## 募集ポスト

OT/IoT セキュリティを対象としたシステム・ソフトウェア開発者

## 採用部署

IoT 事業部

## 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開発と運用を担っていただきます。

開発においては、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）の設計、実装、および最適化を行います。運用においては、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、調査、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 の改善を行います。

## 必要な経験・能力・資格

- 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、合意形成することへの関心
- 新しい仕事に対する責任感ややる気、向上心
- 社会人経験 5 年以上
- SOC（Security Operation Center）アナリストとしての実務経験 2 年以上
- 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
- その他、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

## あると望ましい経験・能力・資格

- 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（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）
- 外部ベンダーと連携しソフトウェア開発を実施した経験
- クラウドネイティブなアプリケーションの開発能力（Microsoft Azure や AWS を使用したシステム開発・構築の経験（Virtual Machine, Blob, ネットワーク関連）等）
- Python を用いた開発経験
- データサイエンス（統計的手法、ビッグデータ解析等）を活用したシステム開発や運用の経験
- ＡＩ（異常検知、故障検知、予知制御、故障の分類等）を活用したシステム開発や運用の経験
- フルスクラッチ開発を基本設計レベルの上流から実施した経験・実績
- 5 名程度以上のシステム・ソフトウェア開発プロジェクトのリーダー経験
- ソフトウェア開発を内製で実施できる能力

- サイバーセキュリティ分野において、顧客からの課題ヒアリング、その解決方法の提案等のコンサル、企画に関する業務経験
- 各種システムに対するセキュリティアセスメント、脆弱性評価の実務経験
- ネットワークもしくはセキュリティアプライアンスのログの分析の経験
- 以下に示す開発環境での実務経験
  - 言語: ECMAScript (JavaScript), Java
  - ミドルウェア・フレームワーク: Flask, Nuxt.js, Vue.js, Apache Flink
  - OS: Linux
  - CI/CD: GitLab CI, GitHub Flow
  - データベース・データストア: Splunk Enterprise, Elastic, MongoDB, MariaDB/MySQL, Apache Hadoop (HDFS, HBase)
  - クラウド・仮想化環境: Microsoft Azure, Amazon Web Services, OpenStack, VMware vSphere, Docker
  - 構成管理: Ansible, Terraform, Azure Resource Manager, AWS CloudFormation, Vagrant
  - その他: nginx, Squid, Prometheus, Grafana, Zabbix, Unbound

**勤務地**

東京 23 区内

**募集人数**

1 名

**雇用形態**

正社員（試用期間 4 カ月）

**勤務時間**

９：００－１７：３０

試用期間後、フレックス勤務（コアタイムなし）

**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