

**数百万台規模のエンドポイントを可視化しコントロール
エンドポイントプラットフォームを提供する「タニウム合同会社」
EDR 運用の効率化を実現する
『Tanium Threat Response』の提供開始**

数百万台のエンドポイントを可視化できるプラットフォームを提供する『タニウム合同会社』（以下：タニウム社日本人、所在地：東京都千代田区）は、EDR 運用の効率化を実現する「Tanium Threat Response」の提供を開始します。これまで提供してきた Tanium IOC Detect⁽¹⁾、Tanium Trace⁽²⁾、Tanium Incident Response⁽³⁾ のモジュールを1つのソリューションに統合し、組み込み脅威情報やリアルタイムアラート機能つきの継続的脅威モニタリングといった拡張機能を提供します。

- 1: IOC(マルウェア等の痕跡)ファイルにより、エンドポイントに同じ痕跡がないかを探すモジュール
- 2: 稼働中のプロセスやファイルのハッシュ値等、IRに必要な情報を取得することができるモジュール
- 3: エンドポイントのプロセス、ファイル、レジストリ、ネットワーク接続等の記録と調査を行うモジュール

本製品は、セキュリティ運用センター(SOC)、インシデント対応(IR)チーム、そして IT 運用チームの運用負担を軽減するために、開発されました。「Tanium Threat Response」は、Tanium™エンドポイントプラットフォーム上で動作します。そのため、IT アセットの可視化、コンプライアンス、管理漏れアセットの検出、ファイル整合性モニタリング、脆弱性の管理、そしてパッチ適用といった重要な各種 IT 機能およびセキュリティ機能を、すべて単一のプラットフォーム上で行うことが可能になります。

またリアルタイムアラートも導入されているため、カスタムインテリジェンスや Tanium の EDR チームからの組み込みインテリジェンスを使用することにより、セキュリティチームは幅広い攻撃を検出することが可能になります。アナリストは、単純化されたリアルタイムアラートのフィードにアクセスし、トリアーじしたり、アクションに対する適切なフォローを調整したりすることができます。インシデント対応担当者は、個別システムの詳細分析や企業全体で追跡を行うことができます。そして運用チームは、企業内のエンドポイントにおけるインシデントを数秒で修復できるようになります。

これらのすべての機能には、細分化されたロールベースのアクセスコントロール(RBAC)が含まれています。RBAC を使用し管理者は責任の定義や委任を行うことが可能になるため、個々のチームにシームレスなユーザーエクスペリエンスを提供可能です。このためインシデント対応チームと調査チームは、単純化されたリアルタイムアラートフィードへのアクセス、個々のシステムに対する詳細分析、そして修復のすべてを、自身の責任スコープに沿って実施可能です。

今後、Tanium Threat Response の製品アップデートなど Tanium™エンドポイントプラットフォームを通じて、より高度なセキュリティ技術による安全・安心を提供できますようサービス導入を進めてまいります。

【タニウム社について】

タニウム社は 2007 年に発足し、5 年間の製品開発を経て 2012 年末にタニウムプラットフォームの販売をアメリカで開始、日本には 2015 年 10 月に本格参入しました。秒単位で数十万台のエンドポイントを保護、制御、管理する独自の価値を提供するタニウムの製品は、IT 部門の担当者に幅広く受け入れ、金融庁が定める G-SIBS(グローバルなシステム上重要な銀行及び国内のシステム上重要な銀行)30 行のうち 16 行に導入されております。

アメリカでは、企業で売上高上位 100 社の半分がタニウムを採用し、その中には銀行の上位 10 社のうち 10 社全て、小売業の上位 10 社のうち 4 社が含まれています。

【タニウム プラットフォームについて】

タニウムプラットフォームは、IT プロフェッショナルが解決しようとする問題がどんなに複雑なネットワーク環境下であっても、迅速に、規模の大小を問わず、しかもシンプルな操作で回答を提供します。集中管理されているサーバーや膨大なデータベースに頼るよりはむしろタニウムプラットフォームは効率的な LP2P(linear peer-to-peer) アーキテクチャーを利用して大規模であっても瞬時に対応いたします。

<特徴>

☑単一のサーバーで

☑どのような問い合わせにも 15 秒以内で回答

100 万台以上のエンドポイントに対応可能

☑他の仕組みと比較し 1 万倍以上高速

☑複雑なスクリプトの知識不要

