株式会社日立製作所

【担当者クラス】防衛・安全保障関連事業部門におけるサイバー攻撃への対応強化を担う社内SE人財

【配属組織について（概要・ミッション)】

■ ディフェンスシステム事業部

ディフェンスシステム事業部は、防衛・航空宇宙・セキュリティ分野を支える技術を核に、日立グループの技術を集結して社会インフラ安全保障事業を推進し、さまざまな事態から私たちの生活と安全を守り、安心して暮らせる社会の実現に貢献します。

【参考情報】

・キャリア採用サイト：https://www.hitachi.co.jp/products/defense/career/index.html

・ディフェンスシステム事業について：https://www.hitachi.co.jp/recruit/newgraduate/field-navi/defense/

・配属組織で働く社員インタビュー：https://digital.careers.hitachi.co.jp/tag/defense/

■ 経営企画本部DX推進部

DX推進部は、ディフェンスシステム事業部を支える、事業部内の社内業務システム/IT環境の検討・開発・維持整備・セキュリティ確保を担うことで、事業部に貢献する部門です。

■ DSIRT(Defense Systems Incident Rediness Team)グループ DSIRTグループのミッションは「ディフェンスシステム事業部およびグループ会社に対するサイバー攻撃に対して、未然防止・早期発見・迅速な対処を実施すること」です。具体的には、ログ分析・脆弱性診断・不審メール解析・フォレンジック調査・OA機器のハードニング・脆弱性情報の収集と分析・サイバーセキュリティ関連のトレンド調査・攻撃者グループ（APT）の動向調査等を行っています。

【携わる事業・ビジネス・サービス・製品など】

ディフェンスシステム事業部およびグループ会社が運用するITインフラや業務システムをサイバー攻撃から守る業務に携わる事が出来ます。

【募集背景】

近年サイバー攻撃は増加傾向にあり、さらに巧妙化・高度化してきています。今後は現行の体制だけでは十分に対応しきれなくなる可能性があります。 こうした将来のリスクに備えるため、新たな人財を採用・育成することで、より強固なセキュリティ体制の構築を計画しています。そのため、今回新規でメンバーを募集することにしました。

【職務概要】

【職務詳細】

■ログ分析：

サーバ、PC、Firewallなどの各種ログを、オープンソースのログ分析ツールやDSIRTグループで開発したスクリプトを活用して分析します。分析結果をレポートに纏め、関係部門と共有します。分析用スクリプトのメンテナンスや新規開発も行います。

※入社後、まずはログ分析をメインで担当していただき、その後は希望や経験に応じて以下のような業務も担当していただく予定です。

・サイバーセキュリティ関連のトレンド調査： 国内外のサイバーセキュリティ関連カンファレンス等に参加し、最新動向の情報を収集します。得られた知見をレポートに纏め、関係部門と共有します。さらに、必要に応じて事業部全体へのプレゼンテーションも担当します。

・脆弱性診断： ディフェンスシステム事業部が運用しているシステムに存在する脆弱性や設定上の不備を見つけるためのセキュリティテストを担当します。専用のツールを用いて実施します。脆弱性診断の結果をレポートに纏め、関係部門と共有します。

・フォレンジック調査： インシデントが発生した時に攻撃を受けたPCに対する、証拠保全・収集・分析を担当します。分析結果をレポートに纏め、関係部門と共有します。

【ポジションの魅力・やりがい・キャリアパス】

■ ポジションのやりがい・魅力

本ポジションでは、サイバー攻撃の早期発見や防御に直結するログ分析・脆弱性診断・フォレンジック調査業務を通じて、ディフェンスシステム事業部の安全を守る重要な役割を担っていただきます。日々進化するサイバー攻撃に対応するため、最新のセキュリティ動向をキャッチアップしながら、実践的なスキルを磨くことができます。さらに、国内外のカンファレンス等への参加を通じて、世界中の最新情報や技術トレンドを直接学ぶことができ、得た知見をディフェンスシステム事業部全体に発信する機会もあります。自らの成長とともに、ディフェンスシステム事業部のセキュリティレベル向上に貢献できる、やりがいの大きいポジションです。 個人の成長に対しては、高度なセキュリティ資格(GIAC、CISSPなど)取得や専門教育(SANSなど)受講を推進し、サポートしていきます。

■ キャリアパス

入社後は、ログ分析や脆弱性診断、フォレンジック調査など、幅広いセキュリティ業務に携わりながら、実践的なスキルを磨いていきます。現場での経験を通じて、セキュリティの専門性を深め、将来的には高度なインシデント対応を担うスペシャリストへと成長できます。

【働く環境】

■ 配属組織/チームについて

・ DSIRTグループは9名の社員が在籍しております。年齢層は30代から60代と幅広いです。サイバーセキュリティに関する探求心の強いメンバーが多いです。

■ 働き方について

・ 入社後、半年程度はOJTとして出社することを想定しています。出社することで、他のメンバーと直接顔を合わせて会話しながら業務に習熟できます。

・ 業務に慣れて頂いた後は業務内容/状況に応じて週2〜3回程度の在宅勤務が可能です。現メンバも計画的に活用しています。

・ 年に数回程度、国内外のサイバーセキュリティカンファレンス等への参加があります。

※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】

・基本情報技術者や応用情報技術者等の情報処理技術者試験の資格を保有する方

・プログラミング言語によるプログラミングの経験（独学・趣味含む）を有する方（目安：2年以上、言語は問わないがノーコード・ローコードは除く）

【歓迎条件】

・ サイバーセキュリティ技術に関する知識・知見の向上に意欲のある方（業務上の経験は必須ではありません）

・ サーバ/OA用PCの動作や出力するログに関する知識のある方

・ Firewallの動作や出力するログに関する知識のある方

・ CTF(Capture The Flag)等技術力を競う大会に参加する意欲のある方

【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】

高専卒以上

待遇:

【想定ポジション】

【給与】

■想定月給：269,000～448,000円

■想定年収：4,900,000～7,600,000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8月27日

勤務地:

神奈川県横浜市戸塚区吉田町２９２番地

※最寄り駅：JR戸塚駅から徒歩10分～15分程度

備考:

【対象年齢】

26歳〜35歳

bloom