重要インフラや産業制御システムはこう守れ！

～ ゼロトラスト時代のエンドツーエンドセキュリティ対策

花村 実, Chief Security Advisor
CISSP, CCSP, C|CISO, MBA, CFE
Microsoft Corp.

製造業は急速に変化

物理

デジタル変革

デジタル

生産資産

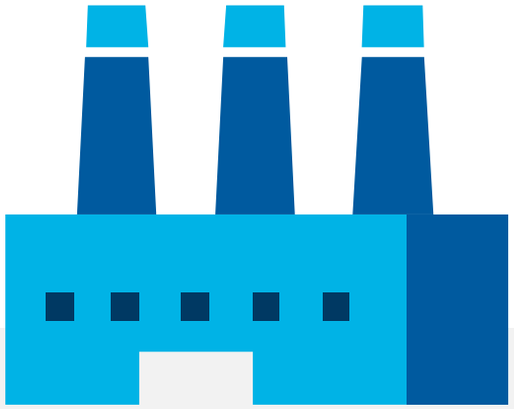
原材料および製品

予防的メンテナンス

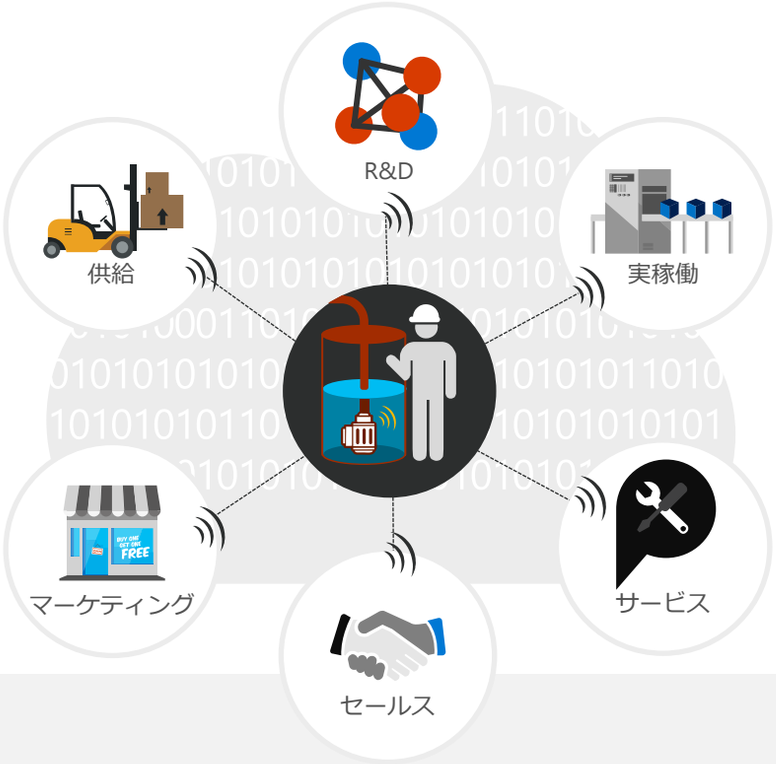
スマートな製品

サービス エコシステム

オンライン消費者



00110100110
0110110101011



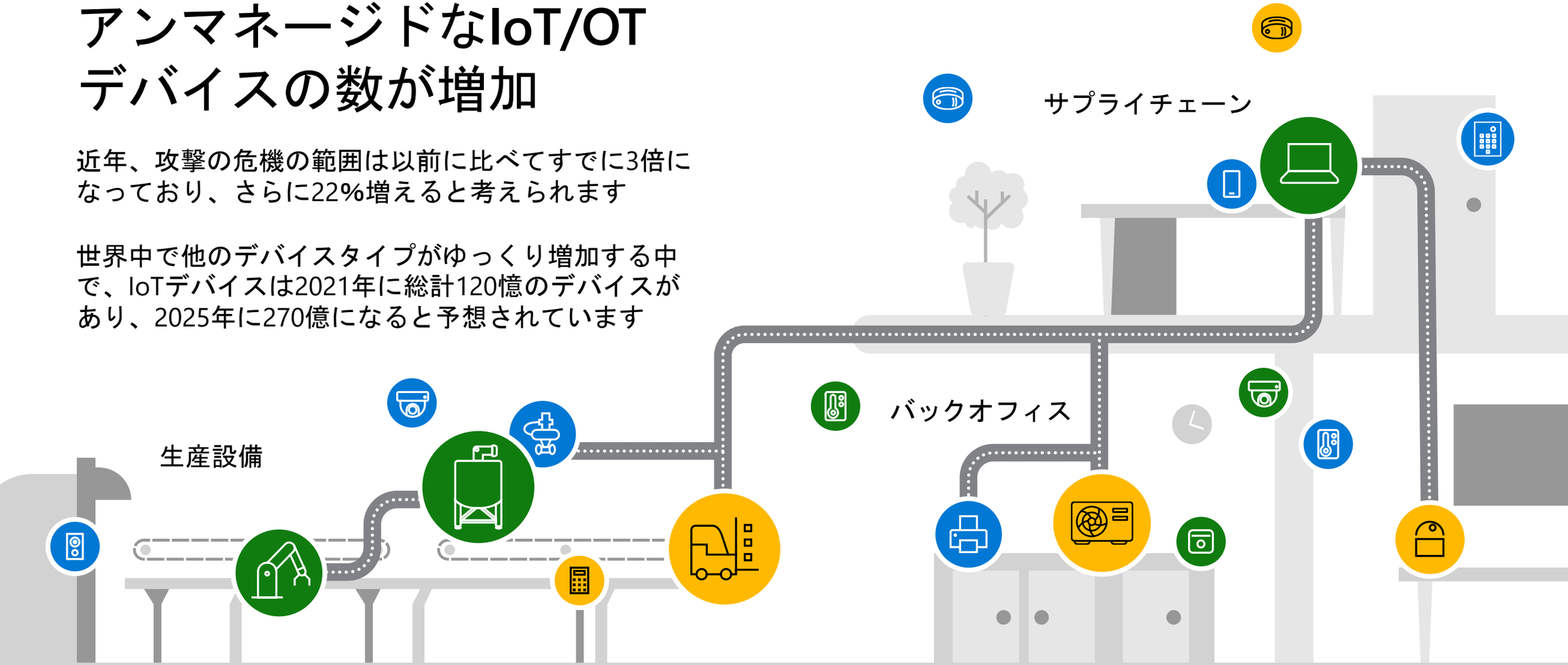
00110100110
0110110101011

現代の製造業者は、顧客重視主義の採用、
迅速な革新、俊敏性の強化を目指す

アンマネージドなIoT/OTデバイスの数が増加

近年、攻撃の危機の範囲は以前に比べてすでに3倍になっており、さらに22%増えると考えられます

世界中で他のデバイスタイプがゆっくり増加する中で、IoTデバイスは2021年に総計120億のデバイスがあり、2025年に270億になると予想されています



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


Microsoft | News Center マイクロソフトについて 製品情報 ブログ & コミュニティ 報道資料

デジタルテクノロジとウクライナでの戦争について

2022年3月2日 | Japan News Center

ブラッド スミス (Brad Smith)
プレジデント 兼 副会長

※本ブログは、米国時間 2 月 28 日に公開された "Digital technology and the war in Ukraine" の抄訳を基に掲載しています。

マイクロソフトの従業員は皆、悲劇的で非合法かつ不当なウクライナへの侵攻について、情報を常に確認しています。今回の出来事は、物理的な戦争のみならずサイバー戦争にまで至っており、ウクライナ中から恐ろしい映像が流れてくるだけでなく、表には見えないコンピュータネットワークへのサイバー攻撃やインターネット上での情報操作活動も起こっています。この件について、また当社の活動について、さまざまな問い合わせが増えてきたことから、このブログで簡潔にまとめることにしました。ここでは 4 つの分野、サイバー攻撃からのウクライナ保護、国家による情報操作活動からの保護、人道支援へのサポート、マイクロソフト従業員の保護について言及しています。

はじめに、マイクロソフトは民間企業であって、政府でも国家でもないということです。このような状況では、政府関係者と協議を進めることが特に重要となるため、今回当社はウクライナ政府をはじめ、欧州連合や欧州各国、米国政府、NATO、国連と絶えず緊密に連携を取っています。

サイバー攻撃からの保護

マイクロソフトでは、企業として政府や国家をサイバー攻撃から守ることがグローバルにおける主要な責任のひとつだと考えています。この役割がこれほどまで重要になるようなことは、ウクライナにおけるこの 1 週間以前にはほとんどありませんでした。ウクライナでは、政府やさまざまな組織、そして個人の方々が、マイクロソフトのお客様であるためです。

2 月 24 日のミサイル発射や戦車移動の数時間前、Microsoft Threat Intelligence Center (MSTIC) では、ウクライナのデジタルインフラに対する攻撃的かつ破壊的なサイバー攻撃が新たに発生していることを検出しました。マイクロソフトはウクライナ政府に対し、新たなマルウェアパッケージ (当

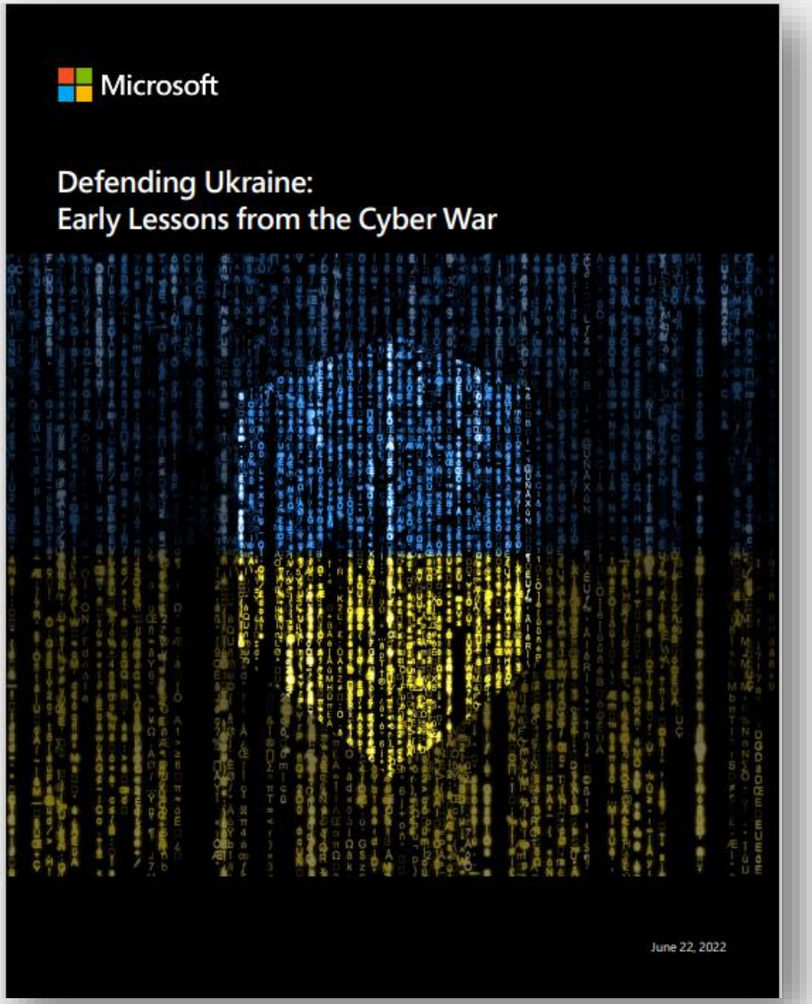
https://news.microsoft.com/ja-jp/2022/03/02/220302-ukraine-russia-digital-war-cyberattacks/


Microsoft | News Center マイクロソフトについて 製品情報 ブログ & コミュニティ 報道資料

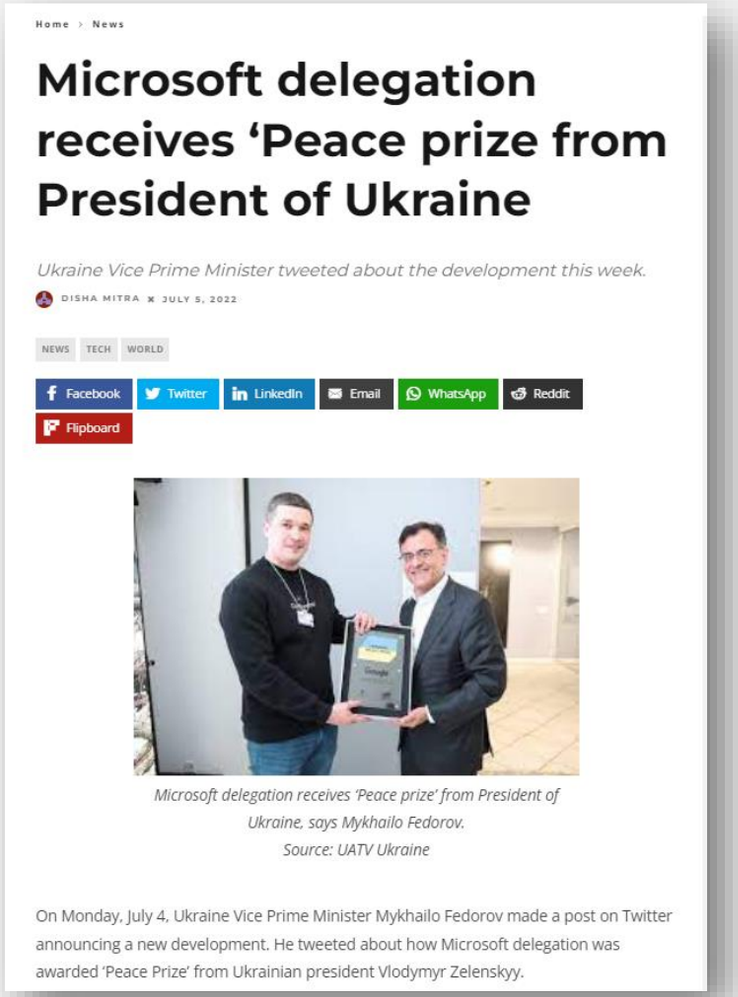
ウクライナを標的にしたサイバー攻撃を阻止

2022年4月11日 | Japan News Center

https://news.microsoft.com/ja-jp/2022/04/11/220411-cyberattacks-ukraine-strontium-russia/



https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/


Home › News

Microsoft delegation receives 'Peace prize from President of Ukraine

Ukraine Vice Prime Minister tweeted about the development this week.

DISHA MITRA × JULY 5, 2022

NEWS TECH WORLD

Facebook Twitter LinkedIn Email WhatsApp Reddit Flipboard

Microsoft delegation receives 'Peace prize' from President of Ukraine, says Mykhailo Fedorov.
Source: UATV Ukraine

On Monday, July 4, Ukraine Vice Prime Minister Mykhailo Fedorov made a post on Twitter announcing a new development. He tweeted about how Microsoft delegation was awarded 'Peace Prize' from Ukrainian president Vlodymyr Zelenskyy.

https://techstory.in/microsoft-delegation-receives-peace-prize-from-president-of-ukraine/

TRITONの攻撃フレームワーク

Remote Access Connection Established
Jun 10, 2018 10:33:22 PM
Connection detected from 192.168.30.10 to 192.168.30.1 using SSH

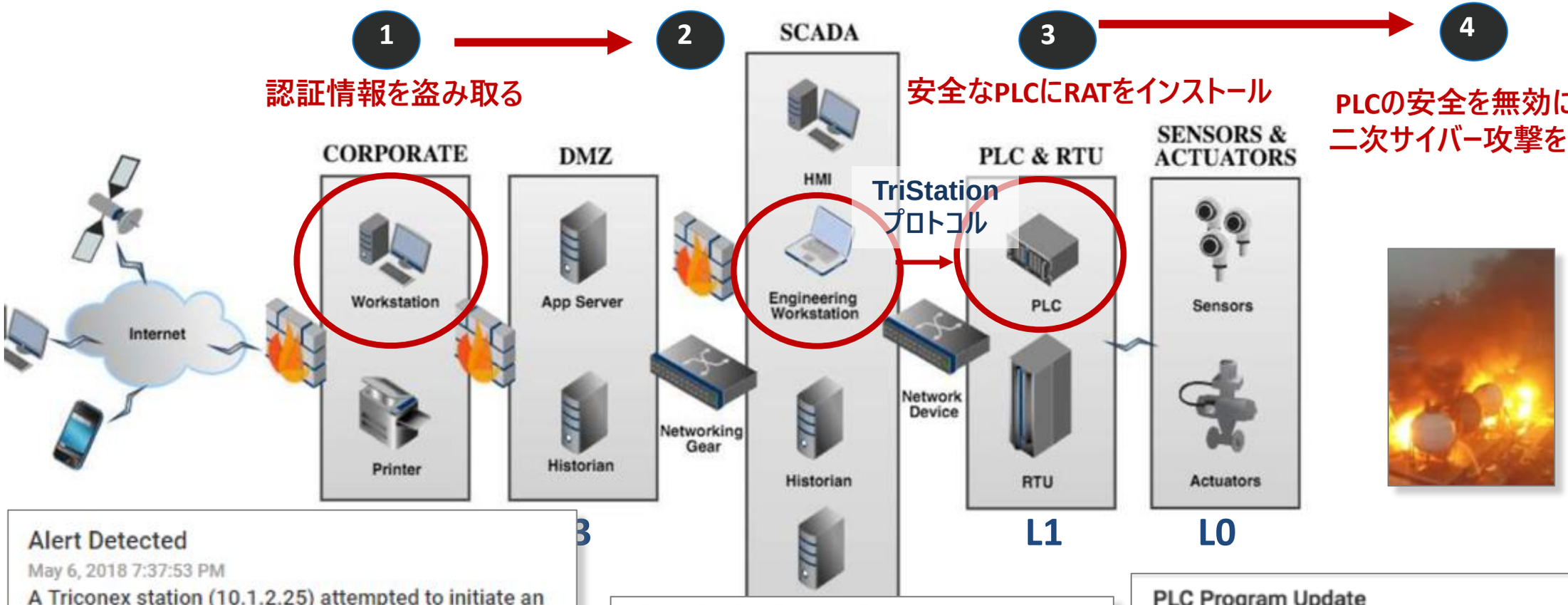
PCマルウェア仕込む

1 → 2 → 3 → 4

認証情報を盗み取る

安全なPLCにRATをインストール

PLCの安全を無効にして二次サイバー攻撃を実行



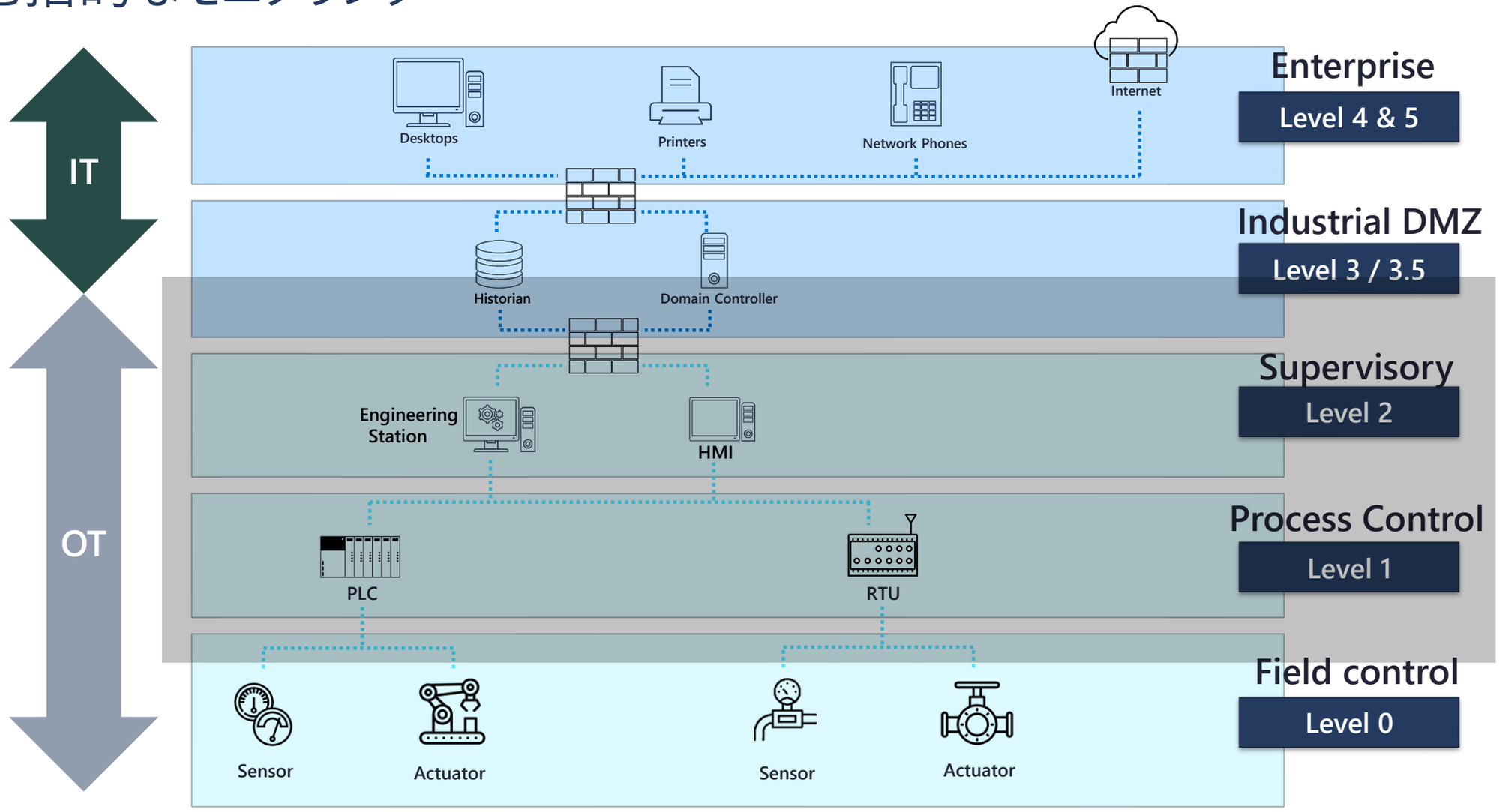
Alert Detected
May 6, 2018 7:37:53 PM
A Triconex station (10.1.2.25) attempted to initiate an operation incorporating an illegal function code value.
Block Source Handle

Scan Device Detected
Apr 22, 2017 8:49:02 PM
Port Scan: Counted 23 distinct ports scanned from 10.2.1.26 to 10.2.1.25

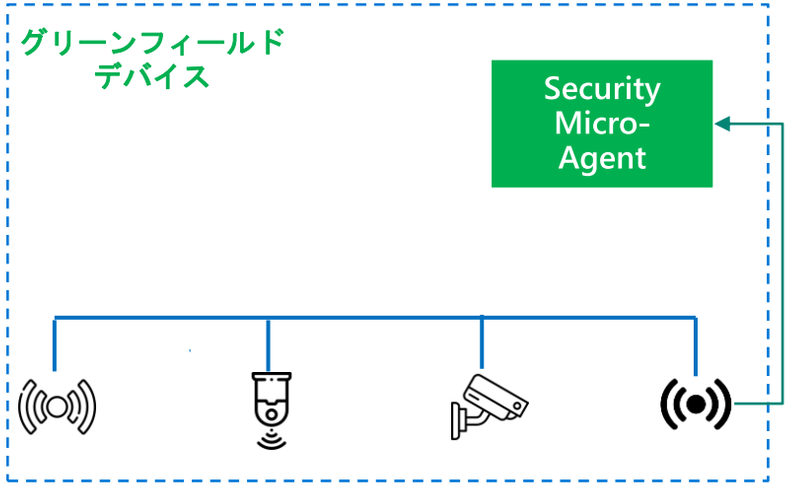
PLC Program Update
Apr 22, 2017 8:53:17 PM
Program update detected, sent from 10.2.1.25 to 10.2.1.14

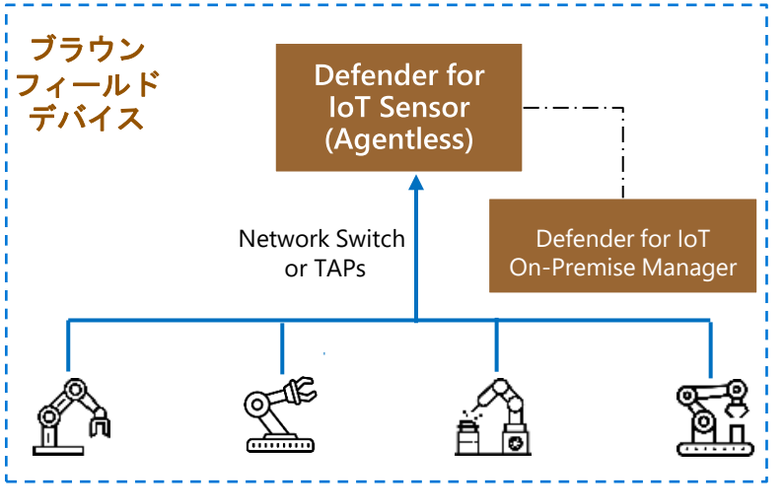
★ 通常のITネットワークファイアウォールではOTプロトコルの制御はできない
★ 制御装置のAnti Virus対応だけでは攻撃通信の検知はできない

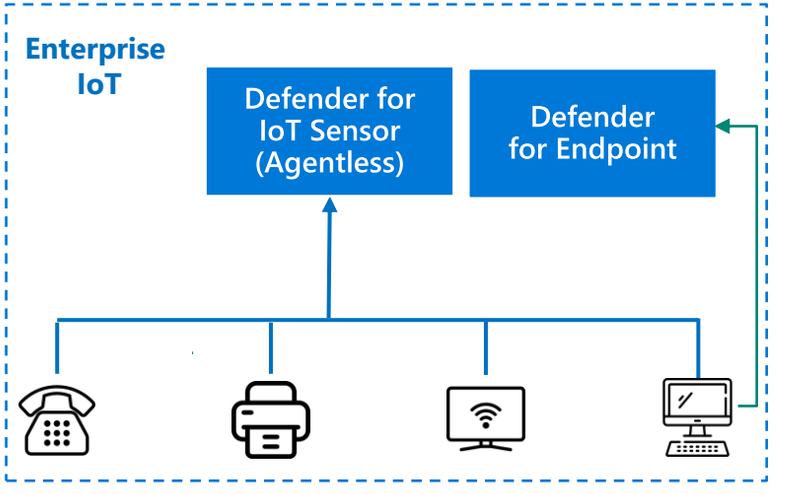
包括的なモニタリング


IT
OT
Desktops
Printers
Network Phones
Internet
Historian
Domain Controller
Engineering Station
HMI
PLC
RTU
Sensor
Actuator
Sensor
Actuator
Enterprise
Level 4 & 5
Industrial DMZ
Level 3 / 3.5
Supervisory
Level 2
Process Control
Level 1
Field control
Level 0

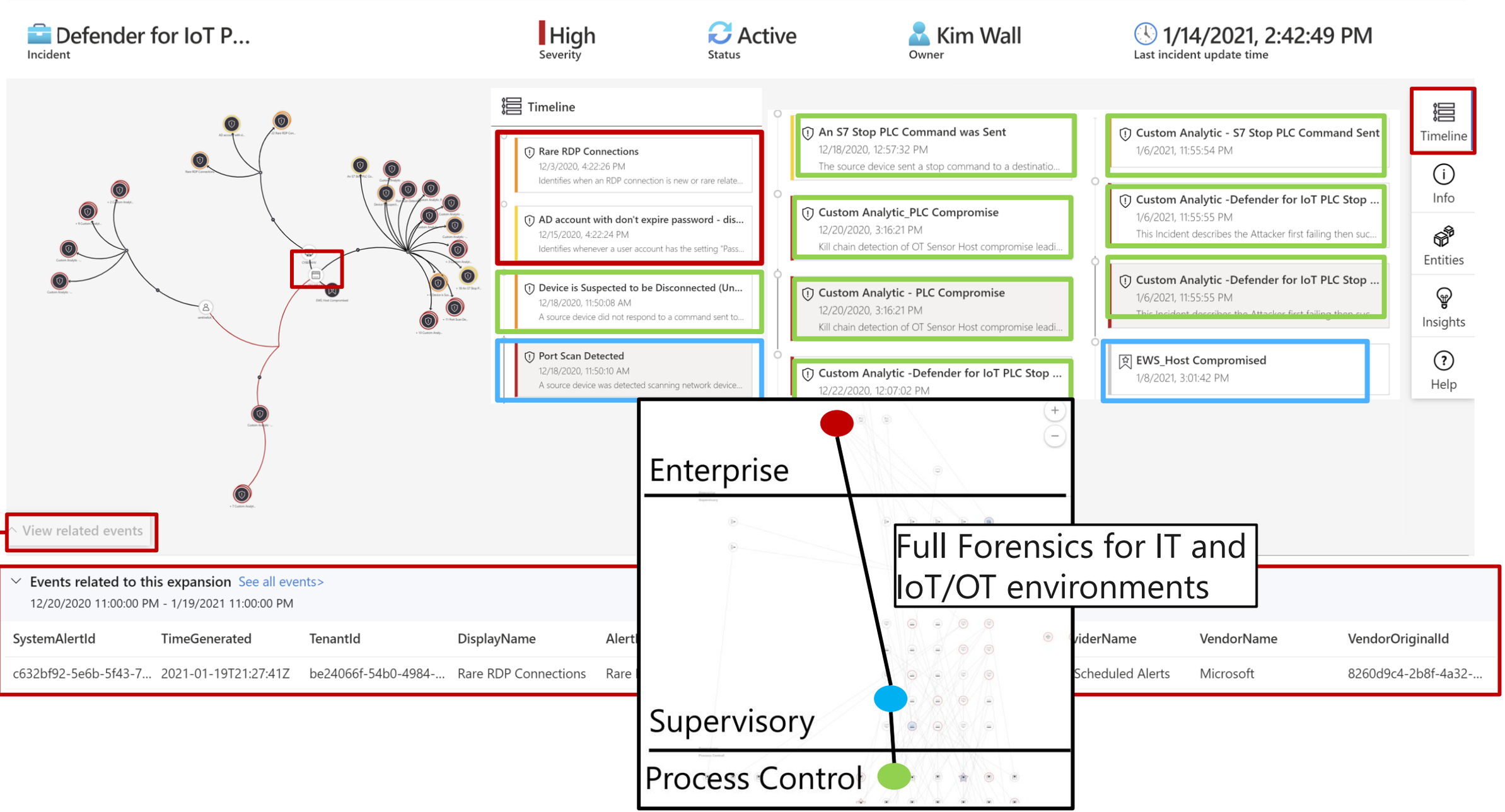
IoT/OTセキュリティ — 参照アーキテクチャー





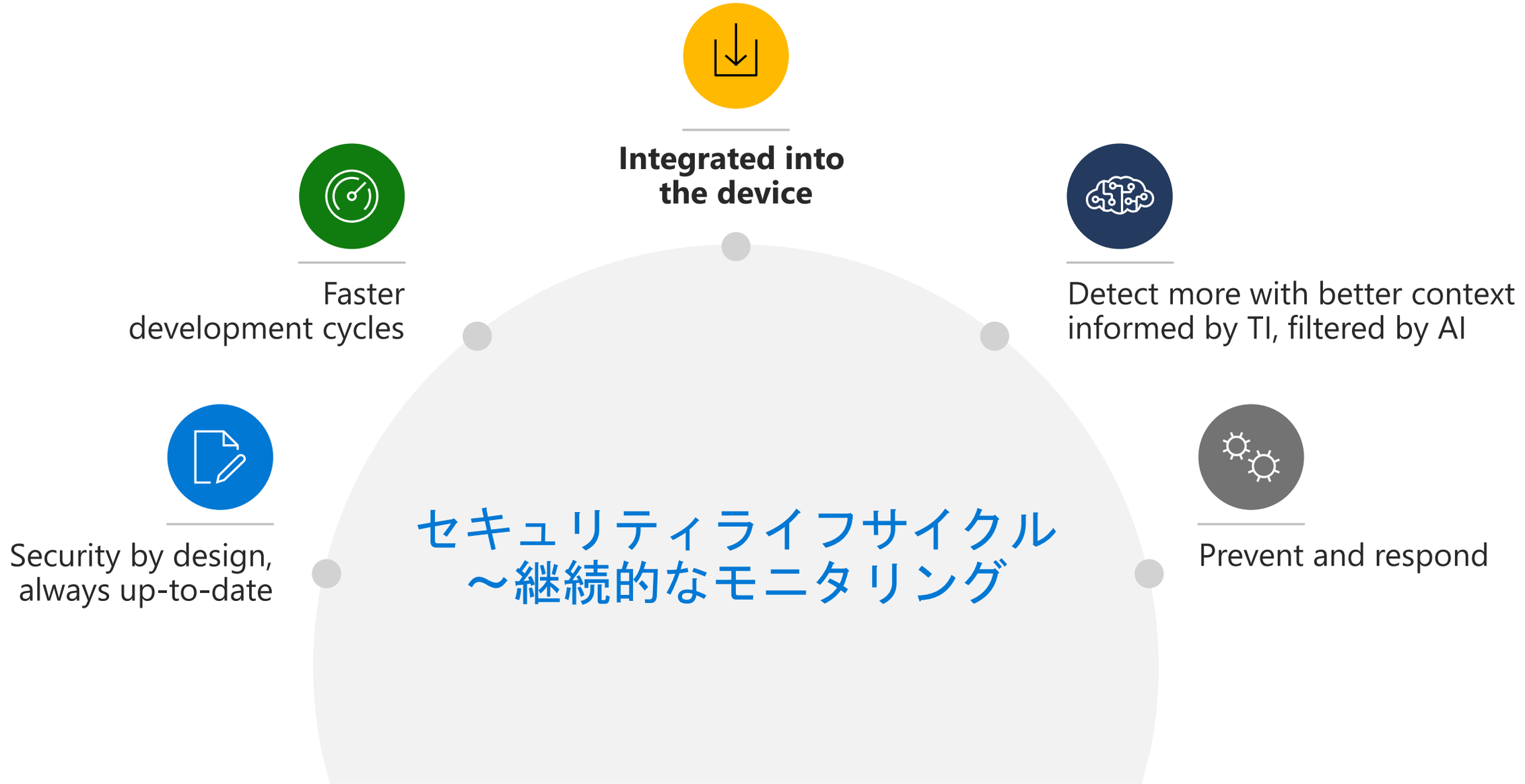


IT, IoT, OT の包括的な管理 - Microsoft Sentinel

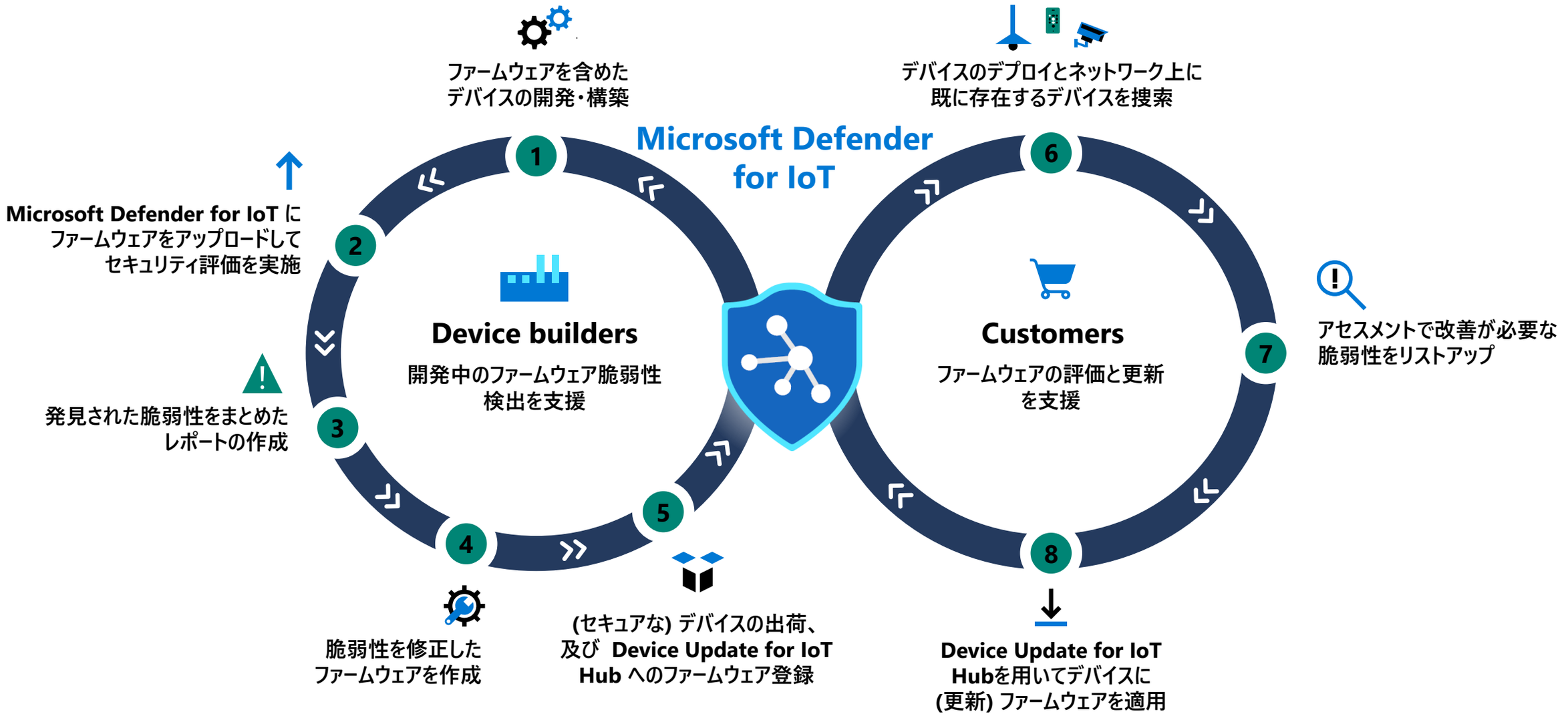


統合化されたエージェント型セキュリティへ

IoT セキュリティの新しいアプローチ



Refirm Labs



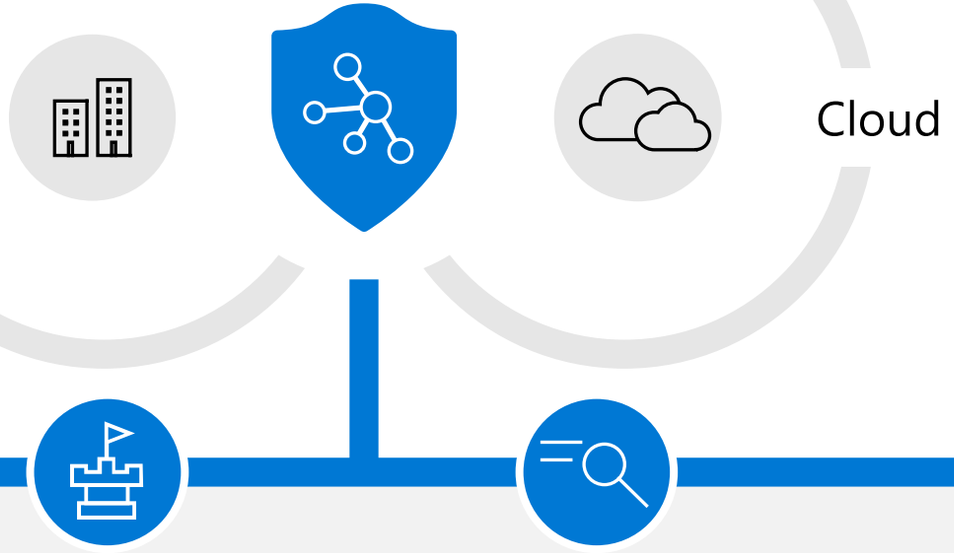
Azure

アーキテクチャー

展開・保守の簡略化

エージェントレス

IoT/OTの統合的アプローチ



包括的なカバレージ

統合化されたIoT/OT ソリューション

継続的なモニタリングと向上

Discover

Complete coverage and visibility focused on IoT/OT devices

Assess

Risk analysis for any device and segment across all networks

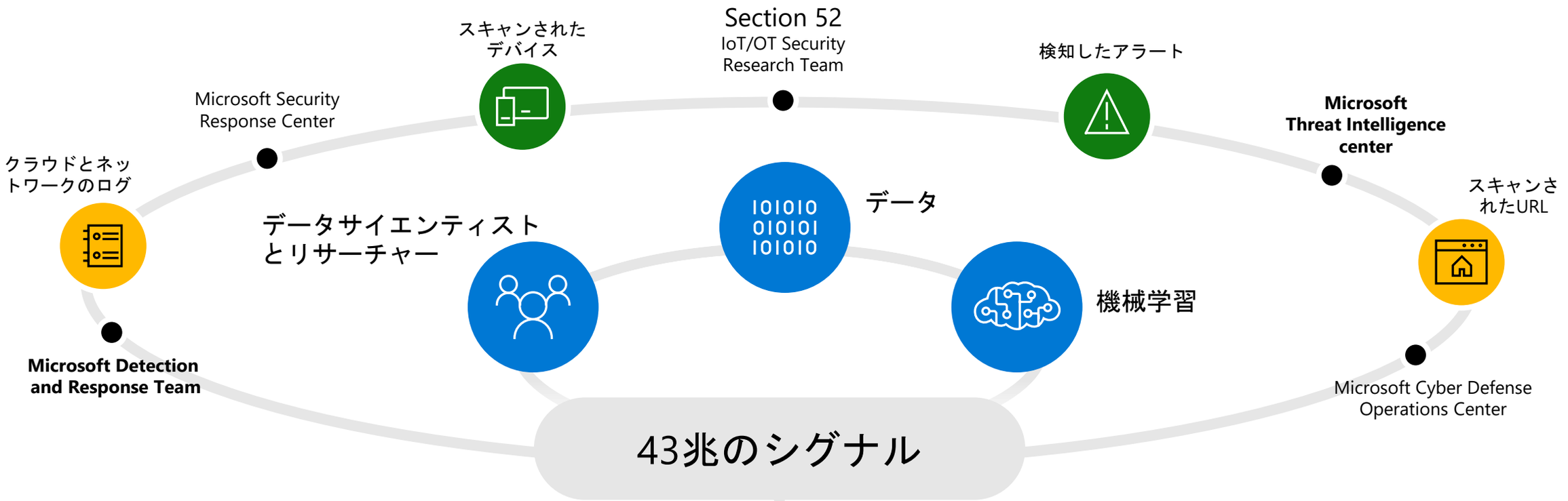
Detect

Behavioral analytics and TI built to adapt to attacker's speed

Respond

Rapidly identify multi-stage attacks across IT/IoT/OT and mitigate with automated playbooks

世界クラスのIoT/OTへの脅威専門知識



Section 52と広範なリサーチチームが世界で最も充実した脅威インテリジェンスを提供

IoT/OTの脆弱性を発見し、攻撃キャンペーンを監視し、独自の検知技術を作成

結論: ICS評価のためのMITRE ATT&CK®でトップレベルの検知可視性カバレッジ

Why Microsoft?

- エンタープライズIoTとOTの統合ソリューション
- 柔軟なセンサーオプション: MDE、ネットワークセンサー、サードパーティ機器
- 既存環境への影響を与えず、迅速に展開可能(通常は各拠点1日未満)なエージェントレスな保護
- 継続的なアセット検出、脆弱性管理、脅威監視
- 世界最大のIoT/OTセキュリティリサーチ組織を構成
- Microsoft SIEM/XDRやサードパーティのSOCソリューションとの統合

Microsoft Security