tenable

NETWORLD

OT環境も脆弱性管理が必要な理由

OT環境が狙われています

たとえクローズド環境であっても、決して安全ではありません。
USBや新規デバイスの感染に気付かないで接続したり、シャドーITによる未確認の外部接続から感染するなどの事例が報告されています。

製造業の心臓部であるOT環境ですが、セキュリティ対策が不十分な場合が多いです。稼働中のOTの見える化だけではセキュリティを守ることはできません。

法規制が強化されました

2022年5月、経済安全保障推進法が成立し、4本の柱が示されました。

経済安全保障推進法 4本の柱

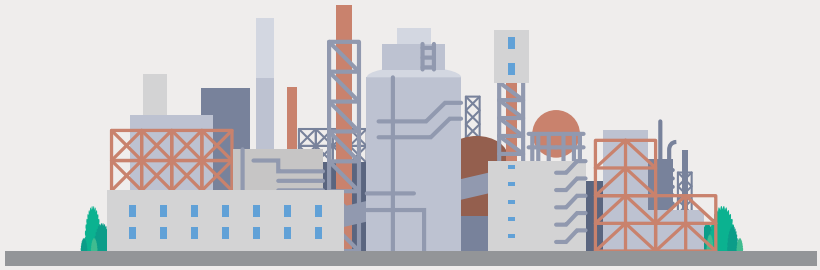
- 先端技術の研究開発
- 特許の非公開化
- **インフラの安全確保**
- 供給網の強化

システムに脆弱性がないかなどをチェックしたうえで、攻撃を受けるおそれが高いとみられた場合には、必要な措置をとるよう国が勧告や命令を出せるようになります。

OTの領域であっても、セキュリティ対策の強化が急務です。
Tenable.otなら脆弱性だけではなく、
そこに潜むリスクまで、IT/OT問わず統合的な管理が可能です。

詳しくは裏面をご覧ください

5 Tenable.ot つの特徴



包括的な可視化

- IT、IoT、OT資産の可視化
- デバイス間のやりとりと相互作用の詳細が調査可能
- カスタム化されたダッシュボードに、デバイスの状態がリアルタイムで表示され、一目で判別
- パッシブ・モニタリングとアクティブ・クエリによって資産を検知

脅威検出と緩和

- 複数の検出エンジンがネットワークやデバイスの脅威を捕捉
- イベントの表示や、タイプ別のソート
- イベントのサマリーとトレンド
- 特定のポリシー違反
- バックプレーン情報まで掘り下げ
- フィルター機能

資産の捕捉

- 個々の資産に対する深い状況認識
- ネットワーク上で通信していない機器を把握
- 正確で常に最新の資産インベントリ
- クエリの実行方法に関する微調整機能
- 安全で干渉しない

脆弱性の管理

- ITまたはOTベースの脆弱性を追跡
- VPRスコアを使用して、最初に対処する必要のある最も重要な脆弱性に優先順位を付ける
- Tenable Researchのパワーとインサイトの活用

構成管理

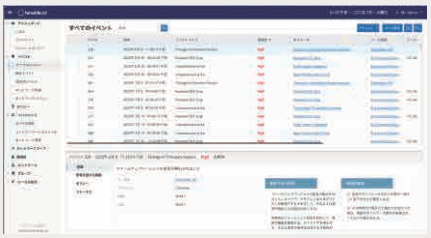
- PLCに加えられた変更に対するすべての変更を追跡
- スナップショットは、時間、イベント、ユーザーの指示によって起動
- 前回と今回のスナップショットとのあらゆる差分がハイライト表示される
- 「最後に確認された良好な状態へのロールバック」を可能にする重要なコンポーネント

資産の可視化

眠っている資産も逃さない

脅威情報の把握

攻撃ベクトルのシミュレーションも可能



脆弱性/リスク、構成情報の管理

インシデントを未然に防ぐ

株式会社ネットワールド https://www.networld.co.jp/

お問い合わせ ✉ tenable-info@networld.co.jp

本　　社	〒101-0051	東京都千代田区神田神保町 2 -11-15 住友商事神保町ビル	TEL：03-5210-5020, 5031, 5095
関西支店	〒530-0001	大阪市北区梅田 3-3-20 明治安田生命大阪梅田ビル 24F	TEL：06-7777-4174
中部支店	〒450-0003	名古屋市中村区名駅南 1-17-23 ニッタビル 10F	TEL：052-588-7611
九州支店	〒812-0013	福岡市博多区博多駅東 2-6-1 九勧筑紫通ビル 3F	TEL：092-461-7815