インシデントレスポンス

～現場で活用できるインシデント対応力を身に付ける ～ 【２日間】

　インシデント対応は、平時の準備と適切な初動対応が重要となります。また、原因特定や改善対策のためには、適切な証拠保存も重要となります。組織内で発生するセキュリティ事故に対して、迅速かつ適切に対応できるよう、インシデント対応に対する基本的な知識や考え方とともに、初動対応に必要となるライブレスポンスの知識や技術を、実践的な演習を通して学習します。

☑研修のゴール

・インシデント対応に関する流れと対応について理解し、説明できるようになる
・フォレンジックについての基本的な手順を理解し、証拠保全ができるようになる
・ログファイルの基本的な調査ができるようになる
・ライブレスポンスを活用し、 端末の基本的な調査ができるようになる

☑受講対象者

・システム管理者、セキュリティ担当者
・SOC担当者、CSIRT担当者
・インシデントに対する対応者、責任者

☑前提知識/望ましいスキルなど

・ネットワークに関する基礎知識
・OS（Windows/Linux）に関する基礎知識
・セキュリティに関する基礎用語
・サイバー攻撃に関する基礎知識

☑実施アジェンダ

【１日目】

１．はじめに（研修内容の全体説明）
２．組織的な対策の進め方
　・ 必要性、機能、役割、体制等
３．インシデントレスポンスの基礎
　・ インシデントハンドリング
４．デジタルフォレンジック基礎
　・ フォレンジックの対応フロー
　・ 調査手法の概要など
５．ログ調査
　・ Linuxコマンドを活用したログ調査
　・ Windows機能を活用したログ調査

【２日目】

6. 巧妙化するマルウェア
　・ マルウェアの特性と検知の仕組み ～
　・ セキュリティラボ
7. インシデント対応に役立つツール
　・自動起動/プロセス/通信の調査
　　検体捕獲時の留意事項
9. インシデント対応訓練
　・模擬インシデントに対する対応
　・状況把握、初動対応、調査、再発防止
　・報告書の作成・報告の実施
　・対応手順の振り返り
10. 総括：インシデントに対する心構え

※アジェンダについては最新のサイバーセキュリティ動向・実施期間により多少変更となる場合もございます。予めご了承ください。

☑開催要項

・コース名：インシデントレスポンス
・開催日数：2日間（ 9:30-17:30 ）
・実施方法：オンライン、または、集合研修
・研修形式：座学 及び 実機を使った演習、ワークショップ
・研修費用：150,000円（税別）／人 （最少催行人数：4名）

当社の定期開催は1名様からお申込みいただけます。定期開催の実施スケジュールは、弊社営業へお問い合わせください。また、個別開催も可能です。随時お問い合わせ下さい。

☑お問い合わせ・お申込み

・ストーンビートセキュリティ株式会社
・TEL 050-6877-5988　メール：training@stonebeat.co.jp
・https://www.stonebeat.co.jp#training

Stonebeat Security
Your Trusted Security Advisor