

コースコード : EL-CO-CASPLUS-6M
税込価格 : 99,000円 (税抜価格 : 90,000円)
日数 : 180日間

コース概要

SecurityX(旧称CASP+)は、オンプレミスやクラウド、またはハイブリット環境でのセキュリティーアーキテクチャとテクニカルスキル、リスクマネジメント、ガバナンスやコンプライアンスの順守といったスキルに加え、企業のサイバーセキュリティの準備状況の評価や企業全体に実装するため必要とされる総合的なセキュリティスキルについて学習します。

ここに注目

ワンポイントアドバイス

SecurityX(旧称CASP+)は、オンプレミスやクラウド、またはハイブリット環境でのセキュリティーアーキテクチャとテクニカルスキル、リスクマネジメント、ガバナンスやコンプライアンスの順守といったスキルに加え、企業のサイバーセキュリティの準備状況の評価や企業全体に実装するため必要とされる総合的なセキュリティスキルを評価します。IT全般の管理者として10年以上の経験、そのうち5年以上をセキュリティに関連する実務で得られる知識やスキルを目安に設計されています。

受講対象者

- ・ SecurityX(旧称CASP+)認定資格(試験番号: CAS-004)の取得を目指す方
- ・ IT全般の管理者として10年以上の経験、そのうち5年以上をセキュリティに関連する実務に携わるエンジニアの方

前提条件

IT全般の管理者として10年以上の経験、そのうち5年以上をセキュリティに関連する実務で得られる知識やスキル(目安)

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。

- ・複雑なIT環境全体におけるセキュアなソリューションの設計、統合、実装をし、企業のレジリエンスを実現する
- ・監視、検出、インシデント対応、自動化を使用し、エンタープライズ環境におけるセキュリティ運用をプロアクティブにサポートする
- ・暗号化テクノロジーやその他のセキュリティ手法を考慮しながら、クラウド、オンプレミス、エンドポイント、モバイルインフラストラクチャの全体にセキュリティプラクティスを適用する
- ・企業全体のガバナンス、リスク、コンプライアンス要件の影響を検討する

アウトライン

レッスン1 リスク管理アクティビティを実施する

- トピック1A リスクアセスメント方法を説明する
- トピック1B リスクライフサイクルについて要約する
- トピック1C ベンダーリスクを評価して軽減する

レッスン2 ガバナンスおよびコンプライアンス戦略を要約する

- トピック2A 重要データ資産を特定する
- トピック2B 規制、認定、および標準を比較、対照する
- トピック2C 法的検討事項と契約の種類を説明する

レッスン3 事業継続と災害復旧を実施する

- トピック3A ビジネス影響度分析のロールを説明する
- トピック3B 災害復旧計画を評価する
- トピック3C テストおよび準備アクティビティを説明する

レッスン4 インフラストラクチャサービスを特定する

- トピック4A 重要なネットワークサービスを説明する
- トピック4B 防御可能なネットワーク設計を説明する
- トピック4C 耐久性の高いインフラストラクチャを実装する

レッスン5 ソフトウェア統合を実施する

- トピック5A 安全な統合アクティビティを説明する
- トピック5B ソフトウェア開発アクティビティを評価する
- トピック5C アクセス制御モデルとベストプラクティスを分析する
- トピック5D 開発モデルとベストプラクティスを分析する

レッスン6 仮想化、クラウド、先端技術を説明する

- トピック6A 仮想化とクラウド技術について説明する
- トピック6B 先端技術について説明する

レッスン7 安全な構成とシステムのハードニングについて考察する

- トピック7A 企業のモビリティ保護を分析する
- トピック7B エンドポイント保護を実装する

レッスン8 クラウドと専用プラットフォームのセキュリティの検討事項を理解する

- トピック8A クラウドテクノロジー採用の影響を理解する
- トピック8B セクター固有のテクノロジーに関するセキュリティ上の検討事項を説明する

レッスン9 暗号化を実装する

- トピック9A ハッシュ化と対称アルゴリズムを実装する
- トピック9B 適切な非対称アルゴリズムとプロトコルを実装する

レッスン10 適切なPKIソリューションを実装する

- トピック10A 暗号化および公開鍵インフラストラクチャ(PKI)の目標を分析する

- トピック10B 適切なPKIソリューションを実装する

レッスン11 脅威と脆弱性マネジメントのアクティビティを理解する

- トピック11A 脅威および脆弱性マネジメントの概念を確認する
- トピック11B 脆弱性およびペネトレーションテストの方法を説明する
- トピック11C リスクを軽減するために設計されたテクノロジーを説明する

レッスン12 インシデント対応機能を開発する

- トピック12A 脆弱性を分析して軽減する
- トピック12B セキュリティ侵害インジケーターを特定して対応する
- トピック12C デジタルフォレンジックの概念を探る