CareerCross

SOC アナリスト

募集職種

人材紹介会社
株式会社NEX-GEN

求人ID
1494354

業種
SIer・システムインテグレーター

会社の種類
外資系企業

雇用形態
正社員

勤務地
東京都 23区

給与
600万円 ~ 1500万円

更新日
2024年09月13日 01:56

応募必要条件

職務経験
3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

最終学歴
高等学校卒

現在のビザ
日本での就労許可は必要ありません

募集要項

標準 MDR サービスの一環として、L3 SOC アナリストを募集しています。

プロジェクト テクノロジーは Microsoft Sentinel です。

お客様はグローバルな製薬会社であるため、ドメインに関する知識や経験があれば有利になる可能性があります。

Cyber-proof は、安全なデジタル エコシステムを構築することで、お客様がより迅速かつスマートに対応し、セキュリティの脅威に先手を打てるように支援することを使命とするサイバー セキュリティ サービスおよびプラットフォーム企業です。Cyber-proof は、プロセスを自動化して脅威を早期に検出して優先順位を付け、迅速かつ断固とした対応を行います。

Cyber-proof は、セキュリティ インシデント、違反、疑わしい活動を監視、調査、解決する、成長を続けるグローバル オペレーション & デリバリー チームの一員となる SOC L3 エンジニアを募集しています。当社のグローバル オペレーション グループは、革新的なアプローチを採用し、最先端のテクノロジーを使用して、お客様の業務を変革し、セキュリティ環境を保護します。

【主な職務】
・重大度の高いセキュリティ インシデントのエスカレーション ポイントとして機能し、潜在的な影響を判断して侵害の範囲を理解するために徹底的な調査を実施します。
・攻撃パターン、ツール、テクニック、手順 (TTP) を分析して、攻撃方法と攻撃ライフサイクルを特定します。
・セキュリティ制御ポリシーの構成変更やセキュリティ衛生の改善などの問題解決活動に関する推奨事項を提供します。
・セキュリティの脆弱性に関連するリスクを軽減するためのガイダンスを提供します。
・クライアントの環境内で侵害の兆候 (IOC) と高度な持続的脅威 (APT) の兆候を探します。
・詳細なログ分析による脅威ハンティングを実施し、自動検出を回避した可能性のある潜在的な脅威を特定します。
・分析を実施して証拠を収集し、根本原因を検証し、クライアントのセキュリティ ツール セットを活用して侵害の範囲を分析します。
・既存のセキュリティ プロセスのギャップと弱点を特定し、クライアントの確立されたインシデント対応方法を改善するための強化策を提案します。
・部門横断的なチームと連携して、セキュリティ インシデントのライフサイクルをエンドツーエンドで管理します。
・インシデント対応プロセスを文書化して更新し、将来の参照用に結果を定義し、継続的な改善を推進します。
・定期的なチーム会議、インシデント対応の戦略会議、およびエグゼクティブ ブリーフィング セッションに参加します。
・グローバル SOC チームの一員として SOC L3 アナリストとして最低 2 年以上の経験があります。
・セキュリティ インシデントの解決と修復に関する推奨事項を解決、エスカレーション、報告、および提示します。
・クライアントの調査のエスカレーション ポイントとなり、パフォーマンスを向上させるための最適化活動を提案します。
・サービスに参加している顧客からの脅威や疑わしいイベントを積極的に監視および確認します。
・異常なアクティビティや疑わしいアクティビティがないか、システム ログ、SIEM ツール、ネットワーク トラフィックの高度な監視を行います。
・SIEM ソリューションを設定し、接続の問題をトラブルシューティングします。
・事後分析を提供して問題と可能な解決策を明らかにし、セキュリティ違反を調査して解決します。
・セキュリティ インシデントとイベント データを照合して、月次例外レポートと管理レポートを作成します。
・定義済みのエスカレーション プロセスを使用して、未解決のネットワーク セキュリティ エクスポージャー、リソースの不正使用、または非準拠状況を報告します。
・セキュリティ ツールの使用、セキュリティ レポートの準備、セキュリティ問題の解決について、チーム メンバーを支援してトレーニングします。
・セキュリティ システムと手順に関するドキュメントを開発および維持します。

スキル・資格

- SOC L3 アナリストとして最低 2 年以上の経験
-プロフェッショナルで積極的かつ個人的なサービスを通じて、優れた顧客満足度を維持できる対応力
- QRadar、ArcSight、RSA、LogRhythm などの SIEM ベンダーの経験 (2 つのツールの経験が望ましい)
- インシデント対応、および手順のランブックとプレイブックの作成の経験
- 顧客の IT チームおよびセキュリティ チームと連携できる能力

会社説明