インシデントレスポンスコンサルタント（募集番号：PF202503b）

POINT

9割リモート/官公庁・大企業向けのインシデントレスポンスサービス/案件充実で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およびお客様の業務への対応として、インシデントレスポンスの支援を多数のお客様から求められています。

今回のポジションでは、弊社へのご相談件数の増加において、弊社コンサルティングリソース強化が急務となっていることから、
セキュリティコンサルタントとして、大手民間企業や公官庁などのお客様に対して、インシデントレスポンス業務を担って頂ける方を募集します。

業務内容

弊社で提供するインシデントレスポンスサービスにて、インシデント対応方針策定サポート、ディスクフォレンジック、ネットワークフォレンジック、マルウェア解析などの解析業務です。インシデントが発生した顧客に対して、ヒアリング実施、対応方針策定からインシデントクロージングまで対応するため、技術だけでなくコンサルタントとしての経験を積むこともできます。希望に応じて顧客対応はせず、解析業務のみを担当することも可能です。ディスクフォレンジック、ネットワークフォレンジック、マルウェア解析、OSINTなど様々なプロフェッショナルフィールドに精通したエンジニアが集まるチームで切磋琢磨することができます。

＜解析業務＞
顧客と策定・合意した対応方針に従い、次のような解析業務を実施

ディスクフォレンジック、ネットワークフォレンジック、マルウェア解析、Compromise Assessment、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、新サービス検討など

＜その他活動内容例＞
・Compromise Assessmentツール開発
標的型攻撃など高度な攻撃に対する安全宣言を行うため、Compromise Assessment によるエンドポイントの網羅的な解析を行っています。Compromise Assessment は自社で開発したツールを使用し全エンドポイントから情報収集・解析をしています。これによりEDRでは見つけられないサイレントバックドアを見つけ出します。データ収集ツールは、C/C++/C#/Python で実装しており、本ツールのアップデートやメンテナンスなどの業務も行っています。最新の攻撃手法を情報収集し、その手法を見つけ出すためのテクニックを即時ツールに落とし込むことは、とても充実感のあるお仕事です。

・品質確保活動
ディスクフォレンジックは、個々人の技術に頼りがちです。当然属人的な領域は存在しますが、非常にセンシティブ、プレッシャーのかかる業務であるインシデントレスポンスにおいて、個々人の負担を軽減するため品質チェックリストを作成しています。最低限実施すべき調査についてチェックリストを使用し、組織として顧客に提供すべき最低限かつ高レベルな品質確保を実現しています。本チェックリストは攻撃者の動向や新たなフォレンジックテクニックの登場に応じて随時アップデートします。これらのメンテナンスも業務の一つです。

・CTFへの参加
DEFCON(Pwn, Rev)、HTB(主にForensic, Rev)、Mandiant(Rev) が開催する CTF に参加しています。大会によっては業務として参加しています。解法はチーム内で共有し、Give&Take を原則にチーム全員の技術力が向上するよう取り組んでいます。なお、CTFや自己研鑽の一部は業務の一環として実施可能であり、スキルを向上させるための環境を整えています。

・カンファレンスへの参加、資格取得支援
業界の最新情報を収集するため、Blackhat などの著名カンファレンスに参加や、高度資格の取得を推進しています。これらにかかる費用は会社負担としているため、費用の心配なくご自身のスキルを伸ばすことが可能です。

この仕事の魅力

◆コンサルティングはもちろん、NTTグループ内のソリューションをフル活用し、顧客の課題解決に深く関わることが可能です。
◆システム開発経験等、これまでのご経験を活かしながら、セキュリティ領域の知見を高めてキャリアの幅を広げて頂けます。
◆安定した案件数により、ワークライフバランスを保ちながら業務を進められることも当ポジションの魅力です。

キャリアパス

本ポジションで配属となるプロフェッショナルサービス部では、インシデントレスポンスサービスのほかに、Redteamサービス、OSINTモニタリング等の脅威情報分析・提供、Web環境向けのセキュリティ開発・運用、脆弱性診断サービスの提供、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官公庁向けのセキュリティトレーニングサービス提供、
SOC（Security Operation Center）で活用されるシステム開発など、「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。
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】
(1)一般的なITスキル（応用情報技術者、またはそれ相当の知識、スキル）
(2)一般的なビジネススキル（メール、コミュニケーション、ドキュメント作成）
(3)Windows, Linux 両方の利用経験
(4)Pythonの利用経験
(5)英文読解力（技術情報は基本的に海外文献を利用するため）

上記に加えて、下記、いずれかを満たす方
(1)情報セキュリティに関して、ライフワークとして学び続けている方
(2)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
(3)インフラ（ネットワーク/サーバ）運用経験のある方
(4)脆弱性診断の経験がある方
(5)フォレンジック経験のある方
(6)マルウェアの解析経験がある方

【歓迎要件】
・セキュリティ技術の習得に関して、「学ばなければ」ではなく「ライフワーク」として楽しんでいる方
・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
・SANS GCFE, GCFA, GNFA もしくはそれ相当のいずれかの資格
・英語でのコミュニケーションに抵抗のない方

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）：250,000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	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。