

Tenable、業界初のサイバーエクスポージャーベンチマークソリューションを発表 ～CISO にサイバーリスクを定量化して理解を容易にする新しいインサイトを提供～

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、CISO が自社の組織のサイバーエクスポージャーを確実に視覚化、分析、測定できるようにする新しい Tenable.io アプリケーションである Tenable.io™Lumin を本日発表しました。

※本リリースは 2018 年 3 月 8 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/tenable-unveils-tenableio-lumin>

デジタルトランスフォーメーションにより、クラウドから IoT/OT にいたるまでの新技術とコンピュートプラットフォームの数と種類は根源的に増加し、アタックサーフェスは劇的に拡大しました。このアタックサーフェスの拡大により、脆弱性攻撃の危険性も増しています。Tenable Research によると、2017 年は脆弱性攻撃の記録的な年であり、テナブル・ユーザーが検知した問題の 60%以上が重大・重篤ランクに分類されています。CISO は常に、この変化するコンピューティング環境の基礎的な可視化に苦勞し、無数の WannaCry レベルの重大な問題に直面した場合、どこに集中して改善すべきかの優先順位付けはほぼ不可能です。同時に、サイバーリスクは、CEO や取締役会のトップビジネスリスクの 1つであり、CISO は、組織のサイバーリスクを定量化し、業界最高レベルのセキュリティや同業他社との比較を常に求められていますが、このデータを測定し、理事会に報告する有効な方法がありません。

Tenable.io Lumin は業界初のサイバー・エクスポージャーソリューションで、現代のアタックサーフェス全体にわたる組織のサイバー・エクスポージャーを視覚化、分析、測定することにより、これらの問題に真っ向から対処しています。また脆弱性データとアセットのビジネス的な重要度、そして脅威コンテキストを組み合わせることで、CISO はチームをビジネスにとっての最重要事項に集中させることができます。

また、業界最多の脆弱性インテリジェンスにデータサイエンスを独自適用しており、CISO は組織のサイバーリスクの数値化、業界ベンチマーキングを行い、理事会レベルでのより良い戦略決定を下すことが可能となります。さらに Tenable.io Lumin は徐々にサイバーセキュリティの有効性を向上させ、サイバーリスクを効果的にビジネスに活かすために必要なインサイトを提供します。他の Tenable.io アプリケーションと連携して、企業が 4 つの重要な質問にいつでも答えられるようになります。

- ・我々はどこに晒されていますか？
- ・リスクに基づく取り組みの優先順位はどこですか？
- ・時間の経過とともにどうやってエクスポージャーを減らすのですか？
- ・私たちのサイバー予防策は同業他社と比較してどうですか？

【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】

「何十年もの尽力にもかかわらず、攻撃者がアドバンテージを握っています。現状のままではリスクが高すぎます。業界一丸となって脆弱性管理を変革し、CISO が主導権を握ることで、組織は生産予測や潜在的なサプライチェーンの途絶制御などの他のビジネスリスクと同様に、サイバーリスクを事前に測定し対処することができるようになります。今度はセキュリティ側がアドバンテージを握る番です。サイバーエクスポージャーはこの変革を促進し、Tenable.io Lumin はこれを実現するための重要な一歩です。」

【Tenable.io Lumin 概要】

Tenable.io Lumin は、IT からクラウド、IoT から OT まで、幅広い現代のアセットを保護する業界初のサイバーエクスポージャープラットフォーム Tenable.io の新しいアプリケーションです。脆弱性管理、コンテナセキュリティ、Web アプリケーションスキャン、およびインダストリアルセキュリティのための Tenable の専用ソリューションと連動し補完します。Tenable は 2018 年第 2 四半期に Tenable.io Lumin のベータ版を開始し、2018 年にかけて新機能を発表する予定です。この製品は、2018 年後半に一般向けに発売予定です。

エクスポージャー分析とベンチマーキング:

内部グループや同業界間で客観的にサイバーエクスポージャーを分析しベンチマークします。例えば、業界最高クラスの組織や同規模の組織と比較して、重大で悪用可能な脆弱性を修正する時、ベンチマークデータは Tenable 独自の製品テレメトリーと Tenable Research の人的インテリジェンスの連携によって促進されます。この連携により、脆弱性インテリジェンスとサイバーセキュリティとデータサイエンスの専門知識が結集されます。

リスクに基づくスコアリングと優先順位付け:

リスクに基づいた高レベルのサイバーエクスポージャースコアリングは、脆弱性、脅威データ、および各アセットのビジネス価値と重要性を評価し、修復作業の優先順位を明確にするためのガイダンスを提供します。

サードパーティデータ API:

Tenable.io 内の Nessus® の脆弱性データとともに、サードパーティの脆弱性およびアセットデータをインポートし、標準化、統合します。すぐに利用可能な API には、脆弱性データのための Qualys、クラウドワークロードデータのための Amazon Web Services、(2018 年に一般的に利用可能な)IT アセットデータの ServiceNow が含まれます。単一ビューにより、複数のソリューションを使用している大規模企業がサイバーエクスポージャーを管理しやすくなります。

【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