コースコード：EC-CSA
税込価格：330,000円 (税抜価格：300,000円)
日数：3日間

ここに注目!!

SOC（セキュリティオペレーションセンター）運用の基礎から、SIEMの活用、インシデント対応、脅威インテリジェンスまでを包括的に網羅した認定資格です。
Tier1（監視）からTier2（分析）、Tier3（脅威ハンティング）のアナリストに必要なスキルセットを体系的に学習できます。

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

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。

【SOCアナリスト】
Tier1（監視）、Tier2（分析）、Tier3（脅威ハンティング）を担当する現職のアナリスト、および目指す方
【セキュリティ運用者】
企業のセキュリティ運用・関し業務（運用管理、ログ分析、アラート対応）に従事するエンジニア
【ネットワークエンジニア】
セキュリティ分野へのキャリアアップを目指すインフラ・ネットワークエンジニア

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。

・TCP/IP基礎知識
IPアドレス、プロトコル、ポート番号などのネットワークの仕組みに関する理解
・セキュリティ技術の基礎
ファイアウォール、IDS/IPS、アンチウイルス等の機能と役割に関する知識
・Linuxの基礎知識
LPIC Level 1 程度（コマンドライン操作、ファイルシステム、情報管理など）のスキル

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、調査」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

運用管理

SOC運用の基礎概念、役割、責任範囲、および運用プロセスを学習

サイバー脅威

最新の脅威動向、攻撃手法、IoC（侵略指標）の特定と活用方法

ログ管理

効果的なログ収集、保存、正規化、および分析のベストプラクティス

検知とトリアージ

アラートの優先順位付け、誤検知の排除、初期分析の手法

プロアクティブ検知

受動的な監視だけでなく、能動的に脅威を未然に防ぐための手法

インシデントレスポンス

インシデント発生時の初動対応、封じ込め、根絶、復旧のプロセス

フォレンジック / マルウェア分析

高度な調査スキル、証拠保全やマルウェアの挙動分析を実施

AWS/Azure等のクラウド特有の脅威監視とログ分析手法