脆弱性管理プラットフォーム

tenable Vulnerability Management

IBC

Tenable Vulnerability Management は、組織の IT 資産の露出と脅威をサイバー攻撃の視点から監視し、クラウドベースで継続的に評価するサービスです。隠れた脆弱性を特定し、最も危険な脆弱性を最初に修正するための優先順位付けと、修復に必要な情報を一体化して提供します。

脆弱性管理の必要性と課題

順位	脅威	昨年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	2位
3位	内部不正による情報漏えい等の被害	4位
4位	標的型攻撃による機密情報の窃取	3位
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位
6位	不注意による情報漏えい等の被害	9位
7位	**脆弱性対策情報の公開に伴う悪用増加**	8位
8位	ビジネスメール詐欺による金銭被害	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	10位

※ 出典：情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2024」

・第7位

ソフトウェアやハードウェア（機器類）の脆弱性対策情報の公開は、脆弱性の脅威や対策情報を製品の利用者に広く呼び掛けられるメリットがある。
一方で、攻撃者はその情報を悪用し、当該製品への脆弱性対策を講じていないシステムを狙って攻撃を行うことができる。近年では脆弱性関連情報の公開後に攻撃コードが流通し、攻撃が本格化するまでの時間もますます短くなっている。

定期的に脆弱性診断をしているが
対応状況の把握ができない

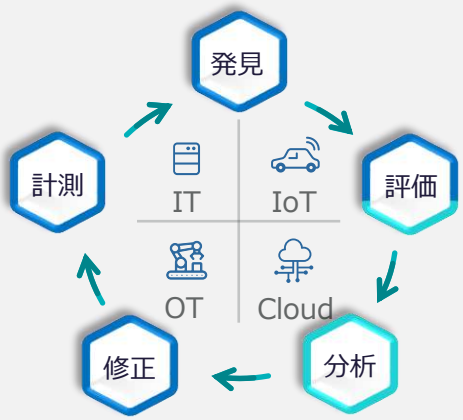
脆弱性診断対象となる
デバイスの把握が難しい

脆弱性診断結果に対する
優先順位づけがわからない

tenable Vulnerability Management による課題解決

脅威へのアプローチ

脆弱性の悪用を未然に防ぐため、リスクの素早い特定と重要資産への修正の優先順位付けを支援する管理プロセスを提供します。



脆弱性状況の把握と管理が可能

オンプレミス、クラウド、コンテナ、Web アプリケーションなど、異なる資産のハイブリッド環境を一括管理し、高リスクな脆弱性を素早く識別します。

Exposure Management（露出管理）

Tenable 社が提唱する「Exposure Management（露出管理）」は、組織が IT 資産のサイバーリスクを効率的に理解し、対応するための戦略です。Web ブラウザを使用して、リスクのある資産の特定、対処策の参照、リスク状況の変化の追跡を正確に把握・管理することが可能です。

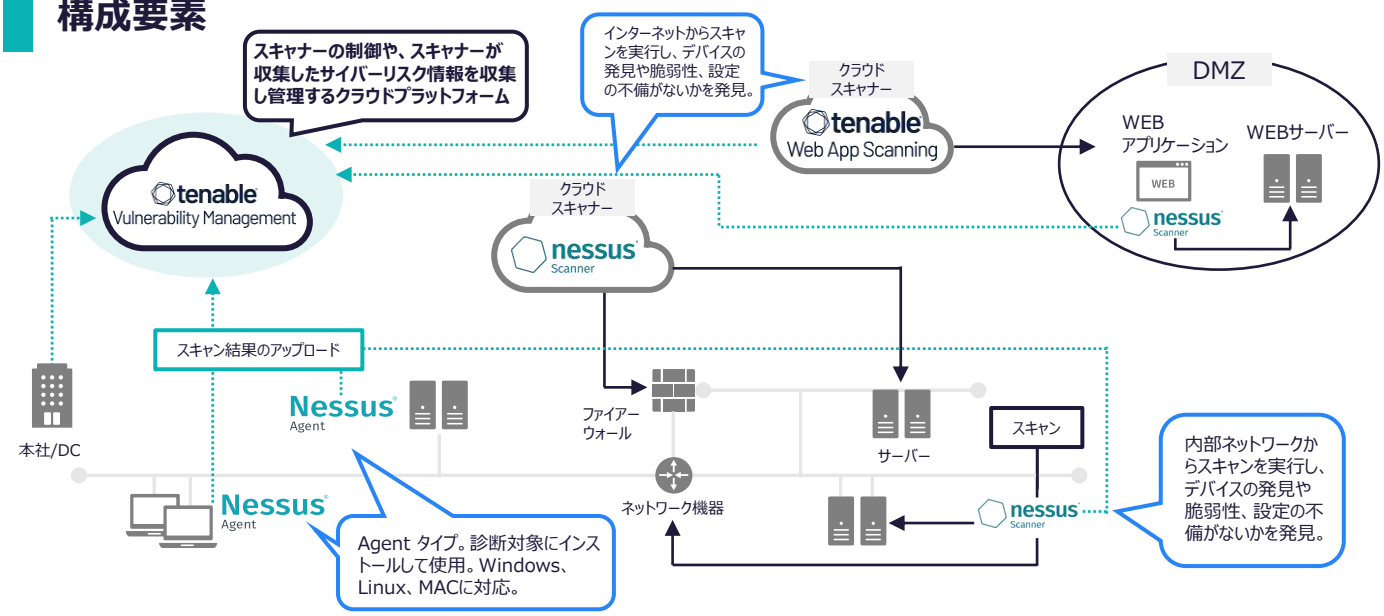
従来の脆弱性管理や資産管理

- 限定的な資産のみの把握
- 資産の不十分な発見
- IP ベースでの管理
- 可視化の間隔が長い
- 不十分な優先順位づけ
- 脆弱性情報だけにフォーカス
- 企業や組織全体のリスクが不明瞭

Exposure Managementによる解決

- 全資産を明確に識別してそれぞれのリスクレベルを評価
- 資産単位のリスクレベル、ビジネスインパクトなどをもとに優先順位を設定
- Web ブラウザのみで一元的なリスク評価が可能
- 定期スキャンにより継続的な監視、経過リスクに応じた危険性を追加判断
- コンプライアンスや業務規制（PCI DSS 準拠など）への評価要件に対応

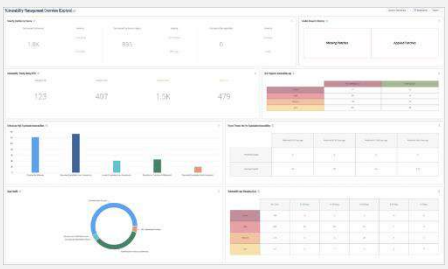
構成要素



tenable Vulnerability Management 機能特徴

シンプルかつモダンな UI

不要な機能をそぎ落とし、シンプルかつ洗練された UI を提供。運用者に必要な UI へと継続的な開発、改善を実施します。

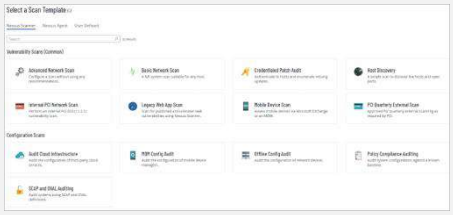


特定の脆弱性を調査

特定の脆弱性が組織内に存在しているかどうかを容易に確認可能。 CVE 番号やキーワード検索などのフィルタリングを用いて、調査したい脆弱性が存在しているかどうかを最新のスキャン結果に基づき可視化します。

スキャンテンプレート

事前設定済みのスキャンテンプレートを使用すると、検証のためのスキャンを実施する前に、スケジュールに従って不良部分をスキャン、修復および提起することができます。



アイビーシー株式会社

本社
〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780 fax.03-5117-2781

西日本事業所
〒532-0003
大阪府大阪市淀川区宮原4-1-14 住友生命新大阪北ビル3F
tel.06-7653-1014 fax. 06-7177-0542