コースコード：CO-CYSAPLUSv4
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+ (CS0-004) 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：CS0-004）は、CompTIA CySA+は、セキュリティ運用および脆弱性管理の役割における脅威の検出、分析、対応能力を検証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。最新の環境におけるインシデントの検出、レスポンス、継続的な監視に重点を置き、脆弱性の管理と重大なリスクの効果的な伝達を支援します。
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。

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：CS0-004）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。

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

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。

・ネットワーク、エンドポイント、クラウド環境全体で不審な活動を特定、調査し、潜在的なセキュリティ脅威を明らかにする
・SIEMやEDRプラットフォームなどの業界標準ツールを用いてデータを監視・分析する
・リスクベースのアプローチを用いて脆弱性を特定、優先順位付けし、リスクを軽減する措置を取る

・体系化されたプロセスと実践的な手法を用いて、セキュリティインシデントを調査し、対応する。
・レポートやダッシュボードを通じて、セキュリティの発見やリスクを利害関係者に明確に伝える
・クラウド環境およびハイブリッド環境全体にセキュリティ対策を適用し、効率的かつ効果的な運用をサポートする

アウトライン

1 セキュリティ運用の基本の理解
1.1 サイバーセキュリティの基礎
1.2 ガバナンス、ポリシー、および統制（コントロール）
1.3 SOCにおけるインシデント対応の概要

2 リスク管理戦略の適用
2.1 リスクの概念
2.2 脅威モデリングのフレームワーク

3 システムセキュリティと構成の管理
3.1 攻撃対象領域（アタックサーフェス）の管理
3.2 システムの堅牢化（ハードニング）

4 システムアーキテクチャの比較
4.1 インフラストラクチャとシステムアーキテクチャ
4.2 現代のネットワークアーキテクチャ
4.3 重要インフラと産業用制御システム

5 アクセス管理の適用
5.1 IDおよびアクセス管理
5.2 デバイスおよびエンドポイント管理
5.3 データ保護と暗号化

6 脅威インテリジェンスと脅威ハンティング
6.1 脅威アクターの概念
6.2 脅威インテリジェンスのソース
6.3 脅威ハンティング

7 ネットワークの脆弱性評価
7.1 脆弱性スキャンの基礎
7.2 脆弱性スキャンの種類
7.3 脆弱性スキャンツールの選定
7.4 脆弱性の分析と優先順位付け
7.5 脆弱性およびインシデントの報告

8 インシデント対応とコミュニケーションの管理
8.1 ログの管理
8.2 インシデントのエスカレーション
8.3 インシデント後の対応
8.4 インシデント対応のメトリクス

9 インシデント対応計画の実行
9.1 攻撃手法のフレームワーク
9.2 インシデント対応プロセス
9.3 インシデント対応技術

10 悪意ある活動の分析
10.1 脅威の検知および分析ツール

10.2 ホストにおける侵害の兆候（IoC）
10.3 ネットワークにおける侵害の兆候（IoC）
10.4 アプリケーションおよびWeb関連の兆候

11 データ分析の自動化
11.1 スクリプト作成の基礎
11.2 スクリプト言語
11.3 セキュリティ分析とパターン認識
11.4 技術とツールの統合

12 自動化によるプロセスの改善
12.1 標準化とチームの連携
12.2 自動化、オーケストレーション、およびエンリッチメント
12.3 AIのリスクとガバナンス
12.4 セキュリティ運用におけるAIの活用

13 アプリケーションの脆弱性評価
13.1 Webおよびアプリケーションの脆弱性分析
13.2 クラウドの脆弱性評価

14 アプリケーションのセキュリティ確保
14.1 セキュアなソフトウェア開発とテスト
14.2 アプリケーションへの攻撃の特定と緩和