CSX 推奨学習コース順序表

2019/8/7 ATACD CSXサポート事務局

2019/8/7版 新コースとして「OWASP TOP 10 リスクの特定と軽減コース（ CSX Identifying and Mitigationg the OWASP Top 10 Course)」と、「CSX Volume8」が新規追加されました。

難易度	コース別　推奨学習順序	コース概要
< Advanced >	Cyber Hunt	「CSXサイバーハント・総合演習コース」は、実践形式によるCTFを模したサイバーセキュリティ演習です。 総合的なサイバーセキュリティスキルを向上できます。
	CSX Threat Hunting	「CSX脅威の追跡コース」は、高度なエクスプロイト（主に脆弱性）について学習するコースです。主に下記の3要素について学びます。 ・APT（高度で継続的な攻撃）攻撃　　・高度なマルウェア　　・Living Off the Land(環境寄生) これの高度な攻撃を検知するため、ネットワークトラフィックアナライザーであるBroを習得したり、メモリー展開から攻撃を検知する手法等を習得します。
	CSX Advanced Exploitation Course	「CSX上級エクスプロイトコース」は、高度な検知機能を習得するコースです。 Metasploit Frameworkを学習し、Metrepreter、ProtProxy、マルチSSHトンネルの実装を習得し検知システム構築方法を学びます。
	CSX Identifying and Mitigationg the OWASP Top 10 Course	OWASP(the Opne Web Application Security Projec)が2017年年末公表した“2017年最も重大なアプリケーションリスクトップ10”に準じた学習ラボです。 各脅威に対応するコーディング方法を習得するLａｂから構成されており、対象者は、アプリケーションプログラマー（アーキテクト含む）です。
	CSX Voulme8	アメリカ国防総省（DoD)、NIST（the National Institute of Standards and Technology）により発行されたWindows Secure Host Baseline（SHB）の各種スクリプトを理解し、コンプライアンスチェックを実行します。このSHBを理解した上で、Windowsサーバ2016群に対し、ペネトレーションテストを実施し、実戦でのSHBチェック方法を習得します。
	CSX Voulme7	MSサーバ、およびLinuxサーバを対象に、高度なハードニング（堅牢化：防御の強化）を実現する設定方法 例：MSサーバに対する、Windows PowerShell/MMCを用いF/W（WFAS)のMMC設定方法、およびLinuxハッキングの技術等を習得します
	CSX Volume 6	サイバーインシデントに対応したデータベース管理の構築 例 ： IDSテスト、ハニーポット、ログ生成と分析、暗号窃盗等に対応したデータベース管理の実装を習得します。
	CSX Forenjic Analysis Course	「CSXフォレンジック分析コース」では、OS設定コマンドForeman、およびPosgreSQLを用いたKali上でのフォレンジック環境を構築し、各工程での必要なフォレンジック作業を習得できます。
	CSX Vulnerability and Exploitation Course	「CSX脆弱性・乗っ取りコース（CVEC）」では、侵入テストの基本的な理解を持つ受講生に対し、脆弱性の識別と乗っ取り能力を習得させます。 受講生は実環境で実際のシステムを操作し、脆弱性分析ツールと活用ツールを習得できます。 修了後、情報システム内での資産をうまく利用し、安全なシステム維持の方法が理解できます。
	CSX Practitioner Exam Prep	「CSXプラクティショナー試験準備コース」では、CSXプラクティショナーの資格受験に適した有益なレッスンと詳細なパフォーマンスベースのラボが提供されており、合格するための技術的なサイバーセキュリティスキルを磨くことができます。 各ラボの修了後、受講者の強みと弱点を特定する詳細な分析レポートが提供され、さらにコースを修了すると、プロの認定資格の維持に適用される継続的な専門教育単位（CPE)が与えられます。
	CSX Volume 5	種々のシナリオ・トピック 例 ： 基本的なスクリプト生成と実行を元に、IoTデバイスからのインシデント検知、トリアージの実際を習得します
	CSX Volume 4	種々のシナリオ・トピック 例 ：主要脆弱性の理解と対策（インテルCPU、Webブラウザのセキュリティ保護手法、、、）を習得します
	CSX Volume 3	種々のシナリオ・トピック 例：主要インシデントの理解（データ漏えい、セッションハイジャック、等）と、主要な対処方法を習得します
	CSX Volume 2	種々のシナリオ・トピック 例： SQLインジェクションを含む、主要なフォレンジニックアクションを習得します
	CSX Volume 1	種々のシナリオ・トピック 例：顧客のWebサービスのIPアドレスがハッカーによって奪取されたときに、役割/機能の操作全体を習得します
	CSX Penetration Testing Overview	「CSX侵入（ペネトレーション）テストの概要（CPTO）コース」では、侵入テストと倫理的なハッキングについての入門的な理解を習得することができます。実環境でリアルなシステムを操作することで、実際の脆弱性分析ツールと活用ツールの使い方を習得できます。 修了すると、実践的な観点からの浸透テストの全体的な概念が理解できます。
	CSX Packet Analysis Course	「CSX Packet Analysis Course（CPAC）」は、パケットとプロトコルの分析環境を提供します。実際のネットワーク環境でネットワークトラフィックのキャプチャを行い、さまざまな通信タイプとそのコンポーネントを分析・理解できます。修了するとパケットキャプチャを自発的に分析し、ネットワークトポロジとデバイス構成を作成することができるようになります。これはサイバーセキュリティ分野の貴重な基礎能力です。
	CSX Network Application and Configuration	「CSXネットワークアプリケーションおよび設定（CNAC）コース」では、ネットワーク接続、プロトコル、およびルーティングについて理解を深めることができます。 ネットワーク環境でライブトラフィックと各ネットワーク機器への設定を習得することで、ネットワーク全体の理解と各端末間で通信される内容も習得できます。
	CSX Linux Application and Configuration	「CSXLinuxアプリケーションおよび設定（CLAC）コース」では、Linuxオペレーティングシステムの理解を深めることができます。 実際の環境でシステム構築を実施することで、キーコマンドを学び、ユーザーアカウントとアイテムを作成し、ネットワーク接続を確立し、Linux端末の基礎を学ぶことができます。
< Beginners >	CSX Fundamentals	サイバーセキュリティの入門 （テキストブック学習の補足テスト集）

	CSX Assessment Tool	攻撃の検出からシステム復元までのイベント対応能力を学習する2時間のチャレンジラボ 受講者の方の能力をNISTのNICE全機能（特定、防御、検知、対応、復旧）のラボを通じて評価し、各受講者に自分の弱みを再発見、認知してもらう（弱い機能を重点的に学習することをおすすめします）。