

News Release

デロイト トーマツ、ランサムウェア攻撃へのセキュリティ脅威 分析サービスを拡充

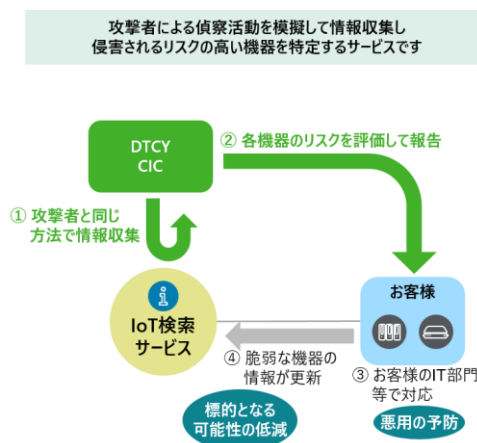
- 侵害されるリスクの高い機器を特定する「侵害リスク評価サービス」を年間サブスクで提供
- 「スレット セキュリティ モニタリング for EDR サービス」の対象 EDR 製品を拡充
- 24 時間 365 日セキュリティ監視を行うサイバーインテリジェンスセンター(CIC)の知見を活用

デロイトトーマツグループのデロイトトーマツサイバー合同会社（東京都千代田区、代表執行者：桐原祐一郎、以下 DTCY）は、企業・団体・自治体がランサムウェアの脅威への対策を強化するために、セキュリティ脅威分析サービスを拡充します。この度、侵害されるリスクの高い機器を特定する「侵害リスク評価サービス」の年間サブスクリプションでの提供を開始、また、機器上での不審な活動を検知する「スレット セキュリティ モニタリング (TSM) for EDR (Endpoint Detection and Response) サービス」の対象 EDR 製品を増やします。

サイバー攻撃、なかでも二重恐喝を含めたランサムウェア攻撃の脅威が近年増しており（※）、DTCY はセキュリティ監視・分析や脅威インテリジェンス提供の実績・知見を活用しながら、攻撃者の活動に着目したランサムウェア対策サービスを提供しています。ランサムウェア攻撃は「偵察」から「初期侵入」、「内部侵害」、「最終攻撃実行」と段階を追ってシステムに入り込み、中枢を掌握してから、ダメージにつながる攻撃を行います。今回の「侵害リスク評価サービス」は攻撃者が公開情報から脆弱な機器の「偵察」を行うことに着目してそれを模擬するものです。また「スレット セキュリティ モニタリング for EDR サービス」は「初期侵入」以降の段階で効果を発揮するもので、監視機能がある EDR 製品において不審な活動を見抜くためのスキルや膨大なデータ処理といったユーザー側の課題にも対応します。

● 侵害リスク評価サービス

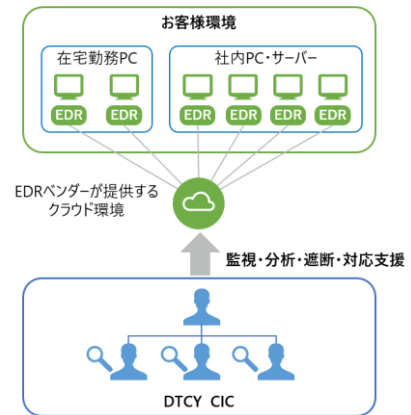
IT ガバナンスの脆弱性から企業にはサプライチェーンを含め自社が認知していないサイバーリスクがあり、昨今アタック・サーフェス マネジメントと呼ばれる手法に注目が集まっています。本サービスでは攻撃者による偵察活動を模擬して情報収集し侵害されるリスクの高い機器を特定します。お客様側からいただくのは評価対象とするドメイン名のみで IT 機器の一覧などを準備いただく必要はありません。疑似的な攻撃コードの送信を行わないため、運用中の機器に対しても安全に調査でき、運用委託業者等との調整も不要です。評価結果は機器の概要、問題点の内容、推奨する対策など経営層の理解に役立つレポートを提供します。全体像を把握するためのワンショット調査、継続的なモニタリングにより問題点を早期に発見できる年間サブスクリプションの 2 つの形態を用意しています。



- **スレットセキュリティモニタリング (TSM) for EDR (Endpoint Detection and Response) サービス**

PC やサーバーなどのエンドポイントにインストールされた EDR 製品をリモートで監視し不審な活動がないクラウド上の分析基盤で分析して異常を検知するソリューションです。EDR 製品は、製品自体に監視機能があるものの導入だけで効果が出るものではなく、不審な活動を見抜くためのスキルや EDR から日々発生する膨大なデータの処理が必要になります。本サービスでは 24 時間 365 日体制での対応分析の結果、危険度が高いと判断したアラートについて推奨対応を含めて通知します。また、事前に取り決めた条件に基づき、DTCY の CIC (サイバーインテリジェンスセンター) のアナリストが不正な通信やプロセスを遮断します。万が一のインシデント発生時にはお客様担当アナリストが初動対応の支援を行います。また定期的にアラート分析の結果や検知傾向をまとめたレポートを提供します。さまざまな EDR 製品に対応しており、EDR のログと他のログを組み合わせることで監視効果の高い統合監視サービスの提供が可能です。

24/365体制のセンターによりお客様のEDRを監視して不審な活動の発見や対応を支援するサービスです



上記はこれまで実績を積んできたサービスであり、この度以下のサービス拡充を行います。

- **侵害リスク評価サービス**

年間サブスクリプションでのサービス提供を開始
<参考価格：100 IP アドレスを対象とした場合>

①ワンショット: 120 万円

②年間サブスクリプション: 720 万円/年額

(継続的な侵害リスク評価サービス提供に加え、脆弱性管理サービスがバンドルされます)

- **スレットセキュリティモニタリング for EDR (Endpoint Detection and Response) サービス**

対象とする EDR 製品を増加

DTCY はサイバーセキュリティに関する Strategy (戦略)、Secure (予防) から、Vigilant (発見)、Resilient (事後対応) に至るまで、高度な知見・機能を一気通貫で企業に提供しています。サイバーインテリジェンスセンター (CIC) を 2016 年に国内に設置し、24 時間 365 日セキュリティ監視サービスを提供すると共に、能動的情報収集でサイバーリスクに関する知見を集積し、攻撃者の手法などを高精度で予見する脅威情報 (スレットインテリジェンス) の提供を行っています。CIC のセキュリティ脅威分析サービスはデロイトグローバルを含む幅広い脅威情報を元にした分析を行っており、その範囲は境界デバイスの検知に留まらず、ネットワーク内部や Web アプリケーションの検知・分析も対象としています。これにより、従来は発見が困難だった高度なサイバー攻撃や不正利用も網羅しています。

※ランサムウェア攻撃はマルウェアが企業の PC 等のデータを暗号化し、それを解除するための鍵と引き換えに金銭を要求し、IT システムそのものを麻痺し事業継続を脅かすものです。近年はデータを盗み出し、身代金の支払いに応じなければデータを公開すると脅す「二重恐喝」の例も増えています (2022 年 3 月中旬までの 2 年間で世界の 4,000 社以上が被害/DTCY 調べ)。昨今の世界情勢によりサイバー攻撃の潜在的なリスクは高まっており政府・省庁からは各企業・団体に対して経営者のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、対策を講じることが呼びかけられています。また、政府・自治体に対しても内閣サイバーセキュリティセンターが策定したガイドラインが 2021 年 3 月提示されており、対策の向上が求められています。

<報道機関の方からの問い合わせ先>

デロイトトーマツグループ 広報担当 内山、菊池

Tel: 03-6213-3210 Email: press-release@tohatsu.co.jp

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザー合同会社、デロイト トーマツ 税理士法人、DT 弁護士法人およびデロイト トーマツ コーポレート ソリューション合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザー、コンサルティング、ファイナンシャルアドバイザー、税務、法務等を提供しています。また、国内約 30 都市以上に 1 万 5 千名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト (www.deloitte.com/jp) をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL および DTTL の各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。

デロイト アジア パシフィック リミテッドは DTTL のメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における 100 を超える都市（オークランド、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザー、リスクアドバイザー、税務、法務などに関連する最先端のサービスを、Fortune Global 500® の約 9 割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの改革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来 175 年余りの歴史を有し、150 を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約 345,000 名のプロフェッショナルの活動の詳細については、(www.deloitte.com) をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited