No.
SO202301b

募集ポスト
セキュリティアナリスト

採用部署
セキュリティオペレーション部

業務内容
セキュリティオペレーションセンター（SOC）にて、サイバー脅威を分析する業務です。
24 時間 365 日のシフト体制が基本となります。シフト勤務以外にも個人の裁量で業務ができる時間が設けられています。様々な方向性の業務に対してチームが組まれており、個人が興味のあるチームに所属することで強みを生かすことができます。

＜SOC アナリスト業務＞
EDR、IPS、Sandbox 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てインシデントを発見
発生事象、情報漏えいを調査し、お客さまにレポート通知

その他に、アナリスト同士でバーチャルチームを組み、以下のような活動に取り組んでいます。
・完全独自 SIEM のチューニング、SIEM 検知ロジック作成
・IPS カスタムシグネチャ作成、EDR カスタム IoC 作成
・マルウェア解析
・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
・海外 SOC との情報交換会や技術交換留学
・新サービス検討
など

（活動内容の一例）
・外部講演、カンファレンス発表
カンファレンス講演実績：CODE BLUE、Japan Security Analyst Conference (JSAC)、Virus Bulletin Conference。Security Analyst Summit(SAS) など多数
・分析効率化ツール開発
高度な相関分析を実現するための SIEM ロジックの考案や解析ツール、普段の業務を効率化する自動化

ツールも自分達で開発・運用しています。
開発言語・フレームワーク：Python、JavaScript/TypeScript(Node.js, React, Vue.js）等

日々変化する攻撃に対して、アナリスト同士で議論し、切磋琢磨しながらチーム一丸となって、楽しく仕事することができます。各自に解析用 PC も別途支給されます。
日本を代表する大企業や官公庁のお客様のセキュリティを守るミッションクリティカルな業務であり、世の中でニュースになるようなインシデントの背後で我々が活躍することもあります。
標的型攻撃をはじめ多種多様な攻撃を観測分析するため、最新の技術や脅威の動向を追跡します。マルウェア解析、OSINT 調査、脆弱性の検証などを通じて、未知の攻撃手法や検知手法を調査し、国内外のカンファレンスや自社発行ホワイトペーパー、技術 blog などのメディアで発表することができます。

また、業務中に外部研修に参加できるなど自己研鑽に関しても手厚くサポートしており、現在所属している多くのアナリストは情報セキュリティに関する各種資格を所持しています
アナリスト保有資格：CISSP、GIAC GREM、情報処理安全確保支援士、博士（情報学）等

必要な経験・能力・資格

下記、いずれかを満たす方
(1)コンピュータサイエンスに関係する学部卒の学位もしくは相当する経験
(2)情報セキュリティに関する強い興味関心
(3)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
(4)インフラ（ネットワーク/サーバ）運用経験のある方
(5)SOC や CSIRT にてアラートの分析経験のある方
(6)脆弱性診断の経験がある方
(7)フォレンジック経験のある方
(8)マルウェアの解析経験がある方

あると望ましい経験・能力・資格

・IT 技術が好きで、物事をロジカルに深く追及することができる方
・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
・英語でのコミュニケーションに抵抗のない方
・中国語、ロシア語などの外国語でセキュリティ関連技術文書の読解が可能な方

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
24 時間 365 日体制でサービス提供するため、シフト勤務あり

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、リモートワーク手当　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、社員持株会、住宅補助　他

退職金

無し