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株式会社

研修内容と習得内容・受講対象者

【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・簡易型机上レッドチーム演習PF）**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
- 情報システム部門
- 他
- セキュリティ運用部門/SOC担当
- CSIRT構成員

研修スケジュール

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 3	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
4	14:30- 16:30	演習	演習説明 ・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とは

オンライン型サイバー演習プラットフォーム

1. セキュリティ担当部門向けの研修、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PF
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、標的型攻撃を疑似体験できる
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>

（参考）CyberBastionの開発背景等

■ 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による演習

■ **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

2022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。

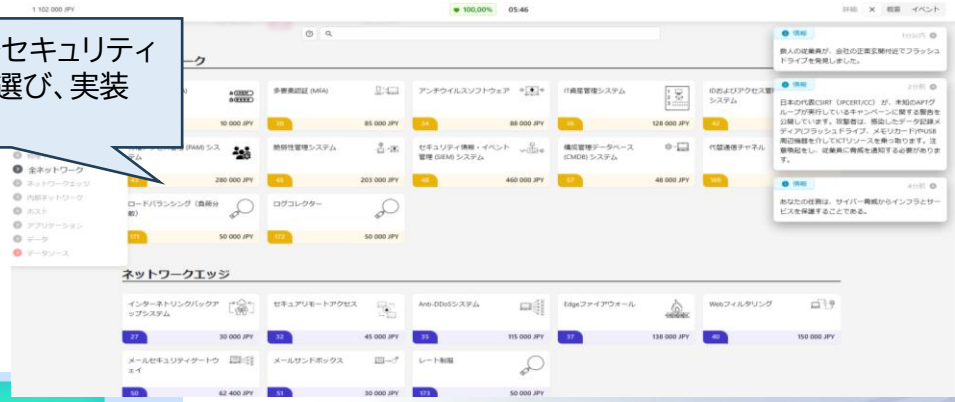
彼らの目的は、企業のICTリソースを乗っ取ることで業務を妨害し、ITシステムで処理されているデータを奪うことでした。攻撃者らは、出勤前の従業員が 「サプライズ」 が仕掛けられたフラッシュドライブを見つけ、興味本位で会社のコンピュータに接続し、社内リソースにアクセス可能とすることを計画していた。

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ーに接続しました。

モニターに表示されたファイルの中には、Bonuses_June_2022.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。

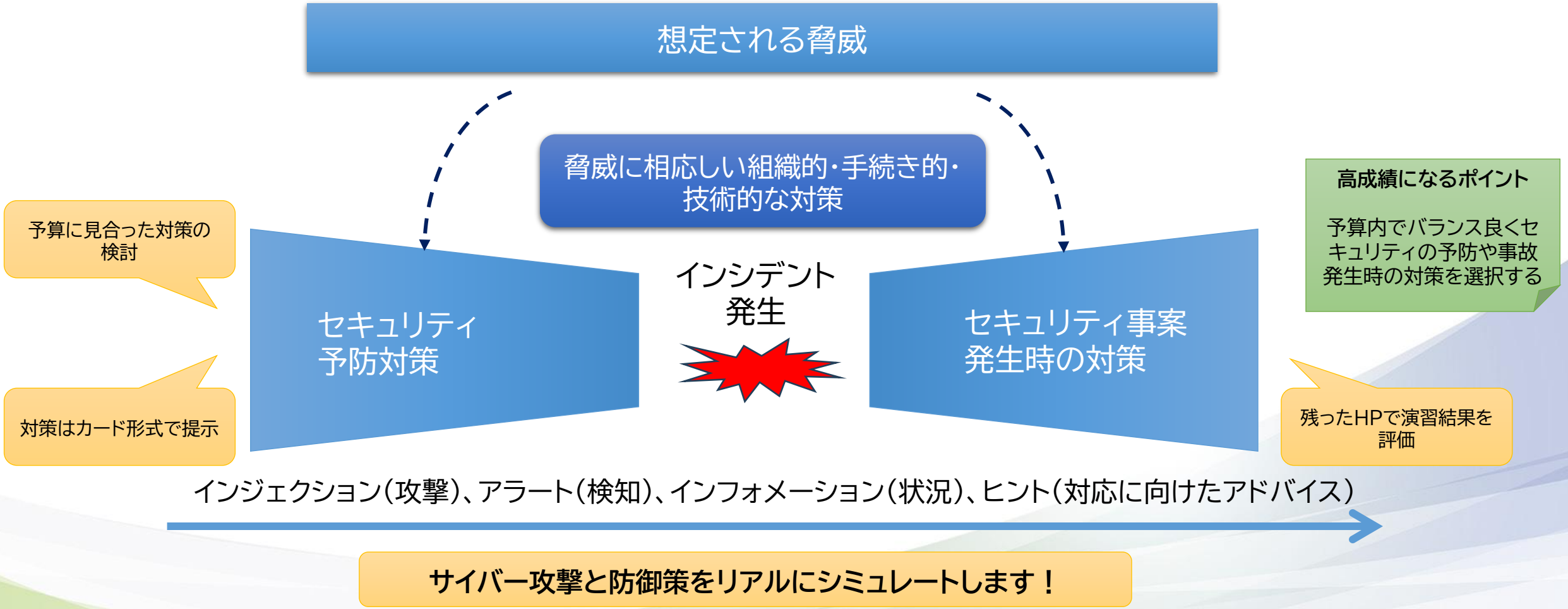
予算制約の中でセキュリティ対策カードを選び、実装



チームごとに対策を競い評価される

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し、実践的なセキュリティ対応能力を養います



サイバー攻撃と防御策をリアルにシミュレートします！

演習シナリオラインナップ

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、技術的な興味の強い方向け

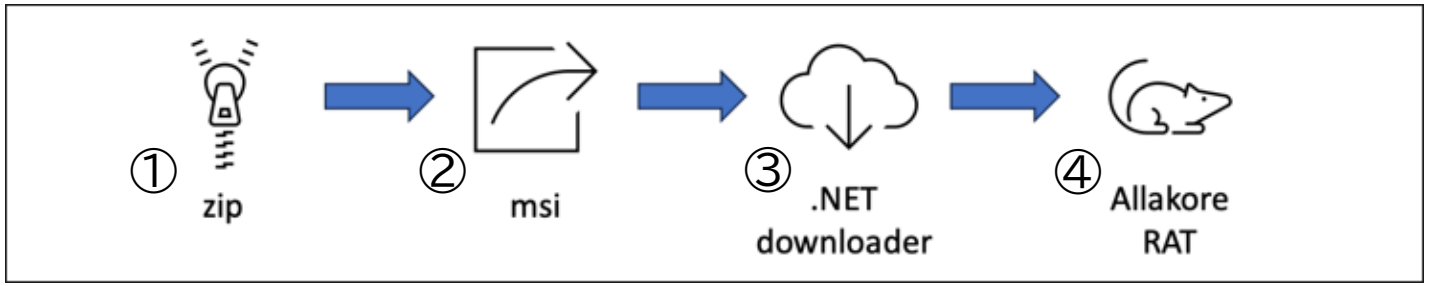
研修に用いる脅威シナリオ

Basic	フィッシング～ランサムウェア	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
Basic/ Advanced	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	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、従業員のメールアカウント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
	水飲み場型攻撃～ランサムウェア	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
	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	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
Advanced	フィッシング～RAT	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

フィードバック(例)

シナリオ解説:実際に報道された本シナリオのベース事案

■ 攻撃の流れ



① 悪意あるzipファイルがスピアフィッシングやドライブバイダウンロードを介して被害者環境に届く

② zipの中には、インストーラファイル(.msi)を含む別のzipと、インストーラを解凍して実行するよう指示するテキストファイルが含まれる

③ インストーラを実行すると、マルウェアのダウンローダーとPowerShellスクリプトが展開

④ ダウンローダーはAllaKore RATを含むzipを外部からダウンロードし、RATを解凍して実行

.msi形式のインストーラファイルは、Windowsの正規のコマンドラインツール「msiexec」によってインストールが実行される

ダウンローダーは、Webサービス(ipinfo.io)を利用して、実行環境がメキシコ内か否かをチェック、メキシコではない場合は終了

PowerShellスクリプトはインストールに使用したファイルを後で削除する痕跡消去用

フィードバック(例)

シナリオ解説:対策のポイント(1)

■ フィッシングメールの送信、メール内リンクによる偽サイトへの誘導

情報 01:30

攻撃者はOSINTの手法を用いて、大手金融機関の財務・経理部門に勤務する人々の電子メールアドレスのリストを特定します。

情報 05:00

攻撃者は人工知能アルゴリズムで作成した偽メールを送りつけ、社会保険庁になりすましています。メッセージには、社会保険庁の偽サイトのリンクが含まれています。

攻撃 06:00

攻撃者が作成したメッセージが、あなたの組織の財務・経理部門の従業員に送信されました。

情報 07:30

財務・経理部門の従業員が、社会保険庁の偽サイトへのリンクをクリックしました。

攻撃 08:30

従業員が社会保険庁の偽サイトを閲覧しました。

初期アクセス

攻撃手法

フィッシング - T1566

緩和策	検知/監視対象
☐ ウイルス対策/マルウェア対策 ☐ 監査 ☐ ネットワーク侵入の防止 ☐ Webベースのコンテンツの制限 ☐ ソフトウェアの構成 ☐ ユーザーのトレーニング	☐ アプリケーションログの内容 ☐ ファイルの作成 ☐ ネットワークトラフィックの内容 ☐ ネットワークトラフィックフロー

初期アクセス

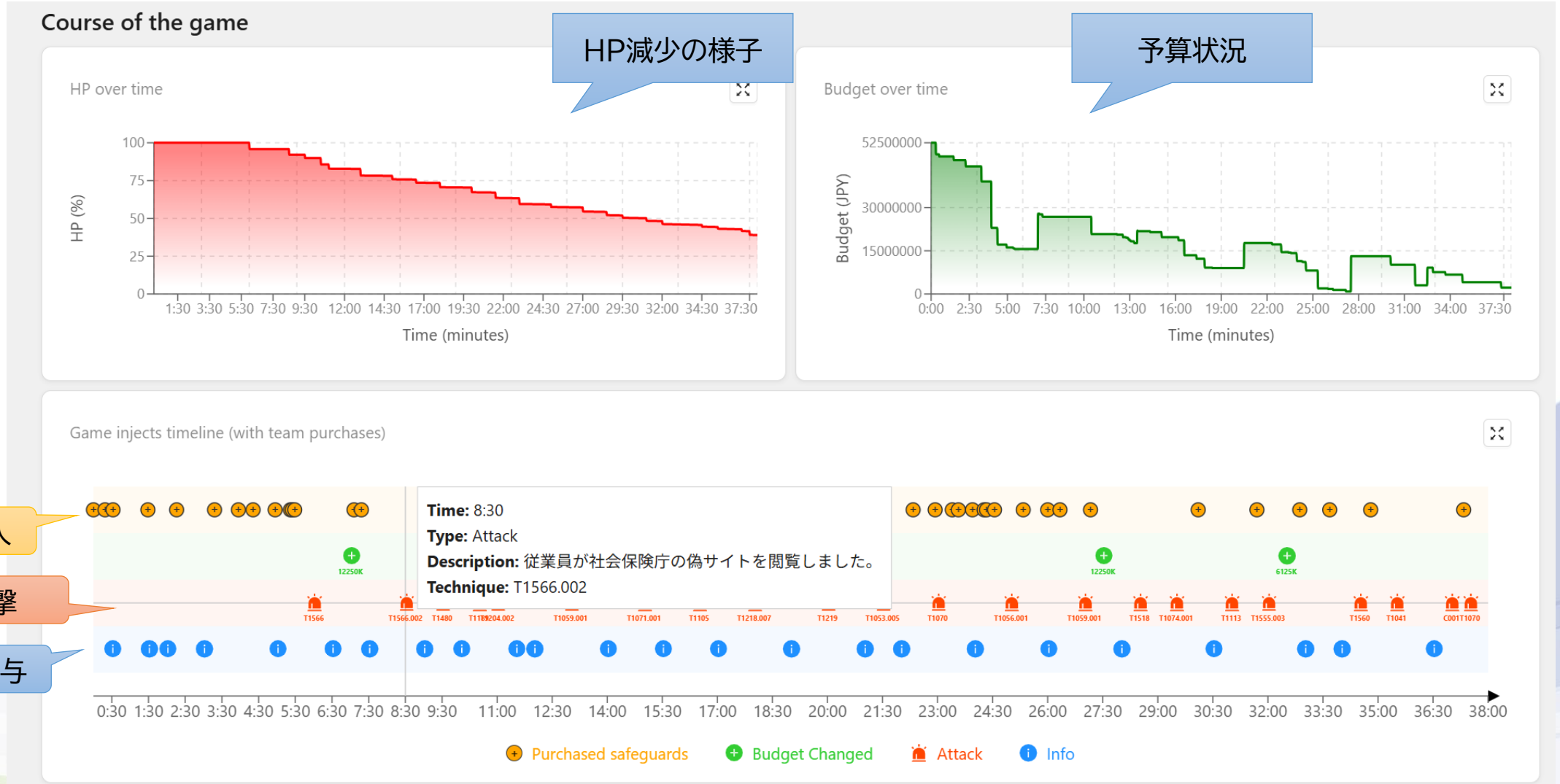
攻撃手法

フィッシング:スピアフィッシングリンク - T1566.002

緩和策	検知/監視対象
☐ 監査 ☐ Webベースのコンテンツの制限 ☐ ソフトウェアの構成 ☐ ユーザーアカウントの管理 ☐ ユーザーのトレーニング	☐ アプリケーションログの内容 ☐ ネットワークトラフィックの内容 ☐ ネットワークトラフィックフロー

フィードバック(例)

チーム個別フィードバック： 参加チームのゲーム進行結果



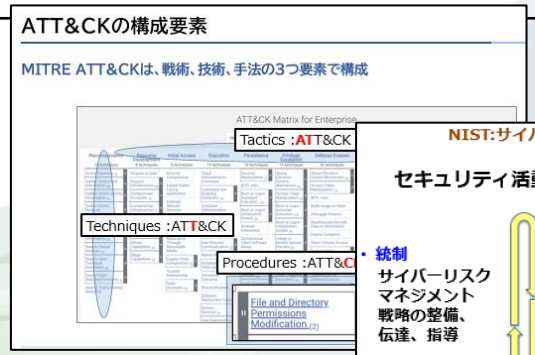
カード購入

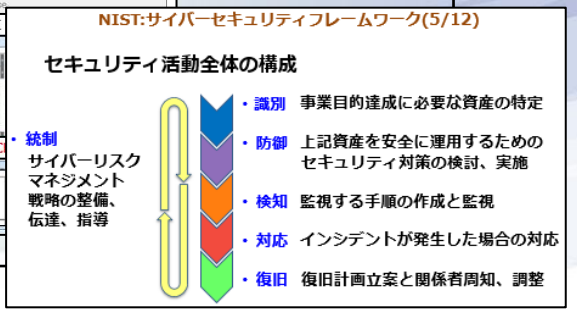
攻撃

情報付与

CyberBastionを活用した研修に関する補足事項

研修講師	NTT-AT社のサイバーセキュリティ部門が講師を務めます。
CyberBastion プラットフォーム	Webベースのアプリケーションで下記を特徴とします。 ・ 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
オンライン開催時の コミュニケーション	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していただきます。）
参考資料	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）





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	・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

Cyberbastionミニゲーム体験会のご案内

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。