AMIYA

超 実践型
サイバーセキュリティトレーニング

経営層から一般社員まで、全従業員のセキュリティ意識 / スキル向上が組織を守る

あらゆる層に適したトレーニング

経営層や一般社員向けのセキュリティ意識付け教育から、
エンジニア向けの実践 的なセキュリティトレーニングまで、幅広いコンテンツをラインナップ。

経営層 & 一般社員
セキュリティ教育

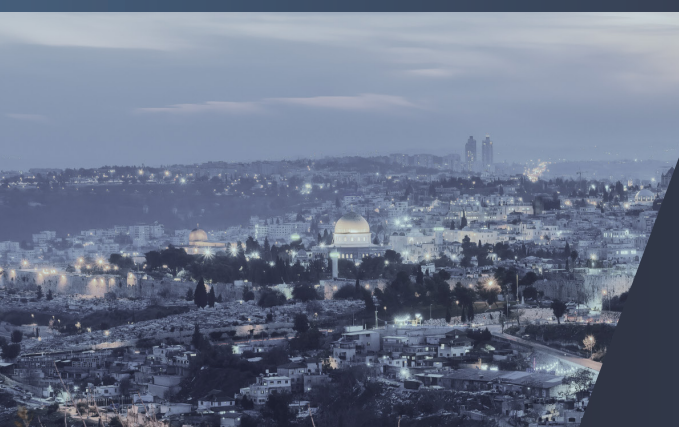
- 利害関係者マネジメント
- e ラーニング
- 情報セキュリティ基礎
- コンプライアンス
- 最新セキュリティ動向
- 標的型攻撃メール
- 規定 / マニュアル整備
- デューデリジェンス

セキュリティエンジニア養成
セキュリティトレーニング

- CSIRT トレーニング
- セキュア開発
- インシデントレスポンス
- OT セキュリティ
- ペネトレーション
- アクティブディフェンス
- デジタルフォレンジック

“リアルタイム” のサイバー攻撃を体感

最新のトレーニング施設で、レッドチームによるリアルタイムの
サイバー攻撃を体験。
実際にサイバー攻撃を受けることで、サイバー攻撃や防御方法
への理解が深まります。



イスラエル発
“最新” セキュリティトレーニング

サイバーセキュリティ先進国であるイスラエル。
重要インフラで培ったセキュリティナレッジをトレーニング化。

Cyber-Threats and Defense Essentials

サイバーセキュリティの基礎の復習と、実際に APT 攻撃を受けて検知する業務を実体験する実践的なトレーニングです。イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術によって安全に分離された環境下でリアルタイムに実際の APT 攻撃を体験できます。

対象

- 社内セキュリティ担当部門として、有事に備えた実践的な訓練を積みたい方
- 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

Goal

実際のサイバー攻撃を受け、複数の検出・監視ツールを駆使してサイバー攻撃を検出し、その分析を行うためのスキルを習得します。

プログラム

1. オープニングセッション	：トレーニングの概要とスケジュール説明
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
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とセキュリティシステムのレイヤー解説
4. WireShark 概論 & 演習	：ネットワーク解析ツール「WireShark」の利用法解説とハンズオン演習
5. Sysinternals 概要 & 演習	：Windows 対応の汎用解析ツール「Sysinternals」での利用法解説とハンズオン演習
6. マルウェアフォレンジック演習	：あら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
7. SIEM 概論	：SIEM ツールの概要と操作について解説
8. 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の説明
9. APT 攻撃演習	：レッドチームによる 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・防御するハンズオン演習
10. 演習レビュー	：行われた APT 攻撃演習の振り返り
11. クロージングセッション	：講習全体の総括と質疑応答

受講者の声

製造業

セキュリティ対策について考えが甘かった。特に脆弱性があるとどうなるのかが理解できた。

金融業

サイバー攻撃に関する調査は実践する機会はあまりないですが、トレーニングを通じて日々の訓練の必要性を痛感しました。

場所

日本橋アリーナ（東京都中央区日本橋浜町）

期間

座学はオンデマンド＆演習１日間

費用

定価：25 万円（税抜）/1 人

【特別価格】10 万円（税抜）/1 人
※5/19(金)、6/9(金)　開催分限定

問い合わせ先

株式会社 網屋
データセキュリティ事業セキュリティサービス部
セキュリティトレーニング担当
TEL：03-6822-9996　E-mail：bv-sales@amiya.co.jp

Penetration Tester Training

脆弱性診断やペネトレーションテストを行う際に必要不可欠となる知識やテクニックを習得します。
イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術によって安全に分離された環境で、実際のペネトレーションテスト演習を行います。

対象

- 社内セキュリティ担当部門として、ペネトレーションテスト / 脆弱性診断の実践的なスキルを習得したい方
- 社内システム開発担当としてセキュリティの品質管理に携わる方
- プログラミングの実務経験があり、セキュリティの知見を身に付けたい方

Goal

的確な脆弱性やマルウェアに関する網羅的な知識をベースとしてペネトレーションテストを実施するための様々なツールや手法について習得することを目標とします。

プログラム

1. オープニングセッション	：トレーニングの概要とスケジュール説明
2. 侵入テストの概要	：侵入テストの背後にある動機、ペンテスターとハッカーの違い、情報収集プロセスの説明、PT レポートを作成する方法論、PT 作業計画書を作成する方法論、ペネトレーションテストの各種方法
3. ネットワーク情報収集と演習	：ネットワーク情報収集と演習
4. Web 情報収集と演習	：Web 情報収集による攻撃ポイント調査と演習
5. Kali Linux 演習	：Kali Linux 概要と実践的な演習
6. Metasploit 演習	：Metasploit の概要と実践的な演習
7. ワイヤレスネットワークへの攻撃演習	：ワイヤレスネットワークの概念、暗号化、攻撃方法と演習
8. モバイルプラットフォームへの攻撃演習	：モバイルプラットフォームの概念と Android OS/iOS のハッキング
9. Web アプリケーションの脆弱性と攻撃演習	：Web アプリケーションへの攻撃手法と攻撃演習
10. クロージングセッション	：講習全体の総括と質疑応答

受講者の声

IT 業界 / システムエンジニア

脆弱性診断を体系的に学ぶことができたため、社内システムに対して、脆弱性診断を定期的に実施したい。

IT 業界 / システムエンジニア

開発案件に脆弱性診断を加えることで、売上向上につなげたい。

場所

日本橋アリーナ（東京都中央区日本橋浜町）

期間

座学はオンデマンド＆演習 2 日間

費用

定価：50 万円（税抜）/1 人

【特別価格】30 万円（税抜）/1 人
※、6/21（水）-22（木） 開催分限定

問い合わせ先

株式会社 網屋
データセキュリティ事業セキュリティサービス部
セキュリティトレーニング担当
TEL：03-6822-9996 E-mail：bv-sales@amiya.co.jp

Secure Coding for Developers

要件定義・設計・コーディングの段階で、セキュリティ上の脆弱性を含まない開発のための開発エンジニア向けトレーニング。イスラエルのホワイトハッカーが実際に攻撃を仕掛け、脆弱性が明らかになった箇所を受講者が改修し、再度攻撃がなされるというサイクルを、ハッカー及び講師からのフィードバックとともに繰り返します。

対象

- セキュア開発の基本知識を習得したい方
- ツールを使用したセキュアコーディングスキルを習得したい方
- 脆弱性に対する修正スキルを習得したい方

Goal

セキュアな製品を完成させるまでの一連の概念と開発手法の習得を目的とし、要件定義・設計・コーディングの段階で製品の安全性を確保するスキルの習得を目標とします。

プログラム

1. オープニングセッション	：トレーニングの概要とスケジュール説明
2. セキュアコーディング概説	：システム開発ライフサイクル（SDLC）に沿った工程ごとでのセキュリティ対応の要点確認
3. セキュアコーディング手法（入力バリデーション、認証と認可、暗号の使用、フレームワーク）	：セキュアコードにおける入力検証やシングルサインオン手順、暗号、効率の良い確実なセキュア開発のためのフレームワークを学ぶ
4. コーディング規約とコードレビュー	：重要なコーディング規約とコードレビューについて解説
5. コードレビュー演習	：脆弱性のあるプログラムコード（JAVA）のソースを目視にてレビュー、脆弱性の発見とその対応について確認
6. 静的コード解析	：静的解析ツール「SonarQube」を用いたコードレビューを体験
7. Web 脆弱性演習	：攻撃手法ごとの脆弱性のあるプログラムコード（JAVA）へ攻撃し、その結果を体験。そして、各プログラムコードの問題点や修正点について解説。
8. クロージングセッション	：1 日の学習のまとめと質疑応答

受講者の声

IT 業界 / システムエンジニア

脆弱性があった時に実際何が起こるか？　ということが体験できた。

IT 業界 / システムエンジニア

開発プロジェクトにセキュア開発を組み込むことで、競争優位性を作れるなと感じた。

場所

日本橋アリーナ（東京都中央区日本橋浜町）

期間

演習 2 日間

費用

定価：30 万円（税抜）/ 1 人

【特別価格】15 万円（税抜）/1 人

※6/28(水)-29(木) 開催分限定

問い合わせ先

株式会社 網屋
データセキュリティ事業セキュリティサービス部
セキュリティトレーニング担当
TEL : 03-6822-9996　E-mail : bv-sales@amiya.co.jp