Deloitte.
デロイト トーマツ

2018 年 1 月 25 日
デロイト トーマツ リスクサービス株式会社

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ーマリ検知機能を、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、アノー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。今回追加するアノーマリ検知は、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。アノー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。

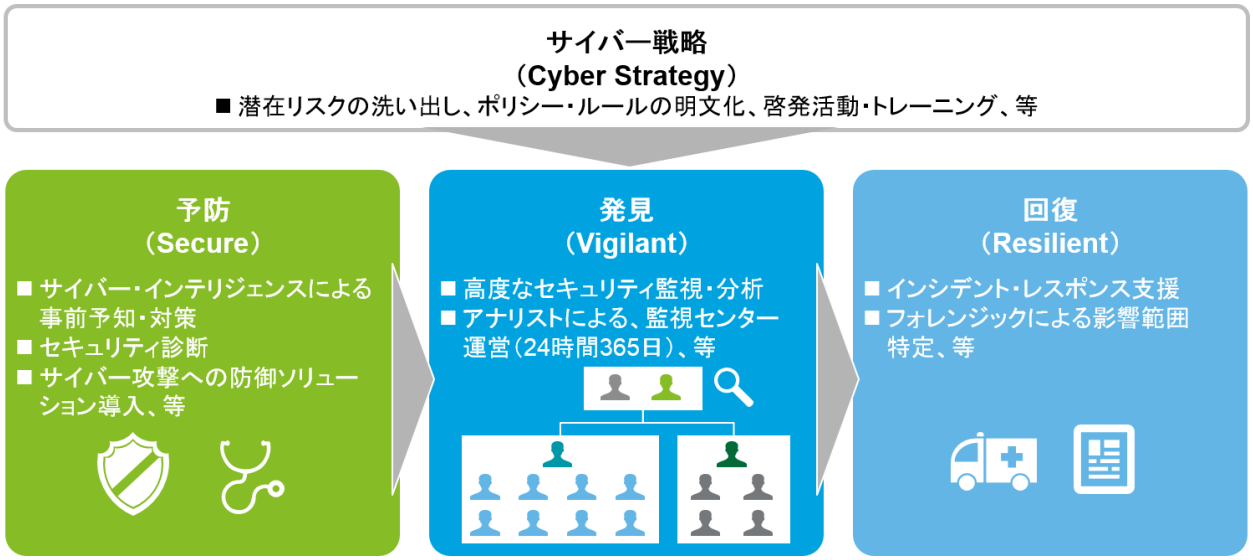
機械学習によって蓄積される知見は今後、TSM だけでなく、デロイト CIC が提供する全てのサイバー インテリジェンス サービスに活用されます。サイバー インテリジェンス サービスが提供する予防（Secure）・発見（Vigilant）・回復（Resilient）の 3 つのフェーズ全てにおいて、精度の高いインテリジェンスを用いることで、クライアントが直面するセキュリティ脅威への対応力を高めていくことに繋がります。

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ー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。今回のアノー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 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@tohmatsu.co.jp