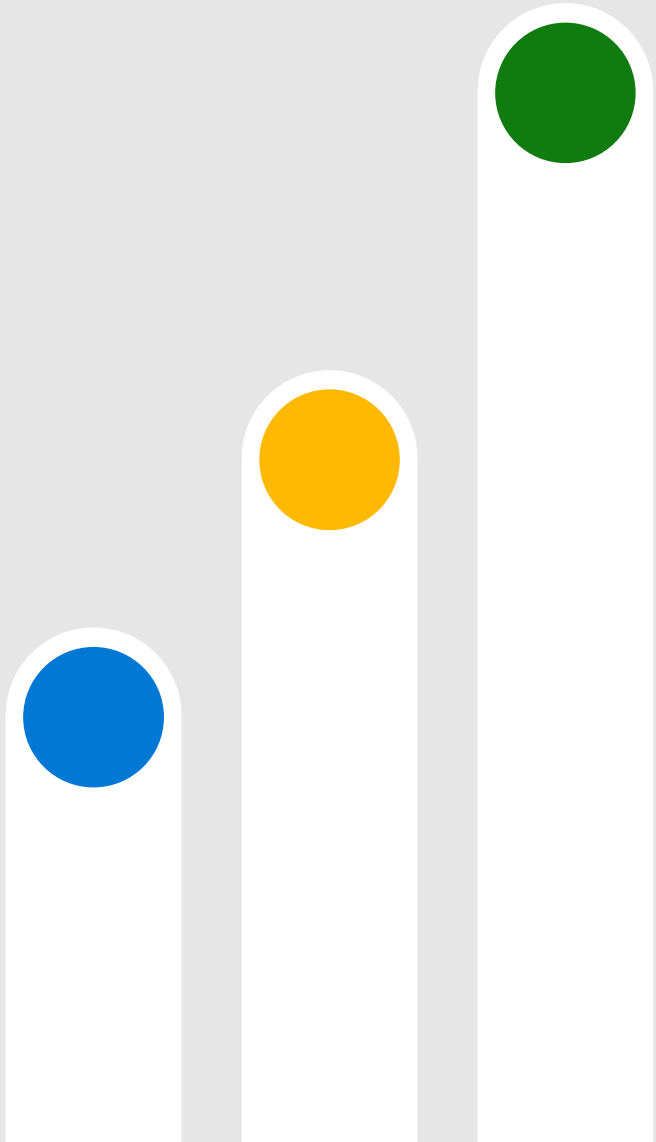
Microsoft Security

Microsoft Defender for IoT

Takehiro Hirai
IoT Technical Specialist
GPS - Global IoT Partner Ecosystem

アジェンダ

- IoT セキュリティ について
- Microsoft Defender for IoT の概要
- ワークショップ について



Microsoft の セキュリティ ミッション :

より安全な世界を実現し、組織のデジタル変革を可能にする

Microsoft にとって セキュリティ は、3,500人以上の体制による 100億ドル規模の ビジネスであり、5つの Gartner Magic Quadrant と 7つの Forrester Wave Report において Leader に選ばれています

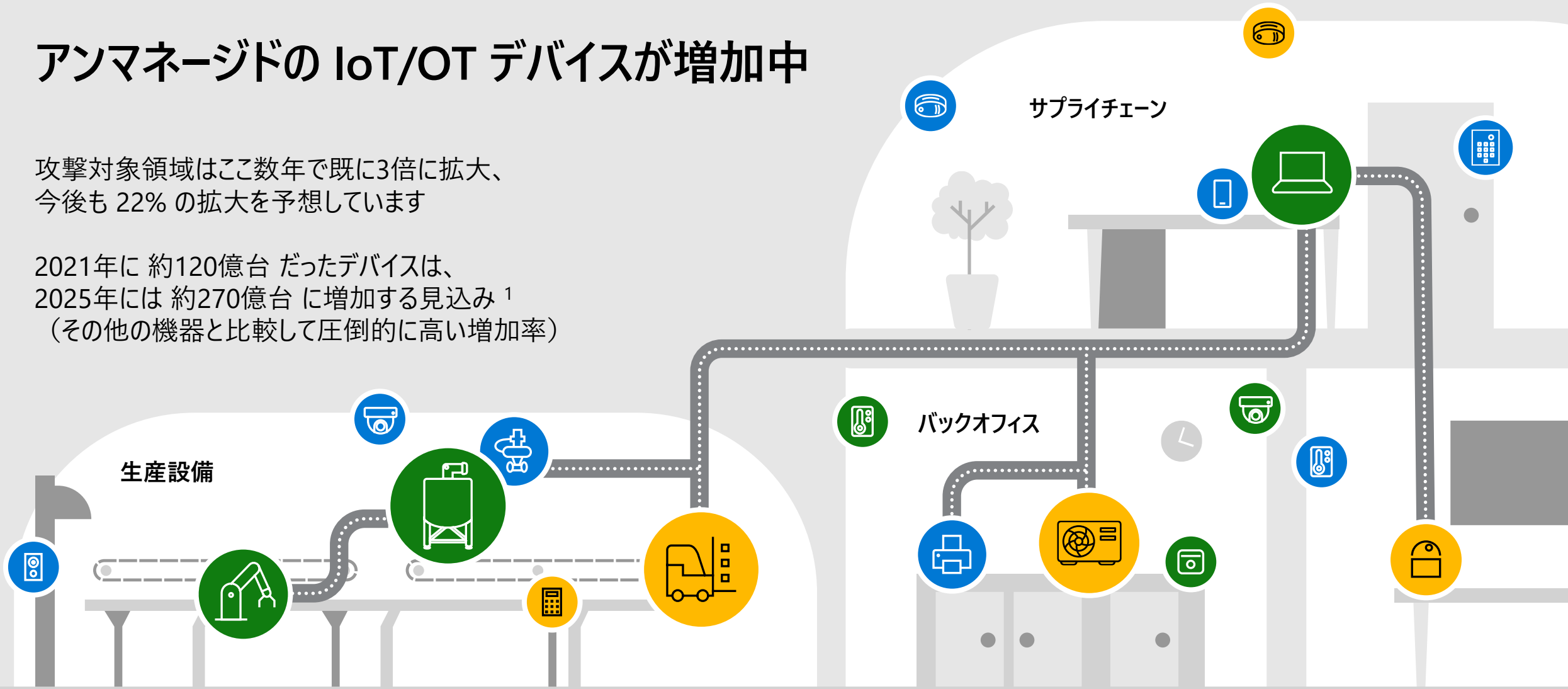
最近のセキュリティ関連の買収として、CyberX、ReFirm Labs、RiskIQ、CloudKnox などがあります

今後5年間でサーバーセキュリティへの投資を4倍の200億ドルへ拡大します

アンマネージドの IoT/OT デバイスが増加中

攻撃対象領域はここ数年で既に3倍に拡大、
今後も 22% の拡大を予想しています

2021年に 約120億台 だったデバイスは、
2025年には 約270億台 に増加する見込み [1]
（その他の機器と比較して圧倒的に高い増加率）



1. https://iot-analytics.com/number-connected-iot-devices/

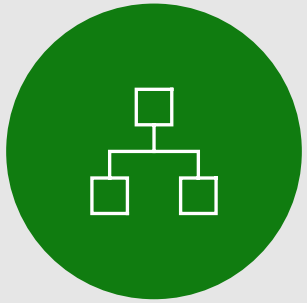
OT/IoT セキュリティ チャレンジ - 特別な考慮事項

数量

多くのビジネスライン
デジタルトランスフォーメーションの加速

セキュリティアナリストあたりの
管理デバイス数の増加

ビジネスへの影響



異なるテクノロジー
多くのソリューション

様々な入力ソースからの
インシデントの把握

優先順位

重要なインシデントの特定
アラートの重要度決定

内容に基づく
インシデントの優先順位付け

実際の IoT 攻撃事例

ZDNet

MUST READ: Firmware attacks are on the rise and you aren't worrying about them enough

NASA hacked because of unauthorized Raspberry Pi connected to its network

NASA described the hackers as an "advanced persistent threat," a term generally used for nation-state hack

DARKReading | SIGN UP FOR OUR NEWSLETTERS

Verkada Breach Demonstrates Danger of Overprivileged Users

In re-evaluating supply chains, companies should classify vendors with super admin privileges to devices or backdoors as a significant threat.

ZDNet

Hackers are attacking smart building access systems

More than 2,300 building access systems can be hijacked due to a severe vulnerability left without a fix.

ZDNet

Triton hackers return with new, covert industrial attack

Traces of a hacking group behind the destructive Triton malware have been found at a new infrastructure facility following an infamous attack in the Middle East.

Bloomberg

Hackers Breached Colonial Pipeline Using Compromised Password

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant

The New York Times

'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town

For years, cybersecurity experts have warned of attacks on small municipal systems. In Oldsmar, Fla., the levels of lye were changed and could have sickened residents.

CIO, CISO が直面する IoT/OT 関連の主要課題

IoT の普及とリスク

68% の組織が、IoT/OT はビジネスイノベーション、戦略的目標の支援に不可欠と回答[1]

60% が、IoT/OT のセキュリティが IT/OTインフラの中で最もセキュリティが低い側面の1つと捉えている[1]

31% の組織が、セキュリティの懸念により IoT/OT のプロジェクト採用の延期、制限、中止を経験

技術的なギャップ

71% IoT/OT デバイスの完全なインベントリが存在しない割合[1]

70% IoT デバイスが安全である（脆弱性が緩和され、セキュアな設定が行われている）という確信が平均以下の割合[1]

61% IoT デバイスのリスクの特定に関する技術的な信頼度が平均以下の割合[1]

1. The State of IoT/OT Cybersecurity in Enterprise Organizations, Ponemon Institute, October 2021

既存ソリューションの課題

ファイアウォール

ネットワーク
アクセス管理

脆弱性
スキャナ

エージェント

境界保護のみ

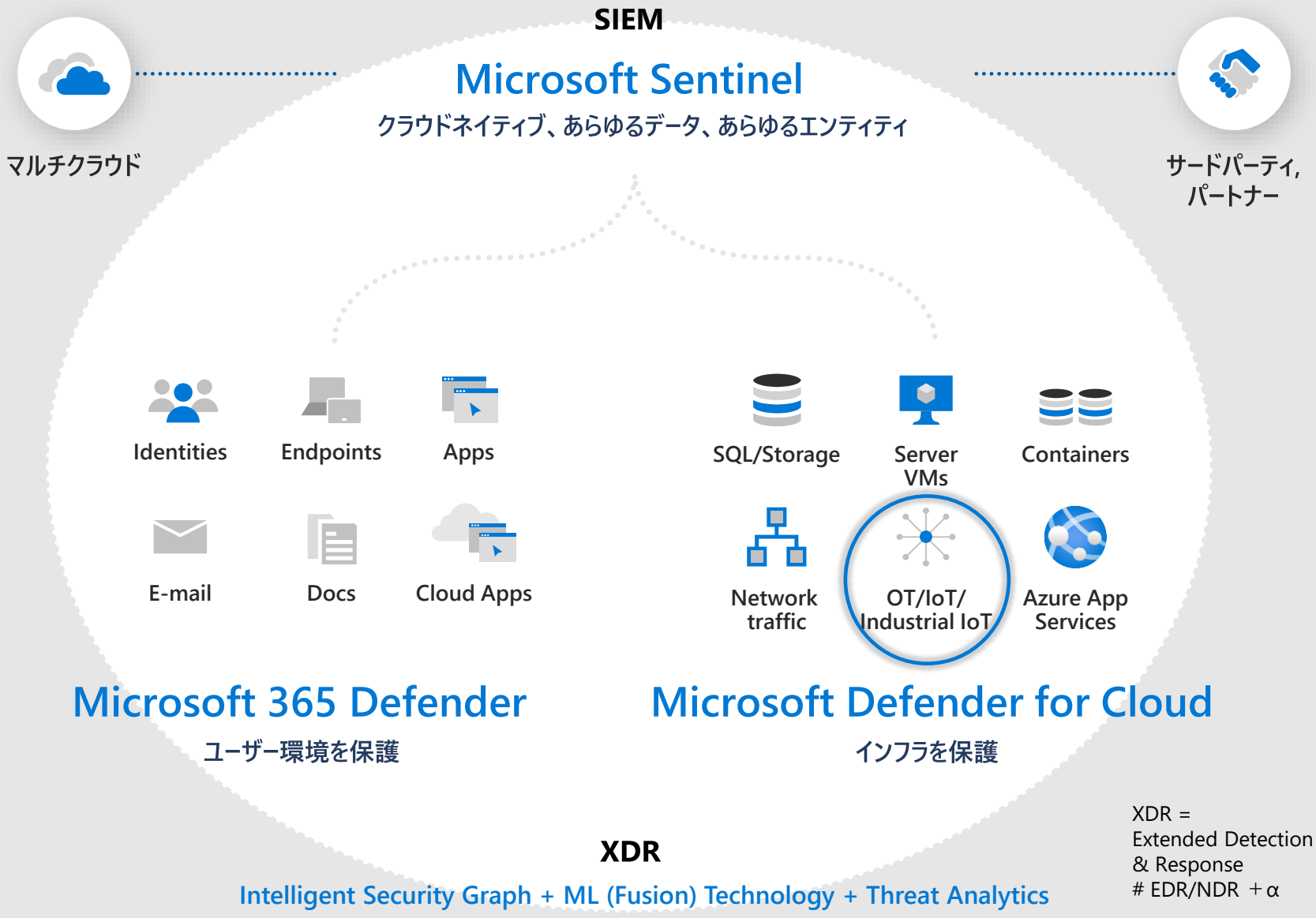
複雑な設定とメンテナンス

限定的な視認性

IoT への理解度の低さ

新しい脅威の検出不可

Microsoft が提供する、統合されたセキュリティ運用エクスペリエンス



SIEM
Security Information
& Event Management

ログ集約 | 相関分析 | インシデント管理

SOAR
Security Orchestration,
Automation, & Response

製品間連携 | 自動化 | 対処の管理

XDR =
Extended Detection
& Response
# EDR/NDR ＋α

ゼロトラスト IoT を実現するためのサービス群

Azure IoT Hub & DPS
IoT アプリケーションとそれが管理するデバイス間の安全かつ信頼性の高い通信を実現

Device Update for IoT Hub
IoT デバイスに over-the-air (OTA) アップデートを展開

Microsoft Defender for IoT
すべての IoT/OTデバイスに対するエージェントレス & エージェントベースのアセット検出、脆弱性管理、脅威検出

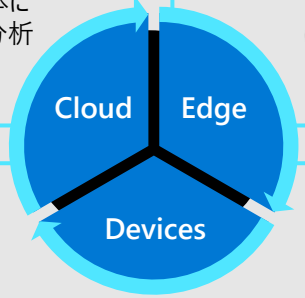
Microsoft Sentinel
業界初のクラウドネイティブな SIEM/SOAR を使用した、企業全体に対するインテリジェントなセキュリティ分析

Azure IoT Edge
デバイス上に適切なソフトウェアが存在し、許可されたエッジデバイスのみが相互に通信出来ることを確認

Azure IoT SDKs
Azure IoT Hub との送受信、テレメトリの送信やメッセージ、ジョブ、メソッド、またはツイン更新を行うアプリケーションを構築

Azure RTOS
組み込み開発者がリソースに制約のあるデバイス向けにリアルタイムアプリを構築可能にする、最先端のマルチスレッドとミドルウェアを備えたリアルタイム OS カーネル

Windows IoT Enterprise
IoT 向けに エンタープライズクラスの性能、セキュリティ、そして管理性



Azure Sphere
ハードウェア、OS、クラウドの各コンポーネントを含む、包括的な IoT セキュリティソリューション

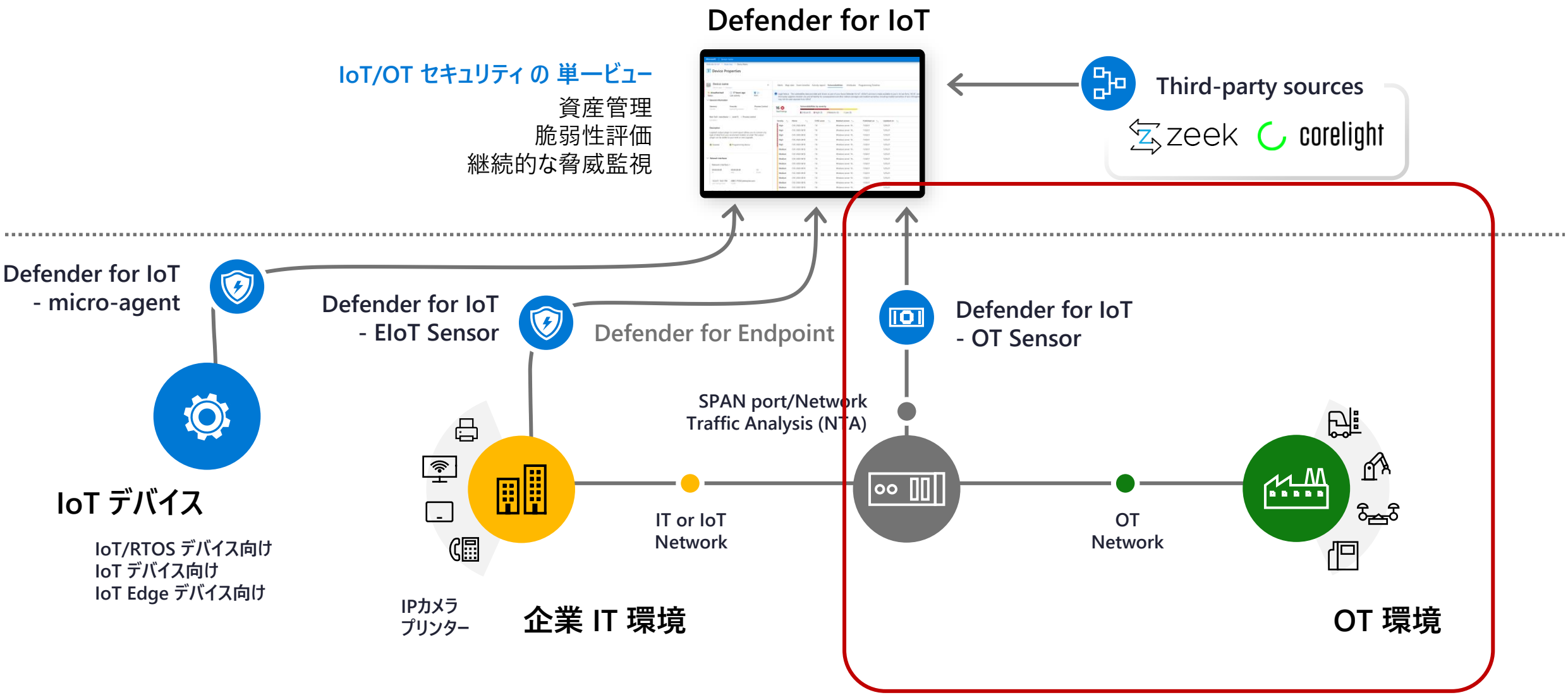
Azure Sphere Guardian
既存の機器に対して安全な接続を可能にすることで、ブラウンフィールドのセキュリティを強化

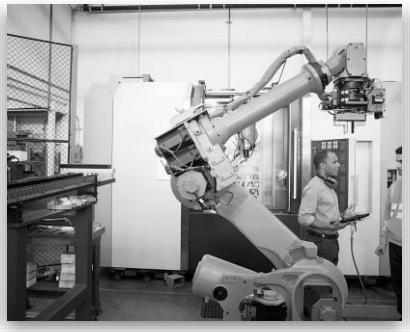
Azure Percept
包括的で使いやすい エッジ AI ソリューション にセキュリティ要素を追加したプラットフォーム

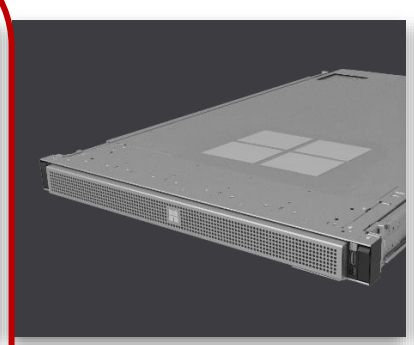
Edge Secured-Core Certified
認定デバイスはデバイスアイデンティティー、セキュアブート、OSハードニング、アップデート、データ保護、脆弱性開示、セキュリティエージェントなどのセキュリティ関連要件を満たす

Microsoft Defender for IoT

Microsoft Defender for IoT - 多様なデータソースを幅広くカバー





センサー + 制御 | センサーからインタラクティブへ | 統合プラットフォーム | グローバルスケール

Microcontroller
Azure RTOS

IoT Devices
Azure IoT Device SDK

Edge Devices
Azure IoT Edge

Edge Appliances
Azure Stack Edge
Azure Stack HCI

Edge Stack
Azure Stack Hub

Hyperscale Cloud
Edge Regions

Defender for IoT - OT sensor

Defender for IoT - EIOT sensor

Defender for IoT - micro-agent (agent)

Azure Sphere

Firewall Manager

Defender for Endpoint

For Servers

For App Services
For Storage
For SQL
For Key Vault
for Container
for RM
For DNS

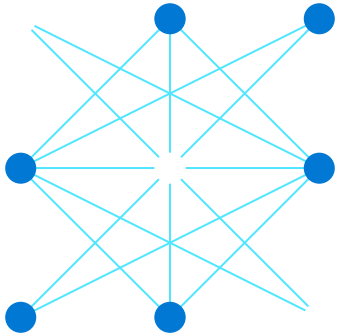
Defender for Cloud for K8S

Defender for Cloud

Microsoft Defender for IoT - OT Sensor

IoT/OT 環境向け エージェントレス セキュリティ
IoT/OT 環境を意識した行動分析と脅威インテリジェンスを備えた NDR (Network Detection & Response)

エージェントレス セキュリティ
生産への影響は “ゼロ”
1日未満の作業で導入が可能

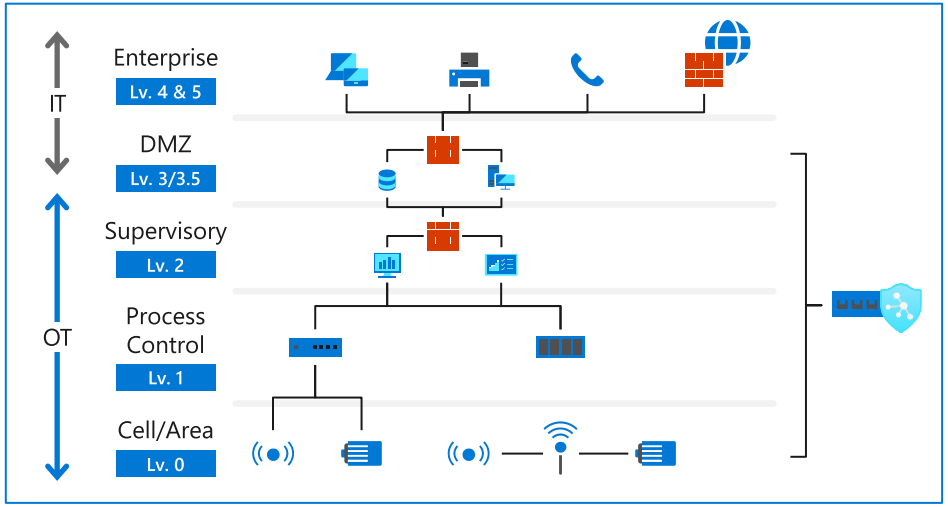


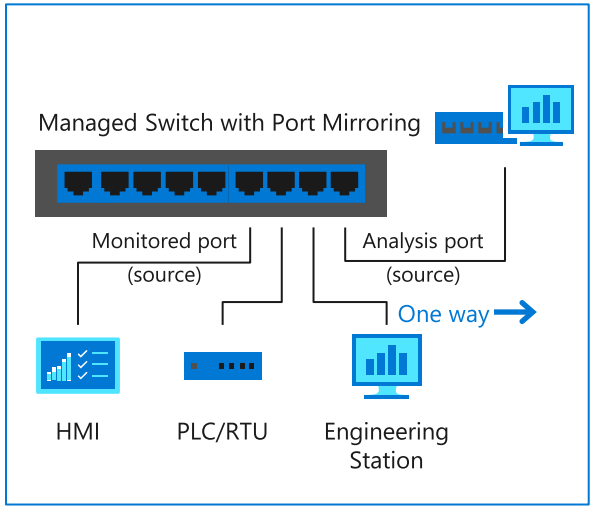
レガシー及び独自のデバイスにまたがる
IoT/OT資産、脆弱性、脅威の
継続的な可視化

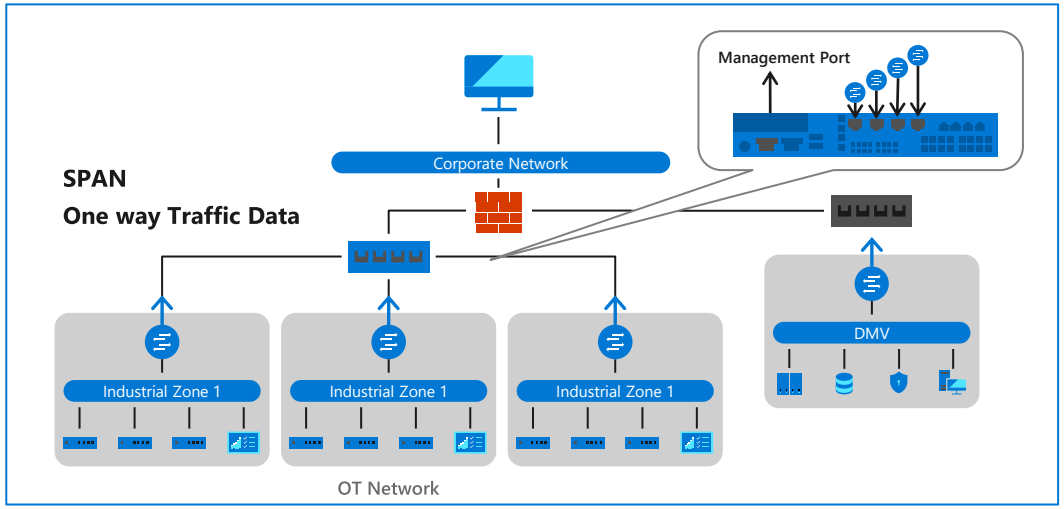
Microsoft Sentinel や既存の SOC ツール
との統合により、IT/OTの統合的な
モニタリングとガバナンスを実現

Microsoft Defender for IoT - OT Sensor

- センサー：物理、または仮想アプライアンス
- ネットワーク・スパン・ポート/ネットワーク・タップ に接続
- 複数のスイッチへの接続
- 完全なパッシブ型の スマートセンサー
- PCAP 分析機能（パケットキャプチャ分析機能）
- オンプレミスの管理用 Web コンソール、または Microsoft Defender for IoT による管理
- SIEM との統合







Microsoft Defender for IoT - OT Sensor

“すべて” の IoT/OT デバイスを検出

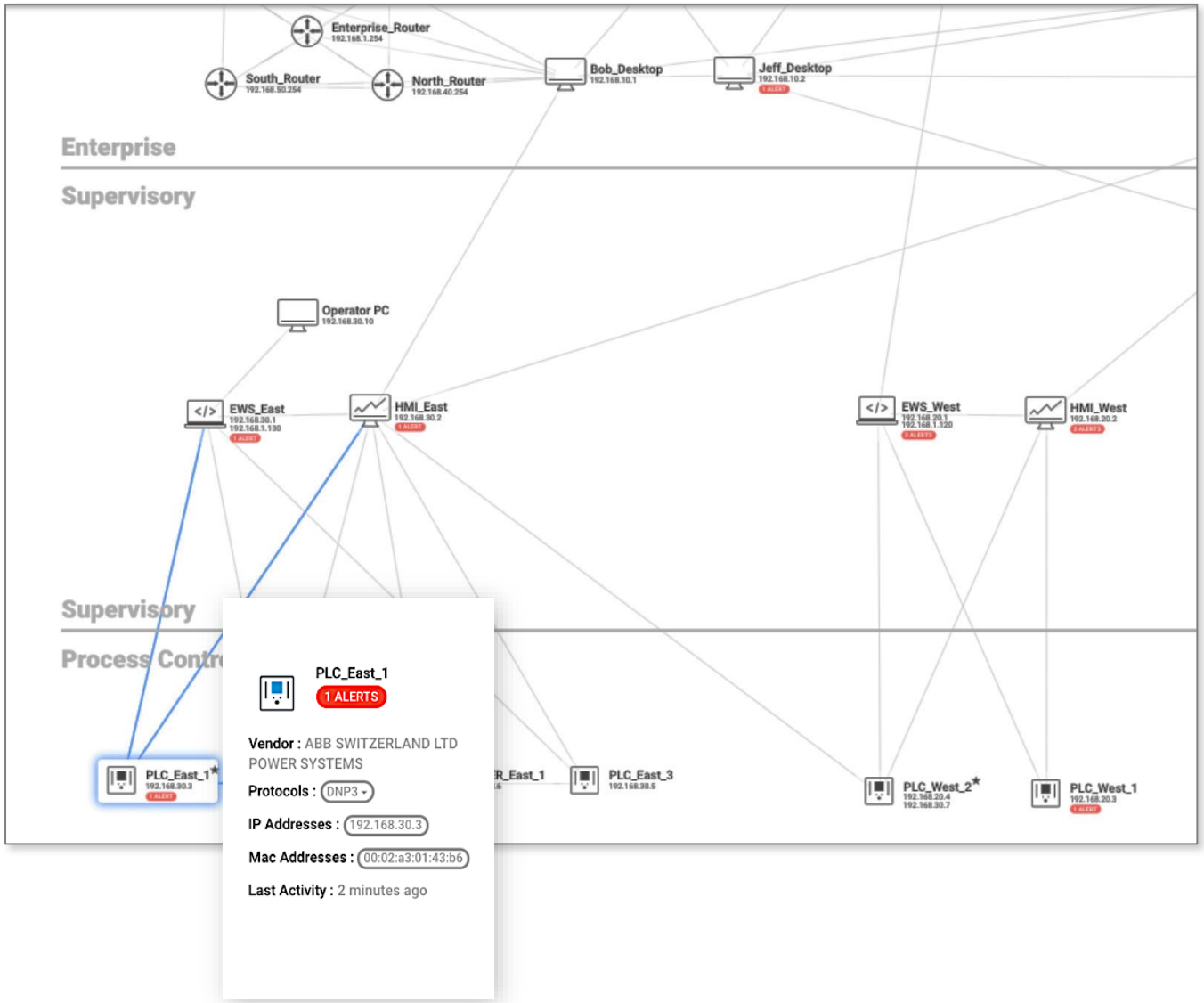
What is it?

パッシブでエージェントレスのセンサーにより
収集された産業プロトコルを分析、デバイスの
詳細情報を特定、デバイスインベントリ、
デバイスマップを自動的に作成

製造元、種類、シリアル番号、
ファームウェアレベル、IP または MAC アドレス

Benefits

IoT/OT ネットワーク トポロジ全体が視覚化、
デバイスの通信パスを通じて運用上の問題
(例: デバイスの構成ミス) の根本原因を迅速
に特定



Microsoft Defender for IoT - OT Sensor

リアルタイムIoT/OT脅威アラート
- 5つのエンジンと機械学習を利用した分析を実施

アラート カテゴリ

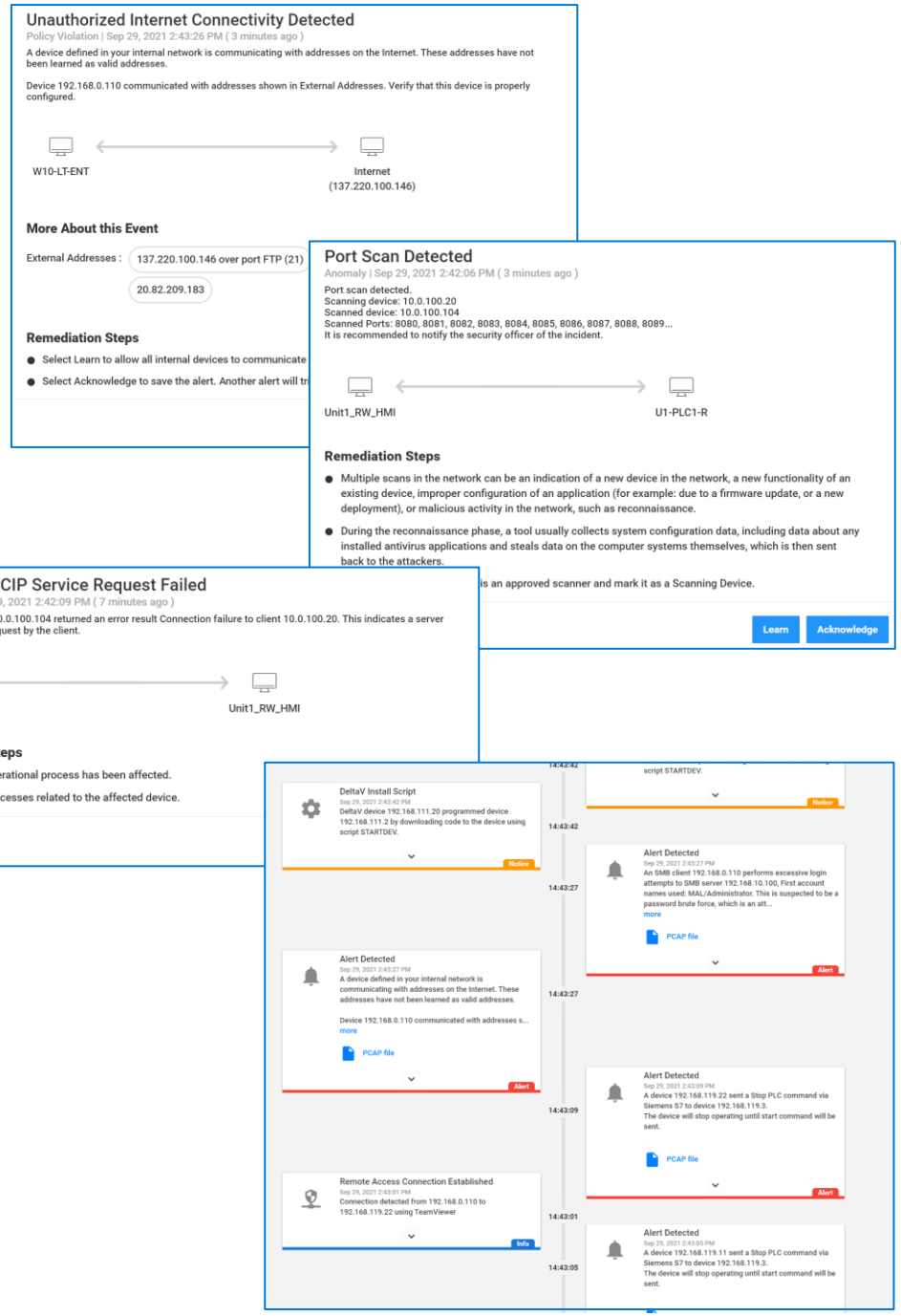
Policy Violation
ポリシー違反エンジンによる
以前に学習したトラフィックからの逸脱の検出をトリガー

Protocol Violation
プロトコル違反エンジンによる
検出プロトコル仕様に準拠していないパケット構造またはフィールド値の検出をトリガー

Operational
運用エンジンによる
ネットワークの運用上のインシデントまたはデバイスの誤動作の検出をトリガー

Malware
マルウェア対策エンジンによる
悪意のあるネットワーク アクティビティや既知の攻撃の検出をトリガー

Anomaly
異常エンジンによる
逸脱 (ネットワークスキャンを想定外デバイスが行っているなど) の検出をトリガー



アラート一覧
https://docs.microsoft.com/ja-jp/azure/defender-for-iot/organizations/alert-engine-messages

Microsoft Defender for IoT - OT Sensor

リスクアセスメント レポート

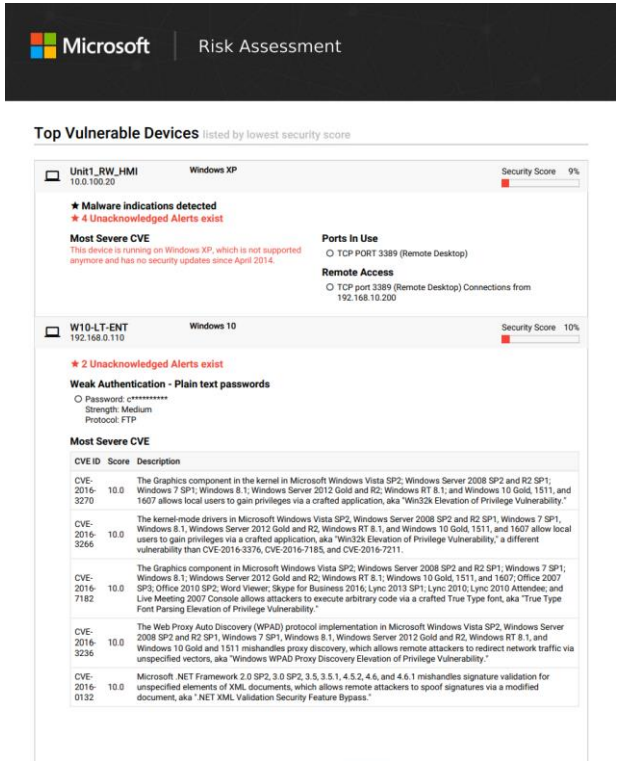
What is it?

センサーにより収集された情報からOT環境の
リスクアセスメントレポートを作成

・デバイス、ネットワークデバイスのセキュリティスコア
・デバイスの内訳 (脆弱, 改善が必要, 保護)
・セキュリティおよび運用上の問題に関する分析情報

Benefits

1クリックでレポート (PDF) を作成



Microsoft Defender for IoT - OT Sensor

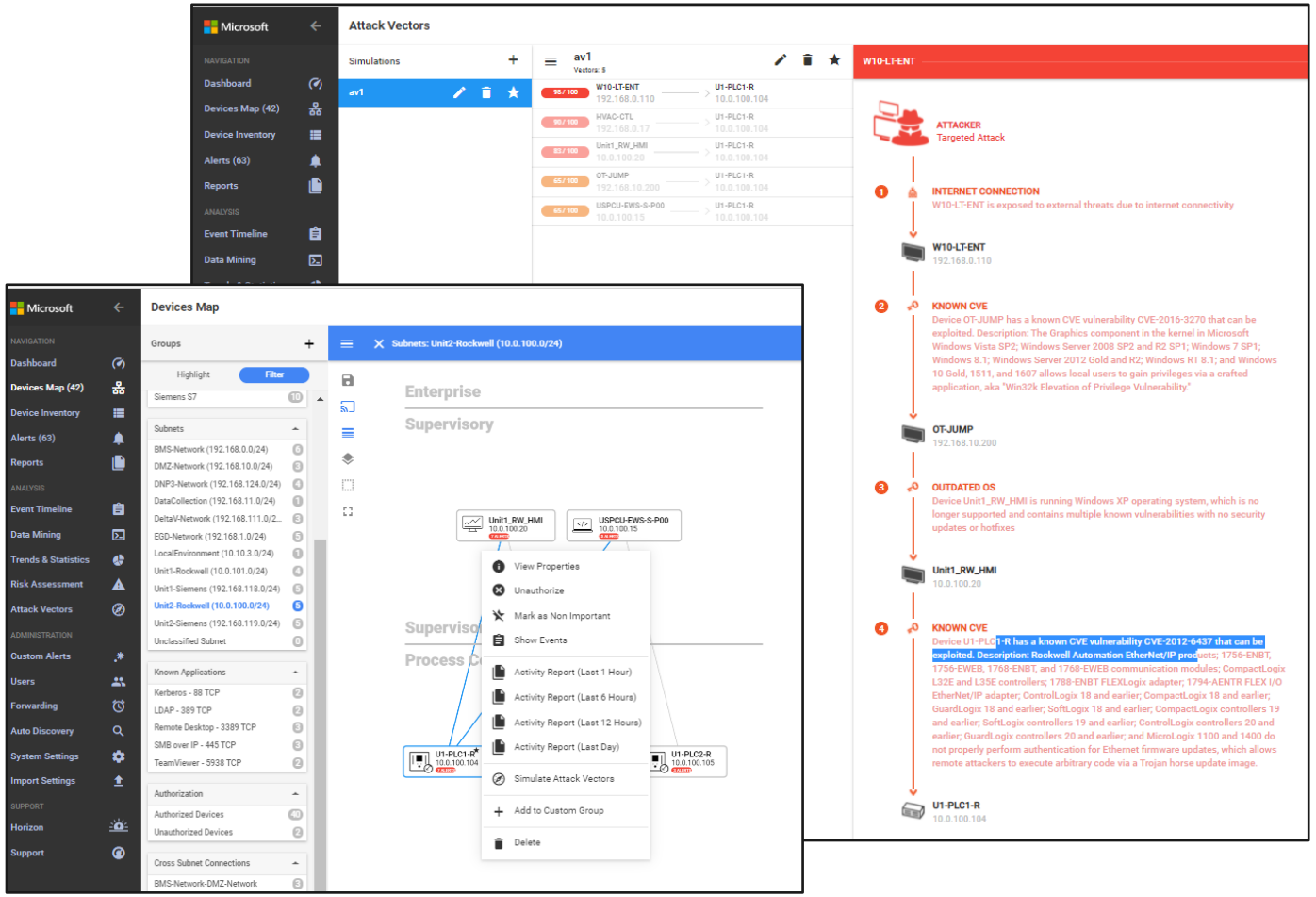
攻撃ベクトル レポート

What is it?

悪用されうるデバイスの脆弱性情報をもとに
攻撃ベクトルをリアルタイムで計算、
特定ターゲットへの攻撃実現可否を分析

Benefits

攻撃シミュレーションを実行することなくリスクを
評価し、攻撃シーケンスを軽減する情報を入手

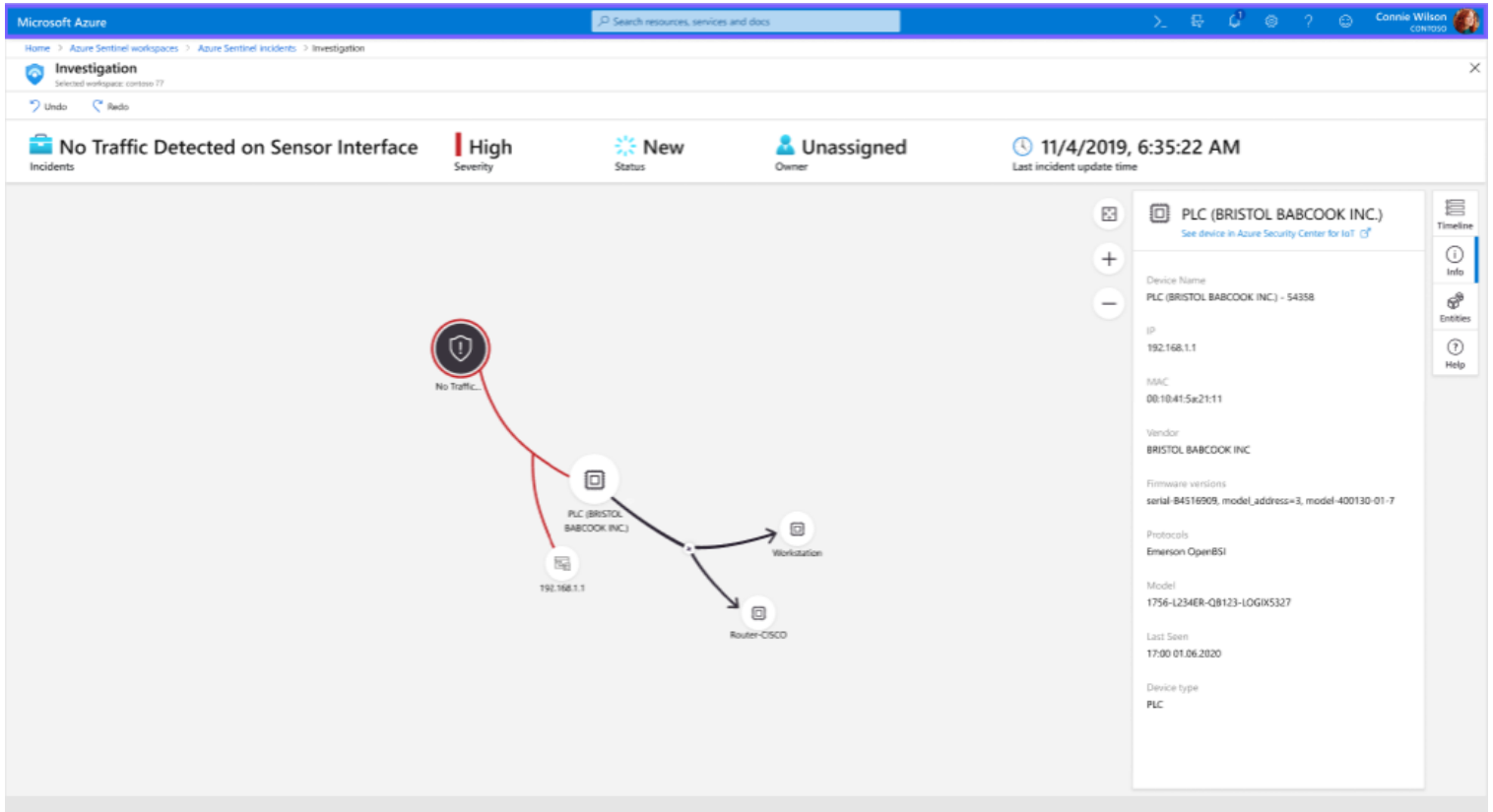


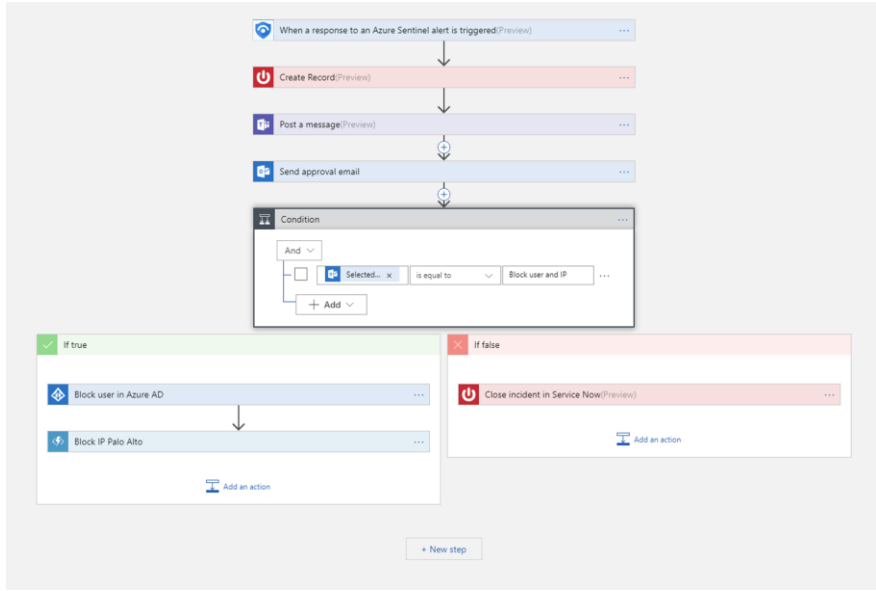
Microsoft Defender for IoT - OT Sensor

Microsoft Sentinel (SIEM/SOAR) との連携

→ IT/OT 境界を越えた攻撃を含む多段階攻撃を識別

→ (OT に特化した) SOAR プレイブック





Microsoft Defender for IoT - micro-agent

ソースコード

- プロジェクトの構築段階で micro-agent をファームウェアに組み込むことが可能
- ソースコードをカスタマイズし、必要なものだけを取り込むことが可能
- 操作系を絞った制限付きデバイスにも対応

バイナリ パッケージ

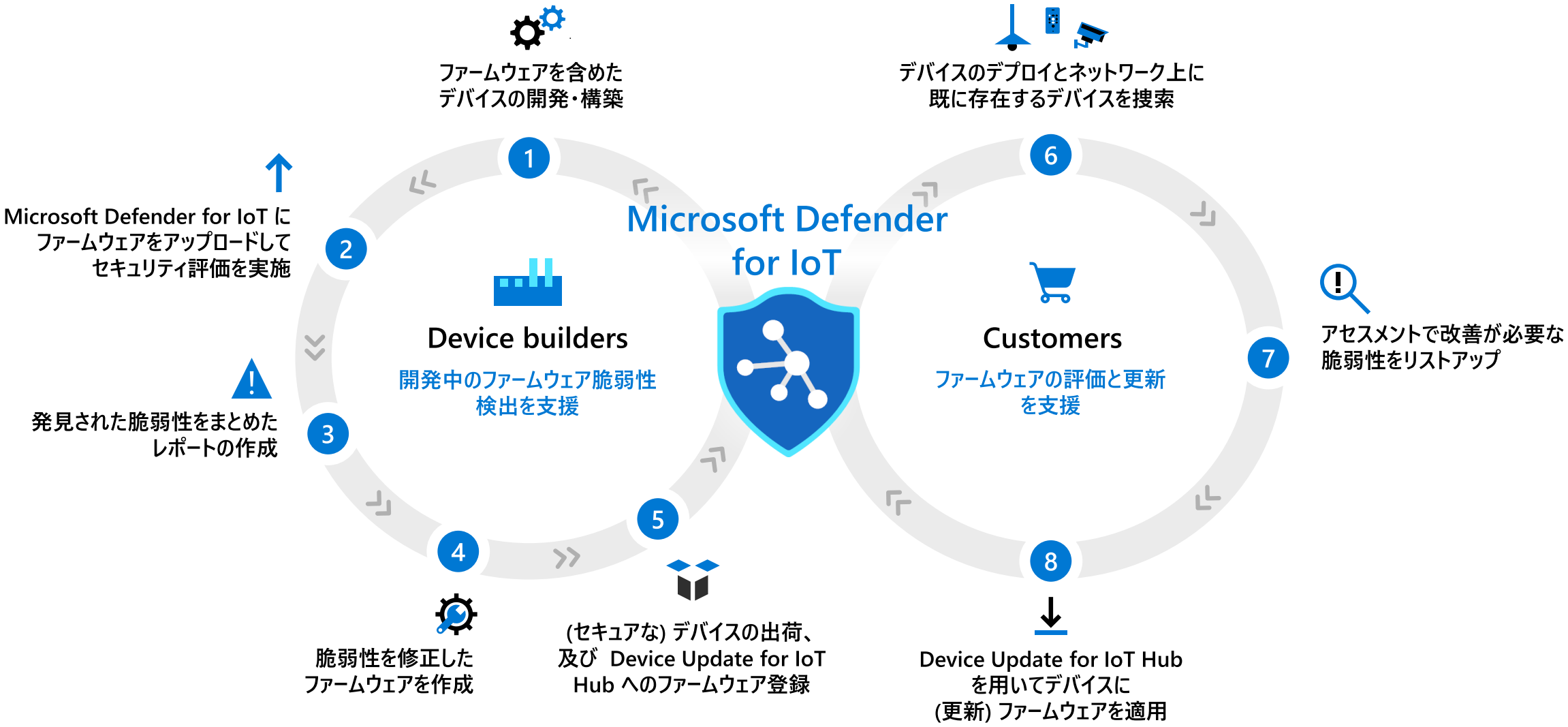
- 一般的な OS を搭載する IoT デバイスに対し、導入後のインストールをサポート

スタンドアローン、または Azure IoT と統合

- スタンドアローンエージェントとして、または Azure IoT エコシステムと統合してデプロイすることが可能
- **Azure RTOS** に組み込み
- **Azure IoT Edge** に統合

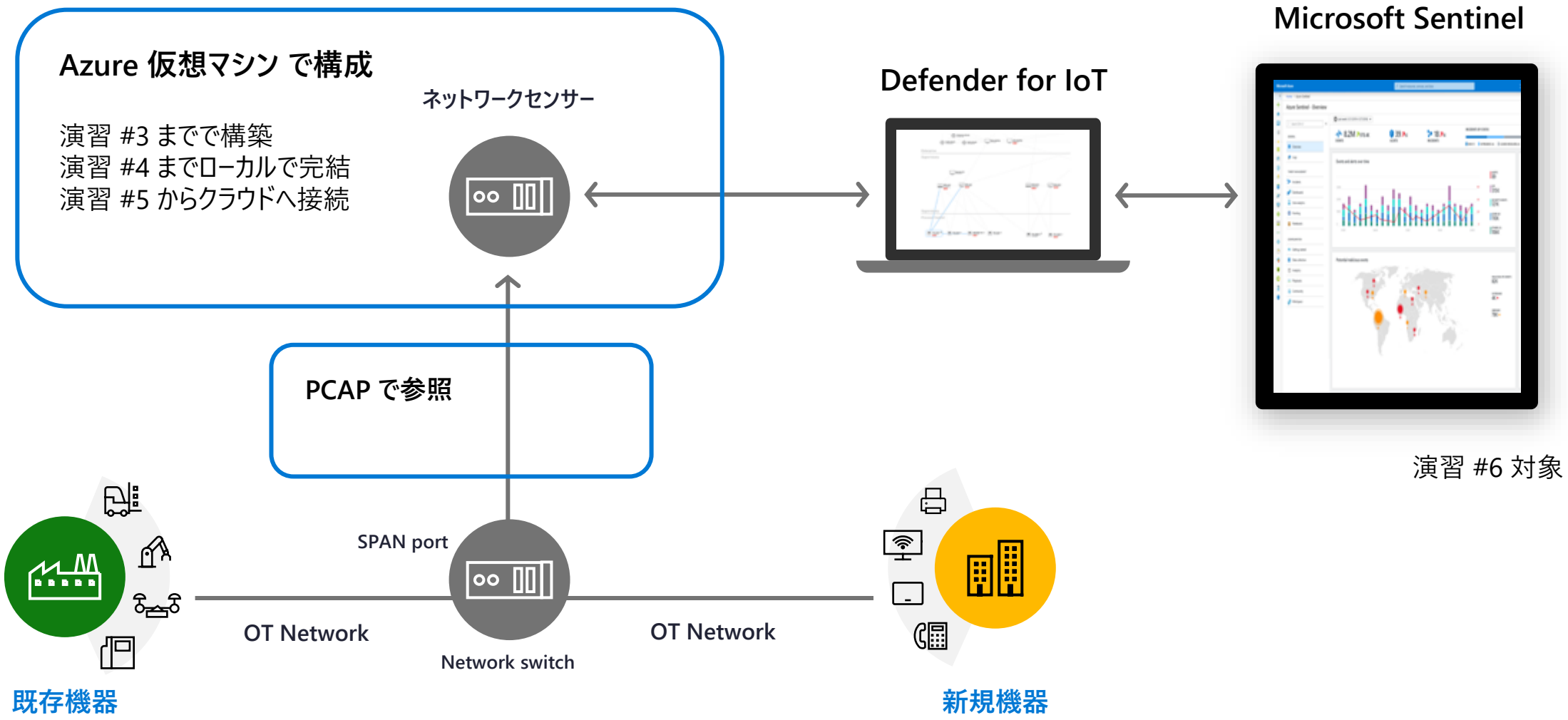
https://docs.microsoft.com/ja-jp/azure/defender-for-iot/device-builders/overview

Defender for IoT に Refirm Labs サービス を統合



ワークショップ について

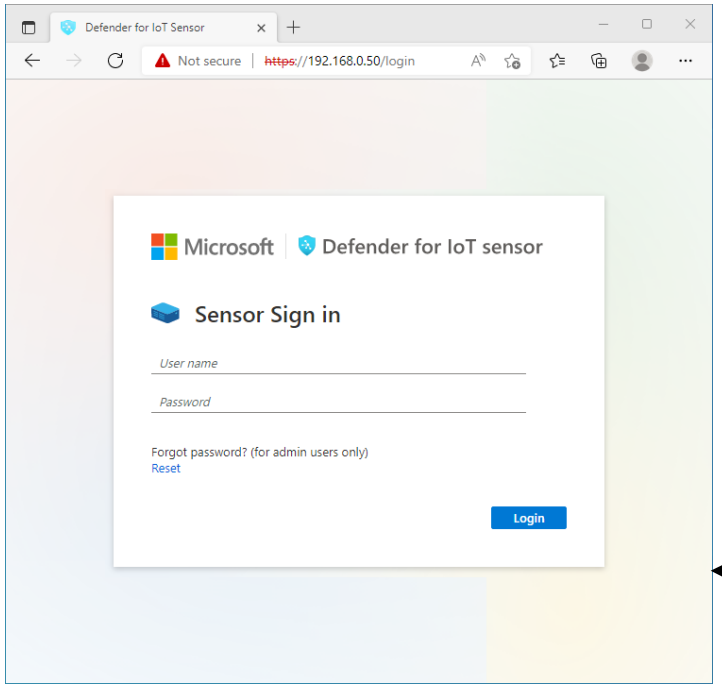
ワークショップ の構成



Defender for IoT - OT sensor に触れていただく

ワークショップ の構成 - 仮想マシン

仮想マシン (Standard_D4s_v3) - Windows 10



Hyper-V

仮想マシン (Defender for IoT Sensor)

eth0
(192.168.0.50)

eth1

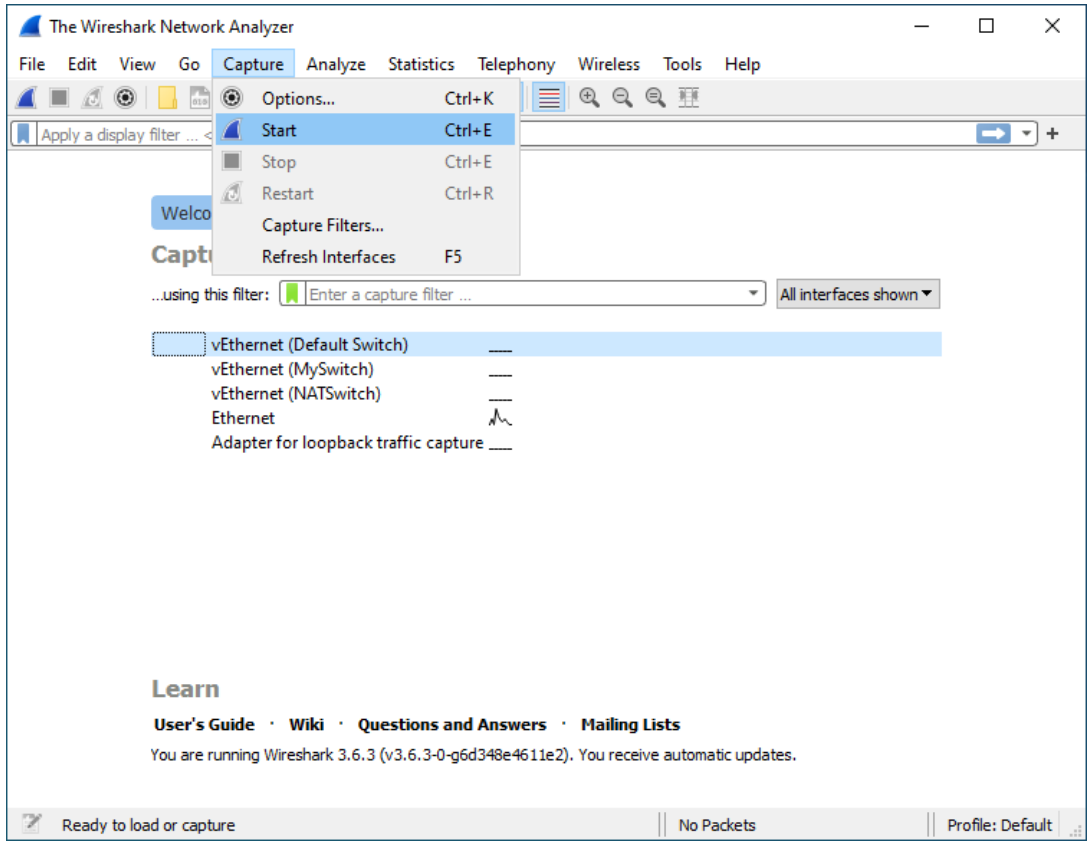
VMSwitch (NAT Switch)
(192.168.0.1)

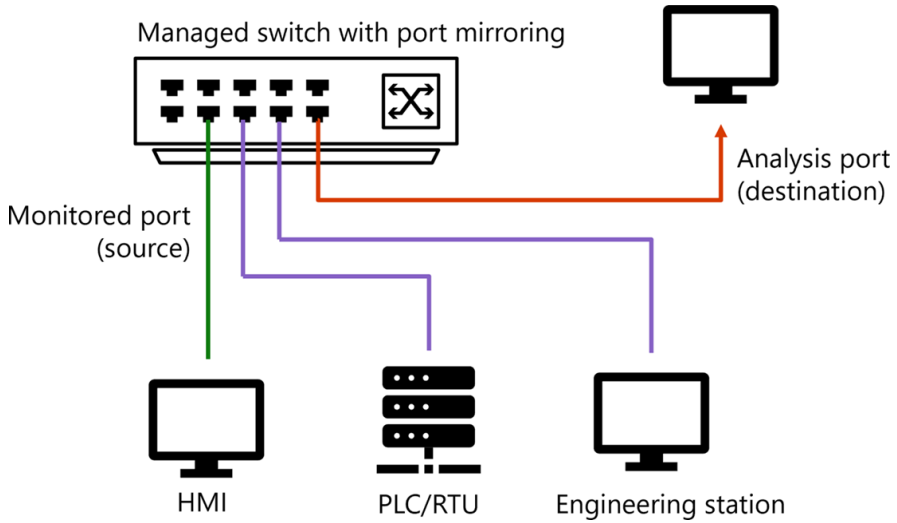
VMSwitch (My Switch)

RDP 接続

PCAP の取得について - Wireshark

- PCAP の取得自体は比較的簡単
- 期待通りのキャプチャが可能なネットワーク構成を組む方がやや難しい





https://docs.microsoft.com/ja-jp/azure/defender-for-iot/organizations/how-to-set-up-your-network

Defender for IoT (sensor) 10.5.x / 22.1.x について

- → 今後の新機能やクラウド連携の拡張は 22.x に対して実施 (日本語対応含む)
- → 10.5.x もまだサポート中（今回は 複数の PCAP ファイル利用のため、10.5.5 を利用）

https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/release-notes

ワークショップで用いる ファイル について

→ https://aka.ms/md4iotiso # Defender for IoT 10.5.x の ISO ファイル

→ https://aka.ms/md4iotpcaps # PCAP ファイル (解凍して利用)