脅威インテリジェンス分析官（募集番号：MSS202508c ）

POINT

9割リモート/最先端のサイバー攻撃動向を調査/Tier1プロバイダであるNTTのネットワークを活かした脅威調査/
業務時間内での自己研鑽時間◎/ライフワークバランス◎

募集背景・求める人物

近年では、高度化・複雑化するサイバー攻撃に対抗するために、国内外のセキュリティベンダーがペネトレーションテストや脆弱性診断・脅威インテリジェンス提供等の幅広いセキュリティサービスを提供しており、サービス品質はベンダー独自の知見をフィードバックできるかに左右されます。
NTTセキュリティ・ジャパンでは、大手民間企業や官公庁などのお客様に対して２０年以上、幅広いセキュリティ対策サービスを提供しており、得られた知見を用いてサービスの品質向上に努めています。

こちらのポジションでは、国内唯一のTier1プロバイダであるNTTのグローバルIPネットワークを活かし、サイバー攻撃に関わる脅威分析及び分析レポートの生成に関わる方を募集します。
調査対象の１つとして、国家支援が疑われる標的型攻撃者グループ（APT）があります。さまざまなソースから取得した情報を多角的な視点で分析し、顧客にレポートします。
セキュリティに関する強い興味関心があり、顧客と中長期的な関係を構築していける方を募集します。

業務内容

標的型攻撃者グループ（APT）の動向や攻撃キャンペーンに関わる情報をさまざまなソースから収集し、その分析結果をレポートにまとめ報告する業務。
OSINTやクローズドな情報源から得た情報、通信ログ、セキュリティデバイスログ、その他センサーから得たデータを横断的に解析し、付加価値の高い独自のレポートをアウトプットします。
攻撃手法（TTPs）の解析に継続的に取り組み、最新の情報をタイムリーに顧客に届けるため、以下の業務をお任せします。

（担当範囲は、経験・専門性・希望を勘案のうえ、ご相談可能です。）
①OSINT、その他情報源（脅威インテリジェンス製品、その他センサー）等から得る情報の収集・分析
②攻撃手法（TTPs）の解析
③分析レポートの作成、及び顧客向け報告
④分析ツールの作成、データ解析プラットフォームの構築、運用

協力会社等含め約20名のプロジェクトに加わり、上記いずれかもしくは複数業務をお任せします。

この仕事の魅力

◆官公庁向けにサービス提供をするため、自身が分析したレポートが日本のサイバーセキュリティの向上に直結します。
◆最新の脅威動向をキャッチアップできる
国外の最先端のセキュリティ製品の動向把握・提案機会に加え、クローズドなカンファレンスに参加する機会があります
◆社内関連組織のみでなく、社外のトップレベル人材と交流する機会があります。
また、BlackHatなどの海外カンファレンスの参加や SANS などの社外研修の参加を含め、業務時間内に技術動向の調査や自己研鑽する時間を取り入れています。
◆在宅勤務・フレックスタイム制の活用、積極的な有給消化の推進を行っており、ライフワークバランスのとりやすい環境です。

キャリアパス

本ポジションで配属となるマネージドセキュリティサービス部では、SOC（Security Operation Center）サービスのほか、そこで活用されるシステム開発や
脆弱性情報の提供、トレーニングサービスの提供など、幅広いセキュリティサービスを提供しています。
また、社内にはそれ以外に、IoT/OT領域のセキュリティサービスやOSINTモニタリング等の脅威情報分析・提供など「サイバーセキュリティ」に関するあらゆる事業展開を行っています。
セキュリティアーキテクト業務を通じて高度なセキュリティ領域の知識・技術を習得いただく中で、将来的に、ご自身の興味がより強くなった分野への挑戦も可能です。

当社のセキュリティテクニカルブログはこちら：https://jp.security.ntt/tech_blog

応募条件

【必須要件】
以下のすべてのご経験・スキルをお持ちの方
・サイバーセキュリティにかかわる基礎知識に加え、ネットワーク/Webセキュリティ/データ解析のいずれかへ強い興味を持つ方
・事象を正確に捉え、データや根拠とともにロジカルに説明できる方
・英語ドキュメントの読解に忌避感の無い方
・顧客と中長期的な関係を構築するため、粘り強く業務に取り組める方

【歓迎要件】
・サイバー攻撃関連技術（リモートエクスプロイトを代表とする攻撃や、Post-exploitation で用いられるツールやテクニック、マルウェア感染およびボットネットの仕組みと、悪性サイトの役割および対策技術 等）に関する正しい知識をお持ちの方
・マルウェア解析、ネットワーク攻撃解析などを自ら実施し、そこで得た情報をもとに技術レポートを作成した経験がある方
・コンサルティング業務にて、顧客とのフロント業務の経験がある方
・ナショナルセキュリティ（国家安全保障）に興味関心のある方
・英語でご自身の専門領域に関するコミュニケーション（質疑応答）が可能な方□

募集要項

募集者	NTTセキュリティ・ジャパン株式会社
雇用形態	正社員
契約期間	期間の定め無し（定年60歳、再雇用制度有）
給与	年収：500万円～1,200万円 ■月給 基本給（役職給）：280,000円～ 勤務実態に応じて支給：時間外手当、休日手当、深夜手当、リモートワーク手当等 ■賞与（業績給）：年に一度、成果達成度合いに応じて支給
退職金	無し
勤務地	東京本社　（変更範囲：全国の当社拠点）
在宅勤務等	在宅勤務制度有　※実施率９割以上
転勤	当面無し
試用期間	有（4カ月）
就業時間	試用期間中：9:00～17:30（休憩60分） 試用期間後：フレックスタイム制（コアタイム無し）
時間外労働	有（平均20～30時間/月）
休日	年間休日数：120日完全週休二日制（土日祝）
年次有給休暇	入社直後最低13日付与（日数はご入社時期によって変動）
特別有給休暇	夏季休暇、年末年始休暇、ライフプラン休暇、病気休暇、特別休暇　他
社会保険	健康保険・厚生年金・雇用保険・労災保険完備
福利厚生	・企業年金基金 ・社員持ち株会 ・資格取得支援制度 ・研修支援制度 ・時短制度（一部従業員利用可） ・住宅手当（自身で賃貸契約をしている、もしくは家賃負担をしている方で カフェテリアプランの住宅補助を選択されている45歳迄の方へ支給） ・副業可（許可制）　他
ワークライフバランス	在宅勤務・フレックスタイム制の活用、積極的な有給消化の推進を行っており、ライフワークバランスのとりやすい環境です。
副業	可（許可制）例：本の執筆・大学での講師等
研修	業務時間の20%を自己研鑽に充てる取り組みを行っております。 数多くの研修プランや講義を揃えており、ご自身の興味のあるものを受講いただく事が可能です。 研修や資格取得に対しては費用補助もございます。
コミュニケーション	■部門 リモートワークが主体となるので、Teamsなどコミュニケーションツールを活用し、意見交換などはしやすい環境を整えています。 また、月に1～2度オンサイトでオフィスに集まって交流もしています。 ■会社 四半期に一度の懇親会や、サークル活動（例：ボルダリング）などを通して部門を超えた交流も盛んです。
受動喫煙対策	屋内全面禁煙
選考フロー	書類選考→1次面接→2次面接 （面接は原則オンラインでの実施となります）※1次面接後、適宜バックグラウンドチェックを実施
会社について	NTTセキュリティ・ジャパンは2013年に設立され、NTTグループにおけるセキュリティ事業の中心的枠割を担っています。 設立以来25年以上セキュリティ分野のリーディングカンパニーとして、欧米エリアを中心に事業を拡大し、APAC（Asia Pacific）にも展開しています。 全世界の社員数は約870名であり、うち500名以上はセキュリティ専門のコンサルタントや業界屈指のセキュリティアナリスト等のスキルを持った人材です。 全世界15ヶ国に広がる本支社、世界7ヶ国に設置したグローバルリスクオペレーションセンタに、上述の社員のうち200名以上のセキュリティエンジニア、 並びにリスクアナリストを配置し、24時間365日、顧客企業のセキュリティ監視と全世界のセキュリティ動向を観測しています。