インシデントレスポンス トレーニング

KASPERSKY
Save the World from IT threats

12月4日(月)　～　12月8日(金)　開催決定！

場所: 株式会社カスペルスキー　東京本社@秋葉原

言語: 英語、同時通訳付き
日本人のエンジニアがサポートします。

費用: *540,000*円(税抜)

9月中のお申し込みで 15% OFF！！
459,000円

申込期限: *11*月6日

お申し込み方法: 添付のお申し込み用紙にご記入のうえ、
販売代理店経由でお申し込みください。

*Kaspersky Lab*オリジナルのトレーニング、他トレーニングとの違い・・・

- **実際に起きた標的型攻撃の解析を体験いただきます。**
- **ツールによるフォレンジック解析に加え、手動での解析方法についても講義**
- **話題のツール *Maltego, YARA, SNORT*他、フォレンジックツールの使い方と活用方法を体得できます。**
- **世界の法執行機関や金融機関などの要請によってインシデント調査を実施する *Kaspersky Lab*のリサーチャーが現場で　”使える”　知識 と スキル と ノウハウを伝授します。**

※最大収容人数*(20*名様) のお申し込みをもって受付を終了させていただきます。
また、お申し込みが、*10*名に満たない場合は開催を見送る場合があります。

コースの内容

対象

- セキュリティインシデントに対応するIT、セキュリティ担当者
- CSIRT、SOC担当者
- これから、そのような業務を担当したり、組織に配属される方

概要

このトレーニングを受講すると以下のことができるようになります。

- インシデント対応フレームワークの理解
- インシデントを速やかに解消するための、迅速かつ適切な対処方法に関する知識とスキルの習得

1日目

インシデント対処するうえでの事前準備、発生時の対応、発生中の対応、収束後の対応について、それぞれ説明します。次に、Kaspersky Labの標的型攻撃対策ソリューションで発見されたAPTの被害を体験して、なぜ標的になってしまうのか？どのようにして脅威が既存のセキュリティシステムを突破してしまうのか？その脅威をどのように検出すればよいのか？を説明します。

トピック

- インシデントレスポンスの用語
- インシデントのタイプ
- キルチェイン(標的型攻撃のステップ)
- インシデント対応のフロー
- APT、標的型攻撃と、それ以外のサイバー攻撃について

ツール、ラボ、デモ

- 実際のAPTの体験、デモ
- Kaspersky Labの標的型攻撃対策ソリューションを使った監視と検知のデモ

裏面に続きます。

2日目

標的型攻撃のシナリオについて説明し、攻撃を検出するためのインジケータやシステム監視のテクニックについて解説します。また、初動での調査方法を習得し、誤検知の見分け方、攻撃を受けたシステムからの悪意のあるURLへの接続を検出する方法など、詳細な調査につながる情報を収集する方法を習得します。さらに調査を進めるために重要な証拠の選択と、証拠を保全して適切に扱う方法を説明します。リモートで証拠を保全する方法についても説明します。

トピック

- APT、標的型攻撃のシナリオ
- インシデントのインディケータ
- インシデントを検知するためのシステム監視方法
- 初動対応と初動での調査方法
- IRCDを使ったライブレスポンス
- 情報の収集と証拠保全(メモリダンプ、ハードディスク、ネットワークキャプチャ、ログ取得)
- オンラインツールの活用方法
- リモートでの情報収集と証拠保全

ツール、ラボ、デモ

- Sysinternals, IRCD(DEFT, dart, CAINE, UFO, HELIX)
- Whois、ドメインツール、Maltego
- オンラインサンドボックス、レピュテーションデータベース
- Dumpit, FTK Imager, HELIX

3日目

デジタルフォレンジックの手法について紹介します。フォレンジックツールを使った調査方法と、知識とスキルを活かした手動での調査方法について解説します。続いて、実際に感染したシステムから取得したシステムのArtifact、ハードディスクイメージ、ネットワークログなど、様々な証拠の分析を行い、分析結果を統合して、一つのインシデントのタイムラインを構築し、サイバー犯罪者による攻撃の流れとマルウェアの活動の履歴を追います。

トピック

- デジタルフォレンジック入門
- フォレンジックで利用するツール
- ディスクイメージの解析
- OSのArtifactの解析
- タイムライン
- メモリフォレンジック
- ログ解析
- トラフィック解析

ツール、ラボ、デモ

- TSK
- Autopsy
- Volatility
- NetworkMiner

4日目

これまで調査、解析した情報から、脅威によるインシデントの再発を防止するため、IOCを作成する方法を講義します。これまでの解析情報からYARAやSnortなど、様々なフォーマットでのIOCの作り方とアップデートの方法を習得します。また、インシデントに関するレポートの作成方法とその必要性について解説します。これが終わると、組織にCSIRTを組織することができるようになります。

トピック

- 検知ルールの作成
- レポートの作成
- CSIRTの組織

ツール、ラボ、デモ

- YARA
- SNORT
- Bro

5日目

4日間のトレーニングで習得した知識、スキルを試すための試験、おさらい、Q&Aを実施します。

KASPERSKY lab
Save the World from IT threats

■ お問い合わせ ■
株式会社カスペルスキー
ビジネスデベロップメント
インテリジェンスサービス　担当
電話　03-3526-8538
E-mail　jp-sis@kaspersky.com
URL　http://www.kaspersky.co.jp

セキュリティインテリジェンスサービス

サービスラインアップ

- **脅威データベース提供サービス**
- **マルウェア解析サービス**
- **マルウェア トリアージサービス**
- **インシデントレスポンスサービス**
- **脅威情報ルックアップサービス**
- **サイバーセキュリティトレーニング**
- **セキュリティアセスメントサービス**
- **APTインテリジェンスレポートサービス**

※記載内容は2017年8月現在のものです。
※記載された内容は、改良の為に予告なく変更されることがあります。

PR-1041-201709