演習シナリオのイメージ	**組織の従業員が標的型メールを受信しました。従業員は取引先からのメールと認識し、添付されていたファイルをクリックしました。その結果、攻撃者に端末を操作され、機密ファイルが外部に持ち出されました。**

インシデントレスポンスの流れ		
インシデント発生		❑ マルウェアが添付されたメールが標的の組織に送信される。 ❑ 社員がメール内に含まれる添付ファイルを実行し、C&Cサーバより RATがダウンロード・実行される
検知・連絡受付	インシデント発生の連絡 	❑ セキュリティイベントが発生した旨の連絡を受け速やかに関係者に情報を連携する。 ❑ 受領した連絡の情報の真偽を確認するとともに、追加で必要な情報を速やかに収集する。
トリアージ	状況把握、対応方針の決定 	❑ イベントがインシデントか否かを判断し、対処中のインシデントがあれば優先順位付けを行う。
初動対応	インシデント対応の実行 	❑ あらかじめ定められた被害拡大の防止のための暫定的措置（抜線など）を行う。 ❑ インシデントに至った直接的な原因（脆弱性など）を是正する。
復旧措置・回復	恒久対策・再発防止策の策定 	❑ インシデント発生前の状態に戻す（データ復旧、システムの再構築、サービスの再開など）。 ❑ インシデントが再発させないため、ソフトウェアのバージョンアップや権限の見直しなどの技術的対策を講じる。
事後対応	振り返り 	❑ 関係者でインシデント対応について振り返りを実施する。 ❑ 同様のセキュリティインシデントが発生しないように、セキュリティ耐性の総点検をするとともに、定期的な訓練の実施を決定する。

日程	2024年9月18日(水)	2024年9月19日(木)	2024年9月20日(金)
内容	インシデント対応の基本的な流れを理解する	攻撃者の立場で標的型攻撃を体験する	実践形式でインシデント対応を体験する
受講形態	個人	個人	グループ
時間	10:00 開始～17:00 終了 （昼休みの休憩を含む） ※時間はおおよその目安です。終了時間は、当日の進行によって多少前後することがございます。		
演習シナリオ	SOCからの通報によりマルウェアに感染したことが発覚する。 組織内で感染拡大し、ファイルサーバの機密ファイルが外部に持ち出された。	標的型メールで組織内に侵入した後、ADに横展開する。 永続化やアカウント情報を収集した後、ファイルサーバの機密ファイルを外部に持ち出す。	標的型メールでC&CとDNSで通信するマルウェアに感染する。 横展開によりドメイン管理者権限が奪取され、機密ファイルが外部に持ち出された。

実践で活かせるスキルを身に着ける

サイバー演習では、机上での演習と比較した場合に、端末を実際に操作してハンズオンを取り入れることで、高い学習効果が実現できます。セキュリティインシデント対応の理解や技術的なスキルの向上に関しても、実機を用いたサイバー演習は不可欠です。本セミナーでは組織のネットワーク環境を模した演習環境を利用します。仮想環境で模擬的に発生させたサイバー攻撃を体験することで、実践で活かせるインシデント対応の知識やスキルが身につきます。

	役割	求められるテクニカルスキル	求められるノンテクニカルスキル
経営層	❑ セキュリティにかかわる人的、システム的リソースの手配 ❑ インシデント対応も含めたセキュリティ施策の最終判断	❑ 攻撃戦術、ステージ、技術、手順に関する知識	❑ 関係者との適切なコミュニケーション ❑ リスクとビジネス継続を考慮して意思決定する能力 ❑ 組織統制能力
CSIRT管理者	❑ CSIRT担当者への対応指示 ❑ インシデント対応状況の管理 ❑ 経営層への説明	❑ セキュリティインシデント対応能力 ❑ セキュリティリスク、脆弱性に関する知識 ❑ マルウェア等各種攻撃に関する知識	❑ インシデントに関する報告ができる能力 ❑ リスクとビジネス継続を考慮して優先順位づけする能力 ❑ インシデントに関する管理
CSIRT担当者	❑ インシデント発生時の各種ログ調査 ❑ 脅威・脆弱性情報の収集 ❑ 外部ベンダーとの連携 ❑ インシデント対応状況の報告	❑ セキュリティインシデント対応能力 ❑ セキュリティリスク、脆弱性に関する知識 ❑ マルウェア等各種攻撃に対する対応能力	❑ インシデントに関する管理 ❑ インシデントに関する報告ができる能力

3つの特徴

01 組織のネットワーク環境を模した演習環境を利用

攻撃者の立場で疑似マルウェアや攻撃ツールを操作する体験や、業者の立場でログから侵害の痕跡を分析する体験を通じて、実践で活かせるインシデント対応の知識やスキルが身につきます。

02 経験豊富な講師・チュータのサポート

セミナーでは複数のチュータが皆様の演習をサポートします。
質問や分からないことは適宜確認しながら進めることもできます。

03 短期集中型の集合演習

3日間の短期間で代表的なサイバー攻撃の全体像を学び、セキュリティインシデントに迅速・適切に対応できるスキルを身につけます。
テクニカルなスキルだけでなく、円滑なインシデント対応を実現するためのノンテクニカルスキルについても学びます。