2019 年 8 月吉日

アライドテレシスアカデミー(株)CSX サポート事務局

ISACA CSX 学習者 様

CSX 学習コース追加のお知らせ

日頃は弊社の ISACA CSX-Training をご利用いただきまして、誠にありがとうございます。

この度、ISACA CSX の学習コースが 2 コース新規に追加されました。これにより、全 21 コース、184 ラボ（シナリオ）での学習が可能となりました。新コースは、すでに利用可能となっております。

引続き ISACA CSX-Training の学習をお楽しみください。

＜＜　記　＞＞

１．追加コース・ラボ概要

◆ OWASP TOP 10　リスクの特定と軽減コース【難易度：17/21】

本コースでは、OWASP(the Opne Web Application Security Project：https://www.owasp.org/)が 2017 年年末公表した“2017 年最も重大なアプリケーショ

アライドテレシスアカデミー株式会社
〒141-0031 東京都品川区西五反田 7-21-11　TEL：03-5437-6066,　FAX：03-5437-6062

ンリスクトップ 10”（https://www.owasp.org/images/2/23/OWASP_Top_10-2017%28ja%29.pdf）に準じた学習ラボが完備されました。各 TOP10 の脅威に対してのアプリケーション開発時の注意点、および OWASP 推奨対策手法を実際に学習していただく事ができます。この学習により、脆弱性を克服した各脅威に対応したコーディング方法をマスターいただけます。

◆ CSX Volume8　　【難易度：16/21】

本コースは、先月リリースされた CSX Vol7 での Window サーバの堅牢化学習に続き、Window サーバに対しペネトレーション試験を実施できるまでの Lab 学習群です。

実際の Windows サーバのアクセス管理、Power Shell の設定方法を学習し、Windows Secure Host Baseline（SHB）（https://github.com/nsacyber/Windows-Secure-Host-Baseline）にて定義されたポリシーに合致したスクリプトを、ガイダンスに従い SHB に基づいたコンプライアンスチェックを実行します。SHB を理解した上での Window サーバへのペネトレーションテストを実施する Lab も準備しております。

これらの Lab により、Windows サーバ 2016 の最新の防御・検知機能を学習していただけます。

以上

アライドテレシスアカデミー株式会社
〒141-0031 東京都品川区西五反田 7-21-11　TEL：03-5437-6066,　FAX：03-5437-6062