅力：
- 一人ひとりの意見が尊重され、日々の業務が人々の体験や生活をより良く変えていく文化を持つチームの一員として活躍できます
- あなたのスキルを最大限に活かしながら、技術力とリーダーシップの両面を伸ばせる学習機会を通じて、さらに大きなインパクトを生み出せる環境があります
- 堅牢で安定した組織だからこそ提供できる成長機会に、きっと驚いていただけるはずです

会社概要
米国に本社をおく世界最大級の金融サービス機関として2008年に創設され、グローバル企業として海外のパートナーとも積極的に連携しながら、今日まで日本のグループ各社にITシステム基盤サービスを提供してきました。「お客さまの経済的な保障と心の平和」を守りたいというグループ各社の強い想いをしっかりと受け止め、テクノロジーとビジネスの双方を支えるパートナーとして、安定し信頼のおけるシステム基盤サービスを提供し続けることを使命としていま

勤務時間： 9:00 – 18:00
勤務スタイル： ハイブリッド（※週に1～2回の出社、月に0～2回の休日出勤があります）
休日休暇： 土・日・祝日、年末年始、有給休暇、その他特別休暇
待遇・福利厚生： 社会保険完備、DC年金プラン、交通費支給、スキルハウス大学、テストペイバックシステム 等

スキル・資格

必須スキル
- 大規模エンタープライズまたは政府機関において、サイバーインシデントレスポンスおよびデジタルフォレンジクスの実務経験10年以上（複雑で分散型のITインフラ環境での経験を含む）
- 技術チームのリーダー／マネージャーとして5年以上の経験を有し、メンバー育成、組織能力の強化、運用品質の向上をリードしてきた実績
- ID基盤：Entra ID（Azure AD）、Active Directory
- クラウド：Azure、AWS
- 業務基盤：Microsoft 365
- OS：Windows / Linux / macOS
- SIEM、EDR、検知基盤における高度なクエリ・検知設計スキル（SPL、KQL などを用いた検知ロジックや調査クエリの設計・運用経験）
- Python、PowerShell、Bashなどを用いたスクリプト作成・自動化の実務経験（調査・対応・運用改善目的）
- X-Ways、EnCase、KAPE、The Sleuth Kit、Volatility など、主要フォレンジクスツールの豊富な実務経験（商用・オープンソース不問）
- 日本語・英語で技術者・経営層の双方に対して、調査結果やリスクを明確に説明できる能力
- MITRE ATT&CK や Cyber Kill Chain などを活用し、攻撃手法を踏まえた検知・調査・対応戦略を実務で構築してきた経験

会社説明