

## No.

SO202303

## 募集ポスト

セキュリティアナリスト(リサーチ・解析)

## 採用部署

セキュリティオペレーション部

## 業務内容

セキュリティ製品（ファイアウォール、IPS、サンドボックス、EDR など）やプロキシサーバ等のログ、ネットワークパケットを分析し、「攻撃の有無、その手法、影響度、情報漏えい」等についてレポートを行います。

また、サイバー攻撃で利用される最新の技術や脅威動向を追跡し、マルウェアや攻撃ツールを解析し、その挙動や機能についてレポートを行います。そうした調査・解析によって蓄積したデータベースを活用し、攻撃者グループの特定などを行い、ブログやホワイトペーパーの執筆、セキュリティカンファレンスなどでの発表を行います。

調査や解析には、専用の調査 PC の他に IDA Pro、VirusTotal、ANY.RUN を含む様々な有償ツールや SOC で観測したデータを活用し、日本を代表する大企業や官公庁といったお客様をサイバー攻撃から守ることが業務となります。また、業務遂行のための教育トレーニング(SANS, Hack The Box など)も幅広く用意されており、マルウェア解析や脅威リサーチなどのスキルアップが可能です。

お客様をサイバー攻撃から守るため、アナリスト同士で解析手法や調査手法などを議論しながら、業務を行います。個々のスキルを極限まで高めながらチーム一丸となって切磋琢磨し、楽しく仕事することができます。

## 必要な経験・能力・資格

下記すべての項目を有すること。

- ・一般的なサイバーセキュリティの知識
- ・技術的な報告書の作成経験
- ・サイバーセキュリティに携わるものとして高い倫理観及び責任感
- ・業務に関する知識や技術を習得する意欲

## あると望ましい経験・能力・資格

- ・マルウェア解析、またはセキュリティ製品のアラート分析の業務経験
- ・ネットワークパケットやアセンブラを理解できる方

- ・ WindowsOS 上のアプリケーションを開発した経験がある方
- ・ 英語での読み書き及び会話が流暢にできる方
- ・ 地政学、外交、安全保障に関する業務経験あるいは研究実績がある方

### 勤務地

東京 23 区内

※2022 年 10 月現在のリモートワーク実施率は 9 割以上

### 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

夜勤シフト業務はありません。

### 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