【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】

[初級者向け]
【サイバーセキュリティ防衛の人材育成講座】

e-learning　初級 Lev.2

＊プログラム提供･運営

本講座は新しくセキュリティ部門に配属される方にとって役立つ知識を集めた講座です。
通信の際に必須となる暗号化と署名に関する知識を初め、業務にて頻繁に目にすることになるであろうログについての知識、そしてより安全に通信するための通信手法について学んで頂きます。

過去にどのような攻撃が大きな脅威となっていたのか、実例と共に紹介した後、どのようにしてセキュリティインシデント（望まない単独若しくは一連の情報セキュリティ事象又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。JIS Q 27000：2019）による被害を最小にとどめるのか、考えるための下地となる情報をお伝えいたします。

また、ウェブサイトの安全性やプライバシー、インシデントからの復旧方法についての学習し、最後に、攻撃を仕掛けてくるハッカーがどのような行動をとる傾向になるのかを学ぶ事で、これまで学んだ知識をどのように業務に生かしていくのかをイメージ出来るようになります。

＊受講者特典としてインシデントハンドリングのテキストを進呈します。

【開催日程】
･随時、受講可能（e ラーニング形式）
･講義時間:約 16 時間（6 か月間、繰り返し視聴可能）

【主な受講対象者】
・プラスセキュリティ人材*を目指される方
・新しくシステム部門／セキュリティ部門に配属となる方
　＊本来の業務を担いながら IT を利活用する中でセキュリティスキルも必要となる人材のこと
　＊プログラミングの知識やセキュリティに関する資格保有の有無は問いません。

【得られる知識･スキル】
・サイバー攻撃を受けた際に実行すべき対応について理解することが出来き、サイバーセキュリティに関連する業務を行う担当者に協力することができる。

【実施方法】
・e ラーニング形式です。インターネットが使用できる環境ならご都合に合わせた時間・場所で受講が可能です。
・お申込み頂いた方には、受講方法をメールでご案内します。
・１つのお申込みに対して、１名のみが受講いただけます。

【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　：26,000 円／名
・非賛助会員：37,000 円／名　　＊10 名以上ご参加の場合は、賛助会員ご入会がお得です。

【全コースのラインナップと本講座の位置づけ】
サイバーセキュリティのコースは、大きく分けて初～上級まで3段階あり、本講座は、初級 Level.2 です。

＊サイバーセキュリティ人材育成講座の全ラインナップの概要は次ページをご参照下さい。

【プログラム】

メニュー	詳細
事前学習テキスト	インシデントレスポンスの基本
暗号化と署名	データ暗号化の概念
ロギングと否認防止	ログの収集とタイムライン
クラウドセキュリティ	クラウドは安全
VPN と在宅勤務	安全な VPN ソリューション
「悪意あるメイド」攻撃	ユーザーが知っておくべきこと
サプライチェーン	サプライチェーン攻撃と調査
インシデントレスポンス	ファーストレスポンダーの重要性
サイバーセキュリティの規則	サイバーセーフティの原則
ウェブサーフィンの安全性	ウェブ上の安全性・プライバシー・匿名性
サイバーインシデントからの復旧	従業員が知っておくべきことと実行すべき対応
ホームネットワーク	ネットワークトポロジー
ハッカーの視点	ハッカーの行動

レベル		到達レベル	実施形態／特徴
上級	Lev.3	○APT 攻撃に関する攻撃ツールと対処概要を理解し、各セキュリティプロダクトのオペレーション能力やフォレンジックやインシデントレスポンス能力を身に着け、幅広い知識とスキルで自社のセキュリティ中核人材を務められる。	世界最高水準のサイバーセキュリティ教育プログラムを提供するCYBERGYM 大阪アリーナ』で実際のサイバー攻撃と対応演習で実践力を習得できます。
	Lev.2	○ペネトレーションテストの計画から報告までの手法が理解でき、脆弱性に関する情報収集手法や、ツールを使用したペネトレーションテストの実施ができる。	
	Lev.1	○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を検出し、検出したインシデントの初期分析ができる。	
中級	Lev.3	○攻撃用のツールを実際に操作することで、防御するための対策を検討できる。	集合研修
	Lev.2	○調査と証拠保全のツールを使用し、マルウェアの発見駆除を行うことで、未知のマルウェアに対しても対応できる。	集合研修
	Lev.1	○講義とデモを通じてハッカーの攻撃手順、調査･証拠保全の手法を理解し、初動対応を行える。	オンライン（ウェビナー）
初級	Lev.3	情報セキュリティとは何か。といった基本的な知識を身に付け、業務を行う上での注意点に気づくことが出来る。	e-learning で実施。都合にあわせて WEB で期間内に繰り返し受講して効率的に学べます。
本講座	Lev.2	サイバー攻撃を受けた際に実行すべき対応について理解することが出来き、サイバーセキュリティに対応する業務を行う担当者に協力することができる。	
	Lev.1	ハッカーの攻撃手法とその特徴、関連する法律を理解し、サイバーセキュリティに対応する業務を行うことができる。 *ISMS や P マークの担当者も該当。	

経営者編	Lev.2	○「サイバーセキュリティマネジメント+法務+交渉」の切り口で、実践的な講義･演習を行います。実際に被害にあった場合の対応方法を習得。	集合研修で実施
経営者編	Lev.1	○経営層として把握しておくべき基礎知識を学習し、善管注意義務を果たすために最低限実施しなくてはならない対応を習得。	ウェビナーで実施

＊今回募集以外の講座は、ご案内の準備ができ次第、ウェブサイト上にリンクを設定し、参加お申込みいただけるようにします。

【サイバーセキュリティ防衛の人材育成講座（初級 Level.2）】

参 加 申 込 書

E-Mail:innovation@ostec.or.jp

（大阪科学技術センター イノベーション推進室 篠崎宛）

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

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。