コースコード：CO-SECPLUS
税込価格：165,000円 (税抜価格：150,000円)
日数：3日間

トレーニング内容

・エンタープライズ環境のセキュリティ態勢を評価し、適切なセキュリティソリューションを推奨および実装する
・クラウド、モバイル、IoTなどのハイブリッド環境を監視および保護する
・ガバナンス、リスク、コンプライアンスの原則など、該当する規制やポリシーを認識したうえで運用する
・セキュリティイベントやインシデントの特定、分析、対応を実施する

CompTIA Security+(SY0-701)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。ラボ教材が含まれていますが、コース内での実施は限定されますので、自己学習が必要です。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：SY0-701) 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。

ここに注目!!

CompTIA Security+認定資格（試験番号：SY0-701）は、IT業務の中でも、最も成長が早く、そして人材が必要とされているセキュリティ分野におけるスキルを評価できるよう設計されています。ただし、対象とする範囲はかなり広く、また内容の理解と習得には(前提知識や経験によっては)、十分な自己学習が必要になります。

ワンポイントアドバイス

受講証明書(修了証)は、70%以上の出席率を満たしているお客様に発行いたします。

英語での一社向け研修も開催可能です。こちらからお問い合わせください。

We can run this training in English. Please ask [Click here].

受講対象者

このコースの受講対象者は次の通りです。

・CompTIA Security+認定資格（試験番号：SY0-701）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広く学習したい方

前提条件

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

・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
- 技術的情報セキュリティ

目的

このコースを修了すると次のことができるようになります。

セキュリティコンセプトの概要
・サイバーセキュリティに関する重要な用語と概念を取り入れることで、試験全体を通じて説明されるセキュリティ管理の基礎を提供します。
脅威、脆弱性、軽減策
・一般的な脅威、サイバー攻撃、脆弱性、セキュリティインシデントへの対応と、ハイブリッド環境の監視とセキュリティ確保のための適切な軽減策に重点を置いています。
セキュリティアーキテクチャ
・さまざまなアーキテクチャモデルのセキュリティ上の意味、企業インフラストラクチャを保護するための原則、データを保護するための戦略を含みます。
セキュリティオペレーション
・セキュリティと脆弱性管理手法の適用と強化、適切なハードウェア、ソフトウェア、データ管理のセキュリティへの影響も含まれます。
セキュリティプログラムの管理と監督
・ガバナンス、リスク管理、コンプライアンス、アセスメント、セキュリティ意識に関するSecurity+の職務に必要な報告およびコミュニケーションスキルをより反映させるために更新されています。

アウトライン

レッスン1 セキュリティの基本概念の要約
- トピック1A セキュリティの概念
- トピック1B セキュリティ制御

レッスン2 脅威の種類の比較
- トピック2A 脅威アクター
- トピック2B 攻撃対象領域
- トピック2C ソーシャルエンジニアリング

レッスン3 暗号化ソリューション
- トピック3A 暗号アルゴリズム
- トピック3B 公開鍵基盤
- トピック3C 暗号化ソリューション

レッスン4 IDとアクセス管理の実装
- トピック4A 認証
- トピック4B 認可
- トピック4C ID管理

レッスン5 エンタープライズネットワークアーキテクチャのセキュリティ強化
- トピック5A エンタープライズネットワークアーキテクチャ
- トピック5B ネットワークセキュリティアプライアンス
- トピック5C セキュアな通信

レッスン6 クラウドネットワークアーキテクチャの保護
- トピック6A クラウドインフラストラクチャ
- トピック6B 組み込みシステムとゼロトラストアーキテクチャ

レッスン7 回復力とサイトセキュリティの概念
- トピック7A 資産管理
- トピック7B 冗長性戦略
- トピック7C 物理的セキュリティ

レッスン8 脆弱性管理
- トピック8A デバイスとOSの脆弱性
- トピック8B アプリケーションとクラウドの脆弱性
- トピック8C 脆弱性特定方法
- トピック8D 脆弱性分析と修復

レッスン9 ネットワークセキュリティ機能の評価
- トピック9A ネットワークセキュリティベースライン
- トピック9B ネットワークセキュリティ機能の強化

レッスン10 エンドポイントセキュリティ機能の評価
- トピック10A エンドポイントセキュリティの実装
- トピック10B モバイルデバイスのハードニング

レッスン11 アプリケーションのセキュリティ機能の強化
- トピック11A アプリケーションプロトコルのセキュリティベースライン
- トピック11B クラウドとWebアプリケーションのセキュリティ概念

レッスン12 インシデント対応とモニタリングのコンセプト
- トピック12A インシデント対応
- トピック12B デジタルフォレンジック
- トピック12C データソース
- トピック12D アラートおよび監視ツール

レッスン13 悪意のあるアクティビティの指標の分析
- トピック13A マルウェア攻撃インジケーター
- トピック13B 物理攻撃とネットワーク攻撃の指標
- トピック13C アプリケーション攻撃インジケーター

レッスン14 セキュリティガバナンスの概念
- トピック14A ポリシー、標準、手順
- トピック14B 変更管理
- トピック14C 自動化とオーケストレーション

レッスン15 リスク管理プロセスの探究
- トピック15A リスク管理プロセスと概念
- トピック15B ベンダー管理の概念
- トピック15C 監査と評価

レッスン16 データ保護とコンプライアンスの概念の要約
- トピック16A データ分類とコンプライアンス
- トピック16B 人事ポリシー