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

マルウェア解析ハンズオン自動解析コース

実施機関名	株式会社ラック		
講習名	マルウェア解析ハンズオン自動解析コース		
特定講習番号	21-005-014		
講習形態	リモート形式又は集合形式	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	330,000（円/税込み）		

対象分野 <ITSS+（セキュリティ領域）>	主な分野	セキュリティ調査分析・研究開発	関連分野	セキュリティ統括 セキュリティ監視・運用 脆弱性診断・ペネトレーションテスト

講習内容	マルウェアの自動解析機能が実装されたサンドボックス（Cuckoo Sandbox）を活用して、不審なファイルやマルウェアを解析する手法を習得します。
具体的な到達目標	・サンドボックスの役割や機能を理解できるようになる ・サンドボックスを利用して、マルウェアの機能を解析できるようになる ・サンドボックスを利用して、マルウェアの影響範囲を判断できるようになる ・最近、流行しているマルウェアの自動解析手法を理解できるようになる
修得できるスキル	・サンドボックス（Cuckoo Sandbox）を活用して、不審なファイルやマルウェアを解析するスキル ・解析されたレポートから、解析対象ファイルの機能や影響を特定するスキル
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・セキュリティ推進部門業務、SOC（セキュリティ運用）要員業務、CSIRT要員業務（技術系）、セキュリティ監査担当等セキュリティ関連業務の実務
講習の理解・習得のために推奨される知識・技術	・WindowsOSの基本的な操作知識 ・ネットワークの基本的な知識
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グループ討議の内容、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/cuckoo_sandbox_2days.html