

CybersecAcademy®

NTTデータでは、SOC/CSIRTを担うセキュリティ人財を育成するため『CybersecAcademy®』を立ち上げ、必要な知識・スキル獲得のための研修コンテンツをご提供しています。

不足が顕著な、
セキュリティ人財の育成を目指す

“グローバルで戦える” MDR実務者を育成できる

世界最大規模(55カ国19万人)の
“ゼロトラストグローバル基盤”
運用ノウハウを活用

“NTTDATA-CERT”※の
知見/メソッドを活用

NTTデータ社内のエンジニア育成
/顧客CSIRT・SOC要員育成
“実績多数”

※ NTTデータにおけるCSIRT組織。インシデント対応の黎明期から活動し、20年以上のノウハウを持つ。

■ ご提供する研修メニュー：セキュリティアナリスト、フォレンジックエンジニアについて、それぞれ「初中級」「中級」の2コースをご用意。

| レベル | 役割 | |
|--------------|-----------------|--|
| | セキュリティアナリスト(SA) | フォレンジックエンジニア(FE) |
| 上級 | タスク | — フォレンジック解析結果の品質に責任を持つ。中級のタスクに加えて、中級以下の教育指導も実施。 |
| | 研修 | — 【今後策定予定】 |
| 中級 | タスク | ログ抽出・分析作業で初・中級メンバをサポートしつつ、フォレンジックの要否や、対応の方向性を判断。顧客や社内関連組織との連絡窓口となる。 サブリーダーとして、初・中級メンバのサポートをしつつ、解析ツールを使用し、幅広く解析を実施。解析結果をまとめ、解析報告書を作成する。 |
| | 研修 | <ul style="list-style-type: none">4 インシデント対応: 2日5 ログ分析実践: 2日 <ul style="list-style-type: none">4 インシデント対応: 2日5 ログ分析実践: 2日6 マルウェア解析(Windows): 3日 |
| 初中級 (準中級) | タスク | Tier1から引き継がれたアラートについて、各組織との連絡やログ抽出・ログ分析を手順書に基づいて実施。 ファストフォレンジックやタイムライン等の情報の抽出、整理。インシデント関連情報の調査も実施する。 |
| | 研修 | <ul style="list-style-type: none">1 SOC・CSIRT: 4日2 フォレンジック基礎(Windows): 2日3 Kali Linuxによるサイバー攻撃基礎: 3日 |

■ : NTTデータでご提供中の研修メニュー

CybersecAcademy®研修プログラム ラインナップ

| レベル | コース名 | 日数 | 受講料(税抜) | 学習形態 |
|--------------|-------------------------|----|----------|-----------|
| 初中級 (準中級) | ① SOC・CSIRT | 4日 | ¥300,000 | Liveオンライン |
| | ② フォレンジック基礎(Windows) | 2日 | ¥150,000 | |
| | ③ Kali Linuxによるサイバー攻撃基礎 | 3日 | ¥225,000 | |
| 中級 | ④ インシデント対応 | 2日 | ¥225,000 | |
| | ⑤ ログ分析実践 | 2日 | ¥200,000 | |
| | ⑥ マルウェア解析(Windows) | 3日 | ¥300,000 | |

※ 個社開催、現地開催も承ります(金額は別途ご相談)。

監修者・講師(一部研修)：新井 悠



Executive Security Analyst (NTT DATA)

- 社内の情報セキュリティ事案対応や、人材育成を担当
- 経産省情報セキュリティ対策専門官、情報通信研究機構協力研究員
- NHK「クローズアップ現代+」出演等、専門家としてメディア発信多数

サイバーセキュリティの分野で20年近くの経験

- ペネトレーションテスト・脆弱性の解析・発見
- リバースエンジニアリング/マルウェア解析
- 数理モデル/機械学習

多くのサイバーセキュリティ関連の本の執筆・翻訳・監修

研修プログラム(一例)：SOC・CSIRT 4日間

本研修では講義を通しSOC、CSIRTの基礎知識の習得、EDR(CROWDSTRIKE)を用いたハンズオンを実施し、SOCについての理解、セキュリティインシデント発生を想定した初動対応について講義、演習を通し学習します。



カリキュラム

Day1 全体知識編

【SOC,CSIRT】

- ・SOC/CSIRTの全体像
- ・SOCとは
- ・CSIRTとは

Day2-3 SOCについて

【SOCについての講義、ハンズオン】

EDR(CROWDSTRIKE)を使用したシナリオを実施、機能についての理解深めます。その後、シナリオについてレポート作成を実施し報告までの流れを体験していただきます。

Day4 CSIRTについて

【インシデント初動対応についての講義、演習】

演習はチーム単位で実施し、特定の時間枠内で進行します。参加者は、与えられたシナリオに基づいて、インシデントの特定、インシデント対応手順の実行、情報共有、コミュニケーションなどを行います。

このような方に受講をオススメします



- SOC、CSIRTにこれから参画される方
- 情報セキュリティについて推進される方
- インシデントレスポンスに携わる方

受講すると?



- 講義を通し、SOC、CSIRTの基礎的な知識を習得。
- 講義、演習を通し、インシデントが発生した際の初動対応について個人の知識、技術レベルをアップします。

お申込期限

開催初日の**10**営業日前まで

キャンセル期限

開催初日の**10**営業日前まで

【本件に関するお問い合わせ先】

株式会社NTTデータ
テクノロジーコンサルティング事業部 CybersecAcademy®事務局
E-Mail: grsecurityacademy@am.nttdata.co.jp