

セキュリティエンジニア CIO Office Company CIO Office（CIOO）

> **楽天グループ株式会社での募集です。 セキュリティエンジニアのご経験のある方は歓...**

募集職種

人材紹介会社
株式会社ジェイ エイ シー リクルートメント

採用企業名
楽天グループ株式会社

求人ID
1624460

業種
インターネット・Webサービス

雇用形態
正社員

勤務地
東京都 23区

給与
750万円 ~ 1500万円

勤務時間
09:00 ~ 17:30

休日・休暇
【有給休暇】初年度10日（入社3か月目より付与）。入社7ヶ月目には最低10日以上付与。【休日】完全週休二日制 祝日 GW 夏...

更新日
2026年11月26日 16:09

応募必要条件

キャリアレベル
中途経験者レベル

英語レベル
流暢レベル

日本語レベル
ネイティブレベル

最終学歴
大学卒： 学士号

現在のビザ
日本での就労許可が必要です

募集要項

【求人No NJB2428462】
■楽天・事業について
楽天は日本最大のマーケットプレイスであり、eコマース、旅行、銀行、フィンテック、フードデリバリー、ゴルフ、保険、インスタントメッセージング、モバイルネットワークなど、70以上の幅広いサービスを提供するインターネットエコシステムです。楽天は世界で140以上のサービスを展開していますが、その中でもコミュニケーションズ エナジーカンパニーは、携帯電話事業をはじめとする情報通信と電力エネルギー関連事業を展開している事業部となります。 コミュニケーションズ エナジーカンパニーのサービスは下記よりご確認ください
https://corp.rakuten.co.jp/about/company/communications_energy.html

■部署・サービスについて
カンパニーCIOオフィスでは、楽天モバイルおよび楽天シンフォニーのITに関わる戦略およびガバナンスの強化を図り、事業の加速および持続的な成長を目指しています。会社上層部にとどまらず多方面とコミュニケーションを行いながら、全社的な経営およびシステム管理の最適化を具現化します。

楽天モバイルおよび楽天シンフォニーが提供する通信サービスにおいて、世界最高水準のセキュリティ基盤の管理運用を継続的に強化し、サービス安定性とデータの安全性を確保し、お客様からの信頼を築き、守り抜くことが最大のミッションです。現状のネットワークやシステムのセキュリティレベルを評価し、リスク特定・分析し、日々拡大するサイバー攻撃の脅威を未然に防ぐと共に、インシデント発生時には真因特定と再発防止を主導します。技術的な専門性を武器に、ビジネスの成長と安全性を両立させる「攻めのセキュリティ」を体現することが、私たちの使命です。

■業務内容
カンパニーCIO直下の組織にて、CISOおよびセキュリティチームと連携しながら、全社セキュリティ戦略の立案・実装に向けて主導いただきます。大規模な通信インフラをサイバー脅威から守り抜き、事業を加速する「信頼されるビジネス基盤」として継続的に進化させることが我々のミッションです。

＜主な業務＞
グローバルな技術チームと連携し、セキュリティレベルや成熟度の実態評価・分析、リスク抑制のためのセキュリティポリシーやルール作り（ガバナンス強化）と、セキュリティレベル高度化に向けた技術支援の両面からビジネスの成長を支えます。
グローバルチームとの英語による議論を通じ、世界最先端の脅威に対抗する技術力を磨ける環境です。

■働く環境
カンパニーCIOオフィス全体では20名弱。
組織全体で中途入社者が多く、通信事業経験者だけでなく、業界未経験の方も多数。その為、中途社員の受け入れなどもスムーズです。
業界、実務が未経験でも、経験豊富なメンバーからのサポートを受けながら、着実に成長できる環境です。

スキル・資格

必須要件：
・ITインフラまたはセキュリティ関連分野における実務経験3年以上
・ ITインフラ（ネットワーク・サーバー・クラウド等）基礎知識
・ セキュリティ関連業務の実務経験（運用、設計、診断など）
・ セキュリティ戦略・ポリシー策定の経験：全社レベル、あるいは事業部レベルでのセキュリティポリシーの策定、ガバナンス構築の実務経験。
・ クラウド環境（AWS/GCP/Azure）でのセキュリティ設計・実装：
クラウド特有のセキュリティ設定、IAM設計、ネットワークセキュリティの実装経験（IaCを用いたセキュリティ実装経験など）。
・ DevSecOpsの導入・推進経験：CI/CDパイプラインへのセキュリティツール（脆弱性スキャン等）の統合や、開発チームと連携したセキュリティプロセス改善の経験。
・ インシデント対応（CSIRT/SOC）の実務経験：大規模環境での監視・分析、インシデント発生時の初動対応から収束までのリーダーシップ経験。
・ ビジネスレベルの英語力：グローバルチームと技術的な議論を行い、調整・交渉ができるレベル。
・ セキュリティのアセスメント：リスク評価、リスク抑制計画のいずれかのご経験

歓迎要件：
大規模環境での経験： 通信キャリアや大規模Webサービスにおけるセキュリティ運用経験
開発・運用の知見： アプリケーション開発、またはインフラエンジニア（ネットワーク、サーバー、クラウドなど）としての実務経験
セキュリティ自動化： PythonやGo等を用いたセキュリティ運用ツールの開発・自動化経験
ガバナンス構築： ISO27001、NIST CSF等のフレームワークに基づくセキュリティ戦略・ルール策定経験

＜歓迎する資格＞
国際資格 PMI CISSP CISM CISA
国家資格 応用情報技術者、情報セキュリティマネジメント、情報処理安全確保支援士
クラウド・技術資格： AWS Certified Security Specialty CompTIA Security+ / CySA+

会社説明

インターネット関連事業