



【トヨタグループ】クラウドセキュリティエンジニア／SCoE G

KINTOテクノロジーズ株式会社での募集です。社内SE（インフラ）のご経験の...

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

KINTOテクノロジーズ株式会社

求人ID

1517031

業種

ソフトウェア

雇用形態

正社員

勤務地

東京都 23区

給与

500万円 ~ 1200万円

勤務時間

08:45 ~ 17:45

休日・休暇

【有給休暇】初年度 10日 1か月目から 【休日】完全週休二日制 有給休暇：初年度・・・入社月に応じ付与 2年目以降・・・毎年...

更新日

2025年02月07日 02:00

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

無し

日本語レベル

ネイティブ

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

【求人No NJB2274814】

SCoE グループは、マルチクラウド（AWS Google Cloud Azure）環境のセキュリティガバナンスを担当しています。KINTO テクノロジーズ内だけでなく、グループ内の関連組織とも協力しながら、業務に行います。新設のグループであり、新たなことに数多くチャレンジする機会があります。

SCoE に関するテックブログ記事

■CCoE活動とGoogle Cloudセキュリティプリセット環境の提供

https://blog.kinto technologies.com/posts/2023_06_22_whats_ccoe_and_security_preset_gcp/

■クラウドセキュリティの進化をリードする SCoE グループ

<https://blog.kinto technologies.com/posts/2024 05 13 SCoE/>

■Azure サブスクリプションの初期セキュリティベストプラクティスを考える

<https://blog.kinto technologies.com/posts/2024 12 01 azure security preset/>

■KTC クラウドセキュリティエンジニアのとある一日

<https://blog.kinto technologies.com/posts/2024 12 14 CloudSecurityEngineer/>

【ミッション】

クラウドセキュリティの専門組織として、KINTO テクノロジーズのマルチクラウド環境のセキュリティガバナンスに責任を持ちます。

- ・セキュリティリスクを発生させない
- ・セキュリティリスクを常に監視・分析する
- ・セキュリティリスクが発生したときに速やかに対応する

【業務内容】

ミッションを達成するために様々な業務を実施します。日々、課題を発見し、それらを解決するために自ら業務を定義します。

SCoE グループは、組織横断型のグループのため、多くの他グループと協力し業務活動を行います。

【現在のコアミッション】

- ・クラウドセキュリティのモニタリングと改善活動
AWS Security Hub などの CSPM (Cloud Security Posture Management) ツールを活用し、マルチクラウド環境のセキュリティモニタリングを実施します。
定期的レポートを作成し、リスクのある設定を特定します。これらのリスクは、プロダクト開発チームと協力して改善を進めます。
改善方法を記載したドキュメントの作成や社内勉強会を通じて、改善の浸透を図ります。
- ・脅威検知と対応
Amazon GuardDuty 等の脅威検知サービスを活用し、マルチクラウド環境や SaaS 環境の脅威検知を日々実施します。
検知したリスクにはリアルタイムで対応し、環境構築やルールのチューニングも担当します。
- ・クラウド環境の提供とセキュリティ設定
プロダクト開発チームにマルチクラウド環境を提供します。提供時には、グループポリシーやセキュリティベストプラクティスに準拠した設定を事前に適用します。
自動化を活用したセキュリティ設定の仕組みづくりやポリシー設計を行います。
- ・設定アセスメントと効率化
プロダクション環境がグループポリシーに準拠しているかをアセスメントします。
- ・内製ツールを開発し、アセスメントプロセスを効率化します。
他グループへのクラウドセキュリティサポート
他グループに対して、クラウドセキュリティの観点からのサポートやアドバイスを実施します。

【今後の取り組み】

- ・CWPP 及び CIEM ツールの導入・運用
マルチクラウド環境での CWPP (Cloud Workload Protection Platform) および CIEM (CloudInfrastructure Entitlement Management) ツールの導入と運用を担当します。
ツール選定から検証、導入、運用までを一貫して実施し、SCoE グループ内での内製開発を進めます。
- ・生成 AI を活用したアプリケーション開発に対応したセキュリティ対策
セキュリティガイドラインや、ガードルールを設計・開発します。
AWS Azure Google Cloud での開発プロセス全体をカバーするセキュリティフレームワークを定義します。

【コミュニティ活動】

トヨタグループ内でのコミュニティ活動や社外のコミュニティ活動に積極的に参加し、情報発信を行っています。

【開発環境】

PC : Windows と Mac より自由に選択可

開発言語 : CloudFormation Terraform など

プラットフォーム : AWS Google Cloud Azure など

ツール : Docker Github JIRA Confluence Slack Zoom Teams など

スキル・資格

- ◆ 必須
 - ・AWS Google Cloud Azure などを用いた業務システム開発・構築・運用経験 (2年以上)
 - ・Well Architected Frameworkや、CIS NIST などのクラウドセキュリティに関する知識
 - ・CloudFormation Terraform CLI などの IaC の開発経験
- ◆ 歓迎
 - ・CCoE の活動経験。特にマルチアカウント管理やポリシー策定など歓迎
 - ・CSPM CWPP 等のクラウドネイティブセキュリティサービスの開発・構築・運用経験
 - ・クラウドベンダーのプロフェッショナルレベル/専門知識レベルの資格保有
 - ・自社/社外コミュニティの立上げ、運用経験
 - ・英語でのコミュニケーションが可能な方 (ビジネスレベル)
グループ会社とのコミュニケーションに利用します
- ◆ 人物像
 - ・クラウドセキュリティに興味があり、最新技術を学びながら実践したい方
 - ・前向きに仕事に取り組む姿勢をお持ちの方
 - ・自ら考え、行動する積極性をお持ちの方
 - ・組織/役割を越えたコミュニケーションが可能な方
 - ・新しいサービスや技術に対する好奇心、チャレンジ精神をお持ちの方
 - ・常に自己研鑽をする方

会社説明

デジタル分野における情報システムの設計、開発、運用管理および販売等の情報処理サービス、企業経営戦略、マーケティング戦略の企画、立案およびコンサルティングに関する業務