

サービス概要説明資料

CyberBastionセキュリティ研修

NTTアドバンステクノロジー株式会社

【研修内容】

- 講義：**セキュリティ対策の方法論 (NIST CSF2.0 / MITRE ATT&CK)**、および最近の脅威状況
- 演習：**CyberBastion** (テーブルトップ演習形式のセキュリティトレーニングプラットフォーム) による**標的型攻撃のセキュリティ対策シミュレーション**

【習得内容】

- サイバーセキュリティリスク(サイバー攻撃)対策に関する**標準的/体系的なアプローチの習得**
- **サイバー攻撃の戦術技術の理解と具体的な対策立案能力の向上**(攻撃手法に対する緩和/検知)
- 脅威シナリオを用いたシミュレーション (CyberBastion) 実施による**実践的能力の向上**

【受講対象者】

- リスク管理/セキュリティ統括・推進部門
- セキュリティ運用部門/SOC担当
- 情報システム部門
- CSIRT構成員
- 上記の業務にこれから携わる方

Webブラウザで行う体験型サイバー対策演習

1. セキュリティ担当部門向けの研修や、その他のセキュリティイベント等で活用できるサイバー演習
2. チームを作りゲーム感覚で演習することで組織全体の協力体制を強化できる
3. 脅威のシナリオが豊富で、標的型攻撃を模擬体験できる
4. 与えられた予算内で組織的・手続き的・技術的な対策をバランス良く適用することがポイント



< InfoSec SEE 2024の様子 >

■ FIRST会議等で著名なポーランドのMIROSLAW MAJ氏により提唱

- CERT-Polka(ポーランドのNational CSIRT)創設メンバー
- ポーランド国防大臣顧問
- ENISAの専門家でCERT等多数の出版物を共著
- セキュリティ関連ツール開発
- サイバー演習および若手育成を推進



■ リアルなカードゲームからオンラインプラットフォーム化へ

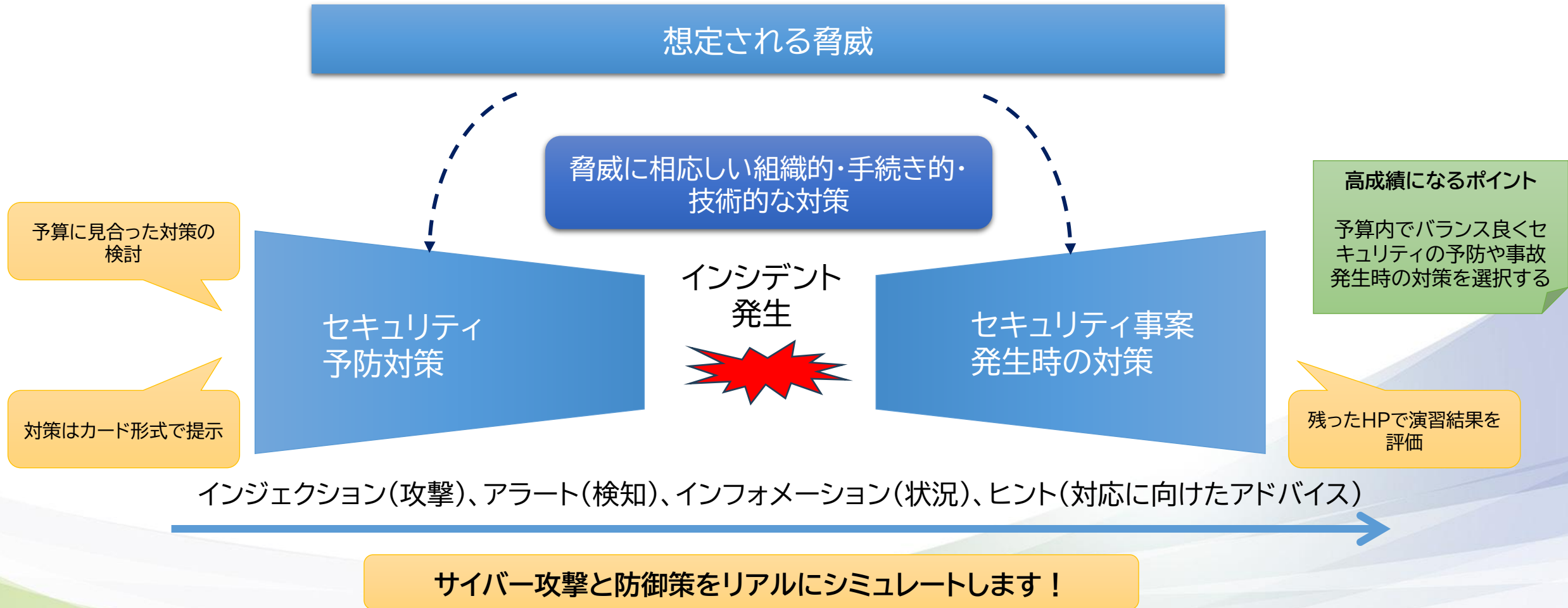
- 当初は、物理的なカードを用いてオンサイトで実施
- オンライン化により、規模的・地理的にスケール可能に

■ 欧州・米国への普及とマルチリンガル化

- 東欧から西欧、米国へと普及拡大。2024年はマルチリンガル化し、現在は日本語対応可能

CyberBastionを用いた演習の概要

脅威に対する事前・事後のセキュリティ対策検討の体験をとおり、実践的なセキュリティ対応能力を養います



■ オンラインのカード型演習

- ・ 発生するイベントに対し、カードを選び被害を抑止

■ 全員の参加を確認したのち、概要が提示

- ・ 開始すると、自動でシナリオが展開
- ・ 各チームに予算とヘルスポイント(HP)が初期に付与
- ・ 予算内でセキュリティ対策を選択し実施

■ イベントが発生するとチームのHPが減少

- ・ 残っている予算と、途中追加される予算を使って、対策を進める

■ 演習終了

- ・ 残ったHPで順位が決定

初期段階の状況付与の例

2024年7月1日 午前4時、何者かによって防衛産業A社の従業員用正面玄関にマルウェアに感染したフラッシュドライブがばらまかれました。

彼らの目的は、企業のICTリソースを乗っ取ることで業務を妨害し、ITシステムで処理されているデータを奪うことでした。攻撃者らは、出勤前の従業員が「サプライズ」が仕掛けられたフラッシュドライブを見つけ、興味本位で会社のコンピュータに接続し、社内リソースにアクセス可能とすることを計画していた。

数人の従業員が路上に落ちているフラッシュドライブを見つけましたが、ほとんどは、社内で規定されている手順に従って、見つけたフラッシュドライブを検証するためにIT部門に引き渡しました。

しかし、内部監査部門のリンダさんだけは、拾ったフラッシュドライブの内容を確認するために、会社のコンピュータに接続しました。

モニターに表示されたファイルの中には、Bonuses_June_2024.xlsxという名前のエクセルファイルがあり、好奇心に駆られたリンダさんは、サイバー犯罪者からの「贈り物」が入ったファイルを開いてしまったのです。

The screenshot shows the game interface with the following details:

- Top bar: データ移動媒体を利用した攻撃 ライブ | 予算 1.3M | 03:02
- Team Rankings:
 - 1. チーム3: 1.5M budget, 5 HP, 79.7% progress
 - 2. チーム1: 1.6M budget, 0 HP, 74.7% progress
 - 3. チーム2: 1.6M budget, 0 HP, 74.7% progress
- Notification (残り19分経過): ストレージメディアを介した攻撃の場合、攻撃者は通常、侵害されたメディアに仕掛けた悪意のあるコード(マルウェア)を使用します。マルウェアは、ドキュメント(*.docx)、スプレッドシート(*.xlsx)、またはその他のファイル(*.pdf、*.mp3、*.mpegなど)に隠されている可能性があります。ファイルの名前は、ユーザーが興味をそそられる名称になっているため、好奇心に導かれてファイルを開いてしまいます。
- Bottom bar: 予算変更 (残り1分経過) | インシデントが発生した可能性のあることを報告し、予算が増額されました。 +350K

チームごとに対策を競いHPで評価される

研修に用いる脅威シナリオ

#1	フィッシング～ランサムウェア	Basic	26分	攻撃者がフィッシングメールを介して従業員に悪意のある添付ファイルを実行させ、マルウェアを展開して感染拡大し、データを窃取した上でランサムウェアを実行してファイルを暗号化するシナリオ
#2	非暗号化通信の傍受 ～ソーシャルエンジニアリング ～VPN不正アクセス～データ窃取	Basic/ Advanced	45分	攻撃者が、予め用意したWi-Fi接続環境に従業員を接続させ認証情報を傍受し、従業員のメールアドレスを乗っ取り社内にフィッシングメールを送信し、別のアカウントを乗っ取ってアクセス範囲を拡大しサーバから重要データを窃取するシナリオ
#3	水飲み場型攻撃～ランサムウェア		40分	攻撃者が水飲み場型攻撃により従業員のコンピュータ上でマルウェアを展開し、重要データを含むサーバを特定した上でランサムウェアを実行してファイルを暗号化するシナリオ
#4	ソーシャルエンジニアリング ～VPN不正アクセス ～データ破壊		40分	従業員のノートPCに不正アクセスした攻撃者が、PC内に保存されていた認証情報を使って企業ネットワークにVPN接続し、サーバから重要データを窃取した後にデータ破壊ツール(ワイパー)を実行するシナリオ
#5	フィッシング～RAT	Advanced	38分	攻撃者がフィッシングメールを介して従業員に偽のインストーラーを実行させ、RAT(リモートアクセス型トロイの木馬)を展開して内部データの取得や収集を行った後に窃取するシナリオ

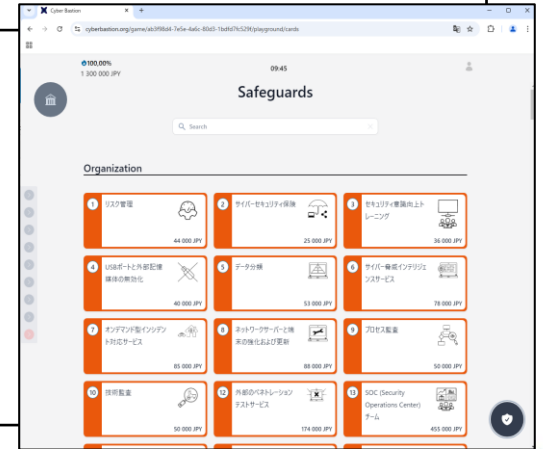
Basicレベル: 各種セキュリティ管理策(ソリューションレベル)を適切に選択したい方向け
Advancedレベル: ITシステム内のマルウェアの振舞いを理解し検出ポイントを設定するなど、技術的な興味の高い方向け

午後半日コース(約4時間)の例

#	時間	概要	内容
1	13:00	オリエンテーション	開講挨拶・連絡事項
2	13:10-14:20	講義 ・ サイバーセキュリティフレームワーク ・ サイバー攻撃の戦術/技術	セキュリティのリスクマネジメントや対策について以下の内容を紹介 ・ NISTサイバーセキュリティフレームワークのコア機能「統治、識別、保護、検知、対応、復旧」、ティア、プロパティ ・ MITRE ATT&CKをベースにサイバー攻撃の戦術/技術、および、緩和/検知等
3			
4	14:30-16:30	演習	<ul style="list-style-type: none">・ CyberBastionの説明・ セキュリティ対策カードの説明・ デモシナリオ 解説あり・ デモシナリオ 解説なし・ デモシナリオ フィードバック・ 本番脅威シナリオ
5	16:30-17:00	フィードバック	本番脅威シナリオ・演習のフィードバックと全体まとめ
6	-	クロージング	閉講挨拶・アンケートのお願い

CyberBastionを活用した研修に関する補足事項

<p>研修講師</p>	<p>NTT-AT社のサイバーセキュリティ部門が講師を務めます。</p>
<p>CyberBastion プラットフォーム</p>	<p>Webベースのアプリケーションで下記を特徴とします。</p> <ul style="list-style-type: none"> ・ セキュリティ脅威に関する課題に対し、対策をカード形式で提示しながら組織を防衛 ・ 脅威のシナリオ(20分～90分程度)に対し、リアルタイムで対策を検討 ・ HPを用いて当該脅威に対する組織防御の度合いを評価
<p>オンライン開催時の コミュニケーション</p>	<p>MS Teams/Zoom を用いて研修を実施します。 (各チーム参加者がリモートから参加する場合は、チーム内コミュニケーションは、MS Teams/Zoomのブレイクアウトルームを利用させていただきます。)</p>
<p>参考資料</p>	<p>MITRE ATT&CK https://attack.mitre.org/ NISTサイバーセキュリティフレームワーク https://www.nist.gov/cyberframework https://www.ipa.go.jp/security/reports/oversea/nist/about.html (右図は講義資料のイメージ)</p>



ATT&CKの構成要素

MITRE ATT&CKは、戦術、技術、手法の3つ要素で構成

NIST:サイバーセキュリティフレームワーク(5/12)

セキュリティ活動全体の構成

- ・ 識別 事業目的達成に必要な資産の特定
- ・ 防御 上記資産を安全に運用するためのセキュリティ対策の検討、実施
- ・ 検知 監視する手順の作成と監視
- ・ 対応 インシデントが発生した場合の対応
- ・ 復旧 復旧計画立案と関係者周知、調整

研修サービスお申し込みのご案内

受講料	弊社営業担当または下記連絡先へお問合せください。
チーム構成	2名以上推奨(4~5名が適切だが、特に上限なし)
研修期間	半日
受講環境	<ul style="list-style-type: none">・ PCやネットワーク等の必要な環境は受講者様にてご準備ください。・ Web会議システムはMicrosoft Teams/Zoomを利用いたします。・ Webブラウザは、Microsoft EdgeまたはGoogle Chromeをご用意ください。 ※Firefox、Safariはサポートしておりません。
申し込み方法	弊社営業担当または下記連絡先へご連絡ください。
問い合わせ先	CyberBastion研修担当 cyberbastion_contact@ml.ntt-at.co.jp

1. CyberBastion演習を活用した研修サービスのご紹介（15分）

- CyberBastion演習の概要説明
- 研修サービス(講義+CyberBastion演習+振り返り)の概要説明
 - 講義で扱う内容
 - CyberBastion演習のシナリオラインナップ
 - 研修スケジュール

2. CyberBastionのミニゲーム(デモシナリオをプレイ)（30分）

- デモシナリオの概要説明
- ミニゲームを実施
- 簡単な振り返り

3. Q&A

申し込み・お問合せ

弊社営業担当、または、CyberBastion研修担当(cyberbastion_contact@ml.ntt-at.co.jp)までご連絡ください。

NTTアドバンステクノロジー株式会社は、IOWN構想を支える技術力と、国内外先端技術・ノウハウを強みとして、
不断のチャレンジを続け、「環境エネルギーとデジタル化」に貢献してまいります。

