

テナブルの新しいイノベーション 単一プラットフォーム内のオンプレミスとクラウド環境の両方で 不正資産を自動的に発見・評価

※本リリースは2019年8月6日(米国時間)に米国で発表されたプレスリリースの抄訳版です。原文は下記URLを参照ください。

<https://www.tenable.com/press-releases/new-vulnerabilities-in-verizon-routers-expose-millions-of-consumers-according-to>

サイバー・エクスポージャーを提唱する Tenable®, Inc. (以下テナブル 所在地:メリーランド州コロンビア、代表:Amit Yoran(アミット・ヨーラン))は、単一プラットフォーム上でオンプレミスとクラウド環境の両方において既知および未知の資産を連続的に発見・評価する Tenable.sc™ (以前の SecurityCenter)と Tenable.io®用追加料金なしの新機能を発表しました。

この新製品はテナブルの Nessus® Network Monitor (NNM)を基にして、受動ネットワークモニタリングを実施します。NNM は過去 10 年以上にわたり連続モニタリングのパイオニアとして認識されており、業界最大クラスの資産カバレッジを持っています。テナブルは顧客のコンピューター利用環境全般において、資産すべてを自動的に感知するだけでなく、脆弱性や設定の問題も評価します。この新機能は Tenable.sc と Tenable.io の基本製品で利用可能で、複数のアプリケーションやデータサイロは不要です。

モバイル機器、コンテナ、クラウドインスタンスのようなテクノロジーが流動的かつ一時的な性質を有することから、セキュリティチームは自らの権限内ではスムーズに資産全てを特定しきれないことがあります。資産を特定しきれないことでサイバー・エクスポージャーのギャップが広がり、事業が混乱に陥る危険性が高まります。テナブルは不正資産の課題を対処すべく、下記製品の強化を公開しました。

<NNM 発見モード>

利用者はプロダクトライセンスを使わずに、Tenable.io と Tenable.sc の中で NNM を使用し、ネットワークを連続的にモニタリングすることで不正資産を発見できます。この機能を活用することでセキュリティチームは、不明な状態であった資産やスキャン中にネットワークに追加された新資産を原因として発生した盲点を除去できます。

NNM 発見モードは、2019 年中に Tenable.sc および Tenable.io で利用可能になります。

<不正資産自動評価>

セキュリティチームが新たに発見した資産のスキャンに対してチーム方針を定義できるようになることで、利用者はマニュアルの介入なしに不正資産を自動的に評価することができます。評価をつけることで組織は全体的なセキュリティ体制を改善しつつ、マニュアルプロセスの作業コストを低減することができます。

不正資産自動評価は、Tenable.sc で一般的に利用でき、Tenable.io では 2019 年の第3四半期に利用可能となります。

<テナブル・クラウドコネクタ自動発見>

テナブル・クラウドコネクタは連続的に展開し切断されるため、AWS、Azure、GCP といったクラウドワーク上での作業をリアルタイムで可視化します。自動発見機能を活用することで、利用者はマスターアカウントと関連する全メンバーアカウントから資産を自動的に収集し追跡することができ、マニュアル操作をすることなく、クラウド環境を完全に可視化することができます。

自動発見機能は、現在 Tenable.io 全般で使用が可能です。

【米国テナブル社 Renaud Deraison 氏(最高技術責任者・テナブルの共同創始者)のコメント】

戦略的サイバー・エクスポージャーのプログラムは、画一的に可視化します。近年においては、企業の資産はクラウドにまたがりつつあり、モバイル、IoT のようなデバイスも爆発的に増えてきているため、全資産がどこに配置されていて、どの程度リスクに晒されているかを把握することが更に困難となります。当社は、既知と未知の両資産を含む攻撃サーフェス全体の完全な可視性を提供すべく、利用者のサイバー・エクスポージャー・ジャーニーをサポートすることに注力しています。」

最新の機能に関する詳細情報は当社の最新ブログ掲載記事をお読みください。

【米国テナブル社プロフィール】

Tenable Network Security は、世界中の 24,000 社を超える組織に対し、総合的なセキュリティソリューションにより、将来のビジネスニーズに合わせてそのテクノロジーを変革し、組織組織の情報保護に向けた有効的な対策を提供しています。Nessus®を開発した Tenable は、脆弱性対策の技術をさらに発展させることで、あらゆる情報資産やデバイスの脆弱性を管理、保護できる世界初のセキュリティプラットフォームを展開。Tenable のセキュリティプラットフォームは、大規模行政機関ならびに、米国ビジネス誌 Fortune が選定する『Fortune 500』(総収入に基づいた全米上位 500 社)に選ばれている組織の 50% 以上、世界の有力組織 2000 社の 25% 以上に導入されています。詳細は tenable.com へ

【米国テナブル社企業概要】

商号: Tenable Network Security
代表: Amit Yoran アミット・ヨーラン
住所: 7021 Columbia、

Gateway Drive Suite 500 Columbia,
MD 21046

【テナブル社企業概要】

商号: Tenable Network Security Japan K.K.
住所: 東京都千代田区丸の内 2-3-2
郵船ビルディング 1 階