セキュリティアーキテクト（募集番号：MSS202506c）

POINT

9割リモート/最先端のサイバー攻撃動向・脅威情報を調査/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

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、脅威ベースの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、数あるセキュリティサービスの中でも、
サイバー攻撃に関わる一連の挙動を正しく理解し、さまざまな組織が収集する各種脅威インテリジェンスを横断的に解析し、新たな知見を創出して結果をお客様に提供します。
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、**セキュリティに関する強い興味関心があり、自身で考え、顧客への付加価値を創出に意欲のある方**を募集します。

業務内容

官公庁や国内大手企業向けに提供する脅威インテリジェンスサービスの設計・開発・運用をする部門において、下記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。）

①サイバー脅威インテリジェンスの収集
②脅威の分析
③顧客への分析結果報告および対策等の提案
④顧客の対策・対応の支援（助言）
⑤上記で使用する手法・環境・ツールの高度化検討（考案・開発・継続的改善）
　例：外部脅威インテリジェンスが提供するAPI等を活用したデータ収集、ダークウェブやSNS等での脅威（情報漏洩・フィッシング・攻撃予告等）監視
　　生成AI等を活用した、脆弱性情報の組織影響評価～アドバイザリ作成
　　大量のセキュリティログ等の処理の高速化・効率化
　　海外ベンダの先進的な脅威インテリジェンスプラットフォームの発掘・検証評価

１案件につき7~8名のチームで動き、無償有償問わず世の中の多くの脅威インテリジェンスを収集していただきます。世界におけるサイバー攻撃の動向を把握し、
その結果得られた知見を、官公庁や企業にとって活用しやすい情報として提供して頂きます。
ゆくゆくは、顧客に対してより魅力的な脅威インテリジェンスサービスの企画立案・設計開発もご担当頂きたいと考えております。

※脅威インテリジェンスサービスとは：サイバー攻撃者の手法・環境・技術・動機、最新の脆弱性等に関するデータを収集・分析し、

この仕事の魅力

◆官公庁・大企業向けにサービス提供をするため、自身のフィードバックが日本のサイバーセキュリティの向上に直結します。
◆脅威インテリジェンスサービスでは情報を収集するだけでなく、取捨選択が重要となるため、
　ご自身の知見・チームの知見を発揮して深めて頂くことがサービスの質向上につながる、介在価値のある業務です。
◆社内関連組織のみでなく、社外のトップレベル人材やお客様とも相談しつつ、データ収集から解析に必要な技術の研究開発や実用化を実施する機会があります。
　また、業務時間内に自己研鑽する時間を取り入れており、業務・自己研鑽を通してスキル向上して頂ける環境があります。

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）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】

サイバー攻撃技術への強い興味をお持ちの方で、以下のいずれかを満たす方
・サイバーセキュリティにかかわる基礎知識をお持ちの方
・セキュリティ対策を目的としたIT システム（製品を含む）の構築、または運用経験のある方
・ネットワーク/システム/Web セキュリティやデータ解析への強い興味

【歓迎要件】

・サイバー攻撃にかかわる情報収集や解析業務経験をお持ちの方（左記のための環境構築やツール作成、プログラミングの経験があれば◎）
・法人向けセキュリティ対策製品の構築、または運用経験のある方
・企業 CSIRT、またはそれに準ずるセキュリティ組織/部門での業務経験（情報収集、インシデント対応等）のある方
・IT 系システムに関する法人顧客向けフロント SE（設計・構築）・運用・保守の経験のある方
・英語のドキュメントを読み解く力をお持ちで、可能であればご自身の専門領域に関する英語の会話を聞き取れる方

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：500万円～900万円 ■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、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。