【フルリモート】“挑戦と安定”を両立した働き方を実現！あなたの経験が、未来のセキュリティを守る力に

募集職種

採用企業名
株式会社ギブリー

求人ID
1545102

業種
その他（IT・インターネット・ゲーム）

雇用形態
正社員

勤務地
日本

給与
600万円 ~ 1100万円

更新日
2026年11月04日 03:00

応募必要条件

職務経験
3年以上

キャリアレベル
中途経験者レベル

英語レベル
ビジネス会話レベル

日本語レベル
ビジネス会話レベル

最終学歴
高等学校卒

現在のビザ
日本での就労許可が必要です

募集要項

＜この求人の魅力＞

- **業務内容の要約**：診断・コンサルを通じて高度なセキュリティ支援を担当
- **この求人のやりがい**：裁量を持ち最前線で活躍 / 自社製品開発に参画
- **このポジションで活かせる経験**：脆弱性診断、クラウド運用、セキュリティ設計、顧客対応経験
- **特色のある働き方や福利厚生**：全国フルリモートOK・地方でも高待遇

ギブリーについて
ギブリーは「すべての人が物心豊かな社会を実現する」をビジョンに掲げ、生成AIやAIエージェントなどを支援する、2009年創業のAIイネーブルメントカンパニー。
グローバルな開発組織と事業創造力、スピードを強みに事業を展開し、累計4000社を支援。生成AI分野の実績は650社以上。
AI業務効率化事業「MANA」、AI共創開発事業「Givery AI Lab」、AIマーケティング事業「DECA」、デジタル人材採用・育成事業「Track」を展開。
東証プライム、またはNASDAQへの時価総額1000億円での上場を見据えて、国内・海外において採用を強化しています。

▶ギブリー採用ピッチ資料

https://speakerdeck.com/givery_recruit/zhu-shi-hui-she-giburihui-she-shuo-ming-zi-liao-64a4a2bf-2526-4e61-8ef3-655354589618

▶ギブリーコンサルティング採用ピッチ資料
https://speakerdeck.com/givery_recruit/givery-consulting-the-entrance-book

募集概要

▼セキュアサイクルについて
生成AI時代の到来とともに、企業のDXは加速し続ける一方、新たなセキュリティリスクも急増しています。

私たちセキュアサイクルは「サイバーセキュリティに悩むことのない社会の実現」のために、システム開発のセキュリティコンサルをはじめ、Webアプリケーション、スマートフォンアプリケーションやIoT機器における脆弱性診断・ペネトレーションテストなどのサービスを展開しています。

システム開発においては、開発後の脆弱性診断だけを行って安心するのではなく、設計の段階からセキュリティを考慮して設計を行い、開発の途中においてもセキュリティのチェックを行うことが重要だと考えています。
システム開発事業においてもそれらの実現ができるような仕組みを構築するために日々研鑽を積んでいます。

また、地方でも給与面・待遇面で東京に劣らない環境を作り、地方の出身者や若者のU/Iターン先になることを目標に北九州本社、仙台オフィスに続き博多オフィスを開所し、業務拡大しております。

▼募集背景
私たちは「サイバーセキュリティに悩むことのない社会の実現」を掲げ、生成AI時代の課題に対応する革新的なセキュリティ製品・サービスの開発・提供を担っています。
脆弱性診断やセキュアなシステム開発を軸に、進化する脅威と向き合いながら、技術面でも事業面でも成長を続けているフェーズです。
今回は、事業拡大のキーパーソンとしてチームを支えていただけるセキュリティエンジニアを募集します。
直近では自社製品の開発にも取り組んでおり、組織やサービスを拡大しています。
事業の中核を担うセキュリティエンジニアとして、次世代のセキュリティを牽引しませんか？

- ギブリー子会社化に関するお知らせ：https://givery.co.jp/news/20240403_1/
- 株式会社セキュアサイクルHP：https://secure-cycle.co.jp/

▼会社全体の魅力・雰囲気

- 和気あいあいとしており、業務後も会社でゲームをしたりと、とても仲が良い環境です◎
- 各自が裁量をもって業務に取り組んでおり、成長できる環境です！

▼配属先　※セキュアサイクルでの採用となります

- 北九州オフィス
- 博多オフィス

募集職種・業務内容

▼募集職種
セキュリティエンジニア

▼業務内容
当社では、セキュリティ分野での経験を活かし、より高度で実践的な支援ができるセキュリティエンジニア・セキュリティコンサルティングをお任せできる方を募集しています。
システム開発やインフラ運用、セキュリティ業務のご経験を即戦力としてご活用いただけるポジションです。

また、地方拠点ですが、首都圏と遜色のない待遇を用意しており、北九州・福岡から、次のキャリアとして“挑戦と安定”を両立した働き方を実現できます。

ご経験やご志向に応じ、以下から業務内容を調整いたします。
あなたにとって「経験を活かす場」として、是非本ポジションをご検討ください。

- Webアプリケーション、API、スマホアプリの脆弱性診断 / ペネトレーションテスト
- OS / クラウド / プラットフォーム環境の設定監査 ~ セキュリティ評価
- クライアント向けセキュリティコンサルティング（現状分析、改善提案、ロードマップ策定など）/ トレーニング
- インシデント発生時の初動対応 ~ フォレンジック支援

▼セキュリティへのこだわり
「サイバーセキュリティに悩むことのない社会の実現」を目指し、単なる“診断屋”ではなく、お客様の事業成長とリスク最小化の両立を支援しています。

システム開発において開発後の脆弱性診断だけでなく設計の段階からセキュリティを考慮して設計を行い、開発の途中においてもセキュリティのチェックを行うことを大切にしております。

▼活かせるご経験

- セキュリティ診断 ~ 設計の実務経験
- ITインフラ / クラウド運用 ~ アーキテクチャ設計経験
- チームリーダーやマネジメントのご経験
- 顧客折衝 / 上流工程 / 提案型業務の経験

▼ご担当いただく業務の魅力/やりがい

- 常に新しい技術を取り入れ、セキュリティの最前線で挑戦できる環境です
- 取締役直下のポジションのため、裁量を持ちながら、経営視点での業務にも携わることができます
- 自社製品の開発中！0→1を経験できます
- 地方でも給与面 / 待遇面で東京に劣りません！

▼1日のスケジュール例
10:00 メールチェック、タスク確認
10:30 脆弱性診断実施
11:00 クライアントMTG
12:00 昼食
13:00 PoC / 調査・検証作業
15:00 自社製品の仕様検討MTG
18:00 提案書作成
19:00 退社

キャリアパス
専門性を深める「プロフェッショナル路線」
現場第一線で技術力を活かしつつ、特定分野（例：診断、インシデント対応、クラウドセキュリティなど）のスペシャリストとして活躍いただけます。
技術レビュー・ナレッジ展開・社内標準化など、“技術の柱”としての役割を期待されるポジションです。
・組織づくりや提案に関わる「マネジメント / 顧客支援路線」
プロジェクトのリードや、顧客に対するセキュリティ改善提案・ロードマップ策定など、戦略的な役割に挑戦可能。
技術だけでなく、ビジネスとの橋渡しとしての立ち回りを期待されるポジションです。

雇用形態
正社員
試用期間：3ヶ月（条件等は変わりません）

給与
年収　600万円〜1020万円

※上記は目安です。現年収・能力やご経験を考慮いたします。

・固定残業手当：月40時間該当分を上記に含む。
（例）年収600万円：127,800円/月
・超過した時間外労働の残業手当は追加支給

賞与・報酬・特記事項
・給与改定年2回 (5月・12月)
・賞与年1回(5月)

勤務時間
10:00 - 19:00

勤務地
■北九州本社
〒808-0138
福岡県北九州市若松区ひびきの北8-1
技術開発交流センター 314号室

■博多オフィス
〒812-0016
福岡県福岡市博多区博多駅南1-8-31九州ビル4F

・就業場所の変更の範囲
　会社の定める場所(テレワークを行う場所を含む)

休日
・完全週休2日制（土日祝休み）
・夏季休暇
・年末年始休暇（12/31〜1/3）
・有給休暇（入社時期によって変動、4月付与 / 入社月に合わせて付与 < 9月末まで入社で10日付与 > 最高付与日数20日 / ）
・慶弔休暇
・特別休暇
・出産休暇
・育児休暇

福利厚生
・企業型確定拠出年金

加入保険
健康保険、厚生年金保険、雇用保険、労災保険完備

選考フロー
1）書類選考
2）1次面接
3）コーディングテスト

4) 最終面接
5) 内定

スキル・資格

▼必須スキル

※以下いずれかの経験が3年以上ある方

- WebアプリケーションやAPIの脆弱性診断のご経験
- クラウド環境 (AWS、GCP、Azureなど) の設定診断や運用経験
- スマホアプリ (iOS、Android) のセキュリティ診断経験
- セキュリティインシデント対応の経験

▼必須言語

- 日本語スキル必須 (N1レベル)

▼歓迎スキル

- サーバー / ネットワークの脆弱性診断実務経験
- ネットワークに関する知識(IPv4-6,NAT等)
- サーバーの運用 / 構築経験(HTTPD,DNS等)
- 各種クラウドでのサーバー / ネットワーク構築・運用経験(AWS,GCP,Azure等)
- セキュリティ関連資格 (例: CISSP, CEH, OSCP, AWS Security Specialtyなど)

▼求める人物タイプ

- セキュリティ分野での幅広いキャリアを築きたいと考えている方
- チームで仕事をしたい方
- 新しい技術や知識を学びたい方

会社説明