tenable®

機械学習を利用した脆弱性の優先度付けと継続的脆弱性管理の自動化

Jumpei Abe

Security Engineer

なぜ脆弱性か

BlueKeep

- WindowsのRDPにおける脆弱性(CVE-2019-0708)
- 認証ユーザでなくてもリモートコードの実行が行われる
- 数百万のPCが脆弱性の影響を受ける状況
- Windowsの複数のOSが対象
  - Windows 7
  - Windows Server 2008/R2
  - Windows XP/Embeded
  - Windows Server 2003ARM 32/64
- WannaCryの再来

https://jp.tenable.com/blog/critical-remote-code-execution-vulnerability-cve-2019-0708-addressed-in-patch-tuesday-updates

各種ガイドライン、フレームワーク

The 20 CIS Controls & Resources

Download all CIS Controls (PDF & Excel) ⇢

Click on a CIS Control below to learn details

Basic CIS Controls

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Work

サイバーセキュリティ経営ガイドライン

Ver 2.0

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策につい

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2019年度4月一覧 ▶ サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました

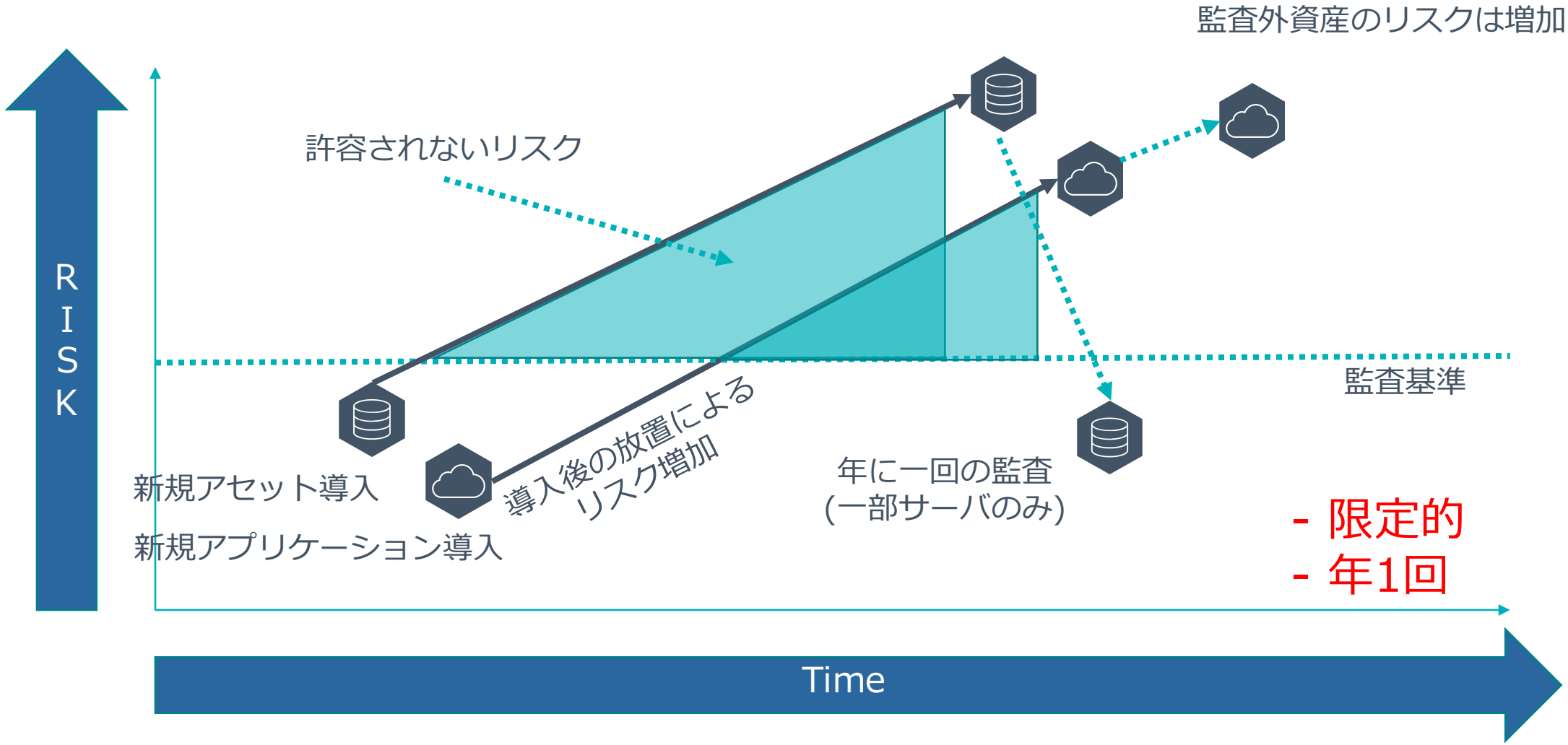
2019年4月18日

▶ ものづくり/情報/流通・サービス

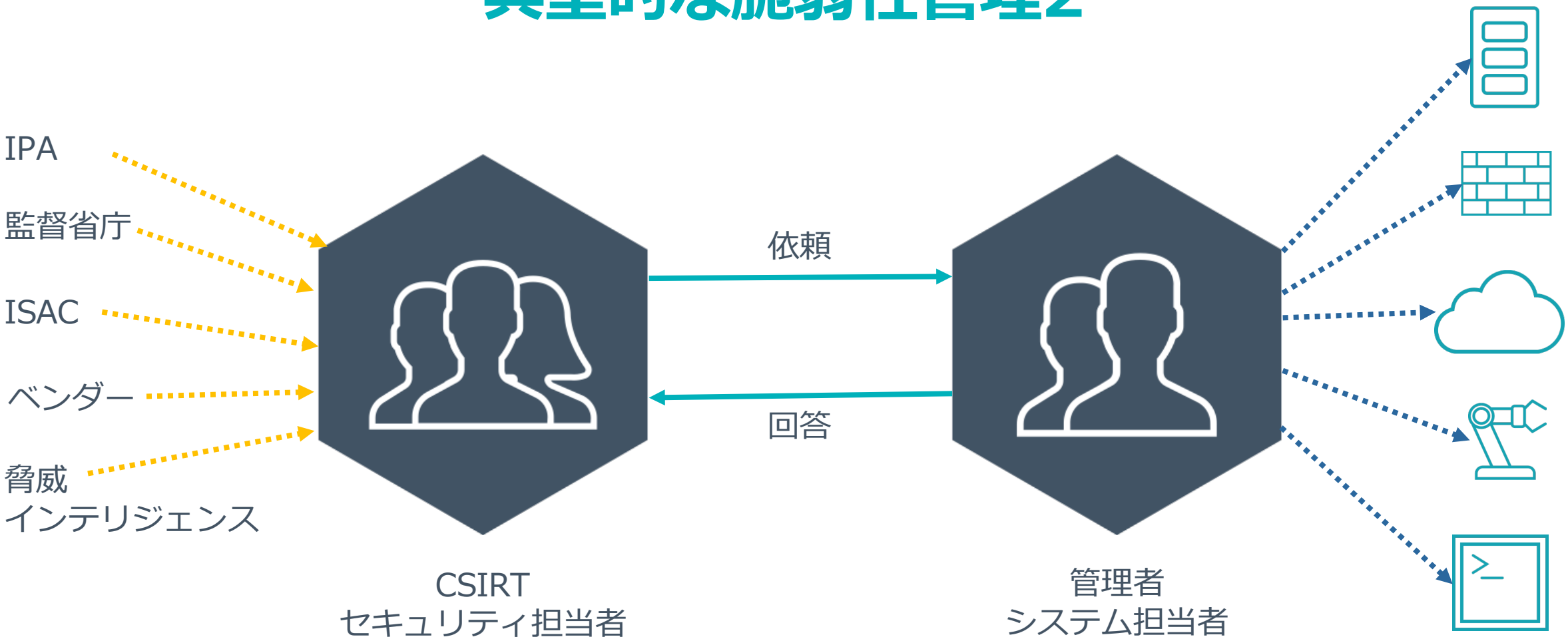
経済産業省では、サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」、様々なつながりによって新たな付加価値を創出する「Connected Industries」における新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理した「サイバー・フィジカル・セキュリティ対策フレームワーク」を策定しました。

脆弱性管理の現状

典型的な脆弱性管理1


監査外資産のリスクは増加
RISK
許容されないリスク
監査基準
新規アセット導入
新規アプリケーション導入
導入後の放置による
リスク増加
年に一回の監査
(一部サーバのみ)
- 限定的
- 年1回
Time

典型的な脆弱性管理2



- 優先度付け
- 該当判断

- 属人的
- 情報の確認方法

手作業による脆弱性管理の限界

膨大な脆弱性

管理の限界

2018年に公開された脆弱性は16500件。その大半が重大な脆弱性。

管理対象数をn倍に増やすと対応が必要な脆弱性もn倍に増加。

人材不足

マニュアル作業の限界

脆弱性管理は膨大な時間と人を必要とするが、組織として人材の確保が困難。脆弱性管理の大半をエクセル管理や手動での状況確認などマニュアル作業が占めており非効率。

優先度付け

膨大な脆弱性に対して

膨大な脆弱性のうち、優先的に対処すべき脆弱性がどれなのかを判断することが困難。

CVSSへ頼る対応の限界。

Tenableによる課題の解決

Tenable Network Securityについて

設立:　2002年　(日本法人は2014年設立)
本社:　メリーランド州コロンビア
米国防総省、Amazon、Google、Microsoft、Apple、VMware、
Cisco、IBM、Oracle、Twitter、Salesforce、Bank of America等、
165ヶ国以上で24,000以上のお客様
Global 2000企業の25%以上、Fortune 500企業の54%がお客様
米国のTop10銀行のうち9行がお客様

2012年に$50M（シリーズA）、2015年に$250M（シリーズB）、
米国ベンチャーキャピタルのAccelから出資を受ける

2011年4月：　パッシブ脆弱性管理特許の取得
2013年5月：　クレデンシャルレスネットワークスキャン特許の取得
2015年4月：　Nessusエージェントをリリース
2017年4月：　業界初Cyber Exposureプラットフォーム、Tenable.ioを発表
2018年2月：　Tenable.ioを中心に日本における本格的なビジネス展開を発表
2018年8月：　NASDAQに上場（TENB)

tenable

世界初のサイバーエクスポージャープラットフォーム

全アセットの
完全な可視化

優先順位分析と
対処ガイダンス

クラウド/オンプレミス
の選択が可能

tenable

Step1 Discovery

tenable

柔軟かつ強力なツールによる完全な可視化


産業用 IoT


ICS/SCADA


コンテナ


クラウド


Web App


エンタープライズ IoT


デスクトップ


ノートPC


モバイル


仮想マシン


エージェントスキャニング


イメージレジストリ


ネットワーク


サーバー


アクティブスキャニング

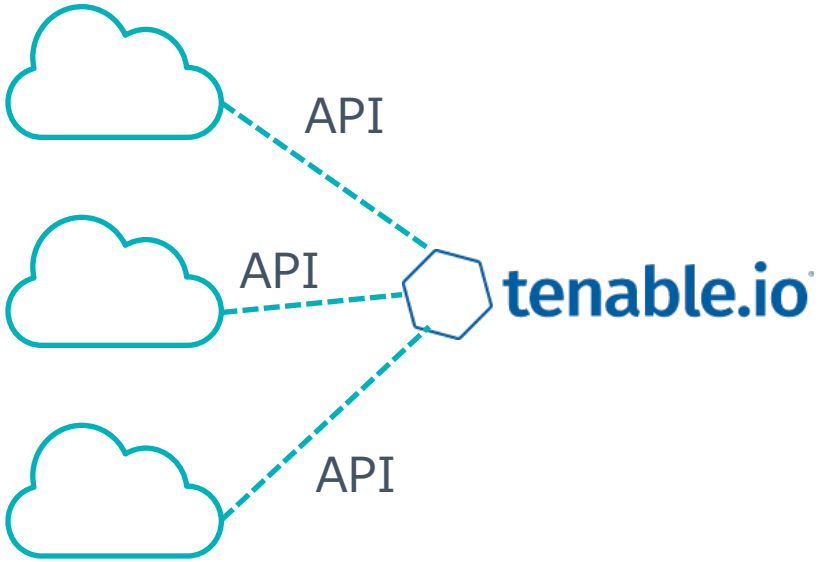

パッシブモニタリング

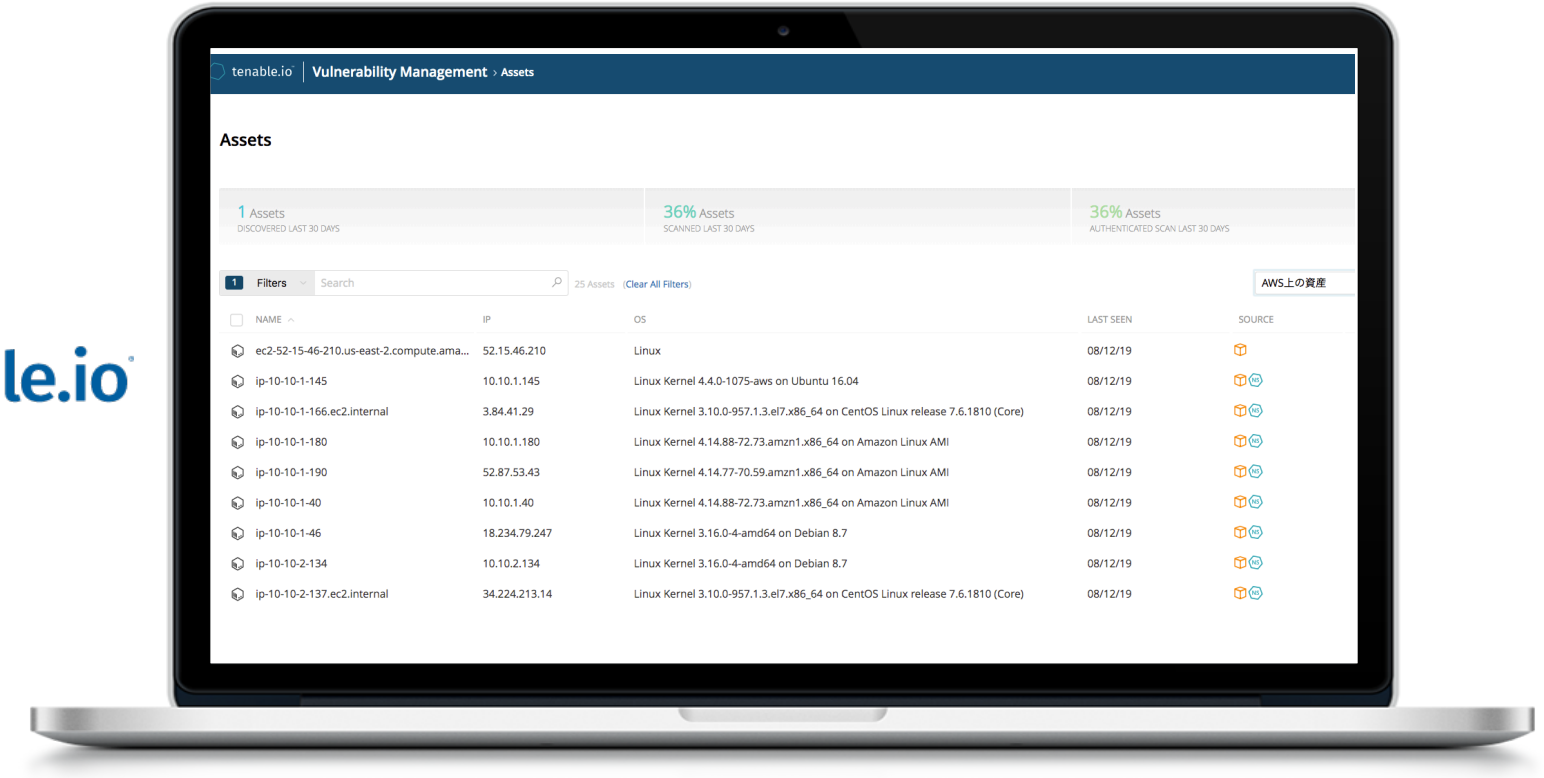
Nessus N

世界で200万人ものユーザに信頼されているツール

tenable

APIコネクタ(AWS,Azure,GCP)





Step2 評価/分析

tenable

使いやすく柔軟性に富んだ管理UI

洗練されたレポート/ダッシュボード

シンプルなデザインのUIを採用。直感的な操作により脆弱性の優先度付けや分析を容易に実施可能。

NISTやHIPPAなど業界標準のレポートに対応したテンプレートを多数用意。

柔軟なスキャナ実行

スキャンのスケジューリング機能により自動的に継続的スキャンが可能。

常に最新の情報を取得することで、新たな脆弱性や設定上の誤りを検出可能。

また、対象端末への低負荷スキャン等環境に合わせてスキャナを制御

分析プラットフォーム

収集したデータを分析することで対応優先度の高いリスクにフォーカスを当てることが可能。

予測的優先度付け機能により将来攻撃される脆弱性に対しての事前対策が可能

優先対応脆弱性予測機能

tenable

CVSSとは

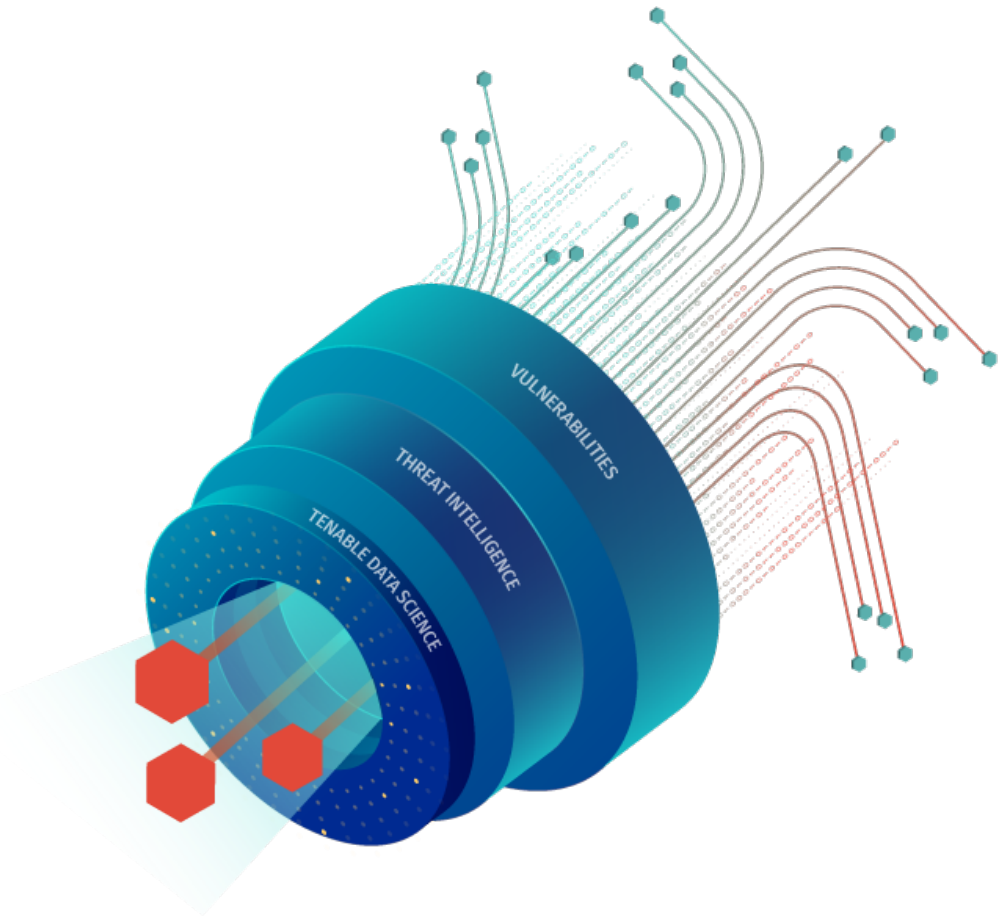
- Common Vulnerability Scoring Systemとは
  - 共通脆弱性評価システムのこと。IT製品のセキュリティ脆弱性の深刻さを評価
  - 管理母体はFIRST。FIRST-SIGで仕様改善等が行われている
- CVSSでは次の3つの基準で脆弱性を評価
  - 基本評価基準 (Base Metrics) → NVDやJVNで公表
  - 現状評価基準 (Temporal Metrics) → NVDやJVNに記載なし
  - 環境評価基準 (Environmental Metrics) → NVDやJVNで記載なし
- CVSSベーススコアの計算方法(v2,v3共通)
  - CVSS 基本値 = ((0.6×影響度)+(0.4×攻撃容易性)-1.5)×f(影響度)

CVSSで客観的に脆弱度合いを表現

Impact Score

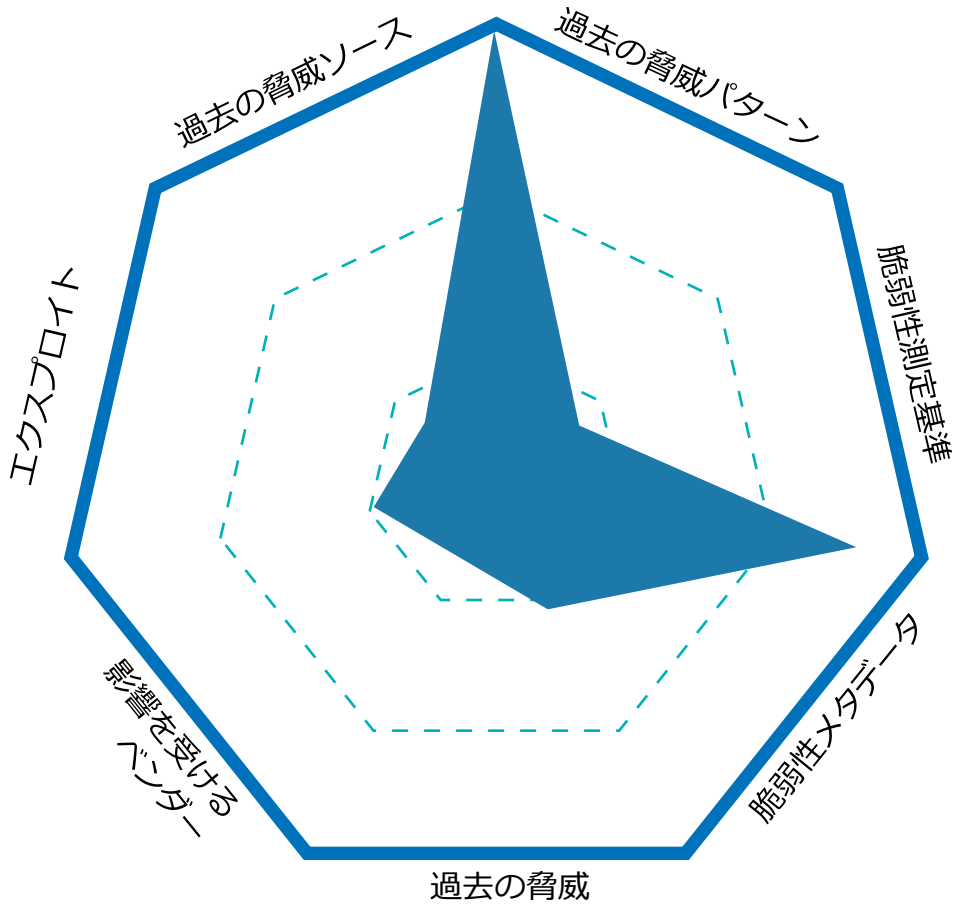
Exploitability Score

優先対応脆弱性予測機能 – 3%に焦点を当てる



- 脅威に基づく脆弱性の優先度付け
  - 今後28日以内に攻撃が成功するであろう脆弱性を**予測**
  - 150ものデータソースより脆弱性優先度のスコアリングを実施
  - 脅威の変化に伴い、常に動的に変化
- 業界初の予測機能
  - 本当に対処が必要な**3%**にフォーカス
  - 継続的にアップデート
- Cyber Exposureの基礎となる機能

優先的に対処すべき脆弱性を正確に予測



150

7つの異なるカテゴリー、
150の異なる要素を、
独自のデータサイエンスに
もどづいて分析。

109K

109,000を超える脆弱性を
継続的に追跡調査し、
リスクの変動に
リアルタイムに対応。

28日

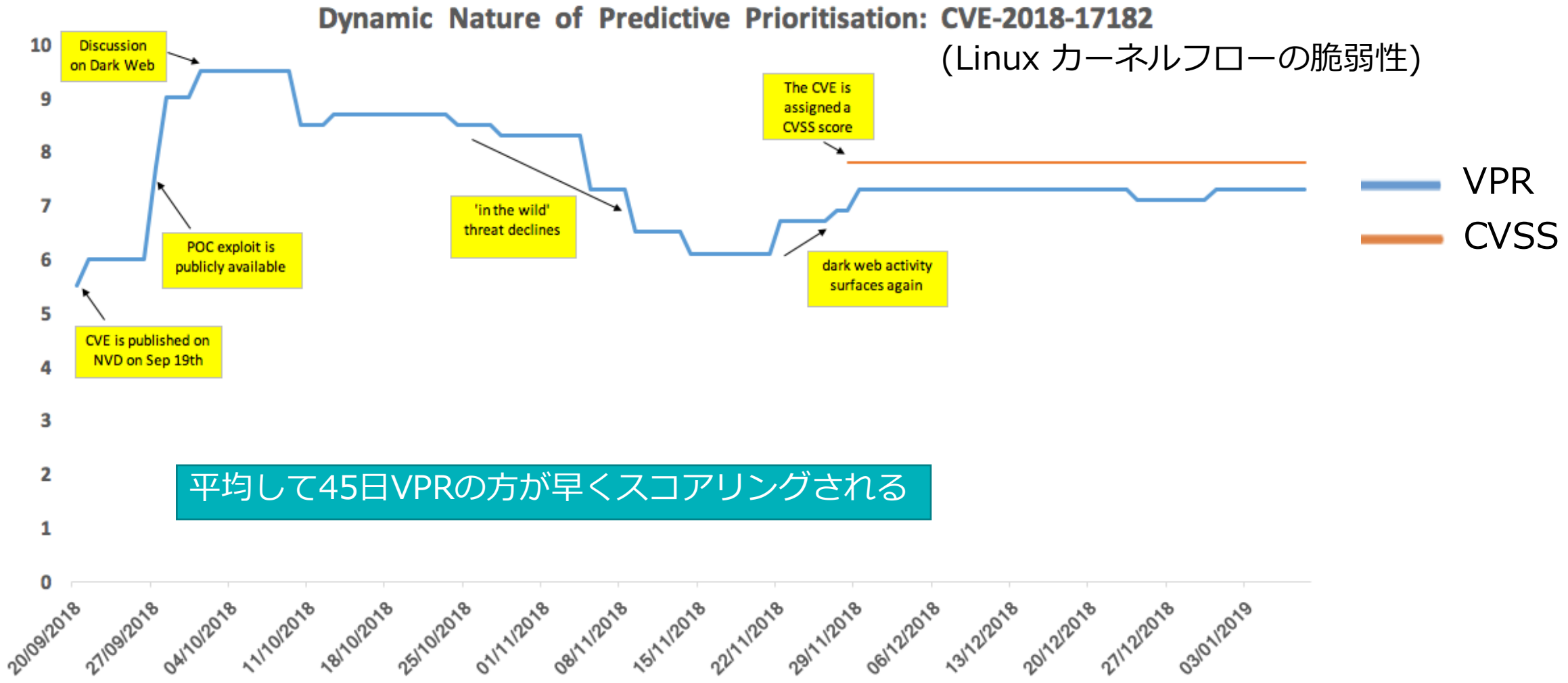
28日以内にエクスプロイト
が利用可能になると
予測される脆弱性を
優先対象と判定。

97%

広く採用されているCVSS
と比較して、緊急度が高い
脆弱性の割合を97%削減。

tenable

実際の例 – CVE 2018-17182



平均して45日VPRの方が早くスコアリングされる

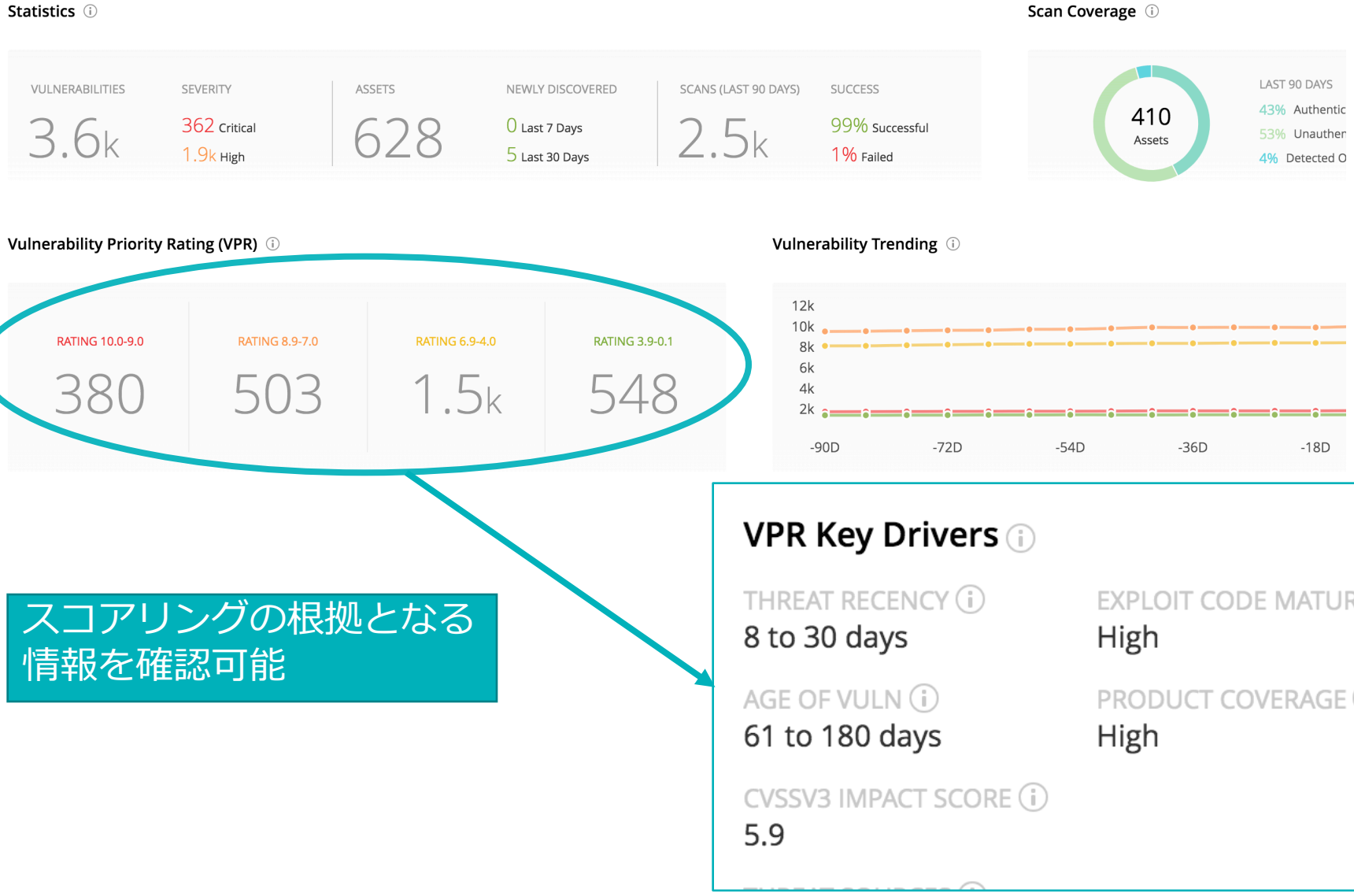
2018年に悪用された脆弱性Top5

	CVSSv2 Score (Acccording to NVD)	CVSSv3 Score (Acccording to NVD)	Tenable (Vulnerability Priority Rating)
CVE-2018-8174	**7.6**	**7.5**	**9.9**
CVE-2018-4878	**7.5**	**9.8**	**9.5**
CVE-2017-11882	**9.3**	**7.8**	**9.9**
CVE-2017-8750	**7.6**	**7.5**	**9.4**
CVE-2017-0199	**9.3**	**7.8**	**9.9**

tenable

Extracted from the Recorded Future Report “Top Ten Vulnerabilities of 2018” 03/19/19

VPRダッシュボード



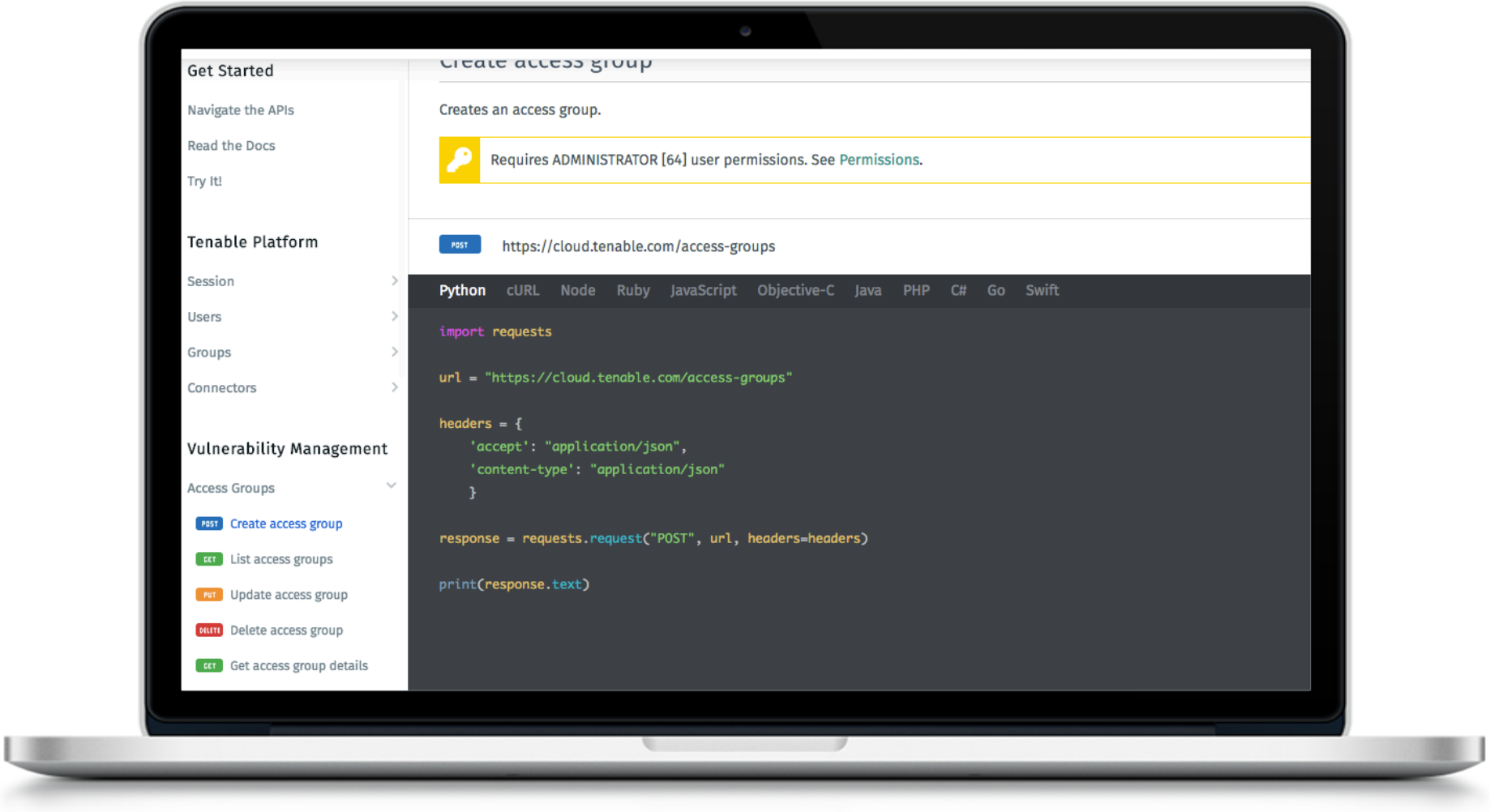
スコアリングの根拠となる
情報を確認可能

tenable

Step3 API/SDKを使用した統合

tenable

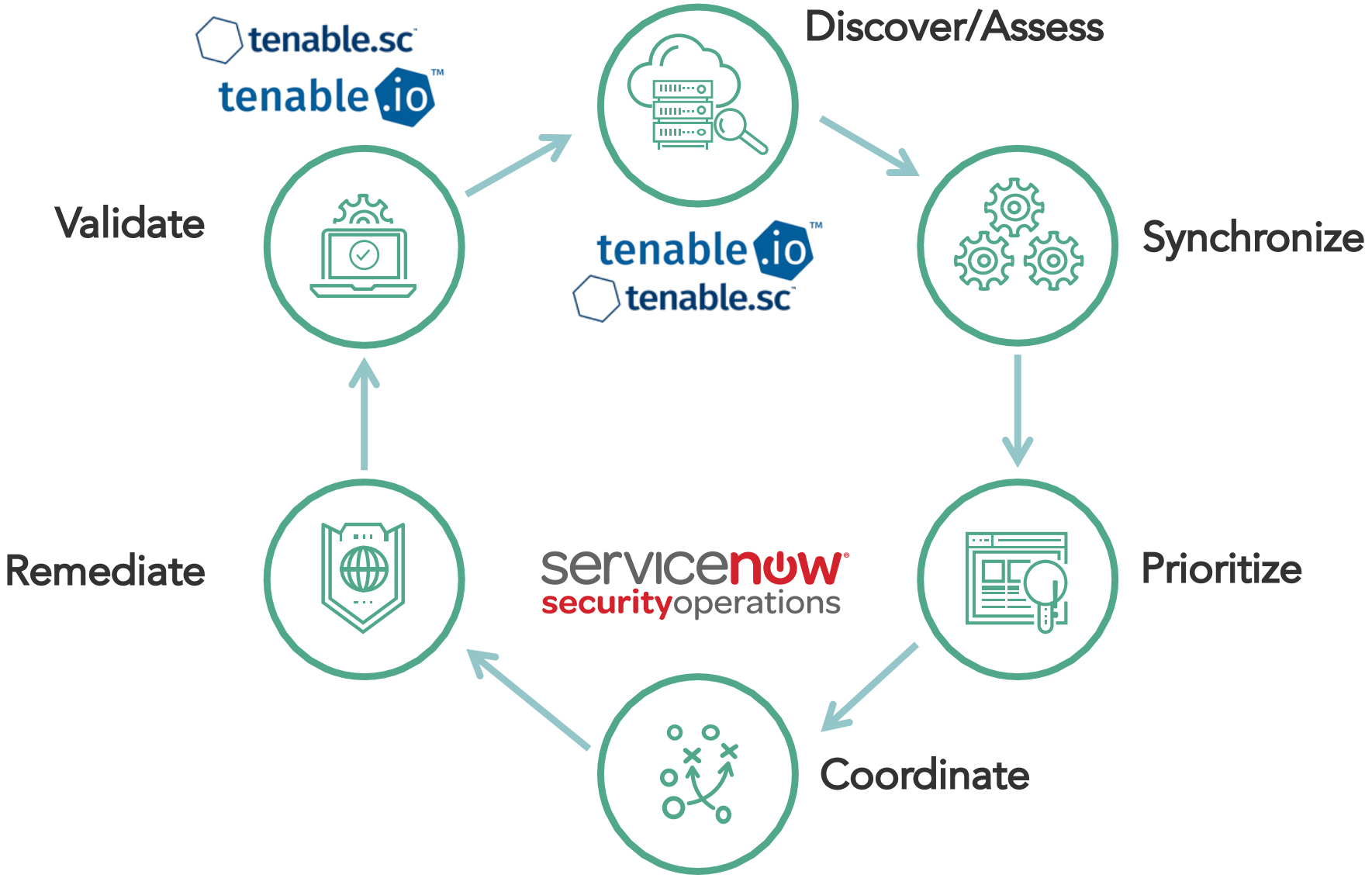
開発者向けサイト



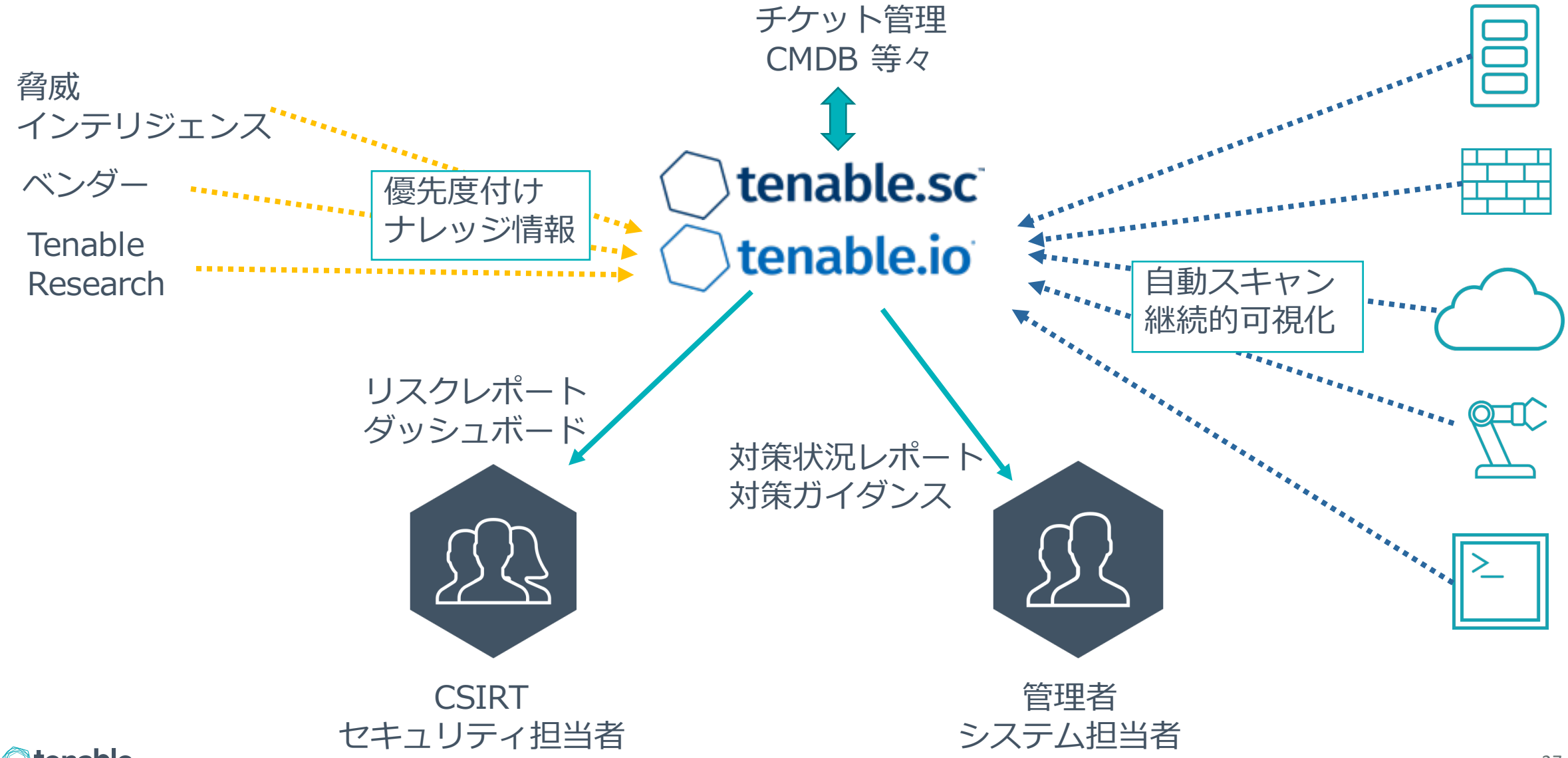
https://developer.tenable.com/

tenable

ServieNowとの統合

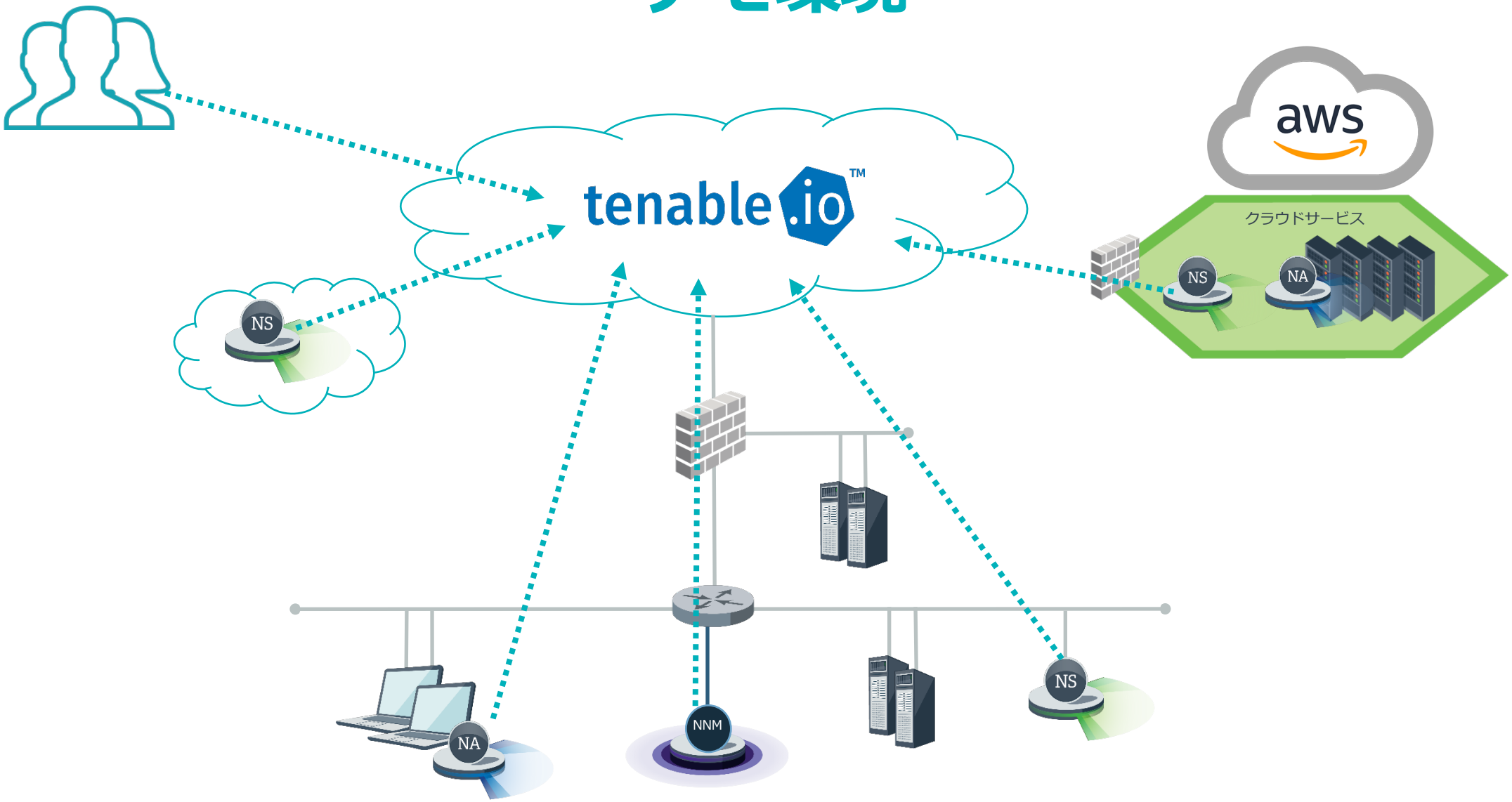


Tenable導入による脆弱性管理の効率化



Demo

デモ環境



まとめ

IT資産全て可視化

IoT/OTからクラウド

サーバやNW機器はもちろんのこと、AWSやAzureなどのPublicクラウドからOTデバイスに至るまでIT資産全てを可視化。

さらにそれら資産が抱えるリスク状況も把握することが可能。

自動化で負荷軽減

自動発見/自動更新

資産情報を自動的に発見、常に最新の情報を所有することが可能。この情報はセキュリティインシデント対応やまた侵害が発生した際の調査にも利用ができる。

高度な優先度付け

自動的な優先度付け

企業で決められたPolicyに沿った優先度基準をTenable側に適用することで優先度付けが行える。

さらには脆弱性の予測的優先対応機能により自動的に優先順位を付与。

試用版

https://jp.tenable.com/products/tenable-io/evaluate

ご清聴ありがとうございました。

お問い合わせ

jp-sales@tenable.com

tenable