コースコード：CO-CYSAPLUS
税込価格：209,000円 (税抜価格：190,000円)
日数：3日間

ここに注目!!

CompTIA CySA+ (CS0-003) の公式カリキュラム (5日間)
と教材をベースに、ご受講いただきやすいよう3日間に短縮したトレーニングです。

CompTIA Cybersecurity Analyst（CySA+）認定資格（試験番号：CS0-003）は、継続的なセキュリティモニタリングによるインシデントの検出、予防、レスポンスを任務とするサイバーセキュリティプロフェッショナル向けの認定資格です。
実務経験3～4年を想定しており、実務経験2年を想定して開発されたCompTIA Security+の次のキャリアとして最適な認定資格です。資格取得後は、実務経験5～10年を想定している実践的なサイバーセキュリティスキルを習得できるCompTIA SecurityXへのキャリアパスへとつながります。

・試験問題のイメージやトレーニングで身につく知識の参考としてお役立てください
CySA+(V3)類似問題 |CompTIA（コンプティア）

・クラウド業務基盤上でのセキュリティを考慮した運用を目的に、本トレーニングを導入いただきました
株式会社パソナテック 様

※本トレーニングはeラーニング形式にも対応しています
CompTIA CySA+ セルフペーストレーニング

受講対象者

このトレーニングはこのような方におすすめです。

・CompTIA CySA+認定資格（試験番号：CS0-003）の取得を目指す方
・ITセキュリティにおける分析と、セキュリティ全体の改善を実行するために必要となるスキルを習得したい方

前提条件/前提知識

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。

インシデント対応アナリストまたはSecurity Operations
Center（SOC）アナリストとして4年程度の実践的な経験が想定されています。

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。

・脆弱性の対応、取り扱い、管理の理解
・脅威インテリジェンスと脅威ハンティングの概念の探求
・重要なシステムとネットワークアーキテクチャの説明
・セキュリティ運用でのプロセス改善の理解
・脆弱性スキャン手法の実装

・脆弱性分析の実施
・脆弱性情報の分類
・インシデント対応活動の説明
・インシデント対応コミュニケーションの実演
・悪意のある活動を特定するためのツール適用
・悪意のある可能性がある活動の分析
・アプリケーション脆弱性評価の理解
・スクリプティングツールと分析の概念の探求
・アプリケーションセキュリティと攻撃緩和策のベストプラクティス

アウトライン

脆弱性の対応、取り扱い、管理の理解

サイバーセキュリティにおけるリーダーシップの概念の理解

制御方式と手段の探求

パッチ管理の概念の説明

脅威インテリジェンスと脅威ハンティングの概念の探求

脅威アクターの概念の理解

活動中の脅威の特定

脅威ハンティングの概念の探求

重要なシステムとネットワークアーキテクチャの説明

システムとネットワークアーキテクチャの概念の理解

IAMの探求

運用可視性の維持

セキュリティ運用でのプロセス改善の理解

セキュリティ運用でのリーダーシップの探求

セキュリティ運用向けのテクノロジーの理解

脆弱性スキャン手法の実装

- **コンプライアンス要件の説明**
- **脆弱性スキャン手法の理解**
- **脆弱性スキャンの特別な考慮事項の探求**

脆弱性分析の実施

- **脆弱性評価の概念の理解**
- **脆弱性に関するコンテキスト上の考慮事項について**

脆弱性情報のコミュニケーション

- **効果的なコミュニケーションの概念の理解**
- **脆弱性レポートの結果とアクションプランの理解**

インシデント対応活動を説明する

- **インシデント対応計画について**
- **インシデント対応活動の実施**

インシデント対応コミュニケーションのデモンストレーション

- **インシデント対応コミュニケーションを理解する**
- **インシデント対応活動を分析する**

悪意のあるアクティビティを特定するツールの適用

- **悪意のある活動を識別する**

攻撃手法のフレームワークの説明

悪意のあるアクティビティを識別する手法を理解する

悪意のある可能性がある活動の分析

ネットワーク攻撃の痕跡

ホスト攻撃の痕跡

脆弱性評価ツール

アプリケーション脆弱性評価の理解

ウェブ脆弱性の分析

クラウド脆弱性の分析

スクリプティングツールと分析の概念の探求

スクリプト言語の理解

分析を通じて悪意のある活動を識別する

アプリケーションセキュリティと攻撃緩和策のベストプラクティスの理解

セキュアなソフトウェア開発手法について

アプリケーション攻撃の成功率を引き下げる管理の推奨

攻撃を防ぐ管理の実装