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　中級編

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　中級編		
特定講習番号	21-005-018		
講習形態	集合形式	定員（１回あたり）	20 名
受講日数	2 日間	受講時間	13 時間
受講料	275,000（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を凝縮し、様々なログや通信から、攻撃の痕跡を検出・判断するポイントを学習します。最終的には、攻撃の検証から検出、成否判断までを自ら試行することで、PSOCやCSIRT等で技術を担当する方が実環境に応用可能で実践的な技術の習得を目指します。 <カリキュラム概要> Webサーバログ解析、IDS/IPSによる通信の解析、IDS/IPSの特性、インバウンド通信解析、アウトバウンド通信解析、Proxyサーバログ解析、脆弱性検証、総合演習
具体的な到達目標	・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、公開サーバへの攻撃やマルウェア感染などの不正な通信を発見したり、攻撃によるシステムへの影響の有無を判断するための要素を会得する ・公開サーバへの侵入やマルウェア感染など、実際の重大インシデントを想定したシナリオを通じて、緊急性の高い事態が自組織で発生した際に、検出から防御までの一連のサイクルを実践するための要素技術を会得する
修得できるスキル	・様々なログや通信から、攻撃の痕跡を検出・判断するスキル ・攻撃の検証から検出、成否判断できる ・これらの技術を応用して、現場の調査解決アプローチを体系的に仕組み化できるスキル
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	・Linuxの基本的な知識とコマンドラインを利用した操作、ネットワークの基本的な知識と、Wiresharkの基本的な操作 ・TeraTerm、puttyなどの Windows用SSHクライアントを利用したSSH接続 ・基本的なHTTP通信の仕組みを理解していること ・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や、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_middle.html