I-CYBERTECHサイバートレーニングサービス

大企業から自治体のお客様に向けた サイバートレーニングサービスをご提供いたします



● i-Cybertech サイバートレーニングサービスの特徴

- 1. 実践的なサイバー訓練プログラムをご提供いたします。
- 2. 既存のセキュリティ製品との連携が可能なため、疑似環境を構築し、本番に備えられる訓練を行います。
- 3. ITだけではなく、ICS/SCADA、モバイル、IoT環境のための訓練も行うことができます。(※1)
- 4. 複数の攻撃方法を組み合わせて、4500以上の既存のシナリオを用意しています。(※1)

このようなニーズにお応えします

- サイバーセキュリティ人材育成を短期間に低コストで実現したい
- スキルアップトレーニングをしたいが、自社のセキュリティエンジニアが不足しているため知識やスキルが分からない
- CSIRTチームを設置したが、インシデント対応力を上げたい
- OTセキュリティエンジニアのトレーニングがほしい

【インシデント対応の流れ】

SOCが対応		CSIRTが対応		
監視・発見	エスカレーション	攻撃の回避・防御	調査・解析	報告
・ 攻撃発見・ 攻撃監視・ 口グ監視・ 情報監視	・ 社内エスカレーション・ 初動対応・ 社外エスカレーション	・ ネットワーク遮断・ サーバ停止・ アカウント停止・ 攻撃遮断・ フィルタリング	ログ解析フォレンジック解析マルウェア解析その他調査	・ 社内報告・ 再発防止策の提示・ 社外広報

訓練チーム構成

ベーシックの訓練は必須のブルーチームおよびレッドチームで構成されますが、部門間連携を促進するための最大7チーム構成 で訓練は可能です。訓練チーム数は調整可能です。



ADMIN TEAM

アドミンチーム

- 演習全体を統括。
- ・ネットワーク全体、デバイ ス、及びポータルを監督。



レッドチーム

- ホワイトチームの管理下で、 サイバー攻撃を仕掛ける。
- 技術者で構成。



パープルチーム

- メディア対応。
- ・法務と危機管理 関連の広報チーム で構成。



BLUE TEAM

ホワイトチーム

- サイバー攻撃の シナリオを作成。
- ・レッド、グリーン、イエロー の各チームを管理。



グリーンチーム

- •ホワイトチームの 管理下で、行動。
- •正当なユーザーと サーバーで構成。



構成。



イエローチーム

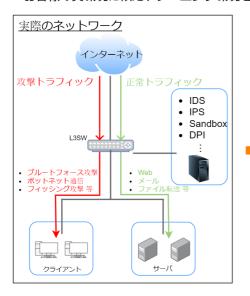
・無意識に悪意のある アプリケーションを インストールしたユーザ。 •グリーンチームの一部 メンバーで構成。

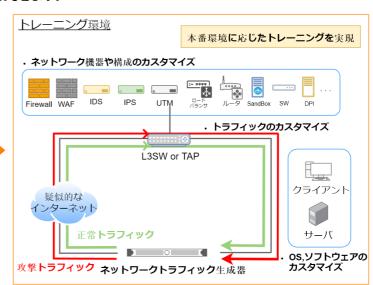


フォレンジックの技術者で

疑似環境構築イメージ図

• お客様の実環境に似たトレーニング環境を構築できます。





ネットワークトラフィックジェネレータについて

- 生成したトラフィックのPCAPも取得可能なため、フォレンジック分析にも役立ちます。
- BACnet DNP3 TCP
 - IEC61850 Modbus TCP Profinet UDP S7comm

…など

対応 ICS/SCADA プロトコル

・ 対応プラットフォーム

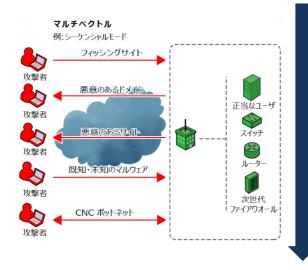
Windows Unix/Linux Mac OS Windows Phone Android/iOS Blackberry OS …など 対応アプリ

Dropbox Skype Line

MS Office/Outlook Amazon Safari

…など

攻撃シナリオ



第1段階

正規Webサイトを装ったメールやWebサイトに 誘導するため、リンク付きのメールを ユーザに送信する。

第2段階

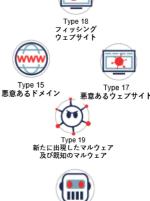
悪意あるドメインやウェブサイトに ユーザを誘導する。

第3段階

ユーザに既知・未知のマルウェアを ダウンロードさせ、端末を感染させる。

第4段階

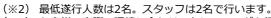
マルウェアに感染した端末は、 攻撃者が用意したC&Cサーバと通信を行い、 機密データのアップロードを行う。



Type 21 ポットネット通信

ご提供プラン

プラン	参考日数	既存のシナリオ	シナリオ作成 (委託)	シナリオ作成 (教育)	参考価格(円/1名) (※2)
シルバー	1日	0	0	-	お問い合わせください
ゴールド	5日	0	0	_	お問い合わせください
プラチナ	常設	0	-	0	お問い合わせください (※3)



(※3) お客様の実際の環境に合わせてトレーニングを行う場合はご相談ください。



i-CYBERTECH

サイバートレーニングサービス



情報セキュリティ株式会社

〒650-0012 神戸市中央区北長狭通 4 丁目 9-26 西北神ビル 3・8 階 TEL: 078-381-8980(10:00~17:00 土・日・祝除く) FAX: 078-381-8979

E-Mail: inquiry@isec.ne.jp URL: https://isec.ne.jp/