カスペルスキー セキュリティ トレーニング コース カタログ

www.kaspersky.co.jp
#truecybersecurity

カスペルスキー セキュリティ トレーニング

日々高度化を続ける脅威に直面するエンタープライズ企業にとって、サイバーセキュリティに対する啓発とそれらの脅威に対処するためのスキル育成はとても重要な取り組みとなっています。特にセキュリティ管理者は、未知の脅威の発見とインシデントへの適切な対処のために高度な技術を習得する必要があります。

カスペルスキー セキュリティ トレーニングはサイバーセキュリティの幅広いテーマをカバーしており、基礎からエキスパートレベルまでの技術が習得できるように設計されています。

全てのコースは理論とハンズオン(ラボ)が用意されています。コース終了後、受講者は習得した知識と技術を実践の場面で使い、評価できるようになります。

トレーニングの利点

デジタルフォレンジック トレーニング

CSIRTなどセキュリティインシデントに対処する技術者(フォレンジック技術者)のスキルを育成、強化します。コースでは、より実践的なスキルを身につけるため、様々なケースで取得されたデータを解析し、インシデントのタイムラインと原因を解明していきます。コースが終わると受講者はセキュリティインシデントの全般的な調査とセキュリティ強化のための再発防止策を提案することができるようになります。

マルウェア解析 & リバースエンジニアリング トレーニング

受講者は悪意のあるソフトウェア(マルウェア)の解析手法を習得してしてIoCs(Indicators of Compromise)を記述することができるようになるります。受講後は、的確に脅威を検出し、感染したファイルやドキュメントからマルウェアを駆除できるようになります。

インシデントレスポンス トレーニング

CSIRTの担当者がセキュリティインシデントに対処するための対応方法を習得し実践できるよう全般的な知識とスキルを身につけます。

Yara トレーニング

脅威を検出するための効果的なYaraルールの記述方法を習得します。

KATA 管理者 トレーニング

KATA[1] の導入設計、インストール、設定の方法を習得します。

KATA セキュリティ アナリスト トレーニング

KATAの監視、運用方法ならびに、検知したセキュリティインシデントのアラート、レポートを解釈しインシデントに適切に対処する方法を習得します。

セキュリティ担当者や専門家に加えて経営者、管理者から一般従業員にわたって、サイバーセキュリティに関する意識を高め、リスクを最小化する行動を習得し、組織のセキュリティ文化を醸成します。

セキュリティの啓発

- ゲーム形式サイバー演習
- 管理職向けサイバー演習
- モジュール型オンライントレーニングプラットフォーム

[1]KATA: Kaspersky Anti Targeted Attack Platform
www.kaspersky.co.jp/enterprise-security/anti-targeted-attacks

トレーニングの概要

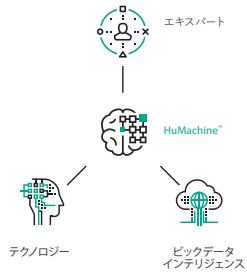
トピック	期間	習得するスキル
デジタルフォレンジック -基礎編-		
• デジタルフォレンジック入門 • ライブレスポンスと証拠保全 • Windowsレジストリの構造 • Windows アーティファクト解析 • ブラウザーのフォレンジック • 電子メールの解析	5 日間	• フォレンジックラボの構築 • 証拠データの保全と適切に取り扱う方法 • タイムスタンプを使ったインシデントの再現 • Windowsのアーティファクト解析による侵入経路の追跡 • ブラウザーとメールの履歴の追跡と解析 • デジタルフォレンジックツールの使い方
マルウェア解析とリバースエンジニアリング -基礎編-		
• マルウェア解析とリバースエンジニアリングの目的とゴール • Windowsの内部構造, PEファイル, x86 アセンブラー • 静的解析の基礎 • PE エントリーポイント, アンパックツールの使い方 • 動的解析の基礎 (デバッグ, 監視ツール, トラフィックのインターセプトによる解析) • .NET, Visual Basic, Win64形式のファイル解析 • スクリプト、PE形式ではないマルウェアの解析方法 (バッチファイル; Autoit; Python; Jscript; JavaScript; VBS)	5 日間	• マルウェア解析のための環境構築: サンドボックスとツールのインストール • Windowsプログラムの動作原理 • オブジェクトのアンパック、デバックによるマルウェア機能の記述 • スクリプト形式のマルウェアの解析と悪意のあるサイトの検出 • マルウェアの簡易解析
デジタルフォレンジック -発展編-		
• Windowsの詳細なフォレンジック解析 • データ復元 • ネットワークとクラウド環境のフォレンジック • メモリフォレンジック • タイムライン解析 • 標的型攻撃の調査、解析、演習	5 日間	• ファイルシステムの詳細なフォレンジック解析 • 削除されたファイルの復元 • ネットワークトラフィックの解析 • メモリダンプの解析と悪意のある振る舞いの抽出 • インシデントのタイムラインの再現
マルウェア解析とリバースエンジニアリング -発展編-		
• 高度な静的解析の技術 (シェルコード、PEヘッダの分析, TEB, PEB, 異なるハッシュアルゴリズムによるロード機能の解析) • 高度な動的解析の技術 (PEの構造, 手動によるアンパッキング, 難読化の解除による実行コードの抽出) • APT、標的型攻撃で使われたマルウェアのリバースエンジニアリング • プロトコル解析 (暗号化されたC&Cサーバとの通信の解析) • ルートキットとブートキットの解析(IdaとVMWareを使ったブートセクターのデバッグ, カーネルデバッグ)	5 日間	• アンチリバースエンジニアリング、アンチデバック機能を持つマルウェアに対する最適な解析方法 • ルートキット、ブートキットに対する最適な解析方法 • 様々なファイルに組み込まれているエクスプロイト、シェルコードの解析方法 • Windows以外のOSに感染するマルウェアの解析方法
インシデントレスポンス		
• インシデントレスポンス入門 • インシデントの検知手法と初動対応の方法 • 証拠の取得とデータの解析 • 脅威の検知ルールの記述方法(Yaraルール、Snort, Bro)	5 日間	• APT、標的型攻撃とその他の脅威の違い • 攻撃者のテクニックとAPT、標的型攻撃が示す不審なシステムの振る舞い • システムの監視と脅威の検出方法 • インシデントレスポンスのワークフロー • インシデントの時系列と再現 • 脅威の検知ルールの作成と検出
インシデントレスポンス -入門-		
• インシデントレスポンスとは？ • インシデント対応のフローと対応内容 • インシデント対応に必要な機材とツール • 証拠保全の方法 • データの簡易解析	2 日間	• インシデントレスポンスの概要とキーワード • インシデント対応に必要な機材とツールの使い方 • 適切な証拠保全の方法

トレーニング概要

トピック	期間	習得スキル
Yara トレーニング		
• Yara 構文 • 効果的なルールを記述するためのコツ • Yara 生成ツールの使い方 • Yaraルールを使った未知のマルウェアの検出(演習) • さらに効率的に脅威を検出するためのYara 外部モジュールの活用方法	2 日間	• 効果的なYaraルールの記述 • 未知の脅威の検出
KATA 管理者 トレーニング		
• ソリューションの導入設計 • ハードウェア構成とサイジング • ライセンスの考え方 • サンドボックスサーバ、セントラルノード、ネットワークセンサー、エンドポイントセンサーの仕組みとインストール • ライセンスのアクティベーションとデータベースのダウンロード • ソリューションの動作原理	1 日間	• お客さまの環境に合わせたKATAの設計と導入 • 各コンポーネントのインストールとセットアップ • KATAの管理と運用
KATA セキュリティ アナリスト トレーニング		
• KATA のインシデント検出とアラートの解釈 • インシデントのログとログ解析 • 脅威のスコアリングとリスク	1 日間	• KATAのインシデント検知の仕組みとアラートの意味の理解 • ログの解釈とインシデントに対する適切な対処

セキュリティの啓発

トピック	習得スキル
ゲーム形式サイバー演習: Kaspersky Interactive Protection Simulation (KIPS)	
以下のシナリオを用意しています。 企業版　自治体版　銀行版　発電所版　浄水場版	• サイバー攻撃によるビジネスへの影響の理解 • ディスカッション、共同作業によるチームワーク • セキュリティ予算の効果的で効率的な使い方 • セキュリティ製品のみならず、セキュリティ監査、トレーニングなどの重要性の理解
管理職向けサイバー演習: CyberSafety Management Game	
日々従業員と接する管理者として、業務の効率を落とすことなく組織の安全を高めるために、いかにビジネス上の判断を下すかをゲーム形式で習得します。	• 日常行動のサイバーセキュリティ対策 • セキュリティを考慮したビジネス上の意思決定 • セキュリティ視点からの日常業務のモニタリング • 従業員に対するセキュリティリーダーシップ
モジュール型オンライントレーニングプラットフォーム: Employee Skills Training Platform	
様々なビジネスの場面における多くのサイバーリスクとその対処方法について、対話形式で継続的にトレーニングを受講できるオンラインプラットフォームです。	以下のモジュールを提供します。 セキュリティの基礎・エグゼクティブ向けセキュリティの基礎・URLの見方・emailセキュリティ・フィッシング・パスワード・ソーシャルネットワーク・ランサムウェア・モバイル端末・USBデバイス・物理セキュリティ・社外でのセキュリティ・安全なウェブブラウジング・ソーシャルエンジニアリング・個人情報・PCI DSS・データ保護・HIPPAに基づく健康情報保護・出張時のセキュリティ



株式会社カスペルスキー
お問い合わせ：jp-sis@kaspersky.com
エンタープライズセキュリティ: **www.kaspersky.co.jp/enterprise-security/**
SECURELIST: **www.securelist.com**
公式ブログ: **blog.kaspersky.co.jp**

www.kaspersky.co.jp

BD-KSIS-CST-02-201708