ソリューションブリーフ

# Tanium Incident Response

## SIEM/EDR製品の補完、セキュリティ運用チームの協業の促進、高度な脅威検知機能で、インシデント対応をスピードアップ

セキュリティインシデントの平均解決時間 (MTTR) を劇的に短縮。単一のプラットフォームに機能を集約したTaniumで、現行製品による死角を可視化し、縦割りのポイントツールを統合することで、SIEM/EDR製品を補完し、インシデントの検知、脅威ハンティング、調査、封じ込め、修復までの過程をスピードアップし、インシデント対応を強化。

### 企業が抱える課題：対応の遅延によりインシデント対応に時間がかかり、ダウンタイムが長期化して被害が増大

インシデントの調査・修復を迅速に行うことで、被害を抑制できるという事実は、データが証明しています。しかし多額を投資してSIEM/EDRツールを導入しても、多くの企業はインシデントが実害に発展する前にすばやく調査し修復することができていません。大企業はサイバー攻撃によるダウンタイムで1時間あたり50万ドルの損失を被ると言われる中で、ITインシデントの調査にかかる時間は平均解決時間 (MTTR) 全体の80%を占め、フォレンジック調査の完了には平均30日もの期間を要しています。

調査が完了しても、修復には別のツールが必要なため、複雑な縦割り型のポイントツールを切り替えて修復作業を実施しなければなりません。

その結果、何が起こるのでしょうか？

**50万ドル/時**

システムの停止によってかかる平均コスト

**30日**

セキュリティ インシデントのフォレンジック調査にかかる平均日数

**80%**

セキュリティ/運用インシデントの平均解決時間 (MTTR) のうち調査作業に費やされる時間の割合

**50%**

標的の企業に侵入した攻撃者が2週間以上、検知/検出されることなく滞留しているインシデントの割合

**データの不足**

IT/セキュリティチームがリアルタイムのデータを用いた脅威ハンティング、アラートの精査、インシデントの可視化、攻撃の局所的阻止を、最適な手段で実施できない

**調査の遅延**

根本原因の究明に必要な調査データすべてを迅速に入手できないことで、インシデントが甚大な被害に発展する前にすばやく復旧することができない。

**ツールの乱立**

調査チームと運用チームが使っているデータ取得ツールの数が多く、シンプルかつ効率的にシームレスに連携できる共有のワークスペースや共通のデータがない

「Taniumを使って状況を可視化しなければ、常に我々を取り巻くセキュリティの脅威に対処することはできないでしょう」

**BAE Systems**
チーフセキュリティオフィサー
Tom Barker氏

## 解決策：Taniumですばやく包括的にインシデントに対応

Tanium Incident Responseソリューションを使えば、SIEM/EDRツールの機能を補完・拡張し、調査や修復に使用されている多数のポイントツールを単一の統合型プラットフォームに置き換えられます。これにより、インシデントの検知から修復までの過程で必要な基本操作を、すべて単一プラットフォーム上で実施でき、調査時間を大幅に短縮して、調査の質を改善できます。

Taniumを使えば、これらを実現できます。

- SIEM/EDRツールが提供していないミッションクリティカルなインシデントデータにリアルタイムでアクセスすることで、セキュリティチームによる脅威ハンティングや調査に必要なエンドポイントデータを漏れなく取得
- 脅威ハンティングや調査に必要なエンドポイントのデータをすべて単一プラットフォーム上で効率的に分析し、共有ワークスペースでチーム同士のコラボレーションも促進
- 局所的措置に必要な機能を単一コンソールに集約したTaniumで、インシデント調査から封じ込め、修復までの操作をシームレスに切り替え
- 大規模環境で管理・実行しやすい脅威インテリジェンス (TI) を追加取得できSIEM/EDRベンダーによるTIを補完

## インシデントの検知・調査・ハンティング

### 進行中のインシデントを検知し、その原因を調査すると共に、脅威の範囲を特定し、阻止する方法を決定

インシデントの全容を検知して調査するには、現在と過去の多岐にわたるデータが必要です。SIEM/EDRツールは攻撃先を正確に特定できても、ハンティングや調査に必要な各種データや遠隔監視の情報をすべて取得することはできません。Taniumを利用すると、以下を実現できます。

- 組織やコミュニティ、新たなサードパーティのインテリジェンスでSIEM/EDRの脅威インテリジェンスを補完
- 脅威ハンティングとインシデント調査の担当者が攻撃規模と影響範囲を正確に見積もるために必要なリアルタイムのデータ、クエリ、インサイト (ラテラルムーブメントなどの情報) をすべて提供
- セキュリティチームとIT運用チームが共有のワークスペースで調査データを共有し、タスクを割り当て、コミュニケーションを取りながら、効率的に連携し一丸となってインシデントを解決

## 検知した脅威とインシデントの封じ込め

### 脅威を自動で封じ込め、修復に先立って脅威の拡散・被害の深刻化を阻止

インシデントの検知・調査が完了したら、迅速に封じ込める必要がありますが、SIEM/EDRツールでは、業務の中断やインシデントの影響を最小限に抑えて攻撃を封じ込めるための臨機応変な対応が不可能です。Taniumを利用すると、以下を実現できます。

- 分離・隔離などの局所的な封じ込め措置を大規模かつリアルタイムに自動で実行
- 分離・隔離措置をカスタマイズ (影響を受けたエンドポイントの完全遮断、または指定された接続先のみ許可するなど)
- 影響を受けた、またはリスクのあるエンドポイントに暫定的・長期的な緩和措置 (AppLocker、ファイアウォール変更など) を適用

## インシデントを最短で解決し通常業務を再開

### インシデントを阻止して攻撃者を撃退し、通常業務を再開して、インシデントへの備えを強化

インシデントを封じ込めたら、次はその解決です。影響を受けたエンドポイントをすべてコンプライアンスに準拠した安全な状態に戻す必要がありますがSIEM/EDRツールには修復機能が完備されておらず、別のポイントツールをつなぎ合わせて対処するしかありません。Taniumを利用すると、以下を実現できます。

- インシデントのアラートから調査、修復措置まで、単一コンソール・単一プラットフォームで実施
- 各エンドポイント、エンドポイントのグループ単位、社内のエンドポイントすべてに対する修復措置をリアルタイムに一括で実行
- 検知・修復手順を保存し、オフラインのエンドポイントがネットワークに再接続した時点で自動で適用

## SIEM/EDRツールの効果を拡張し、インシデント対応の最初から最後までの各プロセスをすべて一元的に実施して脅威の修復を最短で実施できるプラットフォーム

様々な機能を備えたTaniumで、インシデント対応をスピードアップし、あらゆる問題をリアルタイムに修復

### 完全に可視化

インシデントの調査や修復に必要なデータをすべて、オンデマンドでリアルタイムに収集。高度な標的型脅威や新種の脅威への対処に必要なデータ (組織、コミュニティ、サードパーティのデータ) でSIEM/EDRツールの脅威インテリジェンスを拡張。

- 過去データとリアルタイムデータを活用し、インシデントをより正確に評価して、エンドポイントをコンプライアンスに準拠した安全な状態に回復
- 対象環境のすべてのエンドポイントで、インシデント全体の規模 (広さと深さ) を数秒で判定
- 利用可能なエンドポイントデータをすべてリアルタイムで反映した脅威ハンティングにより、他のツールでは可視化できない攻撃を検出
- 誤検知によるアラートをすばやく特定し、真のインシデントに重点対処することでシグナル/ノイズ比を改善
- 根本原因やラテラルムーブメントのリスクの判断材料を提供する充実したエクスペリエンスに沿って対応し、調査担当者にとって最も重要なコンテキスト情報やデータを入手

### チーム間の協業のための基盤

調査にかかわるチームや担当者同士の協力を阻む溝を排除。共有ワークスペースで、関係者全員がインサイトや過去データ・リアルタイムデータを共有し、協力しながら最新状況を把握してインシデント阻止のための最適な措置を検討。

- インシデント調査のあらゆる過程で協業を促進するエクスペリエンスで、調査担当者や各領域の専門家同士の協力を阻む溝を撤廃
- 関係者全員が作業基盤として共有し、必要なエンドポイントデータをくまなく分析できる一元ビューにすべての情報を集約
- 関係チームが協力しながらハンティングや調査を実施できる共有ワークスペースを提供
- 運用チームとセキュリティチームが連携し、インシデント対応の各プロセスを単一プラットフォーム内でシームレスに実行
- 各ロールのアクセス制御をきめ細かく設定し、関係チーム間の協業や権限移譲を促進

### リアルタイムに修復

同一プラットフォーム上で、インシデント調査から修復措置へとシームレスに移行。インシデントの種類や規模を問わず、インフラ上のすべてのサービスやIT資産に、横断的にリアルタイムに対応できる幅広い修復機能を活用。

- インシデントを2種類の方法 (業務中断を最小限に抑える場合は局所的措置、リスクレベルが大きい場合はより大規模な措置による一括阻止) で封じ込め
- 必要な修復を実施し、個々のエンドポイントをコンプライアンスに準拠した安全な状態にリアルタイムで回復
- 攻撃者に改変されたエンドポイントを環境全体で検出し、元の状態に修復
- 動的かつ拡張可能な修復機能を活用し、複数のステップが介在する高度な修復措置をオーケストレーション
- カスタムダッシュボードを作成して修復措置を監視することで、必要な措置が適切かつ完全に実行されたこと、およびインシデント再発を防止できる状態になったことを確認

### デモを申込む

インシデントの規模を問わず、検知、調査、封じ込め、修復までの対応をスピードアップするTanium Incident Responseソリューションを、ぜひデモで実際にご確認ください

詳細を見る →

---

業界唯一のコンバージド・エンドポイント管理(XEM)プロバイダであるタニウムは、複雑なセキュリティとテクノロジー環境を管理するための従来のアプローチにおけるパラダイムシフトをリードしています。デバイス間の包括的な可視性、統一されたコントロールセット、そして「機密情報と大規模インフラの保護」という単一の共有目的に向けた共通のタクソノミを提供する単一のプラットフォーム内にIT、コンプライアンス、セキュリティ、リスクを統合することで、タニウムは、すべてのチーム、エンドポイント、ワークフローをサイバー脅威から保護します。www.tanium.jp をご覧ください。