セキュリティアナリスト（募集番号：MSS202503）

POINT

9割リモート/経験者募集/SOC（Security Operation Center）で解析業務/業務時間内での自己研鑽時間◎/チームで業務課題解決

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、SOC（Security Operation Center）で24時間365日シフト体制で顧客の環境に対するサイバー脅威を監視・分析する業務をご担当頂きます。
監視・分析業務のほかにも、業務効率化・技術向上に対する取り組み（WANTS）をする時間を業務時間内に別途設けています。
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、ログ分析、マルウェア解析のご経験があり、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。
お客様のセキュリティ機器やサーバ等から、リアルタイムにログを受信し、そのログを分析することによりサイバー攻撃から、お客様を守るサービスを提供しており、
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。

①監視業務（業務の7～8割）
セキュリティオペレーションセンター（SOC）にて、サイバー脅威を分析する業務をお任せします。
具体的には、EDR、IPS、Sandbox 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てインシデントを発見し、発生事象、情報漏えいを調査し、お客さまにレポート通知します。
②WANTS（業務の2～3割）
アナリスト同士でチームを組み、以下のような活動に取り組みます。
・完全独自 SIEM のチューニング、SIEM 検知ロジック作成・IPS カスタムシグネチャ作成、EDR カスタム IoC 作成・マルウェア解析・脅威情報リサーチ、OSINT調査
・脆弱性の検証・解析＆検証環境構築・分析効率化ツール開発・外部講演、カンファレンス発表・海外 SOC との情報交換会や技術交換留学・新サービス検討　など

（活動内容の一例）
・外部講演、カンファレンス発表
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を調査し、国内外のカンファレンスや自社発行ホワイトペーパー、技術ブログなどのメディアで発表することができます。
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
・分析効率化ツール開発
高度な相関分析を実現するためのSIEMロジックの考案や解析ツール、普段の業務を効率化する自動化ツールも自分達で開発・運用しています。
開発言語・フレームワーク：Python、JavaScript/TypeScript(Node.js, React) 等

組織構成：
30～40名の組織でマネージャーが4名います。監視・分析業務については、24時間体制でサービス提供する為2交代制となっています。※残業全社平均で25h程

業務内容について詳細はこちら：https://jp.security.ntt/tech_blog/102gm2e
日々変化する攻撃に対して、アナリスト同士で議論し、切磋琢磨しながらチーム一丸となって、業務を進めることができます。各自に解析用 PC も別途支給されます。

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、実際に対応する
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、SOC（Security Operation Center）での監視業務・WANTSを通してサイバーセキュリティ領域の最新の知識・技術を習得することが可能です。
また、NTTセキュリティ・ジャパンでは、SOCで活用されるシステム開発や脆弱性診断情報の提供、
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幅広いサービス提供・研究を行っているため、
ゆくゆくは興味のある分野に特化した部門へのキャリアチェンジなども可能です。

応募条件

【必須要件】
下記、いずれかを満たす方
(1)コンピュータサイエンスに関係する学部卒の学位もしくは相当する経験
(2)情報セキュリティに関する強い興味関心
(3)ソフトウェア/Web アプリケーション開発経験（言語、規模は不問）がある方
(4)インフラ（ネットワーク/サーバ）運用経験のある方
(5)SOC や CSIRT にてアラートの分析経験のある方
(6)脆弱性診断の経験がある方
(7)フォレンジック経験のある方
(8)マルウェアの解析経験がある方
(9)弊社技術blogの内容に興味・関心をお持ちの方
技術blog：https://jp.security.ntt/tech_blog

【歓迎要件】

・IT 技術が好きで、物事をロジカルに深く追及することができる方
・ネットワークパケットやアセンブラを理解できる方
・脆弱性診断業務経験（Web アプリ、プラットフォーム不問）のある方
・SOC やインシデントレスポンスチームでの勤務経験
・セキュリティに関するアプライアンスもしくはクラウドでのサーバ等インフラの運用経験
・セキュリティカンファレンスなどの登壇経験
・CTF や競技プログラミングなどのコンテスト出場または運営経験
・英語でのコミュニケーションに抵抗のない方
・中国語、ロシア語などの外国語でセキュリティ関連技術文書の読解が可能な方

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：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	シフト制（日勤　9:00～17:30、夜勤　17:00～翌10:00） 夜勤は2日分の勤務としてカウントし、翌日はお休みになるよう調整します。
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。 アナリスト保有資格：CISSP、GIAC GREM、情報処理安全確保支援士、博士（情報学）等
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→最終面接 （面接は原則オンラインでの実施となります）
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。