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：IoT202501c）

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

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開発と運用を担っていただきます。
まずは運用担当である車両向けセキュリティサービスのアナリストとして、下記業務をご担当頂きます。

・セキュリティインシデントの検出、調査、対応
・脅威インテリジェンスの収集と分析
・上記を通じた継続的なSIEMの改善

国内ではまだ浸透していないOTセキュリティ・コネクテッドカー・ドローン等の領域において、NTTグループのセキュリティ技術を駆使したサービスを確立し、新しい事業の柱にしていくつもりです。
第一人者として事業拡大に貢献頂くことは大変さもありますが、今後発展し重要度が増す業界のため、やりがいも感じて頂けると思います。

なお、以下のご経験を持たれる方は本業務へスムーズに取り組める素地があります。
・車両の通信やECUに関する業務経験がある方
　→ 車両の通信やログに関するノウハウが、車両への脅威の理解に役立ちます。
・セキュリティアナリストの経験がある方
　→ ITセキュリティの脅威分析の経験を車両の脅威分析に活かせます。
・セキュリティインシデント対応の経験がある方
　→ 攻撃手法の知識を車両セキュティインシデントに応用できます。

この仕事の魅力

◆グローバル＆最先端
　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。
◆業界の第一人者に
　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、第一人者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。

キャリアパス

本ポジションで車両向けセキュリティサービスのアナリストとしてご活躍していただき、その後、よりIT化していく車両へ追随しアナリストの道を究めていくことも、新SIEM開発に携わることも可能です。
配属となるIoT事業部では、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ので、新たなサービスの開発に携わることもできます。
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】

以下のいずれかのご経験をお持ちの方
・SOC（Security Operation Center）アナリストとしての実務経験 2 年以上
・車両の通信やECUに関する業務経験
・SIEM ツールの設計、構築、運用の経験
・セキュリティインシデントの対応と分析の経験

【歓迎要件】

・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
・CISSP
・GIAC Reverse Engineering Malware
・デジタルフォレンジックの実務経験
・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

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→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2013年に設立され、NTTグループにおけるセキュリティ事業の中心的枠割を担っています。 設立以来25年以上セキュリティ分野のリーディングカンパニーとして、欧米エリアを中心に事業を拡大し、APAC（Asia Pacific）にも展開しています。 全世界の社員数は約870名であり、うち500名以上はセキュリティ専門のコンサルタントや業界屈指のセキュリティアナリスト等のスキルを持った人材です。 全世界15ヶ国に広がる本支社、世界7ヶ国に設置したグローバルリスクオペレーションセンタに、上述の社員のうち200名以上のセキュリティエンジニア、 並びにリスクアナリストを配置し、24時間365日、顧客企業のセキュリティ監視と全世界のセキュリティ動向を観測しています。