セキュリティアナリスト（リサーチ・解析） （募集番号：MSS202504c）

POINT

9割リモート/マルウェア解析・レポーティング/セキュリティカンファレンス/業務時間内での自己研鑽時間◎/ワークライフバランス◎

募集背景・求める人物

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、幅広いセキュリティ対策サービスを提供しています。
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、24時間365日体制での顧客企業のセキュリティ監視や全世界のセキュリティ動向観測とレポート、
脅威ベースのペネトレーションテスト・脆弱性診断・脅威インテリジェンス提供等の幅広く高いレベルのセキュリティ対策ニーズが高まっています。

こちらのポジションでは弊社が提供するセキュリティサービス・機器から収集されるログ・ネットワークパケットの分析や、サイバー攻撃で利用される最新の技術や脅威動向を追跡し、レポート・対外発表を行います。
さらなる事業拡大とお客様・日本のサイバーセキュリティ体制強化に向けて、**サイバーセキュリティに携わるものとして高い倫理観及び責任感をお持ちで、**
技術的な報告書の作成経験を有する方等、即戦力としてご活躍頂ける方を募集します。

業務内容

当社では、お客様である大手企業や官公庁のサイバー攻撃の脅威から守るため、複数の先進的なサービス展開を行っています。
こちらのポジションでは、その中で下記の業務をお任せします。

・セキュリティ製品（ファイアウォール、IPS、サンドボックス、EDR など）やプロキシサーバ等のログ、ネットワークパケットを分析し、「攻撃の有無、その手法、影響度、情報漏えい」等についてのレポート作成
・サイバー攻撃で利用される最新の技術や脅威動向を追跡し、マルウェアや攻撃ツールを解析し、その挙動や機能についてレポート作成
・上記の業務を通して培ったデータベースを活用し、攻撃者グループの特定などを行い、ブログやホワイトペーパーの執筆、セキュリティカンファレンスなどでの発表

調査や解析には、専用の調査PCの他に IDA Pro、VirusTotal、ANY.RUN を含む様々な有償ツールや SOC で観測したデータを活用し、
日本を代表する大企業や官公庁といったお客様をサイバー攻撃から守ることが業務となります。
また、業務遂行のための教育トレーニング(SANS, Hack The Box など)も幅広く用意されており、マルウェア解析や脅威リサーチなどのスキルアップが可能です。
お客様をサイバー攻撃から守るため、アナリスト同士で解析手法や調査手法などを議論しながら、業務を行います。

業務内容について詳細はこちら：https://jp.security.ntt/tech_blog/soc-reseacher
公式Xアカウント：https://x.com/NTTSH_JP

この仕事の魅力

◆最新の技術・脅威動向をキャッチアップできる
日本を代表する大企業や官公庁の顧客のセキュリティを守るミッションクリティカルな業務であり、標的型攻撃をはじめ多種多様な攻撃を観測分析するため、最新の技術や脅威の動向を追跡します。
世の中でニュースになるようなインシデントの背後で活躍する場合もあります。
◆個々のスキルを極限まで高めながらチーム一丸となって切磋琢磨し、楽しく業務に取り組むことができる
各領域のプロフェッショナルが社内にはそろっており、顧客から求められるレベルも高いため、社員同士の相乗効果を期待する風土です。
◆業務時間の20%を上限に興味のある分野について自己研鑽の時間に充てることができる
個々人が興味がある、もしくは専門性を磨きたい分野については積極的にインプットし市場価値を高めるとともに業務に活かしていただくことを推奨しています。

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、標的型攻撃をはじめ多種多様なサイバー攻撃を観測・分析しており、最新の技術や脅威動向を継続的に追跡しています。
マルウェア解析、OSINT調査、脆弱性の検証などを通じて、未知の攻撃手法や検知手法の調査・解析に取り組むことが可能です。
また、日本唯一のTire1プロバイダであるNTTのグローバルIPネットワークのバックボーンを活かした脅威調査にも取り組んでいます。
得られた技術・知見は、国内外のセキュリティカンファレンスや自社発行ホワイトペーパー、技術ブログなどを通じて発信する機会があり、実践的なスキルを高めながらセキュリティ業界でのプレゼンス向上やキャリア形成に繋げることができます。

カンファレンス講演実績：CODE BLUE、Japan Security Analyst Conference (JSAC)、Virus Bulletin Conference。Security Analyst Summit(SAS) など多数

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
・一般的なサイバーセキュリティの知識
・技術的な報告書の作成経験
・サイバーセキュリティに携わるものとして高い倫理観及び責任感
・業務に関する知識や技術を習得する意欲

【歓迎要件】
・マルウェア解析、またはセキュリティ製品のアラート分析の業務経験
・ネットワークパケットやアセンブラを理解できる方
・WindowsOS上のアプリケーションを開発した経験がある方
・英語での読み書き及び会話が流暢にできる方
・地政学、外交、安全保障に関する業務経験あるいは研究実績がある方

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：550万円～900万円 ■月給 基本給（役職給）：300,000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
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、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。 入社頂いてすぐの期間は、業務引継ぎをスムーズに行うため、先輩社員が同じ時間帯で勤務します。 ■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→技術試験→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、適宜リファレンスチェックを実施
会社について	NTTセキュリティ・ジャパンは、NTTグループのセキュリティに関わる高度な人財と研究開発成果、 そして20余年以上にわたるサイバー脅威との戦いで磨き続けてきた独自のサイバーインテリジェンスと脅威検知・対応能力を結集した、サイバーセキュリティ専門事業者です。 リスク予測から診断、防御、脅威検知、インシデント対応、復旧までの一貫した「プロアクティブサイバーディフェンスサービス」の提供により、 お客様・社会を守り、安心・安全なデジタル社会の実現に貢献します。