HITACHI
Inspire the Next

株式会社日立製作所

日立グループのサイバーセキュリティ対策強化を目的とした技術的な対策の企画・施策推進とSOC運用の統括

日立グループのサイバーセキュリティ対策強化を目的とした技術的な対策の企画・施策推進とSOC運用の統括

職務内容:

【配属組織名】

情報セキュリティリスク統括本部 サイバーディフェンスオペレーション本部　技術企画部

【配属組織について（概要・ミッション)】

サイバー攻撃は日々巧妙化・高度化・多様化しており、被害が表出するまでの時間も短くなってきています。サイバー攻撃による情報漏洩や操業停止など事業そのものの継続に支障をきたすリスクも大きくなっていることから、サイバー攻撃やデータ漏洩も大きなコーポレートリスクの一つとなっています。このようなサイバー攻撃に対峙するためには、その脅威をいち早く発見し、被害拡大を防止することが重要だと考えており、日立グループではマルウェア感染や不正アクセスなどの脅威を早期に検知し、インシデント発生時の初動から対策までを迅速に対応する取り組みを推進しています。日立グループグローバルにおいてサイバー攻撃や各種サイバーセキュリティインシデントから事業や情報資産を守るための技術的な対策について企画・施策推進を行うとともにSOC運用の統括を行っています。

【携わる事業・ビジネス・サービス・製品など】

日立グループ内のサイバーセキュリティ強化に向けた技術対策の企画・施策推進とSOC(セキュリティオペレーションセンタ)運用の統括。

■参考資料

情報セキュリティ報告書 2024

https://www.hitachi.co.jp/sustainability/download/pdf/securityreport.pdf

【募集背景】

日々、サイバー攻撃は巧妙化・高度化・多様化しています。一方で、社内インフラはクラウドシフトやゼロトラスト化といった変革が進行中です。このような状況下では、新たなITインフラに適したサイバー攻撃対策の最適化が求められています。既存の対策を見直しつつ、巧妙化・高度化・多様化するサイバー攻撃に対抗するための新たな対策も必要です。この重要な取り組みを推進するために、専門的な知識と経験を持つ人財を募集しています。

【職務概要】

日立グループに対するサイバーセキュリティ攻撃に対抗するための技術対策を推進します。具体的には、サイバー攻撃や各種サイバーセキュリティインシデントから日立グループの事業や情報資産を守るための技術的な対策の企画・施策推進を行い、SOC(セキュリティオペレーションセンタ)の業務や運用を統括します。

【職務詳細】

日立グループのサイバーセキュリティ対策を推進するため、以下の業務を担当していただきます：

・社内ITインフラに対するリスク評価を実施し、その評価に基づいた対策方針を立案

・脅威の動向や社内のセキュリティインシデント発生状況を踏まえ、課題を抽出し、技術対策方針を策定

・技術対策方針に基づく施策の立案と、その施策の推進管理

・社内のサイバーセキュリティインシデント対応状況を統制し、分析を行い、社内への注意喚起を実施

【ポジションの魅力・やりがい・キャリアパス】

■魅力・やりがい

・日立グループへの貢献: 日立グループ全体に対するサイバーセキュリティ対策の立案・実行を通じて、グループ全体の安全性を高め、事業の継続性を支える重要な役割を担うことができます。

・最先端技術へのアクセス: 最新のセキュリティベンダの技術、サービス、製品に関する情報を収集し、最先端のサイバーセキュリティ技術を常に学び続けることができます。

・知識の深化: 最新のセキュリティ情報に対する知識を習得し、専門性を高めることができます。

・業界ネットワークの構築: 他社の同種組織と積極的にコンタクトを図り、業界内でのネットワークを構築することで、情報交換や協力関係を築くことができます。

■キャリアパス

・包括的なスキルの習得: サイバーセキュリティ対策の立案から実装、運用までの一連のプロセスに携わることで、セキュリティ人材として求められる幅広いスキルを身につけることができます。

・マネジメントスキルの向上: サイバーセキュリティ対策の推進管理を通じて、プロジェクト管理の経験を積み、マネージャーとして必要なマネジメントスキルを磨くことができます。

【働く環境】

①配属組織/チーム：本部は10名のチームです。各部は、4～6名程度。 ②働き方：基本在宅勤務です。会議内容に応じて事務所や社外ベンダにて議論をする場合があります。

※上記内容は、募集開始時点の内容であり、入社後必要に応じて変更となる場合がございます。予めご了承ください。

応募資格

【必須条件】 (1)サイバーセキュリティ分野に積極的に関わりたいという意識をお持ちの方 (2)ITセキュリティ、サイバーセキュリティに関する一般知識 (3)ステークホルダーと円滑なコミュニケーションを取り、信頼関係を構築できる

(4)新たな知識・技術の習得に意欲を持って取り組める

【歓迎条件】

・サイバーセキュリティ対策実行に関する知識や経験

・サイバーセキュリティ運用の知識や経験

・チームリーダー業務経験

・システム開発におけるインフラ領域の業務経験

・ビジネス英語力（TOEIC650点以上）

【求める人物像】※期待行動・コンピテンシー等

【全職種共通（日立グループ コア・コンピテンシー)】

・People Champion（一人ひとりを活かす）：　多様な人財を活かすために、お互いを信頼しパフォーマンスを最大限に発揮できる安心安全な職場(インクルーシブな職場)をつくり、積極的な発言と成長を支援する。

・Customer & Society Focus（顧客・社会起点で考える）：　社会を起点に課題を捉え、常に誠実に行動することを忘れずに、社内外の関係者と協創で成果に責任を持って社会に貢献する。

・Innovation（イノベーションを起こす）：　新しい価値を生み出すために、情熱を持って学び、現状に挑戦し、素早く応えて、イノベーションを加速する。

【最終学歴】

大卒以上

待遇:

【想定ポジション】

主任クラス

※募集開始時の想定であり、選考を通じて決定の上、オファー時にご説明いたします。

【給与】

■想定月給：463,000～605,000円

■想定年収：7,800,000～10,300,000円

【勤務時間】

8:50～17:20（実働7時間45分、休憩45分）

※事業所によって時間帯が異なる場合あり。

その他採用条件についてはこちら

【更新日】

2025年7月16日

勤務地:

東京都千代田区外神田１丁目１８番１３号　秋葉原ダイビル 20F

備考:

【対象年齢】

25～39才程度

bloom