コースコード：EL-CO-SECPLUS-6M
税込価格：93,500円 (税抜価格：85,000円)
日数：180日間

コース概要

本トレーニングには以下の特長があります。

・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

※本トレーニングは、お客様ご自身のペースでオンラインで学習できるeラーニング形式のトレーニングです。

※講義ビデオコンテンツの総再生時間は8時間20分、180日間閲覧可能です
※CompTIA「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）をテキストとして使用します
※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

受講対象者

・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

・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

下記のコースを受講済み、または同等の知識を有する方

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

セキュリティの基本概念の要約

セキュリティの概念

セキュリティ制御

脅威の種類の比較

脅威アクター

攻撃対象領域

ソーシャルエンジニアリング

暗号化ソリューション

- **暗号アルゴリズム**
- **公開鍵基盤**
- **暗号化ソリューション**

IDとアクセス管理の実装

- **認証**
- **認可**
- **ID管理**

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

- **エンタープライズネットワークアーキテクチャ**
- **ネットワークセキュリティアプライアンス**
- **セキュアな通信**

クラウドネットワークアーキテクチャの保護

- **クラウドインフラストラクチャ**
- **組み込みシステムとゼロトラストアーキテクチャ**

回復力とサイトセキュリティの概念

- **資産管理**
- **冗長性戦略**
- **物理的セキュリティ**

脆弱性管理

- **デバイスとOSの脆弱性**
- **アプリケーションとクラウドの脆弱性**
- **脆弱性特定方法**
- **脆弱性分析と修復**

ネットワークセキュリティ機能の評価

- **ネットワークセキュリティベースライン**
- **ネットワークセキュリティ機能の強化**

エンドポイントセキュリティ機能の評価

- **エンドポイントセキュリティの実装**
- **モバイルデバイスのハードニング**

アプリケーションのセキュリティ機能の強化

- **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**
- **クラウドとWebアプリケーションのセキュリティ概念**

インシデント対応とモニタリングのコンセプト

- **インシデント対応**
- **デジタルフォレンジック**
- **データソース**
- **アラートおよび監視ツール**

悪意のあるアクティビティの指標の分析

- **マルウェア攻撃インジケーター**
- **物理攻撃とネットワーク攻撃の指標**
- **アプリケーション攻撃インジケーター**

セキュリティガバナンスの概念

- **ポリシー、標準、手順**
- **変更管理**
- **自動化とオーケストレーション**

リスク管理プロセスの探究

- **リスク管理プロセスと概念**
- **ベンダー管理の概念**
- **監査と評価**

データ保護とコンプライアンスの概念の要約

- **データ分類とコンプライアンス**
- **人事ポリシー**