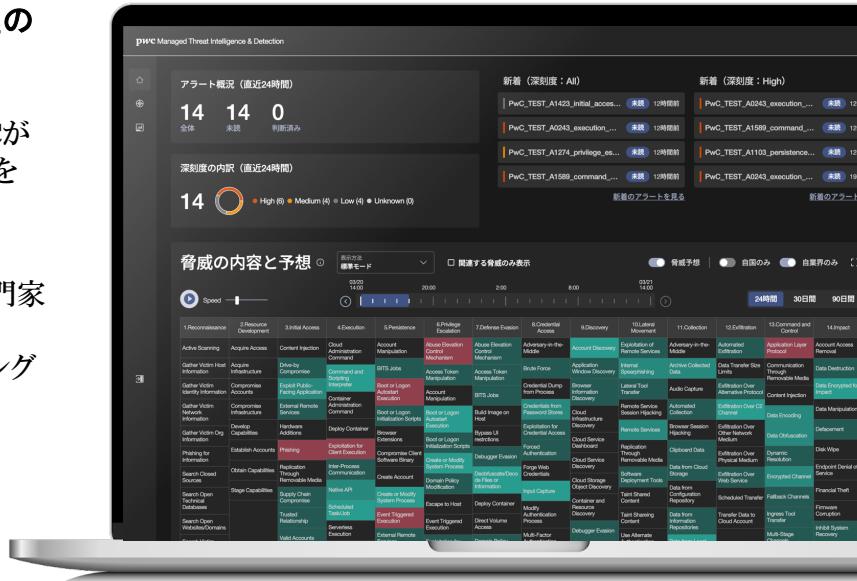


Managed Threat Intelligence & Detection

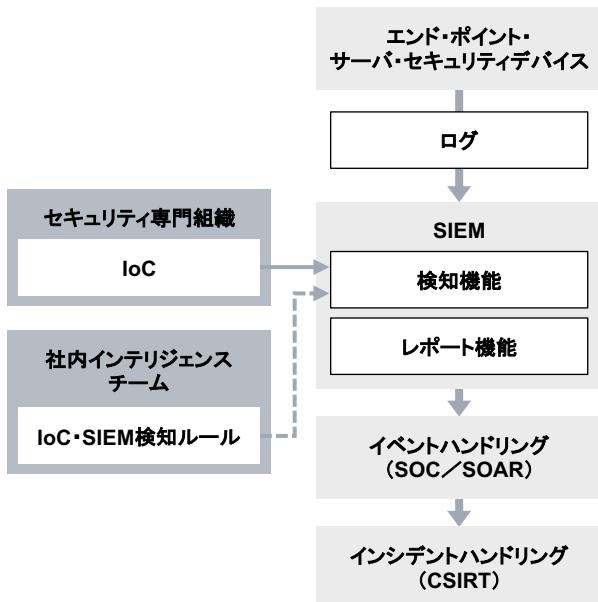
個社ごとの脅威に基づくインテリジェンス主導型のSIEM/SOC支援サービス

Managed Threat Intelligence & Detectionは、PwCがグローバルで整備するサイバーインテリジェンス情報をもとに、脅威の検知やイベントハンドリングの高度化を支援するサービスです。

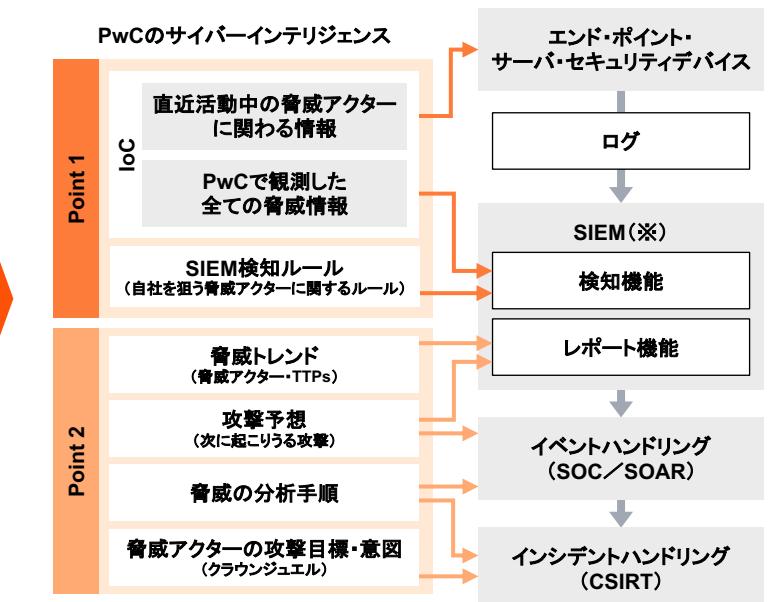
企業を狙う脅威アクターとその攻撃手法をPwCの専門家が特定し、当該脅威の検出と対応に必要となるプラットフォームを年間契約で提供するコンサルティングサービスです。



現在の主流



インテリジェンス主導型



※ Managed Threat Intelligence & Detectionでは、SIEM設備もサービスに含まれます。

PwCのサイバーインテリジェンスとは

PwCコンサルティング合同会社では、日本を含むグローバル全体で数百を超える脅威アクターを常時観測しており、観測された脅威アクターがどの国・どの業界をターゲットとし、どのような戦術、技術、手順(TTPs)を使うのかを分析しています。このように蓄積しているデータを含む、サイバー対策のプロフェッショナルの豊富なノウハウを、PwC独自のサイバーインテリジェンスとして活用しています。

Point 1 貴社を狙うサイバー攻撃手法にフォーカスした、貴社専用の脅威検知エンジンを提供

貴社の業種や活動地域などのビジネス特性を踏まえて脅威アクターを絞り込み、貴社のシステム環境において脅威アクターが実施しうる攻撃手法を特定します。この攻撃手法を検知するための数百～数千のロジックをプラットフォーム上に実装し、貴社専用の脅威検知エンジンを提供します。

なお、PwCグローバルネットワークにて観測した最新の攻撃手法は、常に脅威検知エンジンに反映されます。

Point 2 脅威アクターの動向を先回りすることで、能動的な防御が可能に

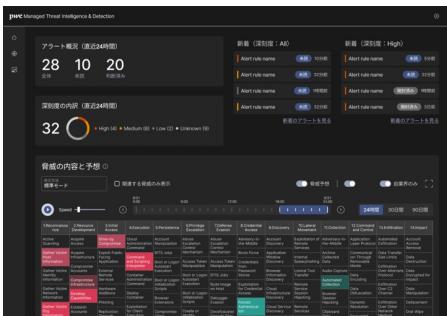
脅威アクターの動機や攻撃戦術などのインテリジェンス情報から、次に発生しうる攻撃を推測することで、先回りして予防する「アクティブディフェンス」の実施を可能にします。

アクティブディフェンス実施の流れ

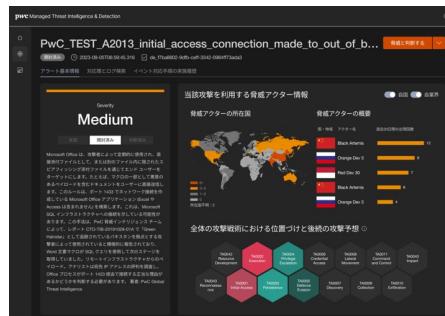
過去と直近に検知した攻撃から
次の攻撃を予想

絞り込んだ脅威アクター候補から
攻撃目的とターゲットを予想

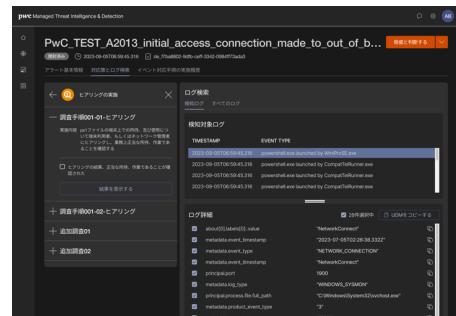
検知ルールごとの対応手順書の
提供で攻撃に効率的に対応



- 直近24時間に検知した攻撃だけでなく、
当該攻撃から推測される次の攻撃も可視化
- 過去90日間の攻撃の変化を時系列で把握

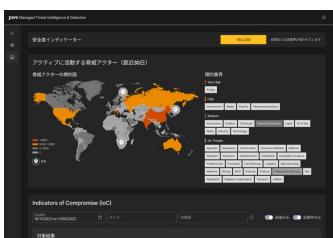


- 検知した攻撃を行う脅威アクター候補の特定
- 金銭目的やスパイ目的など、何を目的とするかでクラウンジュエルの推測が可能



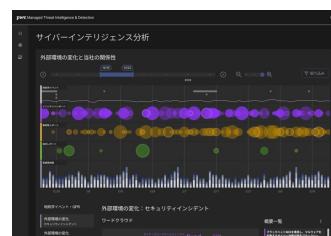
- 検知したイベント単位で求められる対応手順を自動的に表示
- 日々変化する脅威動向の継続分析から検知ルールを追加・更新

アクティブディフェンスを支える、脅威動向分析



活動中の脅威アクター表示と
IoC情報を提供

直近30日間に、脅威アクターが標的とした国や業界およびその手口を可視化。
また、当該アクターに関するIoCのダウンロードが可能



外部および内部環境の変化
が自社にもたらす影響を
時系列で把握

地政学イベント・GPR・インシデン
トレポート・脆弱性レポート・自社
レポート・脅威検知数を連関させ
ることで、セキュリティ要件を抽出
することが可能

お問い合わせ

PwCコンサルティング合同会社

〒100-0004 東京都千代田区大手町1-2-1 Otemachi One タワー

TEL : 03-6257-0700 (代表) | Website : www.pwc.com/jp/a/about-us/member/consulting.html

お問い合わせフォーム : <https://forms.jp.pwc.com/public/application/add/4747>

Managed Threat Intelligence & Detectionについて :

<https://www.pwc.com/jp/ia/services/digital-trust/cyber-intelligence/managed-threat-intelligence-detection.html>



GOOD
DESIGN
AWARD
2025