Tanium + ServiceNow : Better Together

TaniumとServiceNowを連携することで、可視化・制御・是正の能力を最大限に活用し、データやワークフローの品質を向上して、結果を最大化

ServiceNowを利用する企業では、IT資産の可視化、顧客や従業員のエクスペリエンス、脆弱性や脅威の検出・優先度の設定・対応をはじめ、数々の課題に直面しています。このような状況で侵害が発生すると、財務面に加え業務にも多大な影響が生じる恐れがあります。

Taniumのパワフルなソリューションで ServiceNowを強化

TaniumとServiceNowを連携することで、エンドポイントのリアルタイムなデータを、ITの運用・セキュリティのワークフローにシームレスに連携し、IT資産の完全な可視化、従業員/顧客エクスペリエンスの改善、脆弱性リスクの低減 、コンプライアンス全般の向上を実現

Tanium + ServiceNow の統合ソリューションで、以下を実現できます。

- ハードウェア/ソフトウェアのインベントリデータをくまなく可視化し、完全かつ正確な最新の構成管理データベース (CMDB) を構築
- 従業員/顧客向けのデジタルエクスペリエンスを拡充し、生産性を向上して成長を加速
- 脆弱性対応のライフサイクル全体をカバーする自動実行機能で、脆弱性リスクの検出から優先度の判定、対応までのプロセスを自動で実行
- エンドポイントのリアルタイムなデータをIT運用・セキュリティのワークフローにシームレスに組み込むことで、コンプライアンス全般を強化

TaniumとServiceNowを同期して運用することで、両プラットフォームの能力を最大限に高め、コストのかかるポイントソリューションの連携から脱却し、シングルエージェントのTanium XEMプラットフォーム上で、エンドポイント管理をすべて完結することが可能になります。

33%

侵害コストの33%は、システム停止、顧客離脱、 信頼失墜による事業損失コスト

94%

これまで把握していなかったエンドポイントが新たに発覚した経験をもつIT意思決定者の割合

IT資産全体を確実に可視化し、卓越した顧客エクスペリエンス/従業員エクスペリエンスを提供しながら、あらゆる脆弱性と脅威を迅速に検出して対応する

ServiceNowを使えば、新旧のツールが混在する社内環境のデータを一元化・正規化して構成管理データベース(CMDB)に統合できますが、根本的な死角を排除しない限り、十分な投資効果を得られない可能性があります。IT・運用・セキュリティ担当者が、様々なプロセスやワークフローを駆使して顧客や従業員のエクスペリエンスをサポートし、インシデントの切り分けや是正を行って、インフラのセキュリティや最新状態を維持しても、CMDBのデータが不完全で精度が低く陳腐化していると、プロセスやワークフローに支障をきたすこともあります。

IT環境が可視化できないことで様々な問題が発生

- 大規模で様々なIT資産が混在する環境では、正確で完全なIT資産データを維持することが困難に
- 社内の問題が原因で従業員エクスペリエンスが低下すると、影響が波及して、顧客への対応にも支障をきたす
- 異種ツールやポイントソリューションの統合・保守で、予算、管理、使用全般の効率が低下し、複雑性が増加
- ITインフラ全体で横断的に脆弱性をすばやく検出することができず、脆弱性に対応するための大規模パッチ適用もスムーズに実施できない
- 多くの企業では脆弱性スコアの算出やリスク評価を十分に実施しておらず、修復の優先度判定時に必要なIT部門と運用部門の連携も不足しがち

その問題が、ビジネスに悪影響を及ぼす

- 「ネットワークに接続しているエンドポイントの85〜95%を可視化できている」と自信をもって言えるIT運用・セキュリティ担当者は30%しかいない
- IT意思決定者の94%は、未確認のエンドポイントを発見した経験がある
- 侵害によるコストの33%は、システムの停止、顧客の離脱、信頼失墜による事業損失コスト

Tanium XEM プラットフォームで、ServiceNowへの投資を最大化

TaniumとServiceNowを連携することで、機能がそろったCMDBをわずか数分で起動し、IT資産を完全に可視化してリアルタイムにレポートを作成。

さらに、エンドポイントのリアルタイムデータをIT運用・セキュリティのワークフローにシームレスに連携することで、従業員や顧客のエクスペリエンスを改善し、脆弱性のリスクを低減して、コンプライアンス態勢を強化。

> TaniumをServiceNowとSentinelに連携することで、データのサイロを解消し、運用チームが3つの基幹プラットフォーム全体を隅々まで可視化できました
>
> **サルフォード大学 CIO**
> **Mark Wantling 氏**

可視化

リアルタイムの可視化と信頼性の高いCMDBで、ソフトウェア、ハードウェア、クラウドのコストを最適化

- 物理、仮想、ソフトウェア、クラウドベース、モバイル、IoTなどに対応。ハード、ソフト、仮想デバイスをServiceNow側のオブジェクト構造に自動でマッピング
- オブジェクトの自動マッピングとTaniumの高精度なリアルタイムデータをServiceNowのワークフローで活用
- リモートでの制御や、ユーザの業務を中断することなく、エンドポイントのパフォーマンスデータにServiceNow上で直接アクセス

制御

構成アイテムを、リアルタイムの脆弱性、設定のコンプライアンス、変更権限のアセスメントと自動で紐付け

- 既知の脆弱性が存在するIT資産、設定、アクティビティ、トラフィックをネットワーク上で自動検索。SCAP (Security Content Automation Protocol)やOVAL (Open Vulnerability and Assessment Language) コンテンツをサポートしPCI、HIPAA、SOXなどの業界基準や規制にも対応
- セキュリティインシデントの対応時に最も重要な、紐付け先の構成アイテム（ログインユーザー、ネットワーク統計情報、実行中のプロセスなど）のデータをリアルタイムで取得し、インシデント情報を補完。エンドポイント全体を検索してリスクの有無を確認

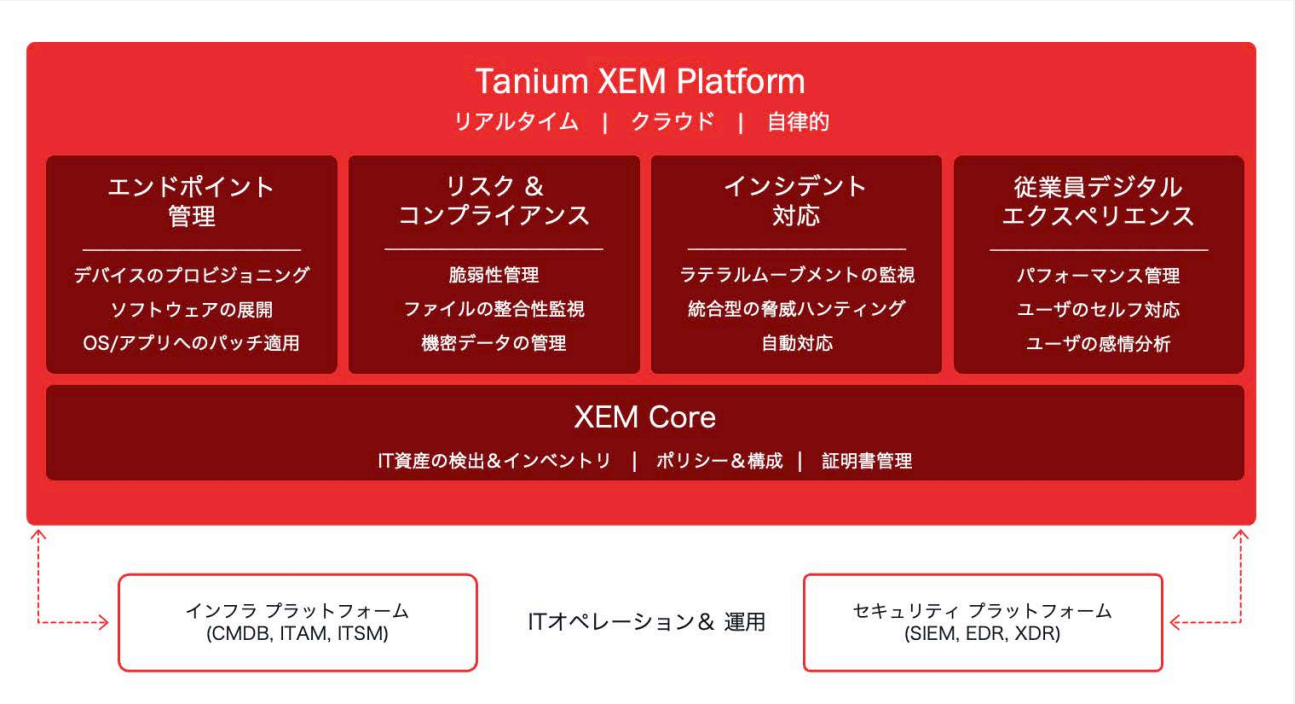
是正

パッチ適用を大規模にコントロールし、パッチの適用先を優先度別に分類して是正し、変更結果を検証

- 既知の脆弱性と算出したリスク値をもとに大規模パッチの適用先を優先度別に分類し、重篤度の高いリスクに優先的に対応
- ServiceNowの変更ライフサイクルに沿ったパッチ展開計画（テスト・展開計画、承認プロセス、ワークフローのスケジュール設定）を作成
- 変更完了後に再スキャンして結果を自動でチェックし、時間をかけて結果を手動で検証する手間を削減

コンバージド・エンドポイント管理

あらゆるエンドポイントを可視化・制御・コントロール



Tanium Platform

ServiceNowとTaniumでIT環境の可視化・制御・是正のプロセスを変革

Tanium ITX for ServiceNow →

ソフトウェア、ハードウェア、仮想資産のインベントリを最適化し、資産をリアルタイムで可視化して、リスクを低減

Tanium Security Operations for ServiceNow →

エンドポイントの脆弱性とコンプライアンスの問題によるリスクをリアルタイムに検出して関連付けし、優先順位を設定

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。