情報処理安全確保支援士特定講習　講習情報

株式会社ラック

セキュリティオペレーション実践コース　初級編

実施機関名	株式会社ラック		
講習名	セキュリティオペレーション実践コース　初級編		
特定講習番号	21-005-017		
講習形態	集合形式	定員（１回あたり）	20 名
受講日数	1 日間	受講時間	6.5 時間
受講料	165,000（円/税込み）		

対象分野 <ITSS+（セキュリティ領域）>	主な分野	セキュリティ監視・運用	関連分野	デジタルシステムストラテジー セキュリティ監査 セキュリティ統括 セキュリティ調査分析・研究開発

講習内容	実際にラック社のJSOCのセキュリティアナリスト養成に使用されているカリキュラムから、ログや通信内容を確認する機会が多いHTTP通信を題材に、攻撃の痕跡を発見・分析できるようなポイントを学習します。最終的には、Webサーバが攻撃通信によって受けた影響を自ら発見、判断できるよう、実践的な技術の習得を目指します。 また、Wiresharkを使用し、所望の通信内容を確認できる手法の学習や、Webアプリケーションに対する基本的な攻撃通信をアクセスログとパケットキャプチャから攻撃通信の解析を実施。尚、総合演習も盛りこまれます。
具体的な到達目標	・Webサーバのアクセスログの見方や通信ログ（パケットキャプチャ）の解析ツール「Wireshark」の基本的な使用方法を会得できる ・アクセスログや通信ログ（パケットキャプチャ）の解析を通じて、公開Webサーバへの攻撃を発見したり、攻撃によるシステムへの影響の有無を判断するための技術を会得できる
修得できるスキル	・ログや通信内容（HTTP通信）から攻撃の痕跡を発見・分析するスキル ・Webサーバが攻撃通信によって受けた影響を自ら発見、判断できるスキル
講習の理解・習得のために推奨される実務経験	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進業務、SOC（セキュリティ運用）要員業務、その他インシデント対応に関連した業務
講習の理解・習得のために推奨される知識・技術	以下のようなWebアプリに対する攻撃の基礎的な知識がある ・SQLインジェクション ・クロスサイトスクリプティング ・/etc/passwd参照 検索エンジンを利用した情報収集経験があると望ましい
技術・知識の到達度の把握・測定方法	・実機による実習状況 ・総合演習の実行状況及び結果 ＊上記を総合的に講師が判断
修了認定の判断基準	100%の出席率に加え、講師が総合的に評価を行った上で修了判定を行います。 判断基準については、実機利用の演習等は「一人で完了できている」～「多少のサポートで完了」～「研修時間内にまったく出来ない」が目安。また、実機演習も含め研修全体を通して講師からの質問への対応、質問の状況など講師と補助講師が随時チェックして最終的に相対評価とします。
修了認定基準に満たない受講者への措置	新規に申込してもらい再度受講してもらう措置となります。
受講者に対するサポート体制	講義内各段階において懸念のある受講者に対し、講師と補助講師で適時認識合わせを実施します。その上で補助講師が個別にサポートを手厚くしていきます。また、研修終了後の学習方法などもアドバイスしていきます。
講習実施施設所在地	東京都千代田区平河町2-16-1　平河町森タワー　株式会社ラック本社
ホームページ	https://www.lac.co.jp/service/education/security_operation_basic.html