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

前提条件

このコースを無事完了するためには、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。

下記のコースを受講済み、または同等の知識を有する方

CompTIA Network+ 任意、受講されていれば望ましい
CompTIA Security+ 任意、受講されていれば望ましい

受講対象者

・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

コース概要

■現在のトレンドに関するスキルを証明する
クラウドやハイブリッド環境などさまざまに変化し、セキュリティに影響を与えるITトレンドに関するスキルを習得し、セキュリティアナリスト業務のスキルを証明することが可能です。
■プロアクティブなモニタリングと検出
脅威インテリジェンス、セキュリティ情報イベント管理（SIEM）、エンドポイントでの検知と対応（EDR）、拡張検知と対応（XDR）など最新の手法とツールを使用して、悪意のあるアクティビティの兆候を検知、分析するスキルを証明します。
■脅威、攻撃、脆弱性への対応
インシデントレスポンスと脆弱性管理プロセスに関する知識を証明し、セキュリティ分析とコンプライアンス遵守に不可欠となるコミュニケーションスキルを習得します。

CompTIA CySA+は、ISO17024の要件に適合しており、米国国防総省による指令8570.01-Mの資格要件として承認されています。また、連邦情報セキュリティマネジメント法（FISMA）に基づく、政府規制に準拠しています。

※本トレーニングでは、CompTIAの 「The Official CompTIA CySA+ Study Guide(試験番号：CS0-003) eBook日本語版」（12か月間利用可能）を使用します。
※本トレーニングでは、知識の補強および理解度向上のため、オンラインラボ（12か月間利用可能）を使用します。
※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

・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