



Cyber Intelligence Service

企業・組織・団体とその活動を
サイバーリスクから守ります

デロイトトーマツサイバー合同会社

Cyber ●

業界最高レベルの サイバーインテリジェンスを セキュリティリスク対応に活用

システムのエンドポイントを狙う巧妙な標的型攻撃やランサムウェアの横行、グローバルにおける同時多発的なサイバー攻撃の増加など、企業・組織・団体を狙うサイバーリスクは高度化・複雑化・悪質化する一方です。セキュリティ機器のログを監視・分析しインシデントにつながる兆候を“インフォメーション”として提供する従来のセキュリティ・オペレーション・センター (Security Operation Center: 以下SOC) では、これからのサイバーリスクに対応することはもはや不可能です。必要なのは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、攻撃者の手口や手法を高精度で予見するプロアクティブな活動です。その活動の源が“サイバーインテリジェンス”であり、これからのサイバーリスクマネジメントに欠かせないリテラシーです。デロイトのサイバー インテリジェンス センター (Cyber Intelligence Center: 以下CIC) では、従来のセキュリティ監視・通報サービスよりも大きく踏み込んだサイバーインテリジェンスを提供しています。その範囲は境界デバイスの検知にとどまらず、ネットワーク内部の検知・分析も対象としているため、従来は発見が困難だった高度なサイバー攻撃や内部不正も網羅。デジタルトランスフォーメーションの加速とともに高度化・複雑化する多様なサイバーリスクから企業・組織・団体を守り、その活動の継続に貢献し続けること。そのために唯一無二のプロフェッショナルサービスをお届けすることがCICの使命です。

CYBER INTELLIGENCE
centre

サイバーインテリジェンスとは

「インテリジェンス」とは「情報」を意味しますが、一般的な「情報＝インフォメーション」とは異なります。「インフォメーション」が未加工の情報を指すのに対し、「インテリジェンス」は加工された情報を意味します。サイバーインテリジェンスとは、企業・組織・団体にとって脅威となりうる情報をサイバー空間から収集、評価、分析し、対応の検討に役立つように整理したものを指します。従来の情報セキュリティ対策では対応が困難だった標的型攻撃やマルウェアなどの攻撃手法から、企業内部からの機密流出やブランド価値毀損につながる情報拡散まで、多種多様なサイバーリスクに対し、より実践的でスピーディな対応を実現するベースとなります。

インフォメーションとインテリジェンスの差異

インフォメーション

- 評価や分析が行われていない「生」の情報
- 信頼性の低いものや不完全なものが混在
- クライアントが意思決定にそのまま役立てるのは困難

インテリジェンス

- インフォメーションを評価・分析・整理した精度の高い情報
- 専門家による評価などのフィルターを経ており、一定以上の信頼性を保持
- クライアントによる活用が容易で、意思決定に即座に役立てることが可能

リスクに備えるインテリジェンス

CICはデロイトがサイバーインテリジェンスサービスを提供する拠点です。サイバーリスクにおける重要度の高い国や地域、20ヶ所以上に設置され、グローバルベースでサービスを提供しています。総勢5,000名を超えるサイバーセキュリティのプロフェッショナルが検知・収集した膨大な脅威情報を各国CICで連携することで、質・量ともに世界最高レベルのサイバーインテリジェンスを日々生成しています。専任チームの研究範囲は誰にでもアクセス可能なWeb領域(サーフェースWeb)はもとより、容易にアクセスできないダークWebを含む広大なサイバー空間を対象とし、クライアントのビジネスやブランドに関連する情報を能動的に収集・監視。情報分析チームは境界デバイスだけでなく企業・組織・団体のネットワーク内部も分析対象とすることで、高度なサイバー攻撃から内部不正までをいち早く検知します。各CICはそれぞれのエリアに最適化された活動を展開し、日本のCICは日本語によるサービス提供を24時間/365日体制で実施。“フォロー・ザ・サン”ではなしえない迅速かつスムーズなサービス提供を可能としています。また、クライアントごとに専任のインシデントコーディネーターをアサインし、万一のインシデント発生時にも速やかな収束と回復をサポートします。CICのサービスを活用することで、検知が困難だったサイバーリスクに備えることができるようになるだけでなく、インシデント発生時の対応工数・時間を大幅に削減することができます。



サイバー インテリジェンス センター (CIC) とは

- サイバーインテリジェンスを活用し、クライアント企業のIT資産や貴重なデータ、ブランド価値などをサイバー攻撃から防御。
- 全世界20ヶ国以上の国・地域に設置したCICから、グローバル規模のサービスを提供。
- 各国CICで収集・分析した高度かつ最新のサイバーインテリジェンスをグローバルで共有。



デロイト CIC のソリューション



セキュア(予防): 出入り口にとどまらない監視

一般的なSOCが境界デバイス、つまりネットワークの出入り口のみを対象としているのに対し、CICではネットワーク機器にとどまらず、サーバーやデバイスを含むエンドポイントセキュリティ製品も監視・分析の対象とし、出入り口をくぐり抜けた不正データの検出も可能としています。徴候の段階でインシデントを検知できるため、クライアントの対応工数の大幅な削減を実現します。



ヴァジラント(発見): 豊富な監視ユースケース

グローバルに展開するCICではそのスケールメリットを活用し、豊富な実績と知見を蓄積しています。これをベースとした監視コンテンツのユースケースは一般的なSOCの約3倍以上もの規模に及んでいます。既存のセキュリティ製品の活用にとどまるSOCでは検知が難しかった高度なサイバー攻撃も、いち早く発見することが可能です。



レジリエント(回復): プロフェッショナルがサポート

クライアント専任のインシデントコーディネーターをアサインし、月次レポート解説など、平時のアドバイザー活動に加え、インシデント発生時にはリモート／オンサイト*による支援を実施。被害を最小限に抑え、速やかな回復をサポートします。また、専任チームによるデジタル・フォレンジックで攻撃の痕跡を可視化。将来の予防的アドバイスも実施します。

*サービス・メニューに応じて提供スタイルは異なります



Deloitte.

デロイトトーマツ

デロイトトーマツ サイバー合同会社

Mail ra_info@tohmatsumatsu.co.jp

URL www.deloitte.com/jp/dtcy

【国内ネットワーク】 東京・名古屋・福岡

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40都市に1万名以上の専門家を擁し、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”) ならびに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のひとつまたは複数を指します。DTTL (または “Deloitte Global”) および各メンバーファームならびに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す。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、オーストラリア、ブルネイ、カンボジア、東ティモール、ミクロネシア連邦、グアム、インドネシア、日本、ラオス、マレーシア、モンゴル、ミャンマー、ニュージーランド、パオ、パプアニューギニア、シンガポール、タイ、マーシャル諸島、北マリアナ諸島、中国 (香港およびマカオを含む)、フィリピンおよびベトナムでサービスを提供しており、これらの各国および地域における運営はそれぞれ法的に独立した別個の組織体により行われています。

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、税務およびこれらに関連する第一級のサービスを全世界で行っています。150を超える国・地域のメンバーファームのネットワークを通じFortune Global 500®の8割の企業に対してサービス提供をしています。“Making an impact that matters”を自らの使命とするデロイトの約286,000名の専門家については、(www.deloitte.com)をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

Member of
Deloitte Touche Tohmatsu Limited

© 2019. For information, contact Deloitte Tohmatsu Cyber LLC.
2019.09_0179