2024

現場受け入れ型インターンシップ

ポスト情報

セキュリティエンジニア

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D1.攻撃者視点に立ち攻撃技術を開発するセキュリティエンジニア	RedTeamサービスに資する攻撃技術や、先進的な攻撃技術の調査・研究・開発を行います。 ■主な業務内容 ・MITRE ATT&CKをフレームワークとした攻撃技術の調査・開発 ・演習形式の企業セキュリティ対策評価、RedTeamテスト ■RedteamPJの業務一例 MITRE ATT&CK Contribution - T1562.009 Safe Mode Boot (https://engineers.ntt.com/entry/2021/12/09/103248) ■2024年冬インターンシップ体験記 Pool Partyという攻撃手法を通じてWindowsの深淵を覗いた7日間) (https://engineers.ntt.com/entry/2024/04/16/091259) ■2023年冬インターンシップ体験記 インターンシップ生があるSaaSを用いた未知のC2脅威を実証してみた (https://engineers.ntt.com/entry/2023/05/10/100203)	【必須】 ・RedTeamや先進的な攻撃技術に興味があり、技術の深堀り、習得する意欲があること ・Pythonを用いたプログラミング経験(2年程度)、もしくは左記に相当する経験があること。 【推奨】 ・情報、通信、コンピュータ系、セキュリティ専攻学科に在籍している、もしくは出身であること ・CTFなどのセキュリティコンテスト入賞経験があること	・〒108-8118 東京都港区芝浦3-4-1 グランパークタワータワー	NTTコミュニケーションズ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D2.脅威インテリジェンスを生成・活用するセキュリティエンジニア/アナリスト	下記いずれかのチームにて脅威インテリジェンスに関する業務を体験していただきます。 なお、チームは本人の希望と適性に応じて決定します。 【チーム1】サイバー攻撃の原理を理解し、攻撃インフラを解明するセキュリティアナリストチーム 実在するマルウェアや攻撃ツールを用いたサイバー脅威について調査分析業務を行っていただきます。 ■業務成果の一例 ランダムサブドメイン攻撃において事業者として行なった対策と解析について（InternetWeek 2023） （https://www.nic.ad.jp/ja/materials/iw/2023/proceedings/c10/c10-kanda-tsuboi-tobioka-hatada.pdf） 日本を狙ったフィッシングサイトの情報配信はじめました （https://engineers.ntt.com/entry/2023/12/03/085650） 偽のセキュリティ警告画面（サポート詐欺）が表示される仕組み （https://engineers.ntt.com/entry/2023/12/03/085650） Operation So-seki: You Are a Threat Actor. As Yet You Have No Name.（JSAC 2024） （https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_1_4_minakawa_kanda_sameshima_jp.pdf） Analysis of Activities and Tools of Phishing Actors Targeting Japan（JSAC 2024） （https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_4_masumoto_tsuboi_jp.pdf） ■直近のインターンシップ体験記 インターンシップ体験記 ～Cobalt StrikeのC2サーバ追跡～ （https://engineers.ntt.com/entry/2023/03/24/081829） 攻撃者はいかにしてフィッシングサイトを隠すか？（インターンシップ体験記） （https://engineers.ntt.com/entry/2023/10/05/085501） フィッシングキットから生成されたサイトの調査 （インターンシップ体験記）（https://engineers.ntt.com/entry/2024/05/17/093642） 【チーム2】サイバー攻撃の情報を利用し、効果的な対策を実現するセキュリティサービス「Metemcyber」の開発を経験していただきます。 セキュリティ情報の収集・分析・運用やSBOMに関する最新の技術動向を学ぶことができます。 ■2022年冬インターンシップ体験記 インターンシップ体験記 ～セキュリティ運用の健全化を目指すMetemcyberの開発～ （https://engineers.ntt.com/entry/2022/03/04/115309）	【チーム1】【必須】 ・情報セキュリティに関する専門教育を1年以上受けていること（高専/大学/大学院） ・サイバーセキュリティ（特にOSINT）に対する興味・関心があること ・習得した技術を倫理的に活用し社会に貢献できること 【チーム1】【推奨】 ・ネットワーク、クラウド、アプリケーションなどのIT技術/知識を有すること 【チーム2】【必須】 ・サイバーセキュリティ（特にOSINT）に対する興味・関心があること ・Pythonを用いたプログラミング経験（2年以上）、もしくは左記に相当する経験（授業、バイト、卒業研究など）があり基本的なコーディングが支障なくできること。 【チーム2】【推奨】 ・MITRE ATT&CKを用いた分析に関するセキュリティの知識があること ・ReactによるWebフロントエンドの開発経験があること	・〒108-8118 東京都港区芝浦3-4-1 グランパークタワー タワー	NTTコミュニケーションズ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D3.制御システム向けセキュリティサービス「OsecT」を開発する開発エンジニア	制御システム向けセキュリティサービス「OsecT」の開発・検証を行っていただきます。 ■本プロジェクトの業務一例 OsecT、サービスリリースしました https://engineers.ntt.com/entry/2022/05/10/110748 OTセキュリティリスク可視化サービス OsecT、リニューアルしました https://engineers.ntt.com/entry/2023/08/31/100633 OsecTにおける運用の自動化 https://engineers.ntt.com/entry/2023/12/23/090934 OT/ICSセキュリティカンファレンス「S4x24」参加報告 https://engineers.ntt.com/entry/2024/04/22/084951 ■過去のインターン体験記 セキュリティ技術開発のインターンシップに参加させていただきました!! https://engineers.ntt.com/entry/2021/10/12/113758	【必須】 ・制御システムセキュリティに興味があり、技術を深堀りし、習得する意欲のあること ・Pythonを用いたプログラミング経験（2年程度）、もしくは左記に相当する経験があり基本的なコーディングが支障なくできること。 【推奨】 ・情報、通信、コンピュータ系、セキュリティ専攻学科のこと ・ネットワーク、クラウド、アプリケーションなどのIT技術・知識を有すること	・〒108-8118 東京都港区芝浦3-4-1 グランパークタワータワー	NTTコミュニケーションズ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D4.組織横断でプライバシーを保護したデータ分析を実現する基盤の進化に向けた研究開発	・安全性を担保することによりこれまで出来なかった新たな価値を創出するデータセキュリティ技術の検討 ・異業種のデータを安全に融合して統計情報を出力する基盤の拡張検討、設計、構築業務	【必須】 ・差分プライバシー、TEE、準同型暗号の概念を理解していること。 【推奨】 仮説検定や確率分布など、統計分野に関する知見	〒100-6150 東京都千代田区永田町2-11-1 山王パークタワー	NTTドコモ
D5.会員認証・NFCに関するセキュリティ基盤の企画・開発・運用	コンシューマー向けdアカウント認証の企画・設計業務を体験いただけます。国際標準規格であるOpen ID ConnectやFIDOといった技術が実際の認証基盤にどのように組み込まれているのかを学ぶことができます。また、専門家によるレクチャーのもとプログラミングや統計計測ツールなどを利用した実演習をご体験いただけます。	【必須】 ・基本情報技術者程度の知識があること 【推奨】 なし	〒100-6150 東京都千代田区永田町2-11-1 山王パークタワー	NTTドコモ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D6.実践型のエンドポイントセキュリティ分析業務インターンシップ	NTTコミュニケーションズのセキュリティエンジニアとしてセキュリティの最前線で、先進的なエンドポイント振舞検知(EDR)製品を使用し、企業が直面するサイバーリスクの評価と対策の立案を行っていただきます。 インターンシップを通じて、エンタープライズレベルでのセキュリティ対策の理解を深め、セキュリティエンジニアとしてのキャリア形成につながることが期待できます。	【必須】 ・Linux、Windows、IPネットワークの基本的な知識を有すること ・エクセルやPythonを用いたデータ集計の経験があること ・サイバーセキュリティに関する専門教育を受けていること(大学・大学院) 【推奨】 ・サイバーセキュリティ関連の資格を保有している ・CTF参加や学会発表を行った経験がある	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ
D7.CSIRTでのサイバー攻撃等に関するOSINT業務等の実施	NTTコミュニケーションズ並びにグループ各社をサイバー攻撃から守るCSIRT業務のうち、OSINT業務やアタックサーフェスマネージメント等の情報収集並びに分析業務を実施していただきます。	【必須】 ・セキュリティに関する教育/学習の経験やCTF等へのイベントへの参加経験があることこと ・新聞やWebニュース等の記事や文章を読み、要点や要旨の要約が出来ること ・パソコンのトラブルは自分で解決できるスキルがあること(エピソードを語れること) 【推奨】 ・Linuxサーバ構築運用経験およびプログラミング言語を1つ習得済みであること	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D8.社内ネットワークに導入しているNDRの運用改善	NTTコミュニケーションズ並びにグループ各社をサイバー攻撃から守るCSIRT業務のうち、新たな脅威検知のためのデータ取得またはその分析業務を実施して頂きます。実際に使われているNDR'(Network Detection and Response)のデータに直接触れながら、分析の実業務を体験していただきます。	【必須】 ・情報セキュリティに関する専門教育を受けていること(高専/大学/大学院) ・Linuxサーバ構築運用経験およびプログラミング言語を1つ習得済みであること ・パソコンのトラブルは自分で解決できるスキルがあること(エピソードを語れること) 【推奨】 ・自身で手を動かし、FWやUTM、プロキシ、エンドポイントセキュリティの構築・設定・運用の一部を行ったことがあること	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ
D9.CSIRTでのサイバー攻撃への対応実践と高度化	NTTコミュニケーションズをサイバー攻撃から守るCSIRTで、EDR、SOARなど実際に使用している先進的なツールを使ったIR(インシデントレスポンス)業務に触れていただきます。 また、IR自動化などCSIRTが取り組んでいる高度化の施策について体験していただくことと併せて、サイバー攻撃対応の現在を学んでいただくポストです。	【必須】 ・情報セキュリティに関する専門教育を受けていること(高専/大学/大学院) ・情報システム(サーバ、ネットワーク等)に係る基本的な知識を有すること ・サイバーセキュリティ(攻撃/対応)に関して興味のあること 【推奨】 ・サイバーセキュリティ(攻撃/解析/対応)に関連する知識、イベント(CTF、Hardeningなど)参加経験があること	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D10.CSIRTでのインシデント対応における高度分析と組織の脆弱性対応実践	NTTコミュニケーションズをサイバー攻撃から守るCSIRTで、フォレンジックツールを用いた分析と、インシデントを抑止する大規模組織での脆弱性管理の現場を体験していただきます。	【必須】 ・情報セキュリティに関する専門教育を受けていること(高専/大学/大学院) ・情報システム(サーバ、ネットワーク等)に係る基本的な知識を有すること ・サイバーセキュリティ(攻撃/対応)に関して興味のあること 【推奨】 ・サイバーセキュリティ(攻撃/解析/対応)に関連する知識、イベント(CTF、Hardeningなど)参加経験があること	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ
D11.CSIRT運用業務の効率化に向けたシステム連携開発	インシデントチケットに関する業務フローを改善する開発の体験をしていただきます。具体的には、SOAR(Security Orchestration, Automation and Response)を活用してSIEM(Security Information and Event Management)から被疑対象の事象を抽出し、関連部署への周知・確認を行うためのツール改善に取り組んでいただきます。	【必須】 ・情報セキュリティに関する専門教育を受けていること(高専/大学/大学院) ・情報システム(サーバコマンド、仮想化等)に係る基本的な知識を有すること ・サイバーセキュリティ(攻撃/対応)に関して興味のあること 【推奨】 ・サイバーセキュリティ(攻撃/解析/対応)に関連する知識、イベント(CTF、Hardeningなど)参加経験があること	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ

セキュリティエンジニア

ポスト名	業務内容	応募要件	勤務地	受け入れ会社
D12.CSIRT運用業務におけるチケットシステムの高度化	セキュリティインシデントのチケットに関する業務フローを改善するシステム開発 の体験をしていただきます。インシデント対応に必要な情報を外部システムからAPIで取得することでチケットシステムの高度化に取り組んでいただきます。	【必須】 ・情報セキュリティに関する専門教育を受けていること（高専/大学/大学院） ・情報システム（アプリケーション開発）に係る基本的な知識を有すること ・サイバーセキュリティ（攻撃/対応）に関して興味のあること 【推奨】 ・サイバーセキュリティ（攻撃/解析/対応）に関連する知識、イベント（CTF、Hardeningなど）参加経験があること	〒100-8019 東京都千代田区大手町2-3-1 大手町プレイスウエストタワー	NTTコミュニケーションズ