OT・IoT・IT 向け
統合アセットインテリジェンス

検 知

1500 万以上のデバイスプロファイルによりベンダー名やファームウェアなど詳細な情報までデバイスを 100% 可視化

攻撃リスク軽減

デバイスの情報・挙動を CVE や他の脆弱性 DB と比較し攻撃リスクを判断して優先順位を付け、修正方法を提示

保 護

アノーマリ挙動検知により、通常から逸脱した通信を行う疑わしいデバイスを検知、マルウェア、ランサムウェアなどから保護

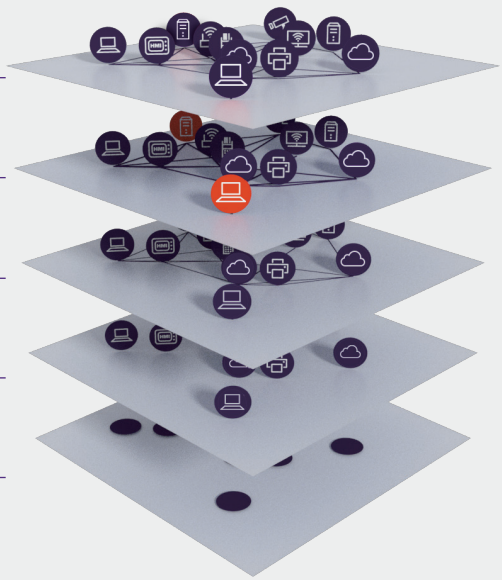
OT・IoT デバイスへのサイバー攻撃の急増

OT 機器や IoT 機器の増加により、脆弱なデバイスを標的にされ業務停止などの被害に合う企業が増えています。こういった被害を未然に防ぐためには、ネットワーク内のデバイスを正確に把握し、脆弱性を判断し、脅威を検知するしくみが必要です。

Armis は従来の IT デバイスの他、新しいアンマネージド・スマートデバイス、例えばスマートテレビ、IP カメラ、プリンター、空調システム、産業用ロボット、医療用デバイスなど様々なデバイスを検出し識別します。検出したデバイスに脆弱性がある場合に警告を発し、常にネットワークを安全な状態で運用することが可能です。さらに Armis は継続的にエンドポイントの挙動を分析し攻撃を検知します。疑わしいデバイスや悪意のあるデバイスは検疫を行うことで重要な情報やシステムを保護します。

Armis 統合アセットインテリジェンス

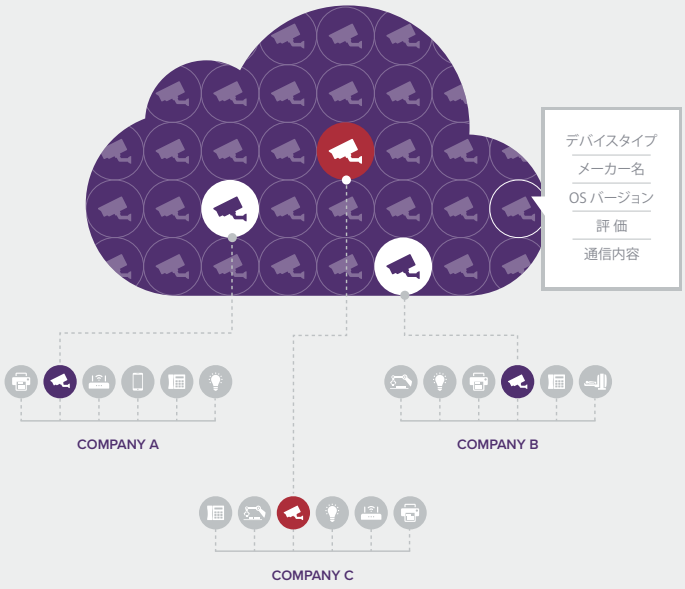
- 管理・防御・他ツールとの連携
- 脆弱性・リスク・脅威を検知
- OT/IT 資産の接続や関連性を把握
- プロファイルと照合し、更に詳細な情報を提供
- OT/IT 資産を発見し、関連情報を統合する



Armis アセット集合知エンジン

☑ 世界中で 20 億を超えるデバイスをトラッキング、そこから得たメタデータをデバイスナレッジベースに保存し膨大な情報を持つ事でより深く詳細なデバイス情報を提供可能。2022 年現在、約 1500 万のデバイスプロファイルを保有し、IP アドレスや MAC アドレスだけでなく**メーカー名、型番、OS・ファームウェアのバージョン、関連するユーザ、接続先、ロケーション**などの情報を提供します。

☑ Armis は、IT・IoT・OT を問わず、サーバー、ラップトップ、スマートフォン、VoIP 電話、スマート TV、IP カメラ、プリンター、HVAC コントロール、医療機器、産業用コントロールなど、環境内のすべてのマネージド / アンマネージド /IoT デバイスを検出・分類します。**Armis はエージェントレスで、ネットワークにシームレスに統合でき**、リモートオフィスや複数のネットワークを一元的に管理・保護することができます。



Armis Threat Detection Engine

☑ Armis Threat Detection Engine は、ネットワーク上および無線トラフィック内のすべてのデバイスの挙動を継続的に監視し、挙動の異常を検出します。Armis は、クラウドのデバイスナレッジベースと連携し、各デバイスのリアルタイムの挙動を以下と比較し通常から逸脱したデバイスを検知、警告します。

- デバイスの過去の動作
- お客様の環境における類似デバイスの挙動
- 他の環境での類似デバイスの挙動
- 一般的な攻撃手法
- CVE などの脅威情報フィードからの情報

Armis は、このようにデバイスと行動に関する情報を複数のソースから得ることで、脅威や攻撃を正確に特定することができます。Armis が脅威を検知した場合、セキュリティチームに警告を発し、自動化されたアクションで攻撃を阻止することができます。

ベストプラクティス

- ネットワーク内の認識できていない OT・IoT・IT デバイスを可視化したい
- 工場、プラント内の制御デバイスを把握したい
- 稼働しているデバイスに脆弱性がないか知りたい
- PLC などセキュリティエージェントを入れられない IoT・OT 機器を保護したい
- セグメント間で未許可の接続が行われていないか検知したい
- 既存の複数のツールを統合し、横断的に情報を把握することで、セキュリティチームの効率性を上げ、コストを軽減する
- 複数のツールのデータを統合し、重複しないユニークなデータとして整形する
- Purdue モデルを基にしてデバイスを自動的にカテゴライズし、逸脱する接続がないかを監視する
- 実際に使用されているソフトウェアの数を把握し、ライセンス数を削減したい
- EDR を入れていない端末・OS のバージョンが古い端末などをリストアップしたい
- 外注の持ち込み PC の検知・監視をしたい
- 買収・合併などで相手側のシステム全体像を把握したい

ABOUT ARMIS

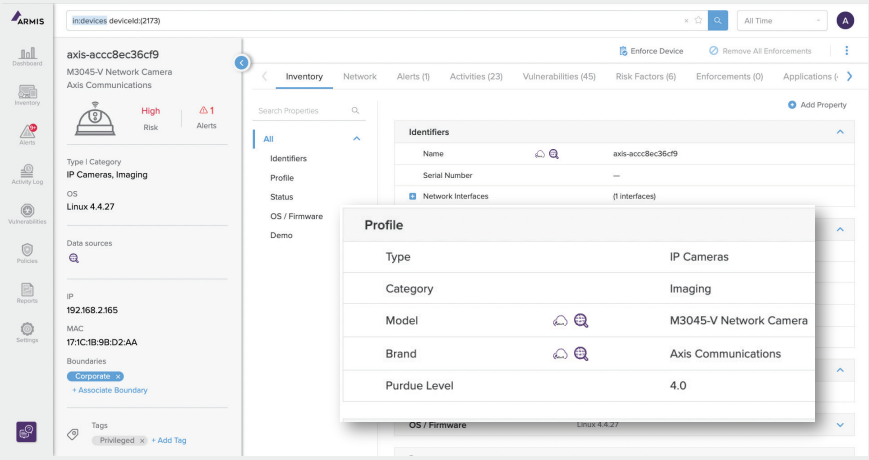
Armis は、アンマネージドデバイスと IoT デバイスの新しい脅威に対応するための、エージェントレスでエンタープライズクラスのセキュリティプラットフォームです。Armis は、マネージド、アンマネージドデバイス、IoT デバイスを含むすべてのデバイスの検出と分析における独自の技術に関して、フォーチュン 1000 企業より信頼を得ています。

ノートパソコンやスマートフォンなどの従来のデバイスから、新しいアンマネージド・スマートデバイス、例えばスマートテレビ、ウェブカメラ、プリンター、空調システム、産業用ロボット、医療用デバイスなど様々なデバイスを検出し識別します。Armis はオン・オフネットワークにあるデバイスを検出し、継続的にエンドポイントの挙動を分析し攻撃のリスクを特定します。疑わしいデバイスや悪意のあるデバイスは検疫を行うことで重要な情報やシステムを保護します。

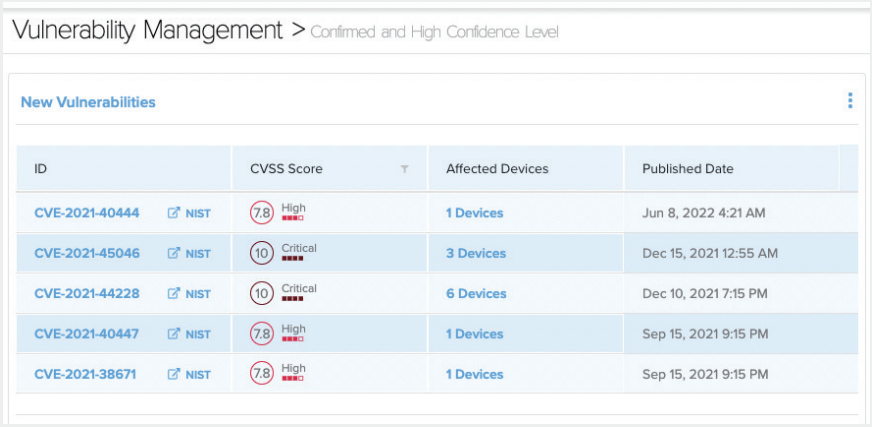
Armis は非上場企業であり、本社はカリフォルニアのサンフランシスコにあります。

1500 万以上のデバイスプロファイルにより、IT・IoT・OT を問わずネットワークにある全てのデバイスをより正確に認識可能。

IT と OT の融合が進む今、一つのコンソールで複数の環境を統合管理でき、また様々なソリューションと連携することで管理チームの人的リソースを節約することができる。

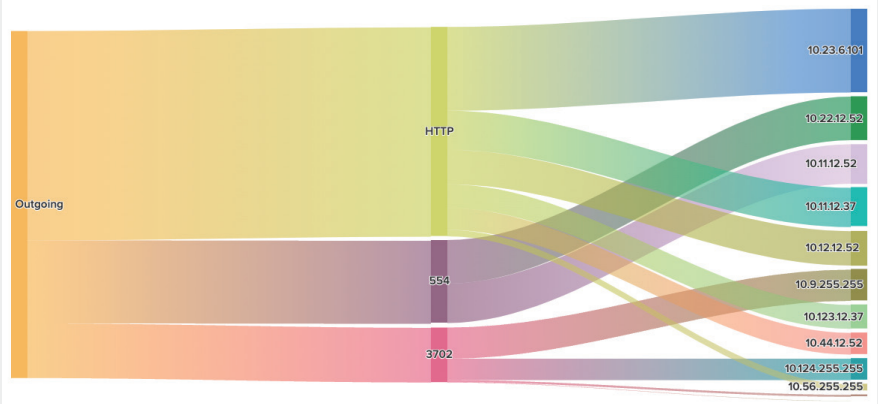


パケットを解析して各デバイスの IP アドレス、MAC アドレスはもちろん、製造元、型番、OS 情報、ファームウェアなどの情報を詳細に確認できる。
特定のバージョンやファームウェアに脆弱性があった場合でも、Armis では脆弱性があるデバイスについてのみアラートが上がるので、対処する対象を絞り効果的な管理ができる。



検知したデバイスの詳細情報と、CVE やその他の脆弱性データベースの情報を照合して、環境に存在するデバイスの脆弱性リスクを効率よく確認できる。

また、この脆弱性を修正するための情報も合わせて提供されるので、迅速にリスクに対応することが可能。



各デバイスの通信先、プロトコル、通信量、パケットロス、再送率、遅延などの情報が視覚的に確認できる。

あるデバイスが特定のアドレスに大量のパケットを送信しているなど、視覚的に異常を発見することができる。

SC Awards finalist BEST THREAT DETECTION TECHNOLOGY
2020 FORTRESS CYBER SECURITY AWARD
Forbes THE Cloud100 2020
BlueBorne CDPwn URGENT/11 TLStorm
GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2022
THE CHANNEL CO. CRN SECURITY 100 2023

ARMIS アルミス・ジャパン
japan@armis.com