

News Release

セキュリティ脅威分析サービスに機械学習を導入し サイバー インテリジェンス サービスを高度化

新たな検知手法の追加によって、脅威検知の能力を向上

デロイト トーマツ リスクサービス株式会社(本社:東京都千代田区、代表取締役社長:丸山 満彦、以下DTRS)は、2018年2月1日より、機械学習を用いたアノマリ検知機能を、24時間365日のセキュリティ脅威分析サービスである「スレット セキュリティモニタリング(TSM)スタンダードサービス」に追加します。今後、機械学習によって蓄積されるインテリジェンスは、全てのサイバー インテリジェンス サービスに活用されます。

近年、サイバー攻撃の高度化が進み、攻撃手法も非常に多岐にわたっています。そのため従来の相関分析による脅威検知だけでは網羅することが困難なサイバー攻撃も増加しています。デロイトのサイバー インテリジェンス センター(CIC)ではサイバー脅威の検知手法として、アノマリ検知を追加します。従来は各種セキュリティ機器のログを基に、相関分析を行い脅威を検知していました。今回追加するアノマリ検知は、機械学習によって得られたベースラインから逸脱するイベント(特異点)を発見し、そのイベントを起因として脅威分析を行います。アノマリ検知を活用することで、相関分析だけでは発見できなかった脅威への対応が可能となり、より幅広いサイバー脅威を検知することが可能となります。

機械学習によって蓄積される知見は今後、TSM だけでなく、デロイト CIC が提供する全てのサイバー インテリジェンス サービスに活用されます。サイバー インテリジェンス サービスが提供する予防(Secure)・発見(Vigilant)・回復(Resilient)の3つのフェーズ全てにおいて、精度の高いインテリジェンスを用いることで、クライアントが直面するセキュリティ脅威への対応力を高めていくことに繋がります。

なお、デロイトの CIC では、Elastic 社(本社:東京都千代田区)の技術を採用しています。同社の機械学習機能は、時系列データの特異点を効率的に発見し、原因解明のきっかけが得られるソリューションです。これまでの国内外での知見の蓄積による従来の検知手法に加え、テクノロジーを積極活用したアノマリ検知を追加しました。

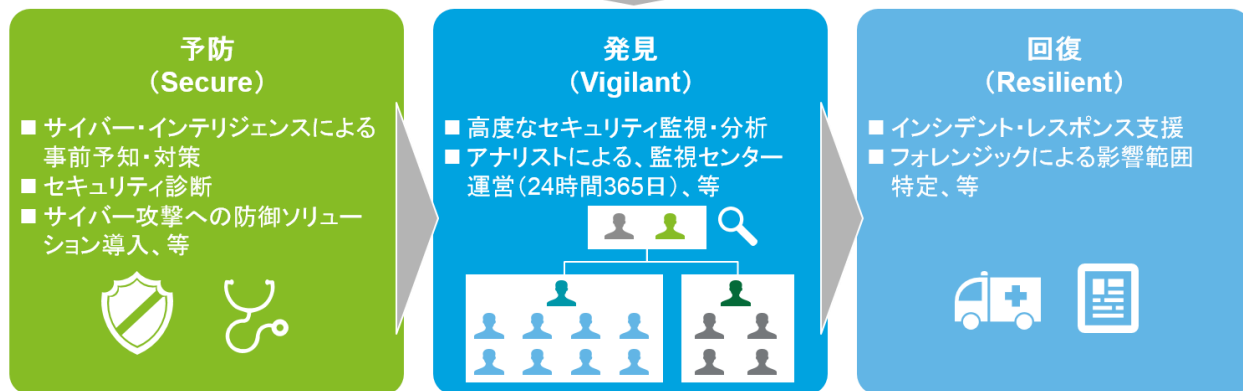
Elastic 社のテクノロジーについては[こちら](#)
Elastic 社については[こちら](#)

■ デロイト CIC が提供するサイバー インテリジェンス サービスの構成

デロイト CIC は予防・発見・回復の3つのフェーズに合わせて、TSM およびスレットインテリジェンス・アナリティクス(TIA)の2つのサービスを中心に提供しています。今回のアノマリ検知の導入以降、「予防」や「回復」のフェーズにおいても機械学習で得られた知見が加わることで、より高度なサイバーインテリジェンスサービスの提供が可能となります。

サイバー戦略 (Cyber Strategy)

■ 潜在リスクの洗い出し、ポリシー・ルールの明文化、啓発活動・トレーニング、等



■サイバー インテリジェンス センター (Cyber Intelligence Center – CIC)について

CYBER INTELLIGENCE center

世界 20 カ国以上に拠点を構えるデロイトのサイバー インテリジェンス センターは、サイバーインテリジェンスの専門家を中心に構成されたチームです。サイバー インテリジェンスを活用し、クライアントのインフラストラクチャをサイバー攻撃から守ることをミッションとしています。クライアントの状況に合わせてサイバーインテリジェンスを提供するサービスである「スレットインテリジェンス・アナリティクス (Threat Intelligence and Analytics: TIA)」や、境界デバイスだけでなく、Proxy・DNS・エンドポイント セキュリティ製品等も分析対象とし、セキュリティインシデント発生時に収束まで支援する「スレット・セキュリティモニタリング (Threat and Security Monitoring: TSM)」を提供しています。

<報道関係者からの問い合わせ先>

有限責任監査法人トーマツ 広報担当 新井、田邊

(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)

Tel: 03-6213-2050

Email: audit-pr@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トウシュー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であるデロイトトーマツ合同会社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、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 都市に約 11,000 名の専門家を擁し、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) 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サービス、リスクアドバイザー、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 Fortune Global 500® の 8 割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約 245,000 名の専門家については、[Facebook](https://www.facebook.com/deloitte)、[LinkedIn](https://www.linkedin.com/company/deloitte)、[Twitter](https://twitter.com/deloitte) もご覧ください。

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ー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を含みます。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。Deloitte のメンバーファームによるグローバルネットワークの詳細は www.deloitte.com/jp/about をご覧ください。

Member of
Deloitte Touche Tohmatsu Limited