車両セキュリティサービスのセキュリティアナリスト（募集番号：IoT202501）

POINT

9割リモート/新領域の車両向けセキュリティサービス/CASE/VSOC/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。

今回のポジションでは、数あるセキュリティサービスの中でも、新規ビジネス創出・拡大を見据えた車両向けセキュリティサービスに携わって頂きます。
サイバーセキュリティおよびサービス開発に関わる専門家とチームを組み、これまでにない新サービス開発を進めて頂くため、
社内外の多様な関係者の中で、複雑な議論や調整を通して合意形成することに前向きで、
新しい技術を取り入れるのが好きな方や、SOC等での分析業務経験を活かして新たな領域に挑戦したい方を募集します。

業務内容

新規ビジネス創出・拡大を見据え、サイバーセキュリティおよびサービス開発に関わる専門家とチームを組み、車両向けセキュリティサービスの業務プロセスの構築、その後運用を担っていただきます。

より詳細に：
業務プロセスの構築については、SIEMソリューション（特にログ分析のための分析ロジック部分）の開発チームと協力の上、セキュリティインシデントの分析手法を考案し、業務設計（業務フロー、業務手順の策定）を行っていただきます。
運用においては、業務プロセス構築において考案、策定した分析手法や業務手順に基づき、車両向けセキュリティサービスのアナリストとしてセキュリティインシデントの検出、分析、対応を実施し、脅威インテリジェンスの収集と分析を通じて、継続的なSIEMの改善を行っていただきます。

この仕事の魅力

◆**新領域のセキュリティサービス開発に携わって頂きます。**国内ではまだ同様のサービス提供をしている企業は少なく、**トップランナーとしてキャリアを築くことが可能です。**
◆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。
◆本事業部が手掛けるサービスはグローバルではマーケットが拡大しており、グループのグローバルメンバーと連携して提案・受注も始まっています。最先端のサービス開発に挑戦いただけます。

キャリアパス

本ポジションで配属となるIoT事業部では、車両向けセキュリティサービスの開発のほかに、OT領域のセキュリティサービス開発・導入支援等を展開しています。
また、社内にはそれ以外に、官公庁向けのセキュリティトレーニングサービス提供や、SOC（Security Operation Center）サービス、SOCで活用されるシステム開発、
脆弱性診断情報の提供、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。
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
OT領域のセキュリティについてはこちら：https://jp.security.ntt/products_and_services/ot_security

応募条件

【必須要件】
・開発要件が不明確な状況においても自ら要件を抽出・整理し業務を遂行するような自立自走能力
・論理的思考力、分析力、コミュニケーション能力
・SOC（Security Operation Center）アナリストとしての実務経験3年以上
・セキュリティインシデントの検知・分析・対応の経験
・セキュリティに関する資格（CISSP、SSCP、CEH、GREM、情報処理安全確保支援士など）以下のいずれかのご経験をお持ちの方

上記に加えて、以下のうちいずれかの経験
・マネージドセキュリティサービスをアナリストの立場で運用設計した経験
・SIEM、EDR、Firewallなどのセキュリティ製品の利用経験
・ネットワーク、ITシステム、ソフトウェアに関する幅広い技術知識、および、実務経験

【歓迎要件】
・インシデントレスポンス、フォレンジック調査に関する知識と実務経験
・海外の企業との英語での議論が可能なコミュニケーション能力（少なくとも、規格書等の英文のドキュメントが読めるレベルがあると良い）
・自動車業界におけるサイバーセキュリティに関する基本的な知識または強い興味関心
・自動車（特にコネクテッドカー、自動運転車）のアーキテクチャ、通信規格（CAN、Ethernet等）に関する知識
・自動車セキュリティ標準・ガイドライン（ISO/SAE 21434等）に関する知識
・組み込みシステム、IoTデバイスのセキュリティに関する知識
・SOARやスクリプト（Python、PowerShell等）による自動化経験

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：600万円～1,100万円 ■月給 基本給（役職給）：350,000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→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。