【セキュリティアナリスト】セキュリティ最先端・脅威インテリジェンスにも携われるポジションです！

Job Information

Hiring Company
GRCS Inc.

Job ID
1580054

Division
GRCSソリューショングループ

Industry
IT Consulting

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

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards, Chiyoda-ku

Salary
5 million yen ~ 7 million yen

Work Hours
コアタイムなしフルフレックス制（1日の標準労働時間8時間）

Holidays
完全週休2日制（土日祝）

Refreshed
May 12th, 2026 12:00

General Requirements

Minimum Experience Level
Over 3 years

Career Level
Mid Career

Minimum English Level
Daily Conversation

Minimum Japanese Level
Native

Minimum Education Level
High-School

Visa Status
Permission to work in Japan required

Job Description

≪募集要項・本ポジションの魅力≫

- 脅威インテリジェンスやASM分析を担うセキュリティアナリスト職
- 最先端の脅威情報を扱い顧客の安全を直接支援できるやりがい
- 内製ツール開発や上流工程にも挑戦でき専門性を高められる環境

- フルリモート×フルフレックス制、資格支援や在宅手当も充実

【業務内容】
セキュリティアナリストとして、脅威インテリジェンス分析サービスとAttack Surface Management(ASM)サービスのアナリスト業務をご担当いただきます。
サイバーセキュリティに関する脅威インテリジェンス、脆弱性情報等の技術的な内容をリサーチしアラートを送付したり、クライアント向けにレポート作成を行うポジションとなります。
脅威インテリジェンス分析サービス、ASMサービスを行うにあたり、SaaS製品で実装されていない機能を内製開発する業務も発生いたします。

■想定業務：

１．脅威インテリジェンス分析サービスのアナリスト業務

- 脅威インテリジェンス製品（SaaS）のアラートトリアージ（優先順位付け）および顧客への通知業務
- 月次・四半期レポート作成（アラートや脅威アクタの分析報告）
- プレ調査、顧客アセットの初期セットアップ、更新対応
- ベンダーへの問い合わせ（英語含む）や顧客対応

２．ASMサービスのアナリスト業務

- ASM製品のアラートトリアージおよび顧客通知
- 新規IT資産の発見と通知、傾向分析のレポート作成
- 攻撃表面リストの作成や顧客問い合わせ対応

３．内製ツールの要件定義・設計支援

- 脅威インテリジェンス分析業務・ASM業務を支援する内製ツールの要件策定および基本設計
- 開発部門との連携（簡単なスクリプト作成スキルがあれば尚可）

■募集背景：
社会情勢の変化に伴いセキュリティ対策への関心の高まりから、弊社セキュリティソリューションへの引き合いを多くいただいております。お客様の7割は大手企業グローバル企業で直受けのプロジェクトになっております。より多くのお客様の声にお応えし、日本企業の「守り」の部分を強化するというミッションをともに実現してくれる仲間を募集しています。

■所属部署：
＜GRCSソリューショングループ＞
約120名のコンサルタント/エンジニア/オペレーターが所属する組織です。 GRC及びセキュリティに関するコンサルティングサービスを提供しております。 8部門に分かれており、各部のマネージャーが営業を担っています。 グループ長はエンジニア出身で外資系企業にてセキュリティ部門のトップを務めていた技術に深い方です。 弊社のコアビジネスとなる部門で、今後も積極的に最新技術を取り入れたソリューション提供を行っていく予定です！ またGRCにおいて長年サービス提供をしてきたコンサルタントも多数所属しております。 部門間でのナレッジシェアも活発でGRC×セキュリティを得ることでさらに市場価値を高めることができます。

■この仕事で実現できること：

- 最新の脅威インテリジェンスおよびASMに関する高度な専門知識の習得
- グローバルセキュリティベンダーとの連携による実践的な知識や経験の向上
- 顧客のセキュリティ強化を直接支援し、社会に安全を提供するやりがい
- 内製ツールの開発を通じた技術力や設計力の向上

■今後のキャリアパス例：
毎期初にマネージャーと今後のキャリアパスについて検討し、方向性を決めていきます。

- 脅威インテリジェンスやASM領域の専門家として成長しPM/PLとしてチームを率いていく/メンバーの育成などマネジメント業務を行う
- 顧客のセキュリティ戦略策定を支援するセキュリティコンサルタントへのキャリアアップを目指す
- 内製ツール開発やセキュリティエンジニアリング領域への転向
- 開発部門や自社プロダクトの企画・設計に携わるキャリア
- 英語でのやり取りや外国からのサイバー攻撃なども調査する場合があるため、知識を身に付けてグローバル案件に積極的に関わっていく

【雇用形態】
正社員
※試用期間あり、3ヶ月（期間中の給与等の待遇に違いはありません。）

【給与】
年収：5,000,000 円 - 7,000,000円
■昇給：年1回（給与改定）
■賞与：年2回（基本給の2カ月分）

【就業時間】
コアタイムなしフルフレックス制（1日の標準労働時間8時間）
※業務時間はプロジェクトや常駐先の勤務形態によります。

【勤務地】
東京都千代田区丸の内１丁目１−１ パレスビル 5F
■敷地内禁煙
※お客様先に常駐の可能性もあります

【休日休暇】 ※正社員の場合
（SOC担当はシフト制勤務となるため適応外。就業時に勤務形態について説明させていただきます。）

- 年間休日120日以上
- 完全週休2日制（土日祝）
- 年末年始休暇
- 慶弔休暇
- 有給休暇（入社時に付与）
- 産前・産後休暇（取得・復帰実績あり）
- 出生時育児休業（産後パパ育休、取得・復帰実績あり）
- 育児休暇（取得・復帰実績あり）
- 介護休暇

【待遇・福利厚生】　※正社員の場合

- フルフレックス制（コアタイム無し、標準労働時間8時間）
  ※SOC担当はシフト制勤務となるため適応外。就業時に勤務形態について説明させていただきます。
- 社会保険完備（雇用・労災・健康・厚生年金）
- 交通費全額支給
- 時間外手当支給
- 在宅勤務制度
- 在宅勤務手当支給（通信費として3000円/月支給）
- 資格取得支援制度（受験料・更新料会社負担/奨励金有）
- 時短正社員制度（1日6時間勤務ペース）
- オンライン社内イベント
- 部活動補助金制度（アウトドア部、ビリヤード部等活動中！）
- インフルエンザ予防接種補助
- 社員紹介制度
- 最新セキュリティ動向勉強会
- EAP/社員支援プログラム制度
- 企業型確定拠出型年金制度（選択制DC）

Required Skills

【必須要件】

- 3年以上のネットワーク機器やサーバーの構築/運用業務経験
- 合わせて、下記いずれかの実務経験　1年以上
  - 脅威インテリジェンスレポート作成経験
  - セキュリティインシデント対応、マルウェア解析などの業務経験
  - ペネトレーションテストの業務経験
  - セキュリティ診断（WEBアプリケーション、プラットフォーム/ネットワーク）の業務経験
  - SOC等でのセキュリティ監視やインシデントハンドリングの業務経験

【歓迎要件】

- サイバーセキュリティ領域の実務経験
- セキュリティ/ネットワーク製品の提案、導入経験
- Pythonを使用したツール・システム（特に基盤領域）の開発・運用経験
- PM／PL経験
- 英語でのレポート作成経験（英語力（TOEIC 800以上））

【求める人物像】

- サイバーセキュリティ分野において新しい知識の習得が好きな方/積極的に行える方
- プロフェッショナルとして責任感をもって仕事に取り組める方
- 新しい製品やプロジェクトに積極的にチャレンジできる方
- チームワークを大切にできる方
- 自発的かつ自律的に活動を行い、自ら積極的に問題解決にあたることができる方

【選考について】

- 募集人数：1名
- 選考フロー：
  １．書類選考
  ２．1次面接+適性検査
  ３．2次面接
  ４．内定
  ※面接は全てオンラインで行います

Company Description