

News Release

サイバー インテリジェンス サービスを提供開始

デロイト グローバルで収集したインテリジェンスを活用した脅威への対応

デロイト トーマツ リスクサービス株式会社(東京都千代田区、代表取締役社長 丸山満彦)は、24 時間 365 日のセキュリティ脅威分析サービスとして、2015年9月28日にサイバー インテリジェンス サービスの提供を開始します。2020年までにサイバー インテリジェンス サービスを提供可能な専門家を30名以上に拡充する予定です。

1. 背景

近年、企業を狙った標的型攻撃等のサイバー攻撃の被害が急増しています。これらの攻撃は、技術、生産、個人情報といった価値の高い情報資産の窃取、破壊、レピュテーションの低下等を目的とし、その対策は企業にとって重要な課題となっています。さらには、攻撃者が未知のマルウェアを使用することにより、従来型の予防対策のみでこれらの攻撃に対処することは非常に困難な状況です。そこで、24 時間 365 日体制のセキュリティ脅威分析サービスであるサイバーインテリジェンスサービスを開始します。

2. サービス内容

デロイト サイバー インテリジェンス サービスはデロイト各国のプロフェッショナルが収集した情報を分析し、クライアントに有益な情報として提供するスレットインテリジェンス・アナリティクスとクライアントのネットワーク、システムの各種ログ情報を分析し、脅威を検出・対策を提言するスレット・セキュリティモニタリングの2つの独立したサービスから構成されています。

① スレットインテリジェンス・アナリティクス (Threat Intelligence and Analytics: TIA)

クライアントのビジネス環境に対応したインテリジェンス^{※1}を提供するサービスです。

➤ 特長

- ・ インダストリーの特徴を踏まえた脅威情報の配信。オプションでより詳細な調査が可能
- ・ 新たな脅威への検知精度を高めるため、クライアントの SIEM (Security Information and Event Management) 製品に取り込み可能な IP アドレス、ドメイン名、IOC^{※2}等のインテリジェンス情報の提供
- ・ オプションとしてマルウェア検体解析(リバースエンジニアリング)サービスの提供

※1 インテリジェンス: 各国デロイトで収集したマルウェアや攻撃手法等、脅威情報を分析・優先順位付けしたクライアント

トに有益な情報

※2 IOC: Indicator of compromise サイバー攻撃の兆候、痕跡

② スレット・セキュリティモニタリング (Threat and Security Monitoring: TSM)

24 時間 365 日体制でセキュリティ脅威分析を提供します。TIA のインテリジェンスをもとに、インダストリーまたはクライアント固有のビジネスリスクとサイバーリスクとの関連性を踏まえた高度な分析サービスです。

➤ 特長

- ・ 特定のベンダーやテクノロジーに依存しない最適なセキュリティソリューションを活用
- ・ 高度な知見を有したアナリストが 24 時間体制でセキュリティ脅威分析とアドバイスを実施
- ・ クライアント専任のインシデント・コーディネーターが定期報告およびインシデント発生時の対応を支援

➤ 2つのサービスメニュー

スレット・セキュリティモニタリングは、クライアントに新たなセキュリティ資産を追加することなく提供可能な「スタンダード」とクライアント環境にオンプレミスで導入する「プレミアム」から選択可能です。スタンダードは 2015 年 9 月 28 日より、プレミアムは 2016 年 4 月以降から提供予定です。

・ スタンダード

ファイアウォール、侵入検知システム (IDS) といった外部ネットワークとの境界に設置されたデバイスだけでなく、クライアントの様々な機器のログを収集・分析することで、従来型のアプローチでは発見が難しかったサイバー脅威を検知し、対応に必要な情報を提供。

・ プレミアム

クライアントのシステム (オンプレミス環境) に SIEM 製品を導入し、外部への持ち出しが困難なログを分析。サイバー脅威や内部不正といったクライアント固有のリスクを発見し、CSIRT と連携することで、インシデント対応を全面的に支援。

3. 世界のサイバー インテリジェンス センターとの連携

サイバー インテリジェンス サービスは、世界のデロイトのサイバー インテリジェンス センター (CIC: Cyber Intelligence Center) のインテリジェンスを活用し、クライアントのサイバー脅威に対応します。CIC は各地域特有のサイバー空間の脅威情報を収集・分析し、対策に必要なインテリジェンスを提供する組織です。すでに稼働中のアメリカ、カナダ、スペイン、インド等に加え、準備・計画中を含めると 20 都市以上にあります (2015 年 9 月 2 日現在)。各国 CIC とのシームレスな連携により、グローバルにビジネス展開されているクライアントをサポートします。

➤ 特長

- ・ デロイトグローバルで収集、分析した高度なインテリジェンスの提供
- ・ 最新のテクノロジーによる 24 時間 365 日のセキュリティ脅威分析
- ・ 各国のデロイト CIC と連携したグローバル対応

<問い合わせ先>

デロイト トーマツ合同会社

コーポレートコミュニケーション 新井 香織

Tel: 03-6720-8090

Email: press-release@tohmatu.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 トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームおよびそのグループ法人(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、税理士法人トーマツおよびDT 弁護士法人を含む)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、税務、法務、コンサルティング、ファイナンシャルアドバイザー等を提供しています。また、国内約 40 都市に約 8,500 名の専門家(公認会計士、税理士、弁護士、コンサルタントなど)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)は、監査、コンサルティング、ファイナンシャルアドバイザーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界 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、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約 220,000 名を超える人材は、“making an impact that matters”を自らの使命としています。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド(“DTTL”)ならびにその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の関係会社のひとつまたは複数指します。DTTL および各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。DTTL およびそのメンバーファームについての詳細は www.deloitte.com/jp/about をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited