報道関係各位

2018 年 6 月 11 日

Tenable Network Security Japan K.K

テナブル・クラウド及びアプリケーション・セキュリティー・ポートフォリオの重要な強化策を発表
強化されたサイバー・エクスポージャーの全体的可視化
～徹底した DevOps プロセスが可能となるように強化～

企業の様々な情報資産の脆弱性を手間なく自動で可視化、改善するソリューションを提供する『Tenable Network Security』（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、高度なダイナミック・クラウド環境におけるサイバー・セキュリティリスクをセキュリティ・チームが検知・評価・管理する手助けとなるよう、サイバー・エクスポージャー・プラットフォームである「Tenable.io®」における一連の新製品とエコシステムの強化策を発表しました。この度発表した企業対応クラウド強化策は、ウェブ・アプリケーションからコンテナやクラウドインフラにおけるサイバー・エクスポージャーの統一見解を配信するという業界初のもので、DevOps の導入を促進し、リスクを軽減するものとなります。

※本リリースは 2018 年 6 月 5 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/key-enhancements-to-tenable-cloud-and-application-security-portfolio-deliver-holistic

パブリッククラウドにより、組織体がインフラをコードとして使用することが可能なり、パブリッククラウド API を呼び出すことで、ストレージサービス、バーチャルマシン、コンテナ、基幹ネットワークを含む、提供している様々なビルディングブロックの全てを修正・変更することができます。クラウド・コンピューティングは組織体に計り知れないスピードとアジャイルという利点をもたらし、DevOps の原動力となり、毎日・毎時間新たなアプリケーション機能を展開できるようになりました。しかしその反面、クラウド・コンピューティングと DevOps は、矢継ぎ早な変更をプロダクション環境もたらすとともに、セキュリティ上の盲点を生じさせる短期的またはサーバーレス資産を含む新たな課題をセキュリティ・チームにもたらします。そのため、インフラそのものの中での可視化を低下させることにつながり、ほとんどの場合、管理不能のサイバーリスクが生ずる結果となります。

組織は包括的な安全への取り組みと、資産、脆弱性、エクスポージャーの可視化の両方を要求します。テナブルの新製品とエコシステム強化は、伝統的 IT 及び異なるクラウド・プラットフォームを網羅したサイバー・エクスポージャーへの統一見解を提供します。そして、ソフトウエア開発のライフサイクル全体でビルドからプロダクションまでのセキュリティ構築を可能にします。

【米国テナブル社 Dave Cole 氏（最高プロダクト責任者（CPO））のコメント】

「広範囲クラウドの採用はセキュリティ・チームに重大な盲点を残すか、またはポイントツールの採用を強要し、後に環境全体像の修正を試みなければならなくなる。これは本当に膨大な作業であり、クラウドの動き、または DevOps の速度を逆に遅らせる。我々は速度を速め、当社顧客が驚くほど簡単に最新リスクの全領域を管理できるようにしたい。これが Tenable.io が立ち向かうべき新たな挑戦だと信じている」

新しい Tenable.io プラットフォームとクラウド・エコシステム強化策には下記が含まれています。

●マイクロソフト Azure とグーグル・クラウドプラットフォーム（GCP）クラウド・コネクターズ

自動的かつ継続的に Azure と GCP クラウド環境の資産変化を検知し追跡し、全クラウドの稼働量を監視し、脆弱性を評価します。Azure と GCP のための Tenable.io クラウド・コネクターズは既存のアマゾンウェブサービス（AWS）用クラウド・コネクターを補完し、最も広く展開している3大パブリッククラウド（IaaS）プラットフォームを網羅したサイバー・セキュリティリスクの統一見解を提供します。

●コンテナ・ランタイム・スキャニング

プロダクションで実行中のコンテナのサイバー・エクスポージャーを可視化します。Tenable.io コンテナセキュリティは、脆弱性を評価するために、プロダクションにおける新しいコンテナを自動的に確認するとともに、実行中のコンテナで変更されたものも検知します。これにより、ビルドプロセスとプロダクションで実行中のドッカーホストの確認を行う間、コンテナイメージのセキュリティテストを行うための既存能力を補完します。Tenable.io コンテナセキュリティと Tenable.io 脆弱性管理はともに徹底した DevOps プロセスの中に切れ目のないセキュリティを組み込む一方、一貫したデータの可視化と統一的なカスタマー・エキスペリエンスを提供します。

●ウェブ・アプリケーションの検知

以前から不明なアプリケーションも含んだ、組織体における横断的に所有・展開しているウェブ・アプリケーションを識別し、組織体のウェブ・アプリケーション資産全体のサイバー・エクスポージャーの存在を認知します。今まで、セキュリティ・チームはターゲットの URL を確認してから、どのウェブ・アプリケーションをスキャンするべきかを特定しなければなりませんでした。ウェブ・アプリケーションの検知が重大な可視化問題の解決につながる理由は、展開しているウェブ・アプリケーションの数がセキュリティ・チームの認識している数よりかなり多いことがよくあり、重大な盲点を作り、サイバーリスクを増大させているからです。

●クラウド・セキュリティ・アライアンス

テナブルはクラウド・セキュリティ・アライアンス（CSA）の法人会員で、Tenable.io は CSA STAR（Security, Trust & Assurance Registry＝安全、信用及び保障登録）の自己評価を完了しています。CSA STAR はクラウドセキュリティ保障に関する業界最強のプログラムです。

【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