No.
SS202304

募集ポスト
セキュリティリサーチャ（エンジニア）

採用部署
ソリューションサービス部

業務内容
高度化・複雑化するサイバー攻撃に対抗するためには、攻撃者の考えや動きを踏まえて適切な対策技術を選択して適用する必要があります。近年では、攻撃者の視点や技術を用いて対象環境への侵入を試行することで対策が必要なポイントを明らかにする「脅威ベースのペネトレーションテスト」を実施する組織が多くなっています。

本業務では、NTT セキュリティがグローバルサービスで蓄積した技術やノウハウを活用し、攻撃視点や防御視点で最新のサイバー攻撃の手法や技術を学ぶトレーニングサービスをお客様へ提供します。官公庁や企業等にトレーニングサービスを提供することで、体制やスキルの強化をサポートし、日本をサイバー攻撃の脅威から守ります。

トレーニングコンテンツを作成するため、必要な環境を用意してサイバー攻撃に関する調査や検証を実施し、知識やノウハウを広げたり深めたりすることが可能です。

社内関連組織のみでなく、社外のトップレベル人材と交流する機会があります。また、BlackHat などの海外カンファレンスの参加や SANS などの社外研修の参加を含め、業務時間内に技術動向の調査や自己研鑽する時間を取り入れています。

必要な経験・能力・資格
・サイバー攻撃技術への強い興味

以下のいずれかを満たす方

・脆弱性診断業務、あるいは、ペネトレーションテスト業務の経験

・マルウェア解析業務、あるいは、フォレンジック解析業務の経験

あると望ましい経験・能力・資格
・セキュリティキャンプや SecHack365 等のセキュリティ人材育成施策への参加経験のある方

・SECCON CTF に代表されるセキュリティイベントやコンテストで優秀な成績を収めた経験のある方

・セキュリティ人材を育成するトレーナーとしての経験をお持ちの方

・サイバー攻撃関連技術（リモートエクスプロイトを代表とする攻撃や、Post-exploitation で用いられるツールやテクニック、マルウェア感染およびボットネットの仕組みと、悪性サイトの役割および対策技術 等）に関する正しい知識をお持ちの方

・解析業務を実施するために必要となるスキルをお持ちの方。具体的には、IDA Pro や Ghidra, Metasploit

や Cobalt Strike, OSS の honeypot や sandbox 等のいずれかのツールを深いレベルで扱ったことがあり、C（,C++）や Python（,Ruby, Java）等でのコーディング力をお持ちの方
・ナショナルセキュリティ（国家安全保障）に興味関心のある方

勤務地
東京 23 区内

募集人数
若干名

雇用形態
正社員（試用期間 4 カ月）

勤務時間
９：００－１７：３０

休日、休暇
週休 2 日制（土、日)、祝日　、年次有給休暇、夏季休暇、年末年始休暇　他

給与・手当
役割給（職務内容に応じて決定します）及び業績給（成果達成度合いに応じて支給します）
その他：通勤費(全額支給)、時間外手当、休日手当、深夜手当、食事手当　他

福利厚生
健康保険、厚生年金、雇用保険、労災保険、企業年金基金　他

退職金
無し