コースコード：CO-SECPLUS
税込価格：132,000円 (税抜価格：120,000円)
日数：3日間

前提条件

・セキュリティ関連業務の2年程度の実務スキル ・以下の基礎知識または経験があるとなおよい - ネットワーク - プログラミング

受講対象者

・CompTIA Security+認定資格（試験番号：SY0-601）の取得を目指す方
・サーバー、クライアント、およびネットワークのセキュリティ、セキュリティマネジメント、トラブルシューティングなどのセキュリティの基本を学習したい方

コース概要

企業の顧客情報漏えい、悪意を持つユーザの不正なアクセス、ウイルスやワームをはじめとする悪意のプログラムによる攻撃など、様々な脅威と各種セキュリティに関する要件に対応する総合的な対策について学ぶことができます。
サーバーおよびクライアントサイドのセキュリティ、ネットワークセキュリティ、リスク分析や運用などのセキュリティマネジメントの基礎についても学びます。
CompTIA Security+(SY0-601)の公式カリキュラム(5日間)と教材をベースに3日間に短縮しています。ラボ教材は含まれていますが、実施は自己学習となります。試験対策コースではございませんのでご注意ください。

※本トレーニングでは、CompTIAの 「The Official CompTIA Security+ Study Guide(試験番号：SY0-601) eBook日本語版」（12か月間利用可能）を使用します。
※本トレーニングには、知識の補強および理解度向上に利用いただける、オンラインラボ（12か月間利用可能）が含まれます。
※受講された方を対象とした自主学習教材としてWeb確認問題(Let's Check)が含まれます。

目的

ネットワークセキュリティ、セキュリティマネジメント、トラブルシューティングなど、
全般的なセキュリティの基礎知識を修得することを目的としています。

アウトライン

レッスン1 セキュリティロールとセキュリティ管理を比較する
- トピック1A 情報セキュリティロールを比較対照する
- トピック1B セキュリティの管理とフレームワークの各タイプを比較対照する

レッスン2 攻撃者と脅威インテリジェンスを説明する
- トピック2A 攻撃者のタイプと攻撃ベクトルを説明する
- トピック2B 脅威インテリジェンスの情報源を説明する

レッスン3 セキュリティ評価の実施
- トピック3A ネットワーク偵察ツールを使った組織のセキュリティ評価
- トピック3B 一般的な脆弱性タイプを用いてセキュリティについての懸念事項を説明する
- トピック3C 脆弱性スキャン技術を要約する

- トピック3D ペネトレーションテストの概念を説明する

レッスン4 ソーシャルエンジニアリングとマルウェアを特定する
- トピック4A ソーシャルエンジニアリングの手法を比較・対比する
- トピック4B マルウェアベースの攻撃のインジケーターを分析する

レッスン5 暗号化コンセプトの基本
- トピック5A 暗号文の比較対照
- トピック5B 暗号動作モードを要約することができる
- トピック5C 暗号化のユースケースと脆弱性の概要
- トピック5D その他の暗号化技術の概要

レッスン6 公開鍵インフラストラクチャーを実装する
- トピック6A 証明書と認証機関を実装する
- トピック6B PKI管理を実装する

レッスン7 認証制御の実施
- トピック7A 認証設計概念の要約
- トピック7B ナレッジベース認証の実装
- トピック7C 認証技術の実装
- トピック7D 生体認証概念の要約

レッスン8 IDおよびアカウント管理制御の実装
- トピック8A アイデンティティとアカウントタイプの導入
- トピック8B アカウントポリシーの導入
- トピック8C 認可ソリューションの実施
- トピック8D 人事ポリシーの重要性の説明

レッスン9 セキュアなネットワーク設計の実装
- トピック9A セキュアなネットワーク設計を実装する
- トピック9B セキュアなスイッチングとルーティングの実装
- トピック9C セキュアなワイヤレスインフラストラクチャを実装する
- トピック9D ロードバランサーを実装する

レッスン10 ネットワークセキュリティアプライアンスの実装
- トピック10A ファイアウォールとプロキシサーバーを実装する
- トピック10B ネットワークセキュリティ監視を実装する
- トピック10C SIEMの使用を要約する

レッスン11 セキュアなネットワークプロトコルを実装する
- トピック11A セキュアなネットワークオペレーションプロトコルを実装する
- トピック11B セキュアなアプリケーションプロトコルを実装する
- トピック11C セキュアなリモートアクセスプロトコルを実装する

レッスン12 ホストのセキュリティソリューションを実装する
- トピック12A セキュアなファームウェアを実装する
- トピック12B エンドポイントセキュリティを実装する
- トピック12C 組み込みシステムのセキュリティのリスクについて説明する

レッスン13 セキュアなモバイルソリューションの実装
- トピック13A モバイルデバイス管理を実装する
- トピック13B セキュアなモバイルデバイス接続を実装する

レッスン14 セキュアなアプリケーションの概念を要約する
- トピック14A アプリケーション攻撃のインジケーターを分析する
- トピック14B Webアプリケーション攻撃のインジケーターを分析する
- トピック14C セキュアなコーディング慣行を要約する
- トピック14D セキュアなスクリプト環境を実装する
- トピック14E デプロイと自動化のコンセプトを要約する

レッスン15 セキュアなクラウドソリューションの実装
- **トピック15A セキュアなクラウドサービスと仮想化サービスを要約する**
- **トピック15B クラウドセキュリティソリューションを適用する**
- **トピック15C インフラストラクチャをコードの概念として要約する**

レッスン16 データのプライバシーと保護の概念を説明する
- **トピック16A プライバシーとデータセンシティビティの概念を説明する**
- **トピック16B プライバシーとデータ保護の制御を説明する**

レッスン17 インシデント対応を実行する
- **トピック17A インシデント対応手順をまとめる**
- **トピック17B インシデント対応に適切なデータソースを活用する**
- **トピック17C 緩和策を適用する**

レッスン18 デジタルフォレンジクスを説明する
- **トピック18A デジタルフォレンジクス文書の主な側面について説明する**
- **トピック18B デジタルフォレンジクスの証拠取得の主な側面について説明する**

レッスン19 リスク管理の概念を説明する
- **トピック19A リスク管理プロセスと概念を説明する**
- **トピック19B ビジネスインパクト分析の概念を説明する**

レッスン20 サイバーセキュリティレジリエンスを実装する
- **トピック20A 冗長性戦略を実装する**
- **トピック20B バックアップ戦略を実装する**
- **トピック20C サイバーセキュリティレジリエンス戦略を実装する**

レッスン21 物理的なセキュリティについて説明する
- **トピック21A 物理的なサイトのセキュリティ管理の重要性を説明する**
- **トピック21B 物理的なホストのセキュリティ管理の重要性を説明する**