コースコード：EC-ECIH
税込価格：360,800円 (税抜価格：328,000円)
日数：3日間

トレーニング内容

ECIHは、インシデントに備え、対処し、根絶するための知識、スキルを学ぶ講座です。
本トレーニングでは、インシデント対応の全プロセスを通して効果的な計画、記録、トリアージ、通知、封じ込めに必要な手順とテクニックを学びます。
受講を通して様々なタイプのインシデントの取り扱い、リスクアセスメントの方法論、またインシデントの取り扱いに関連する法律やポリシーを学び、IH&Rポリシーを作成し、マルウェア、メールセキュリティ、ネットワークセキュリティ、Webアプリケーションセキュリティ、クラウドセキュリティ、内部不正関連のインシデントなど、さまざまなタイプのセキュリティインシデントに対処するテクニックを学習します。

ここに注目!!

インシデント発生前の防御、検知について「CND（Certified Network Defender）」や「CSA（Certified SOC Analyst）」で理解を深めるのに対し、「ECIH（EC-Council Certified Incident Handler）」はインシデント対応領域の専門資格であり、インシデントに対する全プロセスを体系的に学ぶことができます。

ワンポイントアドバイス

受講対象者

このコースの受講対象者は次の通りです。

・CSIRT リーダー/メンバー
・インシデントハンドラ
・インシデントレスポンダ
・インシデント対応 担当者、コンサルタント
・情報セキュリティ担当者、アナリスト、エンジニア
・サイバー防御 担当者、コンサルタント、エンジニア
・SoCアナリスト
・フォレンジック 担当者、アナリスト、コンサルタント
・脆弱性アナリスト
・脅威インテリジェンス アナリスト

前提条件

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。

・セキュリティやインシデント対応に関する基礎的な知識を有していること
例：CompTIA Security+、EC-Council CCT/CNDの資格保持者または同等のスキル保持者

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。

・インシデントハンドリングライフサイクルに基づいて、準備・検知・封じ込め・根絶・復旧・事後レビューを体系的に実施できるようになる
・各種セキュリティインシデント（マルウェア感染、エンドポイント/ネットワーク/Webアプリ/クラウドに関する攻撃等）に応じた対応手順を選択し、適切な初動対応ができるようになる
・事後の改善提案、再発防止策をチームや経営層へ報告できるようになる
・国際認定資格ECIH試験に合格する

アウトライン

インシデント対応/レスポンスについて

インシデント対応/レスポンス手順

初動対応

マルウェアによるインシデントに対するハンドリングと対応

メールに関するインシデントに対するハンドリングと対応

ネットワークに関するインシデントに対するハンドリングと対応

Webアプリケーションに関するインシデントに対するハンドリングと対応

クラウドセキュリティにおけるインシデントに対するハンドリングと対応

内部脅威に関するインシデントに対するハンドリングと対応

エンドポイントに関するインシデントに対するハンドリングと対応