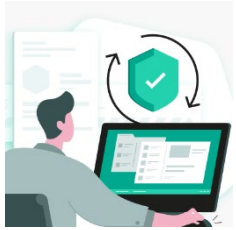
Kaspersky xTraining

2024年12月02日
株式会社カスペルスキー
セールスエンジニアリング本部

V1.1

Kaspersky xTraining：サービス概要



■実務に携わるエキスパートが設計したトレーニングをオンデマンドで提供

-インシデントレスポンス・デジタルフォレンジックを行うチームのマネージャーが長年の経験から培った専門知識を活かして
トレーニングを設計、トレーニングを通じて効果的な脅威検出・緩和に必要な最新の知識を提供

-専門知識の解説は英語字幕付き動画で提供、受講者はインターネット接続可能な端末から好きなペースで学習可能

■仮想ラボでの演習

-必要なツール・実際の攻撃を再現したシナリオがセットされた仮想ラボで実践的なマルウェア解析やインシデント対応を
体験することでスキルを習得

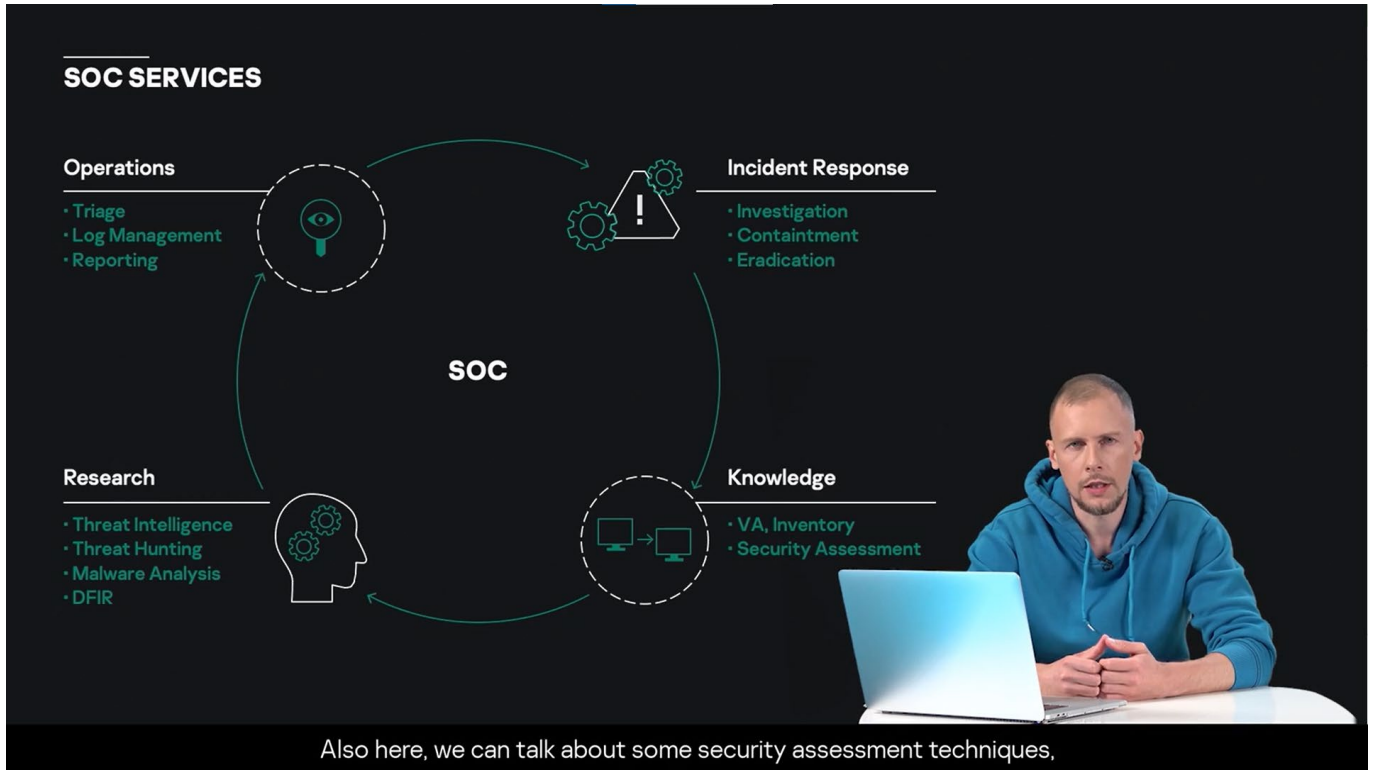
■充実したサポート

-トレーニング中、受講者はカスペルスキーのエキスパートに問い合わせ可能、理解を深めるためのアドバイスなどを提供

-カスペルスキーが定期的に開催するサイバーセキュリティに関するさまざまなトピックのブートキャンプへ参加可能

Kaspersky xTraining：動画講習

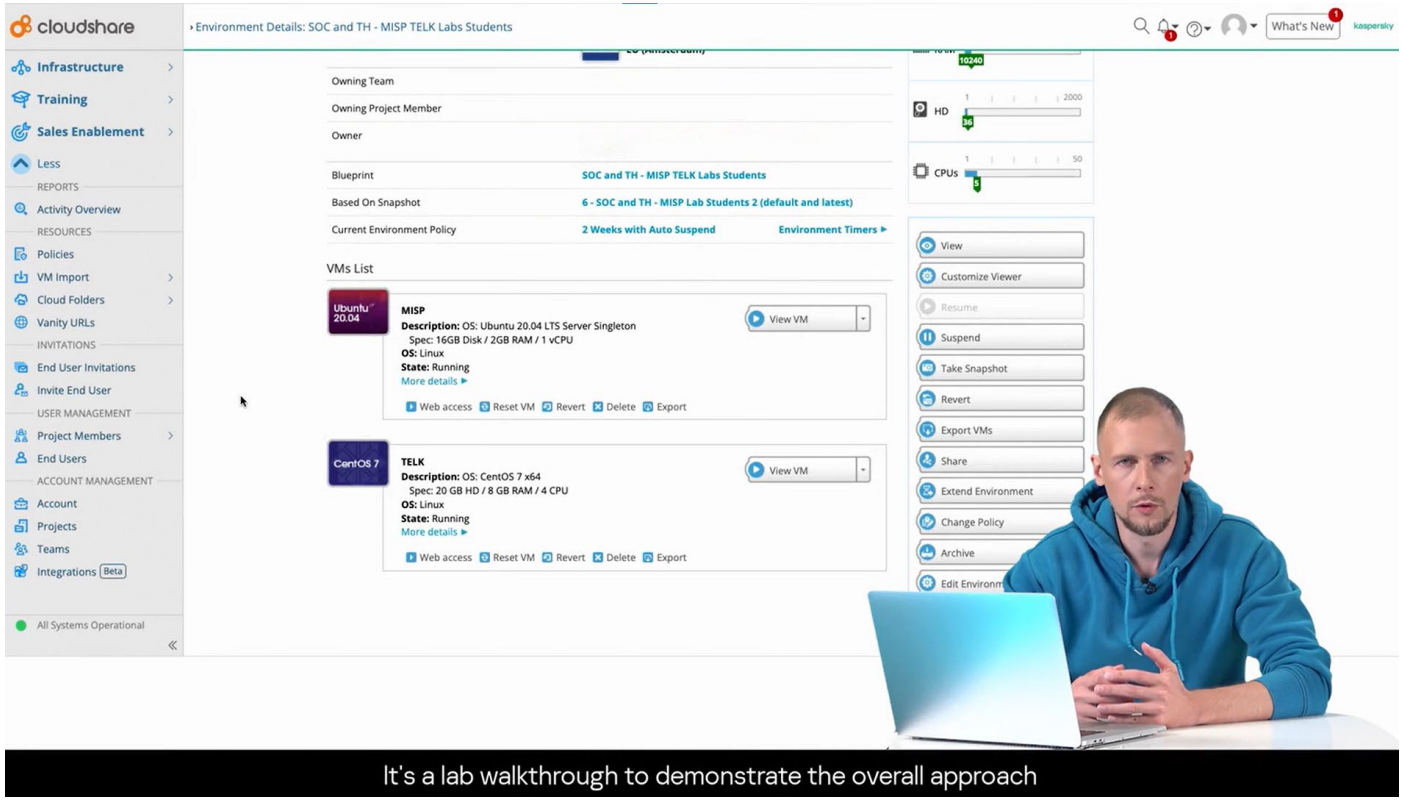
-インシデントレスポンス・デジタルフォレンジックを行うチームのマネージャーが長年の経験から培った専門知識を活かして
　トレーニングを設計、トレーニングを通じて効果的な脅威検出・緩和に必要な最新の知識を提供
-専門知識の解説は英語字幕付き動画で提供、章ごとに用意されたクイズで内容を振り返りながら、自身の理解度を把握
-有効期間：6か月間、受講者はインターネット接続可能なPC・タブレットから好きなペースで学習が可能



参考：動画講習サンプル画像

Kaspersky xTraining：仮想ラボ演習

-必要なツール・実際の攻撃を再現したシナリオがセットされた仮想ラボへのアクセス権を提供（使用可能時間=100時間まで）
-実践的なマルウェア解析やインシデント対応を体験することで動画だけでは学ぶことが難しいスキルを習得
-演習の進め方は動画で講師が同じ仮想ラボ環境を使い、ステップバイステップで分かりやすく解説
-途中で分からないことがあった場合、メールでカスペルスキーの担当者に直接質問が可能（言語：英語）



参考：仮想ラボ演習の解説動画
サンプル画像

講師紹介

Ayman Shaaban

デジタルフォレンジック
インシデントレスポンス
グループマネージャー

＜来歴＞

・2014年、グローバル緊急対応チーム(GERT)のメンバーとして
カスペルスキーに入社、
現在はGERTのデジタルフォレンジック・インシデント
レスポンス(DFIR)マネージャーとして勤務し、様々な
業界におけるサイバーインシデントへの対応・分析に従事

・通信工学の学士号・サイバーセキュリティの修士号
およびDFIRに関するさまざまな認定資格も取得

Igor Kuznetsov

グローバル調査分析チーム
(GReAT)マネージャー

＜来歴＞

・20年以上のリバースエンジニアリングの経験を持ち、
マルウェアキャンペーンの調査と高度なマルウェアを
理解するためのリバースエンジニアリングに従事

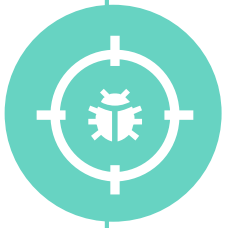
・近年は深い知識とスキルを活かし、iOSデバイスを
標的としたAPT攻撃「Operation Triangulation」の
調査・分析に従事

コース一覧

・中級レベル以上のサイバーセキュリティ専門家を対象に全11トレーニングを提供
・個々のトレーニングは独立しているので、スキル強化に必要なトレーニングだけ受講することが可能

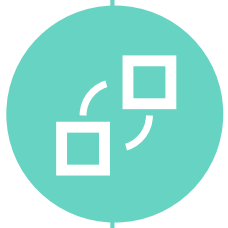
<サイバーリスクマネジメント>

-Cybersecurity for executives online training



<インシデントレスポンス>

-Windows incident response
-Windows digital forensics



<脅威ハンティング>

-Hunt APTs with YARA like a GReAT ninja
-Suricata for incident response and threat hunting
-Security operations and threat hunting

<リバースエンジニアリング>

-Reverse engineering 101
-Targeted malware reverse engineering
-Mobile malware reverse engineering
-Advanced malware analysis techniques
-Advanced reverse engineering with Ghidra

参考:コース体系

コース難易度	1	2	3	4	5
コース名	Cybersecurity for executives online training →	Security Operations And Threat Hunting →	Hunt APTs with YARA like a GReAT ninja もしくは Windows Incident Response → Windows Digital Forensics もしくは Suricata for Incident Response and Threat Hunting	→ Reverse Engineering 101 →	Advanced Malware Analysis Techniques Targeted Malware Reverse Engineering Mobile Malware Reverse Engineering Advanced Malware Reverse Engineering with Ghidra
対象者と必要な知識	経営者向け	トリアージ・脅威ハンティングをメイン業務とするSOCアナリスト	調査・脅威ハンティングをメイン業務とするSOCアナリスト コース難易度2修了と同等の知識	マルウェアアナリスト アセンブリ言語・C言語の基礎知識 or コース難易度3修了と同等の知識	マルウェアアナリスト アセンブリ言語・C言語の基礎知識 or コース難易度4修了と同等の知識

コース概要：サイバーリスクマネジメント

目的： 組織のセキュリティレベルを強化するために必要な知識・スキルを習得

■Cybersecurity for executives online training

概要：

経営者・リーダー向けの必要なサイバーセキュリティの基本的な知識とビジネス、組織への適用方法の学習

-サイバーセキュリティ概要・リスク・ビジネスへの影響
-サイバー攻撃に使用されるツール・手法
-企業をサイバー攻撃から守るために必要なこと
-サイバー攻撃発生時の対応
-サイバーセキュリティの今後

コース概要：インシデントレスポンス

目的： 社内のデジタルフォレンジック・インシデント対応チームの専門知識の向上

■Windows incident response

概要：
インシデントレスポンスに必要な知識・スキルを学習し、
社内のインシデント対応チームを強化

-インシデントプロセスの各フェーズ（準備・検知・分析・
封じ込め・根絶・復旧）解説およびプラン作成
-インシデント検知・分析手法
（IRCD / PowerShellを使用したアプローチ）
-エビデンス収集
-メモリ・ログおよびネットワーク分析
-脅威インテリジェンスについて（IoC/Yara）

■Windows digital forensics

概要：
フォレンジックに必要な知識・スキルの学習と現実の
シナリオ体験を通してインシデント対応を包括的に理解

-インシデントプロセス概要・ケーススタディ
-エビデンス収集
-ライブ解析・レジストリ解析
-Windowsアーティファクト
（RDP / イベントログ / PowerShellログ ）
-フォレンジック手法
（NTFS / ブラウザ（Edge, Chrome, Firefox）/
メール）

コース概要：脅威ハンティング

目的： 効果的な脅威検知に必要な知識・スキル、ツール使用方法の習得

■ Hunt APTs with YARA like a GReAT ninja

概要：
Yaraルールを活用したAPT攻撃の検出手法の学習

-Yara概要
-Stringベースルール
-Yara活用方法
-Virus Totalとの連携
-仮想環境での演習
（実際の攻撃を再現した複数のシナリオ）

■ Suricata for incident response and threat hunting

概要：
Suricataを使ったネットワークトラフィック分析・脅威検出手法

-NIDS、Suricara概要
-ルール作成方法・演習
（HTTP、DNS、TCP、SSL/TLS）
-典型的な攻撃の検出方法・演習

■ Security operations and threat hunting

概要：
SOC専門知識と効率的な脅威ハンティング手法の習得によるSOCの強化

-SOC解説
（役割・ユースケース・手法など）
-脅威ハンティング手法・演習
Windows/Linux/ネットワークにおける脅威検出手法

コース概要:リバースエンジニアリング（1/3）

目的： マルウェアを解析する上で重要な「リバースエンジニアリング」に必要な知識・スキルの習得

■Reverse engineering 101

概要:
マルウェア分析に必要な基本知識の習得

-アセンブリ言語入門
-IDA(逆アセンブルソフト)使用方法、サンプル解析
-C言語:構造解説
-スタック・ヒープ解説
-サンプル解析
（C++、C++ STLのコンテナ型、Go言語、Rust）

■Targeted malware reverse engineering

概要:
実際に使用された標的型マルウェアの分析を通して
さまざまなツールを使用方法と実践的な解析を経験

-マルウェア分析:
使用ツール: IDA Pro、Hex-Rays decompiler,
Hiew, 010Editorなど
APTアクター:Chafer、LuckyMouse、Biodata、
Toniambour、DeathStalker、
MontysThree、Lazarus、
Cloud Snooper、Cycldek’s

コース概要：リバースエンジニアリング（2/3）

目的： マルウェアを解析する上で重要な「リバースエンジニアリング」に必要な知識・スキルの習得

■Mobile malware reverse engineering

概要：
モバイルマルウェア基本事項・解析に必要なスキルの学習

-モバイルマルウェア解析手法解説・演習
サンプル：DuKong、LightSpy、MagicKarakurt
解析手法：静的解析（逆コンパイル、マニフェスト調査、
Ghidraによるライブラリ分析など）
動的解析（Fridaフレームワークによる
コンフィグファイルダンプ、
アンパッキングなど）

■Advanced malware analysis techniques

概要：
実用的なサイバー攻撃の証拠を見つけるために必要な
高度な静的分析、日常的なタスクの最適化の解説

-IDA Pro：機能解説
-Shell：コード・データフロー分析、スタック、レイアウト
手動でのデータ構造の再構築
-静的復号化解説・演習
-単一PEファイルのリバースエンジニアリング演習
-ドキュメントベースのエクスプロイト解説・演習
-動的な復号化/解凍アプローチ、演習

コース概要:リバースエンジニアリング（3/3）

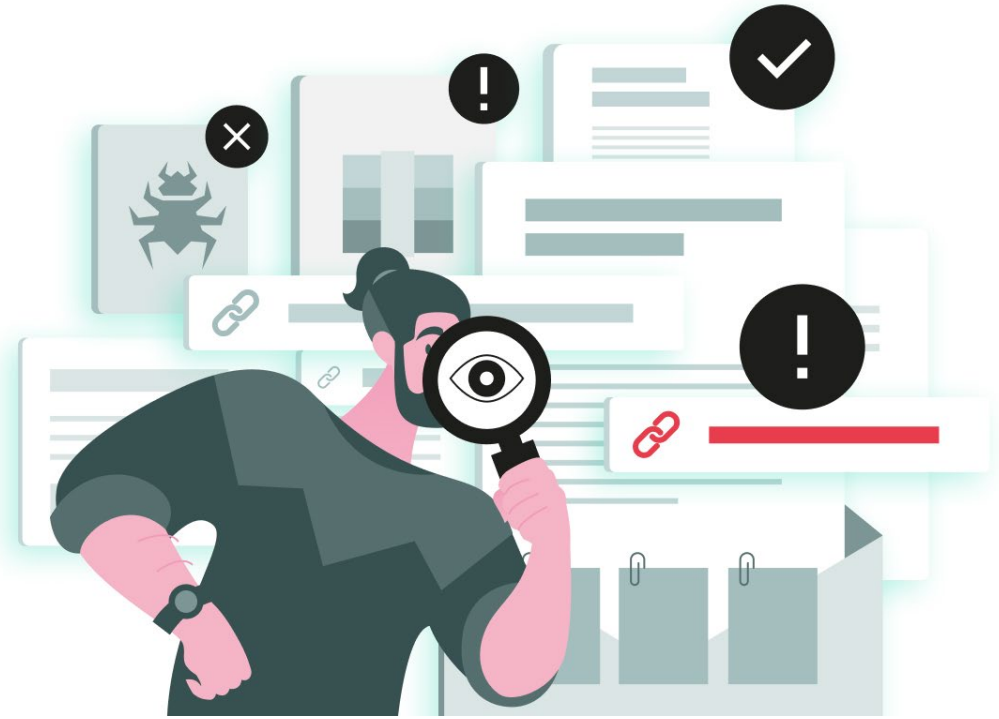
目的： マルウェアを解析する上で重要な「リバースエンジニアリング」に必要な知識・スキルの習得

■Advanced reverse engineering with Ghidra

概要:

リバースエンジニアリングツール「Ghidra」の使用方法と
マルウェア解析への活用方法の学習

-Ghidra概要、分析ワークフロー解説
-PEヘッダー構造を使用するコードの分析
-APIハッシュアルゴリズムの分析、Python・Jayaによる
API分析スクリプト実装
-ライブラリ識別、構造・関数ポインタ、逆コンパイル手法
-Eclipse IDEを使用した機能拡張方法



xTraining価格表

コース名称	市場想定価格
Cybersecurity for executives online training	260,480
Security Operations And Threat Hunting	165,000
Hunt APTs with YARA like a GReAT ninja	97,500
Windows Incident Response	135,000
Windows Digital Forensics	210,000
Suricata for Incident Response and Threat Hunting	102,750
Reverse Engineering 101	106,500
Advanced Malware Analysis Techniques	315,000
Targeted Malware Reverse Engineering	165,000
Mobile Malware Reverse Engineering	102,750
Advanced Malware Reverse Engineering with Ghidra	207,550

税別、全て1ユーザー1ライセンス当たりの価格
契約期間は6カ月

Kaspersky xTraining は、お取引のある販売会社様から購入できます。

詳しくはjp-sales@kaspersky.comまでお問い合わせください。

ありがとうございました

kaspersky