

【900 ~ 1300万円】Japan Information Security Office（ISO）Security En…

AIG損害保険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…

Job Information

Recruiter
JAC Recruitment Co., Ltd.

Hiring Company
AIG損害保険株式会社

Job ID
1619808

Industry
Insurance

Company Type
International Company

Job Type
Permanent Full-time

Location
Tokyo - 23 Wards

Salary
9 million yen ~ 13 million yen

Work Hours
09:00 ~ 17:00

Holidays
【有給休暇】有給休暇は入社時から付与されます 入社7ヶ月目には最低10日以上 【休日】完全週休二日制 土 日 祝日 GW 年末…

Refreshed
October 29th, 2026 18:19

General Requirements

Career Level
Mid Career

Minimum English Level
Business Level

Minimum Japanese Level
Native Level

Minimum Education Level
Bachelor's Degree

Visa Status
Permission to work in Japan required

Job Description

【求人No NJB2342590】
■職務内容
AIGセキュリティスタック（Crowdstrike、Tanium、Qualys、Imperva DAM/DAS、Microsoft Purview/Defender、ProofPoint、Trend Micro、Varonis、SafeBreach、Agari DMARC、Prisma、Wiz）に関連するセキュリティエンジニアリングの取り組みを推進します。候補者は、AWS、Google Cloud Platform（GCP）、Microsoft Azure（Azure）など複数のクラウドプロバイダーにわたる、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a

Service) を含むエンタープライズレベルのオンプレミスおよびクラウドサービスのセキュリティに関する豊富な経験を有している必要があります。また、候補者は、オンプレミスおよびクラウドセキュリティアーキテクチャ、脆弱性管理、ネットワーク防御に関する専門知識を有し、さまざまな種類のクラウドおよびクラウド/ハイブリッドシステムに展開された企業のクラウドワークロードとデータを保護する必要があります。ジャパンセキュリティエンジニアリングリードは、日本およびAPAC地域におけるAIGセキュリティスタックに関連するすべての事項について、情報セキュリティ組織およびその他の情報セキュリティチームにとって重要な技術エキスパートとしての役割を果たします。

■職務責任
・オンプレミスシステムおよびAWS、 Azure、GCPのクラウドサービス向けAIGセキュリティスタックの導入、管理/保守、および「フォロー・ザ・サン」サポートを担当する主要な技術専門家として、サービスのセキュリティを確保するための脅威、リスク、および制御策を特定します。
・オンプレミスおよびクラウドのAIGセキュリティスタックに関する信頼できるアドバイザーとして、ジュニアチームメンバーや開発者に対し、オンプレミスおよびクラウドサービスにおける脅威とリスク軽減策を理解できるよう指導する。
・他の情報セキュリティチームと連携し、ビジネスに対する重大なセキュリティリスクへの対処を支援する。クラウドセキュリティリスクに関連する問題が、IT環境内で適切に監視され、対処されるようにする。
・関係者と協力して、クラウドセキュリティに関するポリシーと手順を策定、維持、および実施する。
セキュリティアーキテクチャチーム、クラウドセキュリティエンジニアリングチーム、セキュリティ対策チーム、アプリケーションおよびインフラストラクチャチームと連携し、オンプレミスおよびクラウドのワークロード、ならびに様々なタイプのオンプレミス、クラウド、およびクラウド/ハイブリッドシステムにデプロイされたデータを保護します。
・クラウドセキュリティソリューションを活用し、オンプレミスおよびクラウドベースのアプリケーションとインフラストラクチャに関するセキュリティポリシー、標準、および手順の開発を支援する。

Required Skills

・サイバーセキュリティ、情報技術、またはコンピュータサイエンスなどの関連分野における学士号、もしくは同等の実務経験。
・英語の流暢なレベルの語学力。
・オンプレミスおよびクラウドセキュリティまたは関連職種で12年以上の経験があり、AWS、Azure、Google Cloudなどのクラウドプラットフォームでの実務経験があること。
・オンプレミスおよびクラウドのセキュリティ態勢管理ソリューションに関して、8年以上の直接的な実務経験を有し、コンピューティングエージェント、DevOpsコードスキャン展開、態勢管理ポリシーのチューニングなどを行い、IaC自動化を活用して効率的かつ安全なクラウド運用を実現していること
・クラウド / クラウドハイブリッドプラットフォーム (IDaaS / IaaS / SaaS / PaaS) および関連するセキュリティツールとプロセスに関する深く幅広い理解。
・Kubernetes (AKS、EKS、GKS) やAzure Functionsなどのクラウドネイティブ環境において、エージェント/エージェントレスワークロードディフェンダーを含む堅牢なセキュリティ対策を実装する能力。
・CISSP、CCSP、Security+、Azure、AWS、GCPの基礎/準/セキュリティ関連の資格など、追加の認定資格があれば尚可。
・脆弱性分析および悪用技術に関する、最近の関連性の高い経験。
・必要に応じて製品内の問題をトラブルシューティングし、さまざまなチームを支援し、クラッシュダンプ、パフォーマンスモニター、リリース阻害要因などを把握する力。
・NIST、CISベンチマーク、DISA STIG規格などの重要なセキュリティ制御に関する深い知識。
・ISO 27001/27002、PCI DSS、SOXなどの国際セキュリティ基準および業界フレームワークに関する知識。
・WindowsおよびLinuxにおけるインフラストラクチャの強化とセキュリティ設定に関する深い知識と専門知識。
・WindowsおよびActive Directory、Unix/Linuxオペレーティングシステムに関する中級から上級レベルの知識。
・PowerShell、Python、Linuxシェルを用いたスクリプト作成に関する十分な知識が求められます。
・クラウドコンピューティング、仮想化の概念、およびPaaS/SaaSサービスに関する高度な知識。
・TCP/IPおよびHTTPプロトコルに関する高度な知識。
・エンドポイントセキュリティの概念とインシデント対応プロセスに関する深い知識
・SIEMおよびツール統合に関する経験？CrowdStrike NextGen SIEMの経験があれば尚可
・セキュリティフレームワークに関する深い知識
・自発的に行動し、主体的に業務に取り組み、個人としても成長中のチームの一員としても成果物に対する責任を負うことができる、意欲的な人材を求めています。
・チームプレイヤーであり、グローバルに分散したチームにおいて、リーダーシップを発揮し、指導を行い、コミュニケーションを取り、協力し、効果的に業務を遂行できる。

Company Description

■損害保険全般・個人：海外旅行・火災保険・自動車保険・傷害保険・医療保険　他・法人：業務災害総合・企業財産・国内物流総合・事業賠償・生産物品質・海外PL・貨物海上・輸出信用　他