AKAMAI ソリューション概要

# Akamai Guardicore Segmentation 向け Tenable Vulnerability Management

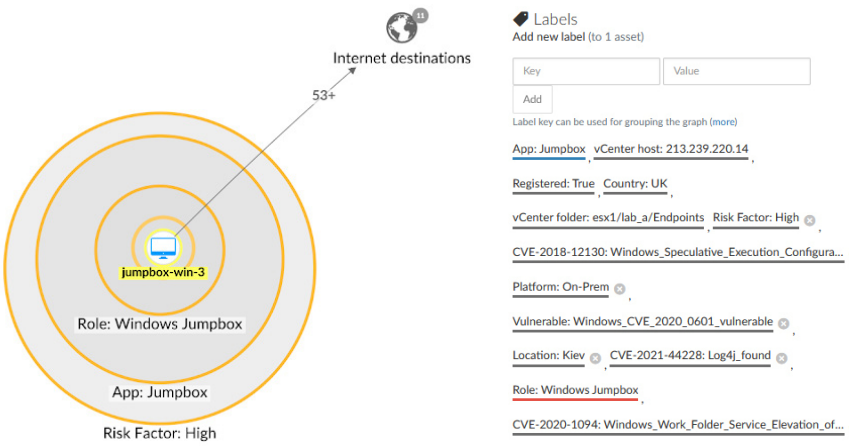
リスクベースのセグメンテーションにより、組織の脆弱性に対処します

Tenable は、アタックサーフェス全体（IT からクラウド、コンテナまで）をリスクベースで可視化します。この知見により、組織はリスク軽減が重要な領域を迅速に特定し、調査することができます。

この強力な脆弱性管理データを Akamai Guardicore Segmentation に取り込めるようになりました。この統合ソリューションを使用すると、関連する共通脆弱性識別子 CVE（Common Vulnerabilities and Exposures）とリスクスコアを資産にラベル付けし、そのデータを使用して不要なトラフィックを自動的にブロックし、より詳細なセグメンテーションポリシーを作成できます。

## Tenable と Akamai を活用してリスクを特定し、修正

- Tenable.io および Tenable.sc との統合は双方向で、Tenable の修正ステータスに基づいて、タグの追加・削除ができます。
- さらに、Akamai Guardicore Segmentation によって検出された（しかし Tenable ではまだ設定されていない）資産データをスキャンできるようになります。
- Akamai Guardicore Segmentation を Tenable.io または Tenable.sc と併用することで、組織はリスクの特定、優先順位付け、迅速な対処が可能になり、セキュリティ体制を強化できます。




**環境内の特定の資産に表示される CVE ラベル**

Akamai Guardicore Segmentation は、Tenable のデータを使用して、オンプレミスのサーバー、クラウドで実行中のアプリケーション、コンテナ、エンドユーザーデバイスなど、ネットワーク内の脆弱な資産をすべて迅速に探索します。ユーザーは、適切な修復が完了するまで、影響を受けた資産を他の環境から簡単に分離できます。

**詳細情報やデモをご希望の際は、**esg-bd@akamai.com **までお問い合わせください**

## 統合の主なメリット

**継続的な可視性**
既知および未知の資産を自動的に同期し、それらに関連する脆弱性を継続的に追跡

**優先的なセキュリティアクティビティ**
Tenable の脆弱性データ、脅威インテリジェンス、データサイエンスを組み合わせ、リスクスコアを分かりやすく提示

**リスクベースの修復**
豊富な脆弱性データに基づいてセグメンテーションポリシーを作成

## テクノロジーコンポーネント

- Tenable.io
- Tenable.sc
- Akamai Guardicore Segmentation

 | サポート | 公開日：2023 年 3 月