一般的な IT スペシャリスト向けの最前線のインシデント対応トレーニング

Cybersecurity for IT Online

評価版
cito.kaspersky.com

kaspersky bring on the future

Kaspersky Cybersecurity for IT Online

Cybersecurity for IT Online（CITO）

サイバーセキュリティと最前線のインシデント対応に関する高度なスキルを身につけるための、一般的な IT スペシャリスト向けの対話形式のトレーニング

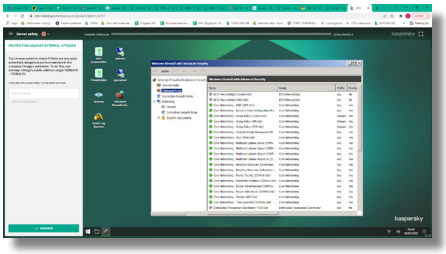
関係する従業員全員の体系的な教育なしには、企業として強固なサイバーセキュリティ体制を確立することはできません。大企業の多くは、サイバーセキュリティに関する教育およびトレーニングを、IT セキュリティチーム向けの専門的トレーニングと IT 担当でない従業員向けのセキュリティ意識向上の 2 つのレベルに分けて実施しています。カスペルスキーは両方に対応した包括的な製品を提供します。しかしそれでは足りないのが、標準的な意識向上プログラムでは十分でない、IT チームやサービスデスクなど、高度な技術的知識を持つ従業員への対応です。このような従業員にサイバーセキュリティのエキスパートになってもらう必要はありません。それでは時間とコストがかかりすぎます。

トレーニング形式

トレーニングは完全にオンラインで実施されます。受講者に必要なものは、インターネットへのアクセスと PC 上の Chrome ブラウザーのみです。6 つのモジュールがあり、それぞれが短い理論概要と実践的なヒント、具体的なスキルについて確認する 4 ～ 10 問の演習で構成されており、日常業務での IT セキュリティツールおよびソフトウェアの使用方法を学ぶことができます。

1 年を通して学習できるようになっています。お勧めのペースとしては、毎週 1 つの演習を進めます。1 つの演習の所要時間は 5 ～ 45 分です。

現行バージョンのトレーニングは、企業の Windows 環境が対象です。



トレーニングの提供方法：
クラウドまたは SCORM 形式

最前線のインシデント対応

カスペルスキーは、ゼネラリスト型の企業 IT 担当者向けに、これまでにないオンラインスキルトレーニングの提供を開始しました。トレーニングは、次の 6 つのモジュールで構成されます*。

- 悪意のあるソフトウェア
- 不要である可能性のあるプログラムやファイル
- 調査の基礎
- フィッシングインシデント対応
- サーバーのセキュリティ
- Active Directory のセキュリティ

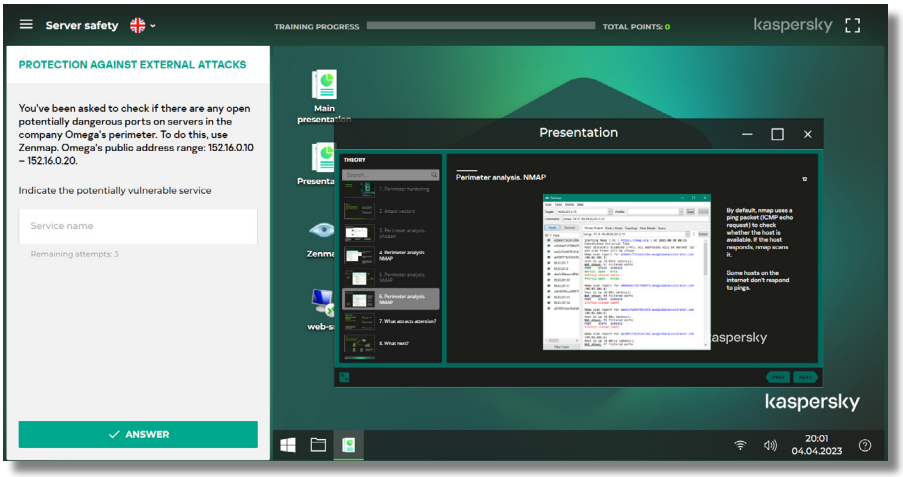
IT 担当者向けのプログラムで、一見問題なさそうに見えるインシデントに内在する攻撃の可能性を識別するための実践的なスキル、および IT セキュリティチームに引き継ぐためのインシデントデータの収集方法を身につけることができます。悪意のあるアクティビティの兆候を見逃さないという意識を高め、IT チームの全員がセキュリティ防御の最前線を担うという役割を固めるうえでも役立ちます。

CITO トレーニングが効果的な理由

- インタラクティブ：コンピューターへのリスクのない、現実的なプロセスのシミュレーション
- スキルと知識の習得：実践形式の学習
- 直感的な学習プロセス：便利なナビゲーションとヒント
- 一般的な IT 担当者が業務で直面する主な IT セキュリティのトピックや問題をすべて網羅

学習プロセス

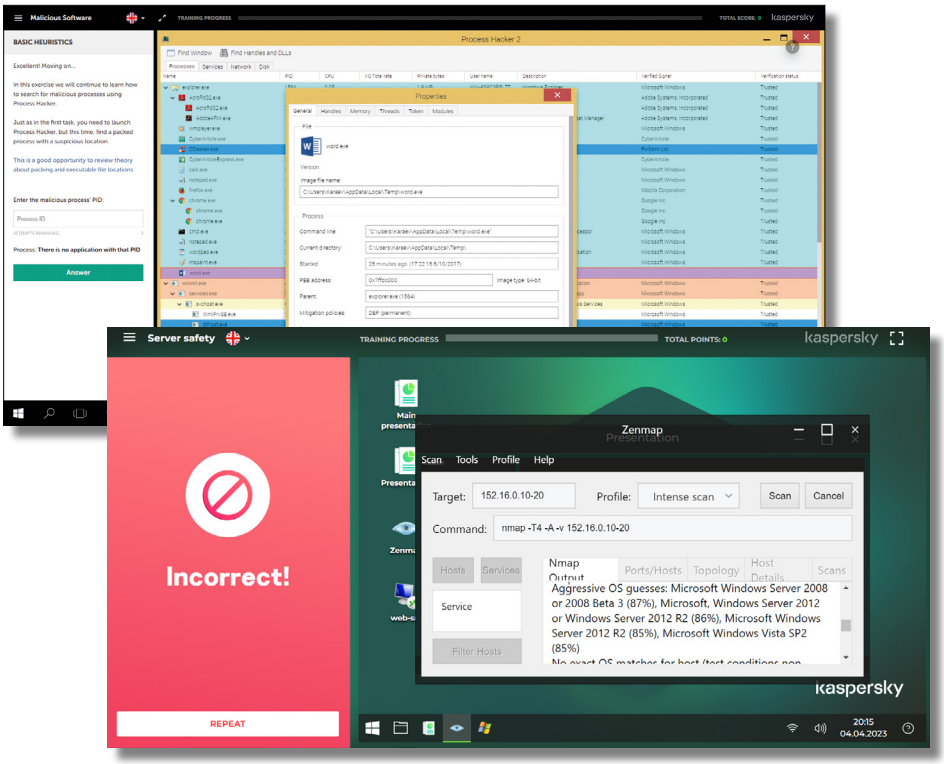
演習の 1 単位は学習と実践の 2 部構成になっており、説明の後にそれに関連する実際のプロセスを想定した課題があります。



* 最新のトピック一覧についてはこちらをご覧ください：cito.kaspersky.com

レッスンを終了したら、課題に取り組みます

正解できれば次の演習に進むことができ、正解できない場合は、ヒントを参考にするか、レッスンの教材を読み直して知識を再確認します

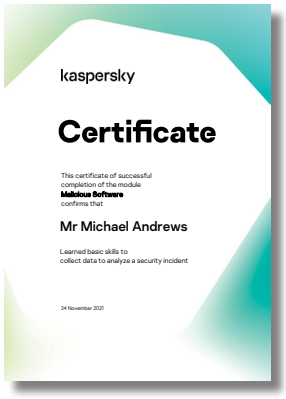


このトレーニングの対象者

このトレーニングは、組織内のすべての IT 担当者向けであり、特にサービスデスク担当者やシステム管理者に適しています。エキスパート以外の IT セキュリティチームのメンバーにも役に立つコース内容です。

認定

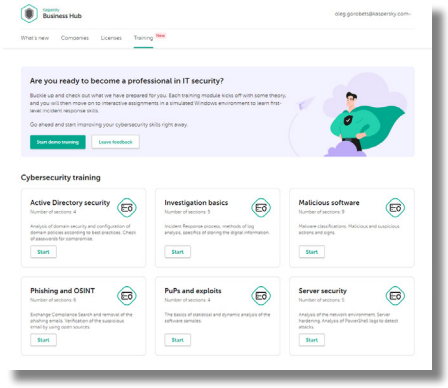
各モジュールを終了すると、個人の認定を取得できます



トレーニングのトピックと成果

モジュール名	対象者	学習内容	個人の姿勢	身につくスキル	モジュールでの演習
悪意のあるソフトウェア	サーバーやワークステーションの管理者権限を持つユーザー	マルウェアの手法と分類 悪意のある / 疑わしいソフトウェアの動作と兆候 ヒューリスティック分析の基本	マルウェアはコンピューターのどこにでも存在しうる マルウェアはさまざまな複雑な方法でデータを窃取できる 疑わしい潜在的なインシデントはすべてセキュリティチームに報告する必要がある	マルウェアに関連するインシデントの有無の確認	ツール（ProcessHacker、Autoruns、Fiddler、Gmer）を使用したマルウェアの検出

モジュール名	対象者	学習内容	個人の姿勢	身につくスキル	モジュールでの演習
不要である可能性のあるプログラムやファイル（PuP）	ソフトウェアを追加でインストールする権限を持つユーザー、および外部から受け取ったファイルを自分で診断したり開いたりするユーザー	ソフトウェアサンプルおよび疑わしいドキュメントの静的分析と動的分析の基本	ドキュメント（pdf、docx）にはエクスプロイトが含まれている可能性がある 署名のないファイルにはマルウェアやリスクウェアが含まれている可能性がある 署名のない実行可能ファイルはすべて　　感染の有無をチェックする必要がある デジタル署名はファイルに悪質な機能が含まれていないことを保証するものではない	システムおよびサンドボックスのイベントモニターの操作 統計情報エンジンの使用 不審なプログラム（PuP）の削除	ソフトウェアサンプルの静的（署名）分析と統計情報（VirusTotal）分析 ProcMon を使用した、エクスプロイトおよびソフトウェアの悪質なふるまいの検索 Cuckoo サンドボックスを使用したファイルの分析 AVZ を使用した、マルウェア削除用スクリプトの作成
調査の基礎	セキュリティチーム主導で行うフォレンジックやインシデント対応にかかわる IT 担当者	インシデント対応プロセス ログ分析の手法 デジタル情報の保存の詳細	サイバーセキュリティインシデントの疑いがある場合、即座にセキュリティチームに報告し、デジタルエビデンスを収集する セキュリティチームの監督のもとで連携しながら分析を行う必要がある	デジタルエビデンスの収集 NetFlowのトラフィック分析 タイムライン分析 イベントログ分析	揮発性データと不揮発性データの収集（FTK Imager） 攻撃のソースとリンクを見つけるためのログ分析（Event Log Explorer） NetFlow分析（ntop）によるラテラルムーブメントの調査 Autopsy を使用したディスク分析
フィッシングとオープンソースインテリジェンス（OSINT）	フォレンジックやインシデント対応にかかわる IT 担当者	最新のフィッシング手法 メールヘッダーの分析手法	フィッシングは非常に巧妙な場合があり、発見は困難ではあるが、手作業の調査で必ず発見できる ユーザーのメールボックスからフィッシングメールを削除する必要がある	フィッシングメールの分析およびユーザーのメールボックスの難読化されたフィッシングメールの削除 自社についてハッカーが何を知っているのかを理解するためのオープンソースインテリジェンス	Exchange メールボックス内のフィッシングメールの検索と削除 Web 調査のための Recon-ng の使用
サーバーのセキュリティ	サーバー管理者	ネットワーク環境の分析 サーバーの保護力強化 攻撃を検出するための PowerShell ログの分析	ネットワーク境界のセキュリティ侵害は主な攻撃ベクトルの 1 つである。すべての脆弱性をなくすことは不可能であり、攻撃の成功をできるだけ困難にするためには攻撃対象領域を縮小する必要がある。それにより侵入を止めることはできなくても、検知の時間を稼ぐことができる。	脆弱性のある、標準でないネットワークサービスの検索 「デフォルト拒否」の原則に従ったシステムの構成 PowerShell のログでの攻撃の兆候の検索	Nmap を使用した、脆弱性のあるネットワークサービスの発見 プログラム制御のためのソフトウェア制限ポリシーとネットワーク制御のための Windows ファイアウォールの構成 Event Log Explorer を使用したイベントの分析
Active Directory のセキュリティ	Active Directory 管理者	漏洩したパスワードのデータベース内のパスワードをチェックするための API の使用 推奨事項に沿ったドメインポリシーの構成 Active Directory ドメインセキュリティの分析手法	デフォルトの Active Directoryの構成は、セキュリティの観点から最適ではない。 攻撃者はさまざまな方法で権限を昇格させることができる。 セキュリティに関する推奨事項について学び、Active Directory の可視性を向上させるツールを使用する	データベース内のパスワードのハッシュ値の確実なチェック 推奨されているドメインポリシーと実際のドメインポリシーの差異の検索 Active Directory の設定のセキュリティの評価	「Have I Been Pwned?」API を使用した、漏洩したパスワードのデータベースの検索 Policy Analyzer を使用した、現在のドメインポリシーとベストプラクティスの比較 Ping Castle レポートの使用



Kaspersky Endpoint Security Cloud との連携

KES Cloud Pro ユーザーが Business Hub から直接利用できる CITO トレーニングで、サイバーセキュリティのスキルを高め、専用のサイバーセキュリティ製品を最大限に活用できるようになります。

Kaspersky Security Awareness – IT セキュリティスキルを身につけるための新しいアプローチ

すべての人が使える、単一のフレキシブルなソリューション

Kaspersky Security Awareness には、長年にわたる世界的な実績があります。企業の規模を問わず **75 か国以上の国々の 100 万人を超える従業員の教育**に使用されているこのソリューションには、カスペルスキーが 25 年以上にわたって培ってきたサイバーセキュリティに関する経験と社会人向け教育の豊富な経験が活かされています。

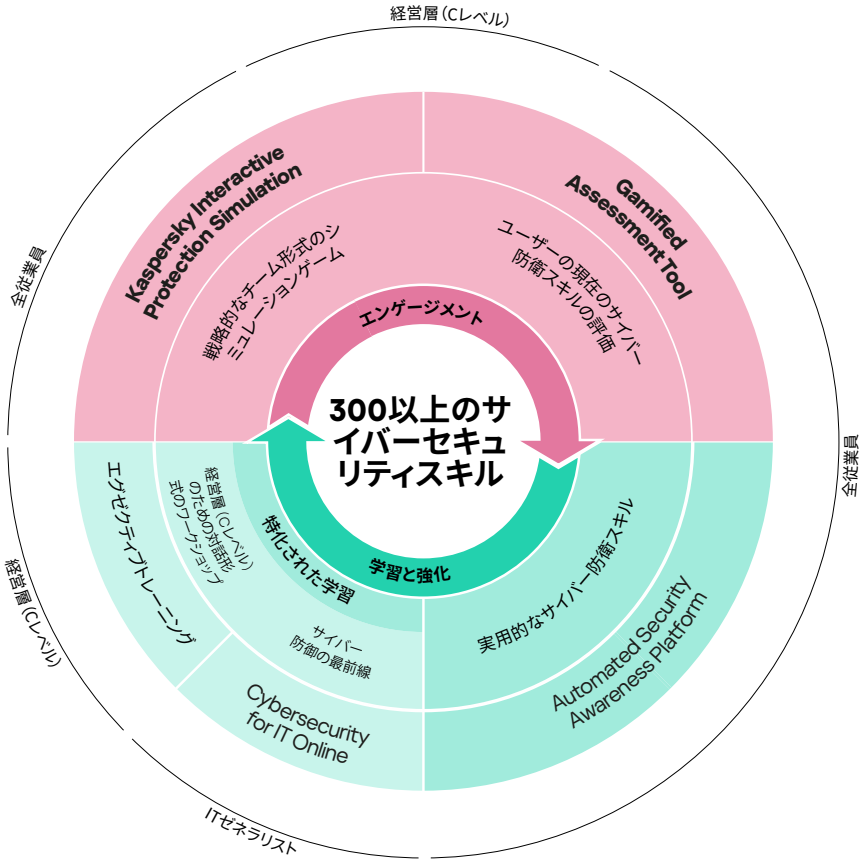
魅力的なトレーニングの選択肢が幅広く用意されており、職位を問わずあらゆる従業員が**サイバーセキュリティ意識を向上させ**、組織全体のサイバーセキュリティにおいて各自が自分の役割を果たせるようになります。

行動に変化をもたらすには長期間を要することから、複数の構成要素が含まれる継続的な学習サイクルの構築に関わるアプローチがとられています。ゲームベースの学習は、上級管理職を巻き込み、彼らをサイバーセキュリティイニシアチブの支持者や、サイバーセーフな行動をとる文化構築の支援者に変えます。ゲームを利用したアセスメントにより、従業員の知識のギャップを明確にし、さらなる学習へのモチベーションを高めることができ、オンラインプラットフォームとシミュレーションにより、従業員に正しいスキルを身につけさせ、強化することができます。

プログラムの主な特長

サイバーセキュリティに関する豊富な知識
25 年以上におよぶサイバーセキュリティの経験をもとに、製品の中核となるスキルセットを構築

組織のあらゆるレベルで、従業員の行動を変えるトレーニング
ゲーム形式のトレーニングはエデュテイメントを活用した、学習意欲のわく内容で、学習プラットフォームを通じて、サイバーセキュリティスキルを吸収でき、学んだスキルを長く記憶することができます。



エンタープライズサイバーセキュリティ：www.kaspersky.co.jp/enterprise
Kaspersky Security Awareness：www.kaspersky.com/awareness
カスペルスキーの Cybersecurity for IT Online：cito.kaspersky.com

www.kaspersky.co.jp

kaspersky bring on the future