【大阪科学技術センター・スキルシステムズ(株)・サイバーコマンド(株)*共催】

[中級者向け]

サイバーセキュリティ防衛の人材育成講座
Cyber-Threats and Defense Essentials
～サイバー脅威と防御の要点～

集合研修　中級レベル

・サイバー攻撃よるインシデントをツールを使って検出し、初動対応に必要な初期分析を身に付けたい方
・社内セキュリティ担当として、有事に備え実践訓練を積みたい方
・システム部門とセキュリティ部門の調整役を担っている方
・新しくセキュリティ部門に配属される方

＊プログラム提供・運営

サイバーセキュリティの脅威は、日々進化しており、その種類もマルウェアやフィッシング詐欺、ランサムウェア、DDoS 攻撃、APT 攻撃など多様化しています。IoT 機器やスマートフォンなどの普及により、それらの脆弱性を突いた攻撃も増えており、総務省の発表によると、2021 年に観測されたサイバー攻撃関連通信数は各 IP アドレスに対して 18 秒に 1 回攻撃関連通信が行われていることに相当するとされています。

本講座で体験する APT 攻撃は、その中でも近年増加しており、特に、政府機関や防衛産業、金融機関、エネルギー、インフラなど、重要な情報を保有する組織が標的とされることが多く、その被害は深刻です。また、中小企業や個人でも標的型攻撃の被害を受けることが増えています。さらに、APT 攻撃は、攻撃者が長期間かけてターゲットの情報を収集し、情報漏洩やシステム破壊などを行うため、一般的なサイバー攻撃と比較して高度で対策が難しく、検知が遅れることが多いのも特徴の一つです。

本 Cyber-Threats and Defense Essentials では、サイバーセキュリティの脅威や APT 攻撃について学び、対策を講じるためのトレーニングを行います。講座を受講することで、実際の攻撃事例から脅威に対応する優先順位の設定や脆弱性の管理など、サイバーセキュリティに関する専門知識を身につけられます。

【開催日程・場所】

日程:2023 年 **12 月 7 日(木)、8 日(金)** 10:00～17:30（集合研修）

場所:CYBERGYM　大阪アリーナ　（アクセスマップ:https://cybercom.co.jp/access）
（大阪市東淀川区東中島1－17－26　スキルインフォメーションズビル4F）

【受講推奨対象者】

・サイバー攻撃のインシデントをツールで検出し、初動対応に必要な初期分析を身に付けたい方
・社内セキュリティ担当として、有事に備え実践訓練を積みたい方
・システム部門とセキュリティ部門の調整役を担っている方
・新しくセキュリティ部門に配属される方

【受講レベル】

・システム部門またはセキュリティ部門で1年以上従事経験がある
・インターネットブラウザを使用して日本語で各種情報を検索・閲覧できる
＊プログラミングの知識や経験は問いません。

【得られる知識・スキル】

・複数の検出・監視ツールを駆使してサイバーインシデント攻撃を検出できるようになる。
・検出したサイバー攻撃インシデントの初期分析をできるようになる。

【講師】

・横濱　悠平(サイバーコマンド(株)取締役 CTO、Certified Ethical Hacker:認定ホワイトハッカー)
・浦中　究(サイバーコマンド(株)代表取締役、(一社)情報処理安全確保支援士会　近畿担当理事)

【その他】

・1日目は、講義が中心で、2日目は演習が中心となります。
基本的には両日とも会場で実施しますが、1日目のみ、どうしてもご都合が付かない方は、講義の録画を事前視聴できるように準備いたしますので、11/30(木)までにご連絡下さいますようお願いいたします。

【プログラム】

1日目(12/7)

メニュー	詳細
①オープニングセッション	本日のトレーニング概要とスケジュールの説明
②サイバーセキュリティの概念	サイバーセキュリティの概念の解説
③アクティブディフェンスの概念	・情報セキュリティの概念 ・セキュリティシステムのレイヤー解説
④WireShark 概要	ネットワーク解析ツール「WireShark」利用法の解説
⑤WireShark 演習	演習用の解析データを実際に WireShark で解析するハンズオン演習
⑥マルウェアフォレンジック演習	あるかじめマルウェアを配置した OS 環境で脆弱性を検知するハンズオン演習
⑦SIEM 概論	SIEM(Security Information and Event Management)ツールの概要と操作について解説
⑧デイリーサマリー	1 日のまとめと質疑応答

2日目(12/8)

メニュー	詳細
①オープニングセッション	本日のトレーニング概要とスケジュールの説明
②アリーナインフラについて	トレーニングで利用するアリーナのセキュリティシステムとインフラについて説明
③APT 攻撃演習	イスラエルのレッドチームが行う APT 攻撃に対して、受講者(ブルーチーム)がチームで連携して攻撃を検知・崩御するハンズオン演習
④演習レビュー	行われた ATP 攻撃演習の振り返り
⑤クロージングセッション	講習全体の総括と質疑応答

＊トレーニングプログラムは、一部変更となることがあります。

【定　員】**先着14名**　＊定員超過の場合は、開催日を別途設ける予定です。＊最少催行人数:3 名

【申込み方法】

別紙の参加申込書に記入の上、事務局あてに、メールでお送り下さい。
お申し込みを受領後、請求書を送付いたします。

【参加費】(税込)　**参加費にテキスト(PDF)、修了証を含む。**

・賛助会員　：233,000 円／名
・非賛助会員:275,000 円／名　＊3 名以上ご参加の場合は、賛助会員ご入会がお得です。

【参加募集の締め切り】

応募締切り：2023 年 11 月 30 日(木) ＊定員に達し次第、締め切ります。

【講　師】

横濱　悠平
(サイバーコマンド(株)取締役 CTO、Certified Ethical Hacker：認定ホワイトハッカー)

2000 年から SIer 数社にてネットワークエンジニアとしてネットワーク、セキュリティ、開発の経験を積む。2003 年～2005 年 中国における飲食店検索サイトを開発、運営。2006 年から東京に戻り、システム開発会社を設立。主に web サービス系の開発事業、プログラマー育成事業を行う。

キャリア当初はネットワークやセキュリティのテクニカルな部分を担当。社内ネットワーク(オンプレ数百台)の設計、構築、実装を担当。その後、web 系の開発を担当する。主に PM やテックリードを担当。

浦中 究
(サイバーコマンド(株)代表取締役、(一社)情報処理安全確保支援士会 近畿担当理事)

国内大手 SIer、世界的なソフトウェアメーカーにて、プロジェクトマネージャ、サービスマネージャとしての実績と、サーバインフラ、ネットワーク、データベース、クラウド、サイバーセキュリティのエンジニアとして経験を積み、ベンチャー企業にて CISO(情報セキュリティ統括責任者)を務めた後、サイバーコマンド株式会社代表取締役に就任。

自社の「ホワイトハッカー育成事業」ではエンジニア育成を自ら行っているほか、一般社団法人情報処理安全確保支援士会の近畿担当理事を務め、近畿地方における「産・学・官・個」の連携推進、活性化のためのイベントを主催するなど、積極的な活動を行っている。

＜スキルインフォメーションズビル　アクセスマップ＞

スキルインフォメーションズ　ビル外観

スキルインフォメーションズ ビル ：
・JR 新大阪駅(東口)から徒歩5分、Osaka Metro 御堂筋線 新大阪駅から徒歩 7 分
・大阪市東淀川区東中島 1-17-26　　受付：スキルインフォメーションズビル 1 階
※当日の連絡先：090-3925-6257(大阪科学技術センター事務局携帯)

［中級者向け］

【サイバーセキュリティ防衛の人材育成講座】
Cyber-Threats and Defense Essentials

参 加 申 込 書

E-Mail:innovation@ostec.or.jp

（大阪科学技術センター 技術振興部 篠崎宛）

＜申込締切日＞

2023 年 11 月 30 日(木)まで

機関名:		
所在地:〒 TEL:( ) — FAX:( ) —		
氏 名	所 属 ・ 役 職	メールアドレス

【キャンセルについて】

参加者のご都合が悪い場合は、原則、代理の方がご出席ください。

キャンセル料はお振込みの有無にかかわらず下記のとおりです。

キャンセルご連絡日	キャンセル料
開催7日前～前々日(開催当日含まず)	参加料の 30%
開催前日および当日	参加料の全額

＊既にお振込済みの場合は差額をご返金します。返金口座をご連絡ください。

個人情報の取扱いについて

・本講座へのお申込みにあたり、個人情報保護のため、(一財)大阪科学技術センターが、適切に取り扱います。
・ご記入頂いた個人情報は、本ワークショップの運営・管理等に関するご連絡及び関連する事業等のご案内以外には使用致しません。個人情報の取扱いは、当財団の「個人情報保護規程」に従って対応いたします。