Threat Intelligenceの活用による セキュリティ対策の効率化と高度化

Internet Week 2022 C43

EYストラテジー・アンド・コンサルティング株式会社

Building a better working world

登壇者紹介

松下 直（まつした なおし）

EYストラテジー・アンド・コンサルティング株式会社
Technology Consulting / Cybersecurity - Partner
CISSP / CISA / CISM / RISS

情報セキュリティ・サイバーセキュリティの分野での25年以上の経験を有し、先端的セキュリティベンダーとの提携を通じ企業のITインフラを防御するマネージドサービス、インシデントの検知・対応を行う商用SOC/CSIRTの開発と提供、国内外でのセキュリティアセスメントなど幅広い経験を有する。セキュリティ専業会社・セキュリティサービスの海外拠点の立ち上げ、また、国内外の先端的ベンチャー企業への経営への参画などの経験も有する。現在は、EY Japan RegionにてCybersecurityのLeaderとして、EY Japan, Globalのリソースをミックスし、日系企業のセキュリティ対策支援を国内外で提供している。

登壇者紹介

雨宮　崇（あめみや　たかし）

EYストラテジー・アンド・コンサルティング株式会社

Technology Consulting / Cybersecurity - Partner

サイバーセキュリティの領域において侵入テストや脆弱性診断、レッドチームなどといったオフェンシブサービスやCSIRT運用・インシデント対応支援、マネージドセキュリティサービスのリーダーとして組織をリード。
これまでサイバーセキュリティエンジニアリングチームを一から構築し、25に及ぶサービスを立ち上げた経験を持つ。
前職ではグローバル大手ソフトウエア、ネットワーク企業、eコマース企業にてリーダを経験。

Contents

拡大する情報漏洩事故の被害

Optus社（AU通信事業者）における940万件の個人情報漏洩

9月24日 – ハッカーグループのオンラインコミュニティに攻撃者と思われるユーザーが、Optus社の940万件の個人情報を外部に公開されていたAPIから盗んだと投稿。

攻撃者は1週間以内に100万米ドルの身代金を支払うことを要求。

9月27日 – 攻撃者は1万200人の個人情報を公開し、身代金を払わなければ、毎日同じ量の情報を公開し続けると脅迫。

最初の個人情報の公開から4時間後、攻撃者は公開した情報を削除したとアナウンスし、合わせて身代金要求を撤回し謝罪（Optus者は身代金の支払いを行っていない）

オンラインコミュニティの他のユーザーが、1万200人分の個人情報を取得ている可能性が高い。この中に含まれている顧客は、なりすましなどの被害にあるリスクが拡大。

(参照)
https://www.abc.net.au/news/2022-09-27/optus-data-breach-cyber-attack-hacker-ransom-sorry/101476316
https://www.thestar.com.my/tech/tech-news/2022/09/27/australia039s-no-2-telco-optus-government-clash-over-massive-data-breach
https://www.theguardian.com/business/2022/sep/29/optus-data-breach-everything-we-know-so-far-about-what-happened など

Optus社（AU通信事業者）における940万件の個人情報漏洩

本セキュリティインシデントの特徴

Optusのインシデントにおいては、情報が漏洩した人数の大きさもさることながら、加えて、身分証明書の情報漏洩による影響が大きい。このインシデントの影響は、Optus社のみにとどまらない。

求められるセキュリティ対策

他社で起きたセキュリティインシデントの場合においても対応が必要となる

- 正規のユーザーからの個人情報の更新が同時に大量に起こりうる
- 身分証明書が漏洩している前提で多重の本人確認を行う必要がある

自社で保有する機密情報（特に個人情報）において情報漏洩事故を想定した対策が求められる

- 個人情報の保管場所を特定し不審なアクセスについての監視・調査を常に行う
- 情報漏洩リスクについてのモニタリングを行う
- インシデント対応フローを作成し定期的に対応訓練を行う

Threat Intelligence

サイバーセキュリティにおける脅威について分析収集した情報

Threat Intelligenceの種類（例）	
トレンド	セキュリティインシデント、レギュレーションなど
IoC	Indicator of Compromiseセキュリティインシデントと特定するための根拠となる情報 攻撃者が利用したことのあるIPアドレス、URL、ファイルハッシュなど
Threat Actor	サイバー攻撃を行うグループに関する情報 APTXXなどのグループ名を付与。最近の攻撃活動の動向、攻撃の対象、攻撃手法など
ブランド モニタリング	特定の企業・ブランド名などをキーとして Surface/Deep/Dark Webを広くサーチして、情報漏洩の可能性、フィッシングサイト、シャドーITなどを検出

セキュリティインシデント検知・分析での活用

SOC/SOARにおけるセキュリティインシデント検知精度の向上

- Internetに公開されているシステムを守るFW/IPS/WAFで検知した攻撃元IP　Address をIOCで検証
- Outbound通信の宛先URLをプロキシより取得し、リスクの高い宛先へのアクセスを検出
- EDRやDLPにより検出されたファイルがマルウェアでないか確認

Threat Hunting での活用

Intelligence based Threat Huntingの概要

Threat Huntingとは

既存のセキュリティ対策を回避する高度な脅威を検知・隔離するために、能動的・再帰的にネットワーク内を探索するプロセスである。

Intelligence based Threat Huntingとは

インテリジェンス調査による把握したIOC情報や攻撃グループがよく使用した攻撃手法（TTPs）をインプットとして仮説を構築し、攻撃の痕跡を調査する手法である。

TTPs：Tactics, Techniques, and Procedures

Threat Huntingが必要な脅威パターン

現在のセキュリティ対策ツールや監視といったオペレーションでは未知の脆弱性を突くゼロデイ攻撃や検出回避の技術を持つマルウエの検知が難しい課題があり、以下4つの項目は代表例である

他のマルウエアの侵入経路確保パターン

- 気づかれずに侵入が成功した後、更なる活動を進めるために新たなる侵入経路を密かに作りこみます。
- 作りこまれた侵入経路を使いマルウエアを忍び込ませたり、情報を抜き取るルートとして活用します。
- エスカレートしていくと新たなツールを持ち込み、内部にインストールされることによって権限昇格・乗っ取りなども行います。

ログ改ざん等により検知回避を行うパターン

- 内側から足跡が残ったり、侵入したことにつながるようなログを改ざんすることによって検知されるリスクを減らすことができます。
- ログを改ざんすることによって侵入後の動きを追跡されることを防ぎます。

長期潜伏パターン

- 検知されないよう時間をかけて少しずつ様々なファイルサーバー等に対して侵入を試みます。
- 機密情報等価値のあると判断された情報は一度に持ち出すと検知される確率が上がるため、少しずつ持ち出し漏洩があることに気が付かせないようにします。
- 長期潜伏することにより常に新しい機密性の高い情報を入手し続けることができます。

暗号化することにより身代金要求パターン

- 暗号化することによって身代金や何らかの利益を強制的に要求してきます。
- 暗号化することによって自身の痕跡をも消すことができる為、別のサーバーや隣接するネットワークにおいても同様な行動をとることを可能とします。

Threat Intelligenceを用いたThreat Hunting調査の事例

Threat Intelligenceの調査結果によって、ランサムウェアが利用されている攻撃手法を把握し、MITRE ATT&CKフレームワークと突き合わせて、攻撃の痕跡をStep-by-Stepでハンティングする

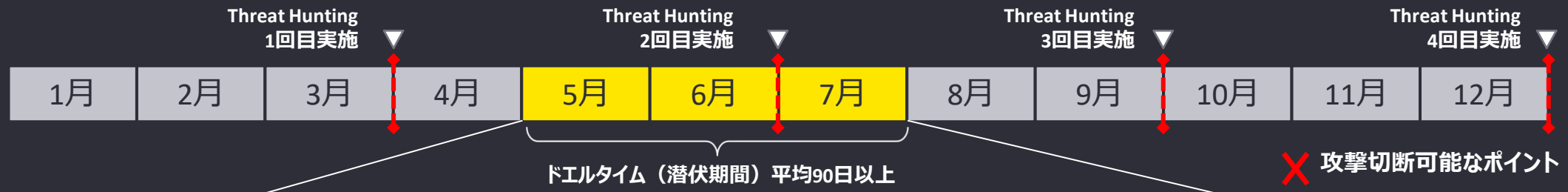
MITRE ATT&CKフレームワーク

検知された攻撃手法の特徴によって、攻撃者とランサムウェアの種類を特定

(参照) MITRE ATT&CK フレームワーク：https://attack.mitre.org/

潜伏期間内のランサムウェアがデータ暗号化する前に検知が可能

攻撃者の潜伏期間（ドエルタイム）は、平均で90日以上となっていることから、定期的にThreat Hunting調査を行うことによりランサムウェアの攻撃プロセスを切断することが可能



攻撃事例：ランサムウェア攻撃プロセス

実行の段階では、cmd.exeやPowerShellなどWindows OS標準の機能が利用されることが多く、個々のコマンドの実行内容だけでは、攻撃活動と判断することは困難です。Threat Hunting調査では、一連のコマンドの実行内容を統合し、相関分析よって攻撃活動であるかを判断します。

持続性確保の段階では、攻撃対象システムに対し、Autorunの設定を追加される、Backdoorツールをインストールされるといったことが考えられます。Threat Hunting調査では、Baseline分析よって、システムの設定の変化を洗い出し、不正な攻撃活動を検知します。

検知回避の段階では、攻撃対象システムに対して、アンチウイルス、EDRなどの防御対策の有無を確認し、それら防御対策のプロセスをKillすることが一般的な手法となります。 Threat Hunting調査では、防御対策ソフトがOff-lineになることを不審な動きとして検知します。

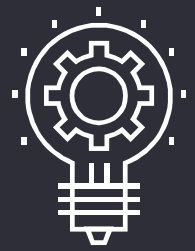
最近のランサムウェアは、利益の最大化のため、データの暗号化の前に秘密データを盗み取ることが行われます。この際、効率的にデータを転送するため、圧縮ツール(ZIP)が利用されることが多いことから、Threat Hunting調査では、大量のデータの圧縮操作と外部向けのデータ送信を不審な動きとして検知します。

Threat Led Penetration Testing での活用

脅威ベースのペネトレーションテスト – 方法論

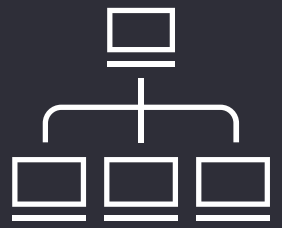
ATT&CKシミュレーションは、企業のセキュリティ態勢を強化するために、脅威アクターが標的とするであろう弱点領域を特定し、実際の攻撃に対応できるようにするものです。このシミュレーションにより期待できる成果は、組織の検知能力と対応能力を向上させることです。テストには、疑似的に作成したコマンド＆コントロールサーバーを使用します。このアプローチは、環境が侵害されていることを前提としており、MITRE ATT&CKフレームワークに従った、適用可能なすべての戦術、技術、手順（TTP）を包括的に実行、評価することで、複数のAPTの活動をシミュレーションすることを目的としています。

MITRE ATT&CK シミュレーションの全フェーズの概要を以下に示します。



脅威インテリジェンス

適切な脅威アクターとその戦術（TTP）を決定。



脅威シナリオの作成

足場確立のための最適なシミュレーションシナリオを作成。

攻撃

脅威シナリオを作成する際に合意したシミュレーションを実施。

侵害後

事前合意した目的を達成。ブルーチームの評価。

レポート

実施内容の報告。評価の最も重要な側面。

脅威インテリジェンス – 方法論

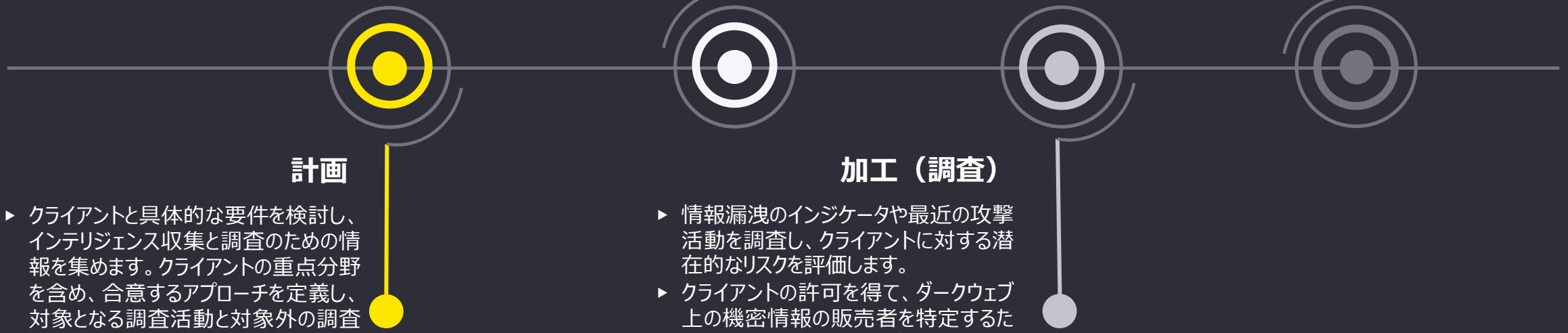
脅威インテリジェンスは、インテリジェンスサイクルの最初の**4段階**に焦点を当てています。（後段の配布とフィードバックはプロジェクトの実施に含まれます。）

収集

- 電子記録の漏洩：商用ツールを使用して、クリアネットおよびダークウェブのサイトやフォーラムで公開された認証情報や機密情報データベースを検索します。
- 標的インジケータ：表層、深層、またはダークウェブでのコミュニケーション、活動、履歴に基づき、クライアントに対する攻撃活動の証拠を収集します。

分析（脅威の評価）

- 脅威の影響と発生可能性、情報漏洩の具体的な詳細を評価し、推奨事項とともに、クライアントのための脅威インテリジェンス報告書を作成します。



計画

- クライアントと具体的な要件を検討し、インテリジェンス収集と調査のための情報を集めます。クライアントの重点分野を含め、合意するアプローチを定義し、対象となる調査活動と対象外の調査活動を特定します。

加工（調査）

- 情報漏洩のインジケータや最近の攻撃活動を調査し、クライアントに対する潜在的なリスクを評価します。
- クライアントの許可を得て、ダークウェブ上の機密情報の販売者を特定するための追加調査を行うことができます。

シナリオ作成 – 脅威アクターの決定

このシミュレーションでは、次のいずれかのタイプの脅威アクターを模倣します。これらの脅威アクターは、それぞれ異なるクラウンジュエルを狙う、異なる動機を持っており、その結果、様々な影響が発生する可能性があります。

シナリオ作成時に必要となる質問：

- 過去18カ月間にどのような攻撃を受けたか？またそれらは誰によるものか？
- 今回のシミュレーションでは、どのような脅威アクターを想定するか？
- どのような重要資産や重要情報を最も懸念しているか？

脅威アクター	標的	動機	影響
国家支援	▸ M&A情報 ▸ 個人情報 ▸ 知的財産	▸ 経済的、政治的利益に関わる戦略的優位性	▸ 競争上の優位性の喪失 ▸ 規制当局による調査/罰 ▸ オペレーションの混乱
サイバー犯罪者	▸ 知的財産 ▸ 金融資産	▸ 金銭的利益	▸ 消費者および株主による訴訟 ▸ ブランドおよび評判の低下 ▸ 消費者からの信頼感の低下 ▸ 規制当局による調査／罰金
インサイダー	▸ 取引情報、企業戦略 ▸ 事業活動 ▸ 人事情報 ▸ 認証情報	▸ 金銭的利益 ▸ 贈収賄、脅迫	▸ オペレーションの混乱 ▸ ブランドおよび評判の低下 ▸ 消費者からの信頼感の低下
ハクティビスト	▸ 主要な役員、従業員、顧客、ビジネスパートナーに関連する情報 ▸ 企業の機密情報	▸ 政治的、社会的変化 ▸ 恐怖と不安の煽り	▸ 事業活動および資産の妨害 ▸ ブランドおよび評判の低下 ▸ 消費者からの信頼感の低下

シナリオ作成 – 攻撃方法の最終化

脅威アクターは、次の攻撃方法の1つまたは複数を使用します。シミュレーションでは、このリストの中から実際に実行可能な攻撃を行います。

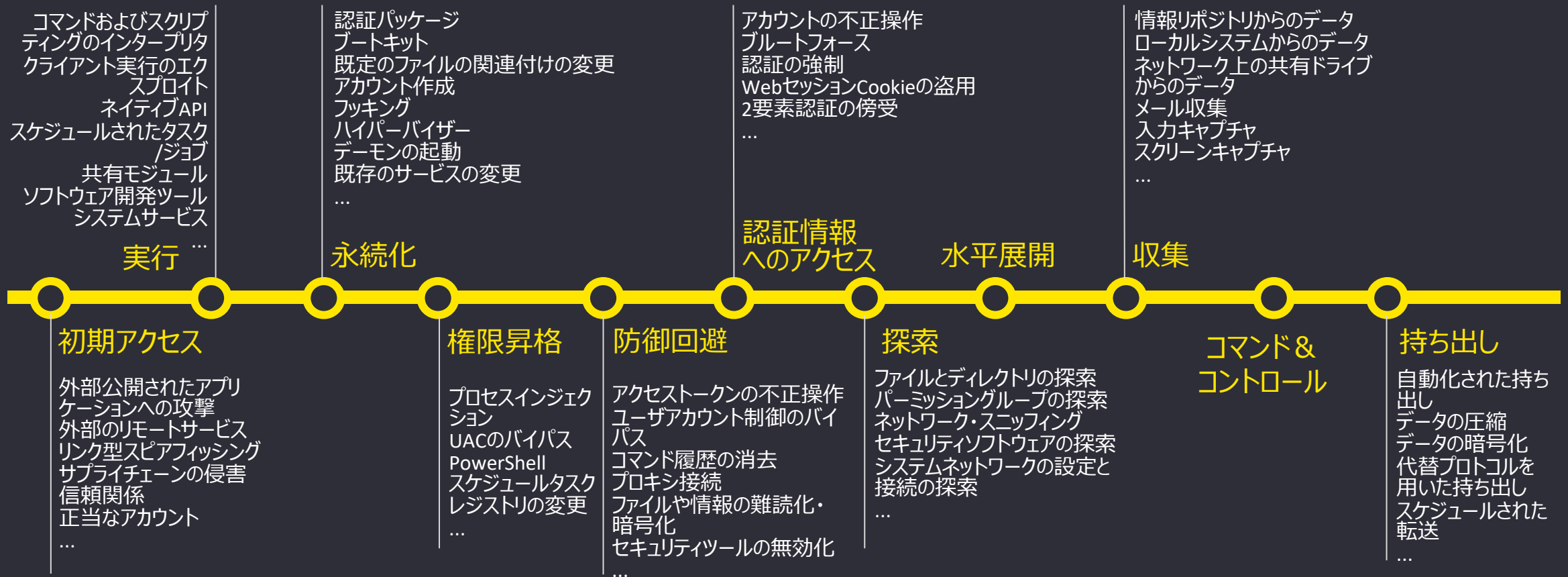
シナリオ作成時に必要となる質問：

- 今回のシミュレーションでは、どのような攻撃を対象外とするか？
- 今回のシミュレーションの一環として、どのような追加の防御策をテストしたいか？

攻撃手法	説明	テスト例
能動的または受動的な傍受/認証情報の再生/中間者攻撃/不正AP	攻撃者は、2者間のコミュニケーションに密かに介入します。	積極的な盗聴
マルウェア（ランサムウェアまたはリモートアクセスツール）	コンピュータの操作を妨害したり、機密情報を収集したり、システムにアクセスする悪意のあるソフトウェアを使用します。	トロイの木馬
Webアプリケーションの脆弱性	Webアプリケーションの脆弱性を利用します。	SQL インジェクション、PHP（オープンソースのスクリプト言語）の設定の悪用
OSやネットワーク機器の脆弱性	オペレーティングシステムやネットワークドライブの脆弱性を利用します。	OSレベルでの設定の不備などを利用
サービス妨害（例：DoS、DDoS）	意図したユーザーがマシンやネットワークを利用できないようにします。	分散型サービス妨害攻撃
第三者によるアクセス/妨害行為	一時的なアクセス権を持つ個人が、その後に必要なアクセス権を取得したり、認可されていないタスクを実行したりします。	雇用した契約社員によりインストールされたバックドア
人為的ミス／誤った指図／受信者のミス	人為的ミスによる攻撃の機会を作り出します。	意図しない受信者に機密情報を誤って送信

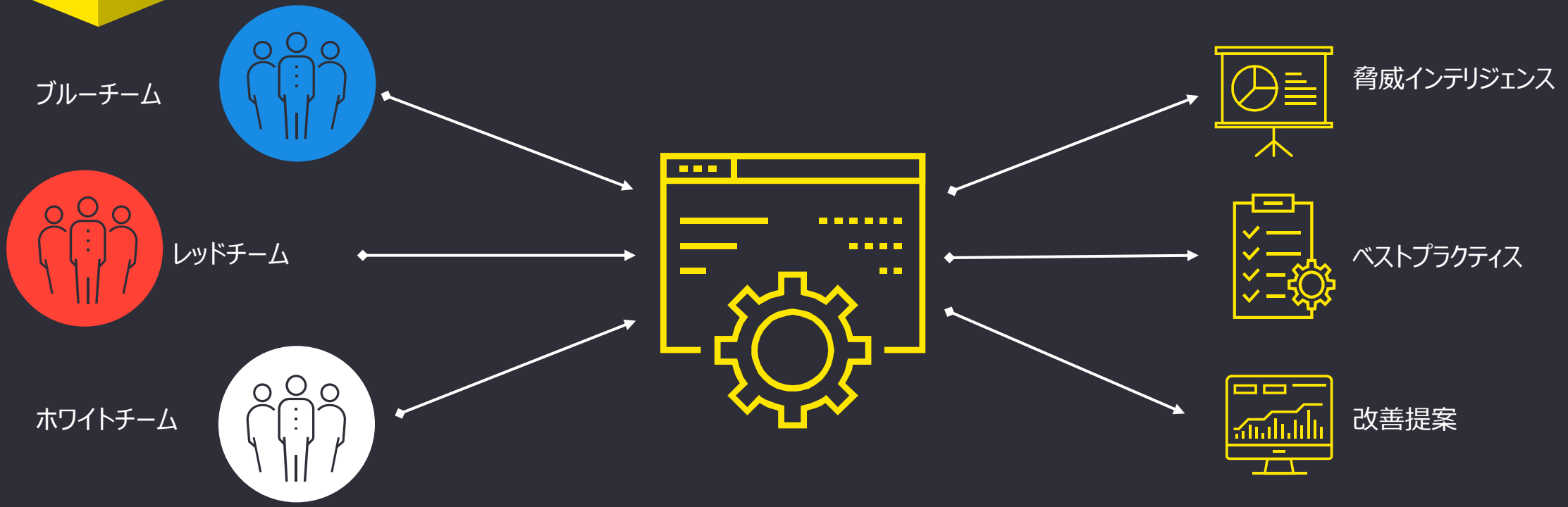
MITRE ATT&CKフレームワークの利用

組織に対して悪意のあるアクターが行う活動（不正アクセス、機密情報の流出、長期的な潜伏など）をシミュレートするためにプロの攻撃者や国家レベルの脅威アクターが使用する敵対的な戦術、技術、手順（TTPs）を集めた、最も包括的なオープンソースのリポジトリです。TTPの一例のリストを以下に示します。



レポート

脅威ベースのペネトレーションテストの報告書は、脅威インテリジェンス、ブルーチーム、ホワイトチーム、レッドチームからの情報を受け取り、アクティブな脅威アクターからの防御について改善のための推奨事項を提供します。



まとめ

サイバー攻撃の被害を極小化するためにThreat Intelligenceの活用が有効です

サイバー攻撃の被害は大きくなる一方で、その攻撃手法は高度化しまた、攻撃者間の連携やツール化により攻撃が容易になってきています。防御においても様々Intelligenceを駆使することにより、インシデントの検知の効率を上げ、早期発見と封じ込めを行うことが可能になり、また、自社のセキュリティ対策の見直しにおいても効果を上げます。

SOC/SOARにおける活用

- IOCの活用によるインシデント検知精度の向上と判断の迅速化

Threat Huntingにおける活用

- 自社における驚異の把握
- Threat Actor の攻撃手法との比較検証

Threat Led Penetration Testingにおける活用

- Threat Actor の攻撃手法のシュミレーション
- 自社セキュリティ対策の検証

EY | Building a better working world

EYは、「Building a better working world ～より良い社会の構築を目指して」をパーパス（存在意義）としています。クライアント、人々、そして社会のために長期的価値を創出し、資本市場における信頼の構築に貢献します。

150カ国以上に展開するEYのチームは、データとテクノロジーの実現により信頼を提供し、クライアントの成長、変革および事業を支援します。

アシュアランス、コンサルティング、法務、ストラテジー、税務およびトランザクションの全サービスを通して、世界が直面する複雑な問題に対し優れた課題提起（better question）をすることで、新たな解決策を導きます。

EYとは、アーンスト・アンド・ヤング・グローバル・リミテッドのグローバルネットワークであり、単体、もしくは複数のメンバーファームを指し、各メンバーファームは法的に独立した組織です。アーンスト・アンド・ヤング・グローバル・リミテッドは、英国の保証有限責任会社であり、顧客サービスは提供していません。EYによる個人情報の取得・利用の方法や、データ保護に関する法令により個人情報の主体が有する権利については、ey.com/privacyをご確認ください。EYのメンバーファームは、現地の法令により禁止されている場合、法務サービスを提供することはありません。EYについて詳しくは、ey.comをご覧ください。

EYのコンサルティングサービスについて

EYのコンサルティングサービスは、人、テクノロジー、イノベーションの力でビジネスを変革し、より良い社会を構築していきます。私たちは、変革、すなわちトランスフォーメーションの領域で世界トップクラスのコンサルタントになることを目指しています。7万人を超えるEYのコンサルタントは、その多様性とスキルを生かして、人を中心に据え（humans@center）、迅速にテクノロジーを実用化し（technology@speed）、大規模にイノベーションを推進し（innovation@scale）、クライアントのトランスフォーメーションを支援します。これらの変革を推進することにより、人、クライアント、社会にとっての長期的価値を創造していきます。詳しくはey.com/ja_jp/consultingをご覧ください。

© 2022 EY Strategy and Consulting Co., Ltd.
All Rights Reserved.

ED None

本書は一般的な参考情報の提供のみを目的に作成されており、会計、税務およびその他の専門的なアドバイスを行うものではありません。EYストラテジー・アンド・コンサルティング株式会社および他のEYメンバーファームは、皆様が本書を利用したことにより被ったいかなる損害についても、一切の責任を負いません。具体的なアドバイスが必要な場合は、個別に専門家にご相談ください。

ey.com/ja_jp