Product Security Engineer_Full Remote Work

募集職種

人材紹介会社
株式会社ブルームテック

採用企業名
製造業に特化した受発注プラットフォーム開発企業

求人ID
1530210

業種
インターネット・Webサービス

会社の種類
大手企業 (300名を超える従業員数)

雇用形態
正社員

勤務地
東京都 23区, 台東区

給与
850万円 ~ 1200万円

勤務時間
フレックスタイム制

休日・休暇
土日祝、夏季休暇、年末年始、有給休暇等

更新日
2025年12月10日 10:00

応募必要条件

職務経験
6年以上

キャリアレベル
中途経験者レベル

英語レベル
無し

日本語レベル
ビジネス会話レベル

最終学歴
大学卒： 学士号

現在のビザ
日本での就労許可は必要ありません

募集要項

■募集背景
私たちCADDiは「モノづくり産業のポテンシャルを解放する」をミッションに、製造業におけるデータプラットフォームプロダクト「CADDi Drawer」を展開しています。
2022 年にローンチした「CADDi Drawer」は、製造業の中でも最重要といわれる図面データを機械学習など様々な技術により構造化し多様な情報と結び付けることで、情報資産としての活用を可能にしました。既に国内の大手製造業から加工会社のお客様にまで活用いただいており、急成長中です。2023 年からは海外（アメリカ・タイ・ベトナム）での販売も開始

し、グローバル展開も加速させています。

今後は、図面以外にも製造業の知見をテクノロジーによって再現・集約することで、部門や会社を超えた全体最適の実現を目指しています。
開発としては、データプラットフォームとしての機能強化、プラットフォーム上で動く複数の新規アプリケーション開発、飛躍的に増加するユーザー数・データ量に耐えうる基盤の強化など、取り組みたいテーマが数多くあります。
難易度が高くチャレンジしがいのあるプロダクト開発に一緒に取り組む仲間を募集しています。

■業務内容
Enabling Group Product Security Teamへの配属を想定しています。

・主にプロダクトのセキュリティレベル向上をミッションとするチームです。セキュリティに関してオーナーシップを持ち、攻めと守りのどちらも意識しながら事業成長を後押しすることを目指しています。
・現在はエンジニア3名が在籍しています。実際の推進業務は各プロダクトチームやコーポレートITチーム・法務と協働して業務を行っています。今後もチーム体制を拡充し、1年後には5名ほどの体制にしたいと考えています。

以下に業務例を示します。
実際の業務はこれに限定されるものではありません。
入社後の業務内容は、技術や専門知識、経験等を考慮のうえ決定します。

・各種セキュリティ要件の定義
・プロダクトのセキュリティ対策に関連する開発・運用・導入支援
・インシデントレスポンスを適切に行うための環境や仕組みの立案・整備
・セキュリティチェックの実施や改善のサポート（外注マネジメントを含む）
・DevSecOpsの高度化
・インフラのセキュリティに関する設定やポリシーの監査

■このポジションで得られる経験
・急成長する組織におけるセキュリティレベル向上の中心的役割を担う経験
・グローバルでビジネス展開を行う組織におけるセキュリティ推進経験
・セキュリティチームの立ち上げ・強化を担う経験
・熱量の高いメンバーと共に課題に集中できる環境
・事業会社×プロダクトセキュリティを中心に、希望に応じて幅広くセキュリティ業務に携われる環境

スキル・資格

＜必須スキル＞
・プロダクトセキュリティにおける実務経験
・Webアプリケーションセキュリティの基礎的知識
・OSおよびコンテナ技術の基礎的知識
・パブリッククラウドの基礎的知識
・日本語での流暢なビジネスコミュニケーション能力
    ・テキストコミュニケーションやミーティングを含め、日常業務を日本語で完結できること
    ・例：日本語能力試験N2程度、日本語環境での3年程度の就業経験をお持ちである等

＜歓迎スキル＞
・※1人が下記の全範囲に精通している必要はなく、フォレンジック系に強みがある方、基盤・インフラ系に強みがある方など、それぞれ得意領域を持つ方が集まり価値を発揮できるチームにしたいと考えています。
面接を通して確認していきますので、今までのご経験、今後得たい経験等をお話していただけると幸いです。

・セキュリティチームでの実務経験
・Ops
・DevSecOpsの構築・運用経験
・セキュリティ対応、診断
・ネットワーク情報・アセット情報の収集や評価などの活動
・Webアプリケーションへの脆弱性診断の経験
・ネットワーク(プラットフォーム)診断の経験
・Kubernetes等のコンテナ技術のセキュリティ診断・対策の経験
・Google Cloudを利用したシステムのセキュリティ診断・対策の経験
・SCA(Software Composition Analysis)やSBOM(Software Bill of Materials)などを活用した脆弱性の管理や運用の経験
・ペネトレーションテストや標的型攻撃耐性評価などの経験
・インシデント対応, プロダクトセキュリティ活動、リアルタイムアナリシス等の監視活動経験
・セキュリティインシデント対応経験
・CSIRT, PSIRT の経験
・デジタルフォレンジックの経験(ファストフォレンジック、フルフォレンジック)
・ネットワークフォレンジックの経験
・セキュリティ対応システム開発・運用
・IPS・IDS・WAF等の導入・運用経験
・オンプレミス環境におけるセキュリティ対策経験
・SIEMの導入・運用経験
・SIEM以外のシステムのログやネットフロー・パケットキャプチャデータを扱ったシステムの構築・運用経験
・Computer Scienceなどの学問的知識
・OS・ネットワークなどの低レイヤーの知識や関連する実務経験
・教育、啓発、情報発信、連携などの活動
・セキュリティ教育・啓蒙活動の経験
・セキュリティアドバイザーとしての活動
・セキュリティ人材の確保やキャリアパスの構築についての活動
・脅威インテリジェンスの収集および分析と評価
・内部脅威の整理・分析・評価の経験
・外部脅威の収集・分析・評価の経験

・実際のサービスの開発経験
・事業戦略に基づくセキュリティ対策の提案・実装経験
・Webサービスの開発、運用経験
・C(++), Rust, TypeScript, Python, Goなどの言語による開発経験
・ビジネスレベルの英語力

会社説明