コースコード：EC-CSA
税込価格：300,300円 (税抜価格：273,000円)
日数：3日間

ここに注目!!

本トレーニングに関連する資格を取得された方にお話しを伺いました。
合格体験記は こちら

SOC（セキュリティオペレーションセンター）とは、防ぐことのできない脅威を検知し、対応するための「脅威検知戦略」を計画・実施実行する組織のことです。

SOCアナリストの役割：
・様々なソースからの何千ものアラートとイベントの監視とトリアージする
・アラートとイベントの初期分析を行い、最も重要なものを検証し、優先順位をつける
・インシデントレスポンスチームへのエスカレーションが必要なアラートを決定し、詳細な分析および修正を行う

また、SOCアナリストの役割と責任は以下の2つのレベルに分類されます。

・SOCアナリスト - レベル1
SIEMからのセキュリティアラートを監視し、必要に応じてイベントの詳細をクローズするか、ティア2に渡して最終的な分析を行う

・SOCアナリスト - レベル2
セキュリティ警告の調査、検証、優先順位付けをする
不審な行動に関するデータを収集・記録し、次のレベルに転送して調査する

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。

初級から中級のサイバーセキュリティに関わるエンジニアの方に効果的なトレーニングです。

・SOC運用者（L1およびL2）
知識とスキルを向上させる資格を取得することができます。
・SOCアナリストを目指す方
SOCアナリストに必要な知識・スキルを習得することができます。
・ネットワークセキュリティに関わるエンジニア / 運用担当者
脅威の検知と対応に関する知識とスキルを習得し、組織ネットワークの強力なセキュリティ体制を維持するのに役立ちます。

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。

・ネットワークの概念、TCP/IPプロトコルおよびセキュリティ技術（Firewall、IDS/IPSなど）サイバー脅威などに関する基本的な理解を有していること
・CCT (Certified Cybersecurity Technician) を受講された方

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。

・SOC運用の基礎を理解し、「ログの管理と関連付け」「SIEMの理解・運用」「インシデント検出と対応」を習得する
・SOCプロセスを理解し、必要な時に上位のアナリストおよびCSIRTと協力した対応ができるスキルを習得する
・国際認定資格CSA試験に合格する

アウトライン

セキュリティの運用と管理

サイバー脅威、IoC、攻撃手法の理解

インシデント、イベント、ロギング

SIEM（セキュリティ情報およびイベント管理）によるインシデント検知

スレットインテリジェンスによるインシデント検知の強化

インシデントレスポンス