News release

2024 年 4 月 10 日
PwC コンサルティング合同会社

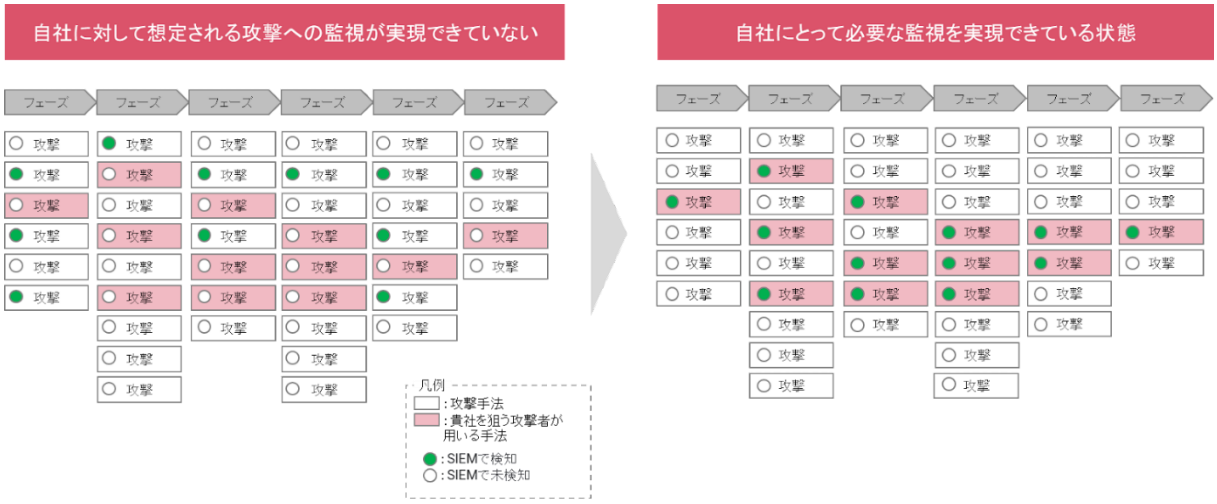
サイバーインテリジェンスに基づくサイバー攻撃検知プラットフォーム「Managed Threat Intelligence & Detection」の提供を開始
脅威アクターの分析・監視ルールの提供や改善を支援、日々巧妙化する攻撃に先んじた能動的なサイバー防御体制の構築策を提供

PwC コンサルティング合同会社（東京都千代田区、代表執行役 CEO: 大竹 伸明 、以下「PwC コンサルティング」）は本日、サイバーインテリジェンスに基づいてサイバー攻撃を検知する新たなプラットフォームの提供を始めます。SIEM（Security Information and Event Management）と呼ぶ仕組みを導入し、サイバー空間上の脅威アクター分析、攻撃手法の戦術や技術、手順などを監視するルールを整備します。

新たなプラットフォームの名称は「Managed Threat Intelligence & Detection」（MTID）です。同プラットフォームに採用する SIEM とは、クラウドやネットワーク機器などから集めたログ情報を一元的に管理し、ログ同士の相関関係を分析できるシステムです。機器単体だけでは見つけられない不正アクセスなどの動きや兆候の検知や分析、可視化ができるようになります。

SIEM による監視で重要なのは、自社への攻撃が想定される脅威アクターがどんな戦術や技術、手順で攻撃を仕掛けてくるかを分析して対策を施すことです（**図表 1**）。多くの日本企業にとっては専門人材の確保や効果的な運用の継続が課題となっています。

図表 1：SIEM と専門的な知見を組み合わせ、適切に自社の脅威アクターを「見える化」できる



こうした日本企業の課題を解決するため、PwC コンサルティングは以下の 4 つを柱にした新たなサービスを提供します。

① 企業の課題に応じたサイバーインテリジェンスに基づく監視ルールの提供
② 監視ルールごとの対応手順書の提供
③ 検知された攻撃手法や自社を狙う攻撃者が用いる手法の可視化
④ 直近のインシデントや攻撃キャンペーンの表示とそれらに紐づく IoC 情報を提供

新サービスのウェブページ及び新サービスの概要は以下です。
https://www.pwc.com/jp/ja/services/digital-trust/cyber-intelligence/managed-threat-intelligence-detection.html

【新サービスの概要】
■サイバーインテリジェンスに基づく監視ルールの提供
・サイバー攻撃の動向を常時分析し、新たな攻撃手法を観測するたびに分析・評価をして防御や検知の方法を策定する PwC 独自の「サイバー脅威データベース」を活用
・企業の進出国・地域、業種などに応じた脅威アクターを分析し、優先すべき対応を特定
・既存のセキュリティ対策製品の導入・運用状況に応じてルールを設計
・変化する脅威動向を継続して分析し、監視ルールを追加・更新

■監視ルールごとの対応手順書の提供
・SIEM が検知したイベントに関して、企業が直面する脅威ごとに対応すべき「マニュアル」を作成

■検知された攻撃手法や自社を狙う攻撃者が用いる手法の可視化
・SIEM が検知したイベントで用いられた攻撃手法や、企業の進出国・地域、業種などに応じた脅威アクターが用いる攻撃手法を可視化
・任意の時間内でのコマ送り表示や表示速度調整などインタラクティブな操作を支援し、攻撃の変化の過程を明瞭に把握

■直近のインシデントや攻撃キャンペーンの表示とそれらに紐づく IoC 情報を提供（**図表 2**）
・直近 30 日間において脅威アクターが標的としている国や業界を表示
・上記に紐づく IoC 情報の提供

図表 2：検知した攻撃や自社を狙う攻撃者の攻撃手法可視化（左）とアクティブに活動する脅威アクターによる標的国や業界の表示（右）

PwC コンサルティングはサイバーセキュリティを「戦略」「運用」「技術」の 3 つの観点から総合的に日本企業のインテリジェンスを創出するサービスを展開しています。

【戦略】
適切な情報開示、セキュリティへの投資や組織づくり、対策の策定などを支援します。独自の情報開示の要件を基に、最新のガイドラインの内容や改正動向と企業のセキュリティ対策の現状を掛け合わせ、最適な開示内容を導きます。投資家などから ESG など非財務情報の開示の要求が高まる中、独自のデータベースと評価基準によってグローバル基準の最適な情報開示を後押しします。

【運用】
各国の関連規制の動向をリアルタイムで把握するほか、最適なセキュリティ体制を整えます。「技術」では脅威情報や脆弱性情報を分析・検証し、強固な防御につなげます。インシデントが発生した際、原因の調査から公表の是非の判断基準、当局への適切な報告、外部有識者による調査委員会の設置まで、事例ごとにどのタイミングでどう対処するべきか、企業に合わせた最適な解決策を提供します。

【技術】
サイバー攻撃の影響は世界規模でより大きく、深刻になっています。法令やガイドラインに沿った対策だけではもはや、危機の芽を事前に摘むことは難しくなっています。自社に及びかねない攻撃の兆候を早く察知し、被害を防ぐあるいは最小限に抑えるためには、リスクベースで危機の芽の可能性を把握し、先手を打って態勢を整える能動的なサイバー防御の実践が欠かせません。

PwC コンサルティングは今回の新プラットフォームと既存のサービスを結び付け、企業の抱える課題に応じてテーラーメード型の支援体制を構築します。サイバー対策の豊富なノウハウを有するプロフェッショナルと PwC グローバルネットワークを活用したサイバーインテリジェンス機能を基に、日本企業の能動的サイバー防御の構築に一段と貢献していきます。

以上

PwC コンサルティング合同会社について www.pwc.com/jp/consulting

PwC コンサルティング合同会社は、経営戦略の策定から実行まで総合的なコンサルティングサービスを提供しています。PwC グローバルネットワークと連携しながら、クライアントが直面する複雑で困難な経営課題の解決に取り組み、グローバル市場で競争力を高めることを支援します。

PwC Japan グループについて www.pwc.com/jp

PwC Japan グループは、日本における PwC グローバルネットワークのメンバーファームおよびそれらの関連会社の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japan グループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約 11,500 人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。