実践OTセキュリティ対策
OTシステムの可視化と異常検知

株式会社 ソリトンシステムズ
サイバーセキュリティ事業部 鶴田亮

2022/09/14 v.001

アジェンダ

I. OT セキュリティ対策に重要な三要素

II. Microsoft Defender for IoT

III. SOC / CSIRT サービス「セキュリティ監視サービス for IoT/OT」

I. OT セキュリティ対策に重要な三要素

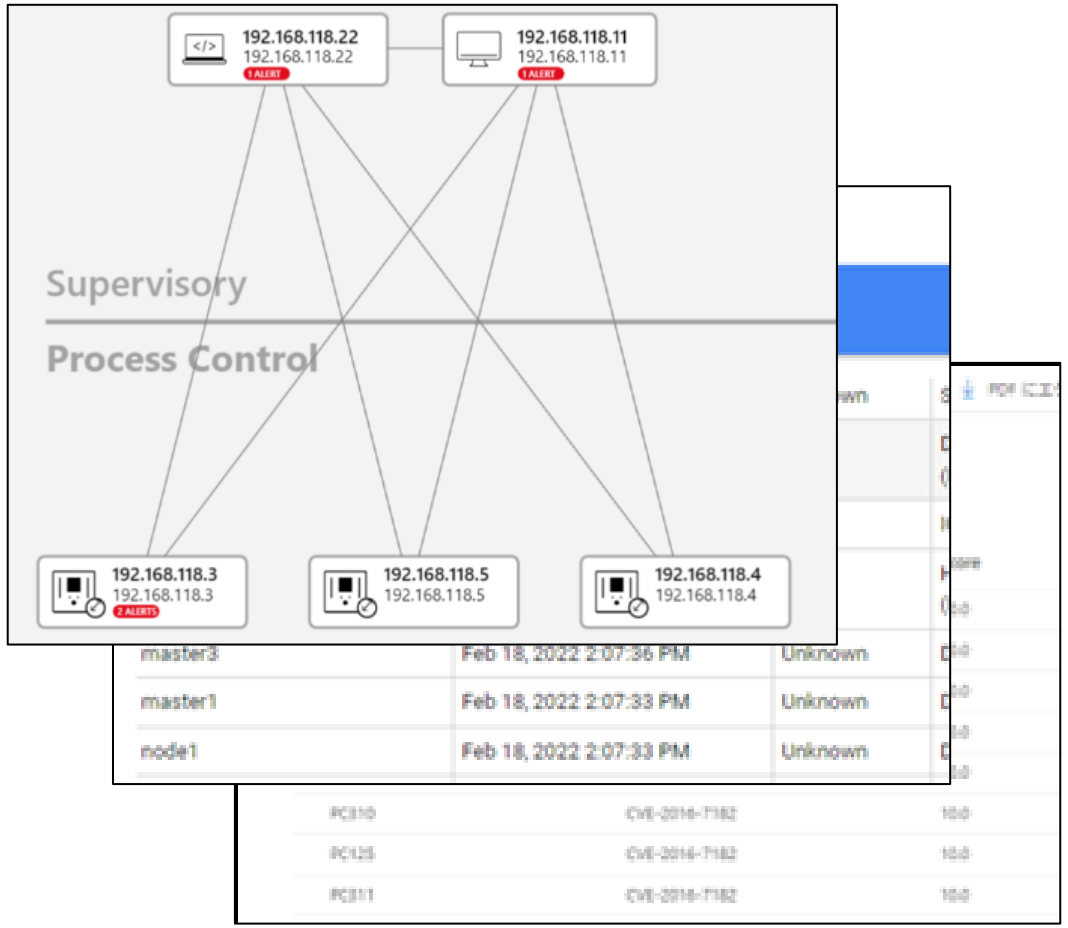
- 可視化
- 異常検知
- 防御

可視化

OT システムの例：
ロボットアームの作業セル

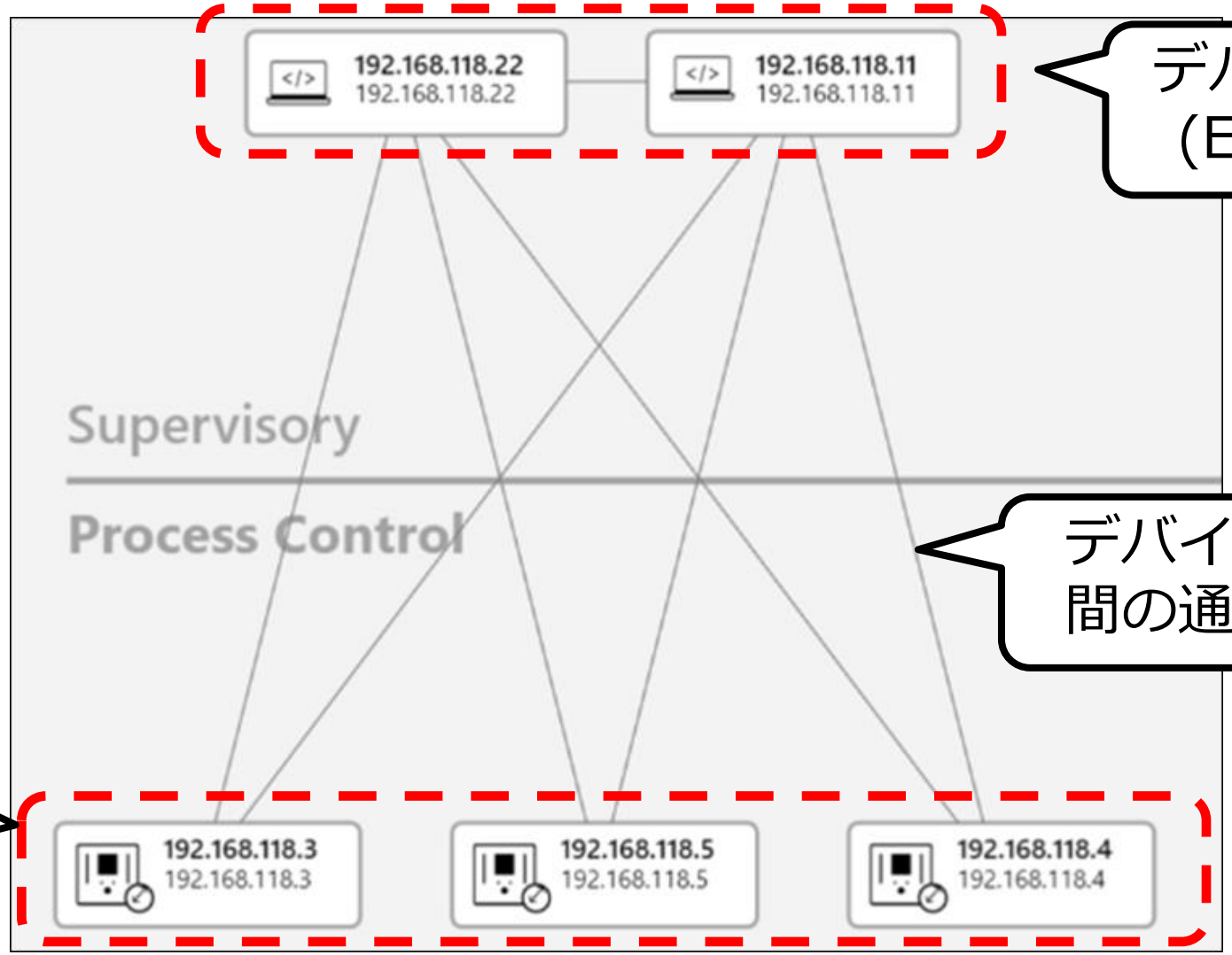
可視化

ネットワーク構成図



出典：NIST SP1800-10B
産業用制御システム環境における情報とシステムインテグリティの保護
製造業のためのサイバーセキュリティ

可視化：ネットワーク構成図



デバイス
(EWS)

デバイス
間の通信

デバイス
(PLC)

可視化：デバイス一覧

Soliton

Device Inventory

IPアドレス

最後に通信した時間

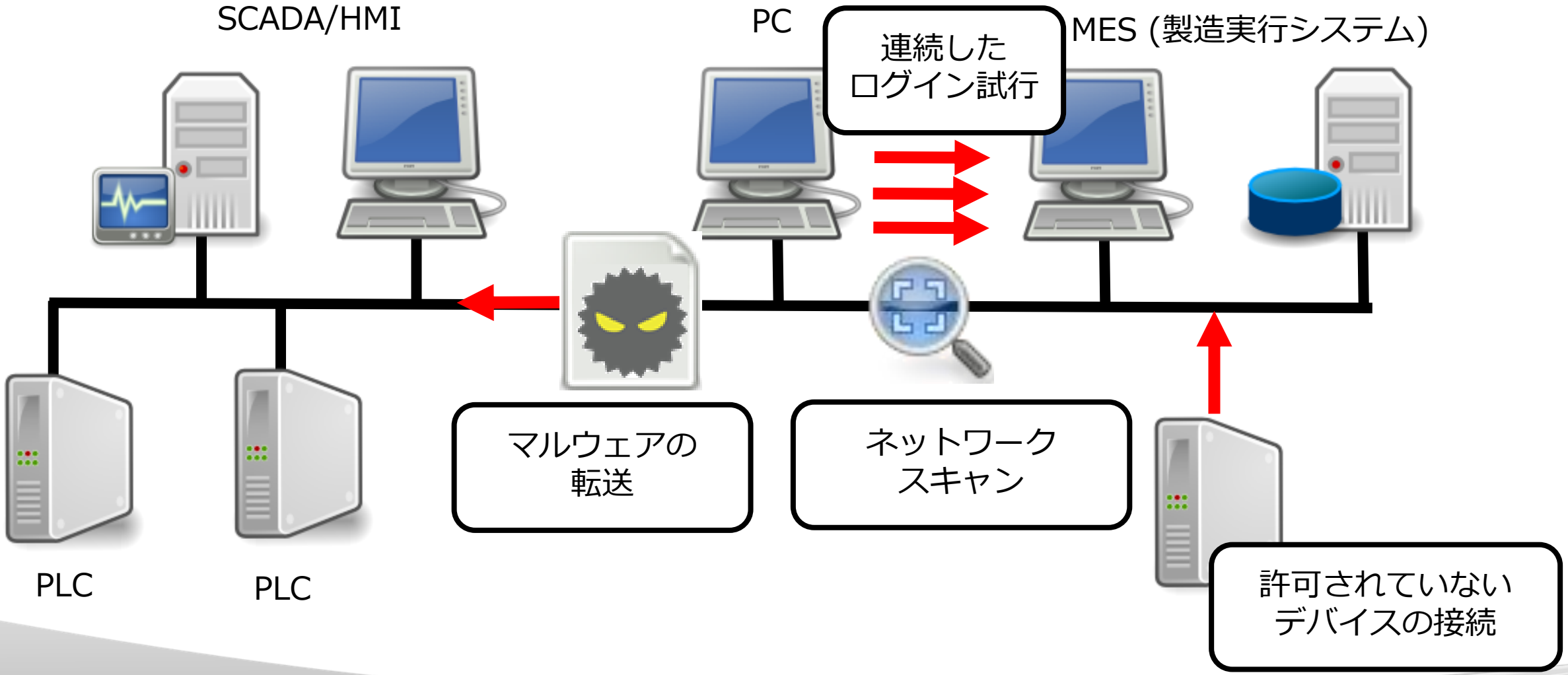
デバイスタイプ

通信プロトコル

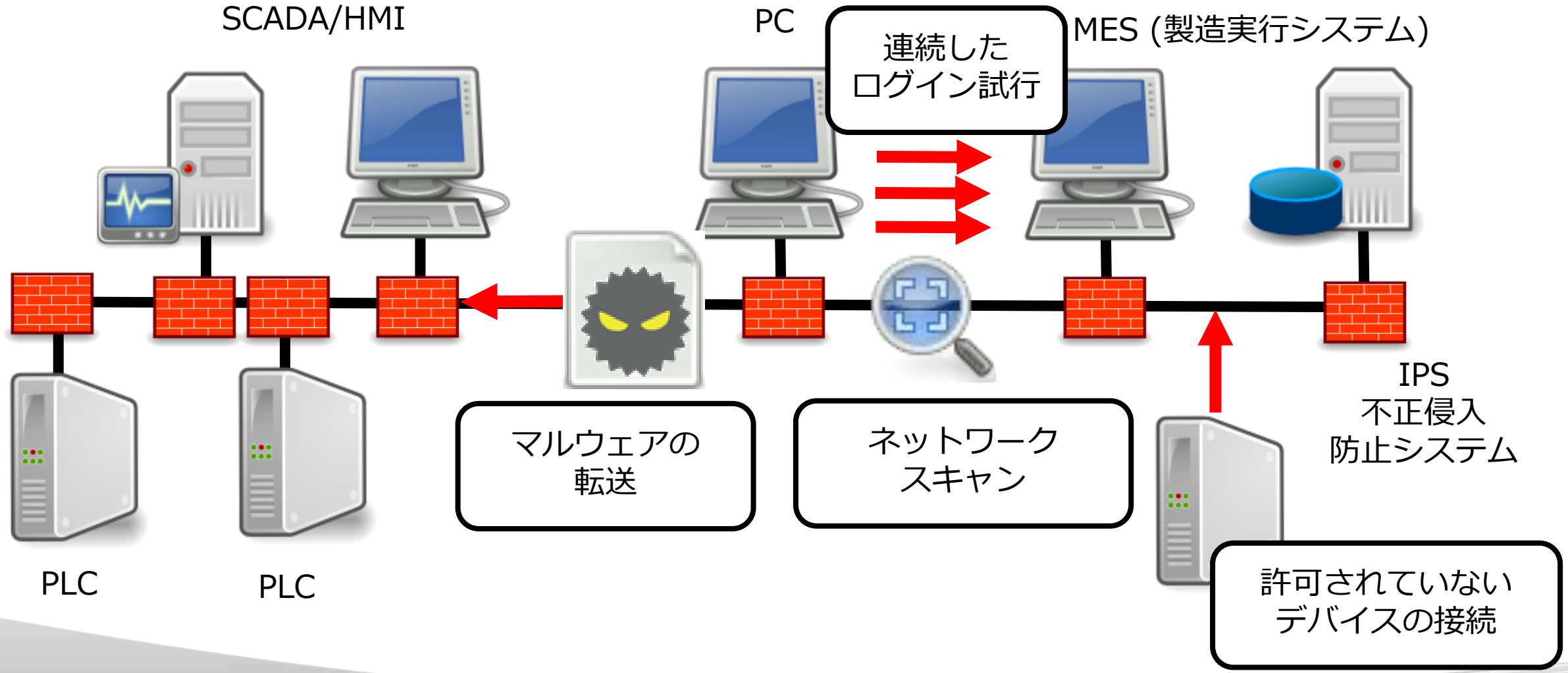
デバイスベンダー

IP Address	Last Activity	Type	Protocols	Vendor
192.168.17.8	Aug 4, 2022 6:29:51 PM	PLC	ICMP, Netbios Datagram Service, SMB, Siemens SICAM	SAT GMBH & CO.
192.168.18.22	Aug 4, 2022 6:29:50 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7	
192.168.18.5	Aug 4, 2022 6:29:50 PM	PLC	Netbios Datagram Service, SMB, Siemens S7	SIEMENS AG
192.168.18.4	Aug 4, 2022 6:29:50 PM	PLC	Netbios Datagram Service, Netbios Name Service, SMB, Siemens S7	SIEMENS AG
192.168.23.10	Aug 4, 2022 6:29:49 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7 Plus	VMWARE INC.

ＯＴネットワーク


SCADA/HMI
PC
MES (製造実行システム)
連続した
ログイン試行
マルウェアの
転送
ネットワーク
スキャン
許可されていない
デバイスの接続
PLC
PLC

ＯＴネットワーク


SCADA/HMI
PC
MES (製造実行システム)
連続した
ログイン試行
マルウェアの
転送
ネットワーク
スキャン
IPS
不正侵入
防止システム
許可されていない
デバイスの接続
PLC
PLC

I. まとめ

可視化

　システム構成や稼働状況を機械や人間が分析できる形にして明らかに

異常検知

　システムを継続的に監視して、普段とは異なる動作を捉える

防御

　不正な通信を遮断してサイバー攻撃からシステムやデータを保護する

三要素の実現で効果的な OT セキュリティ対策

II. Microsoft Defender for IoT

- 概要
- システム構成
- 機能
  - 操作方法
  - 可視化
  - 異常検知
  - 他のセキュリティ製品との連携

概要

製造業や重要インフラなど OT システム向けに作られた資産管理、脅威監視を行うセキュリティソリューション

システムの可視化、リスク分析

デバイス一覧やネットワークマップを自動作成。自動リスク分析機能により脆弱性やリスク緩和策を提示

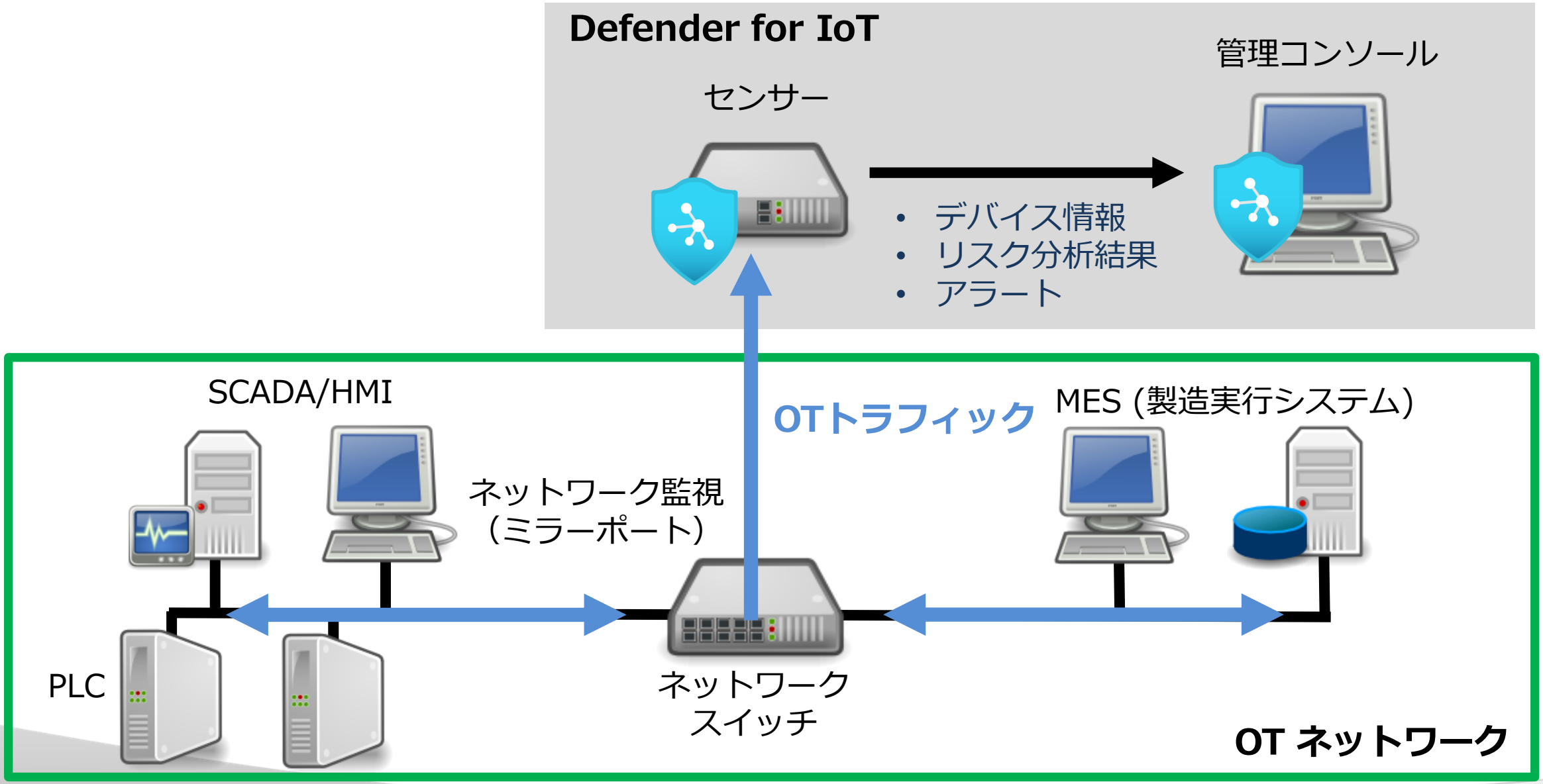
異常検知

OT 対応の行動分析と脅威インテリジェンスにより異常を検知

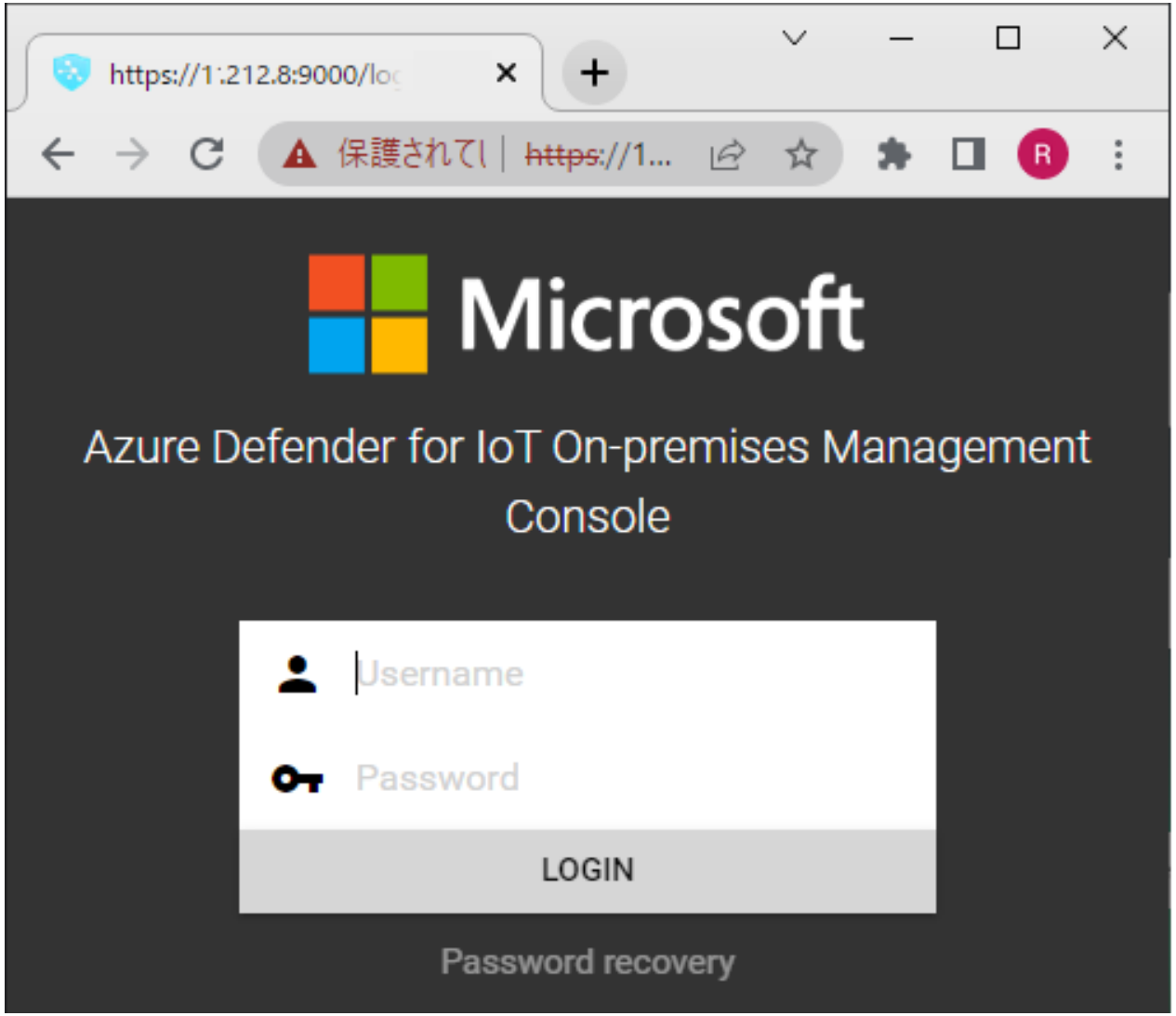
他のセキュリティ製品との連携

SIEM、SOAR、ファイアウォール、IDS/IPS など様々なベンダーのセキュリティ製品と連携

システム構成

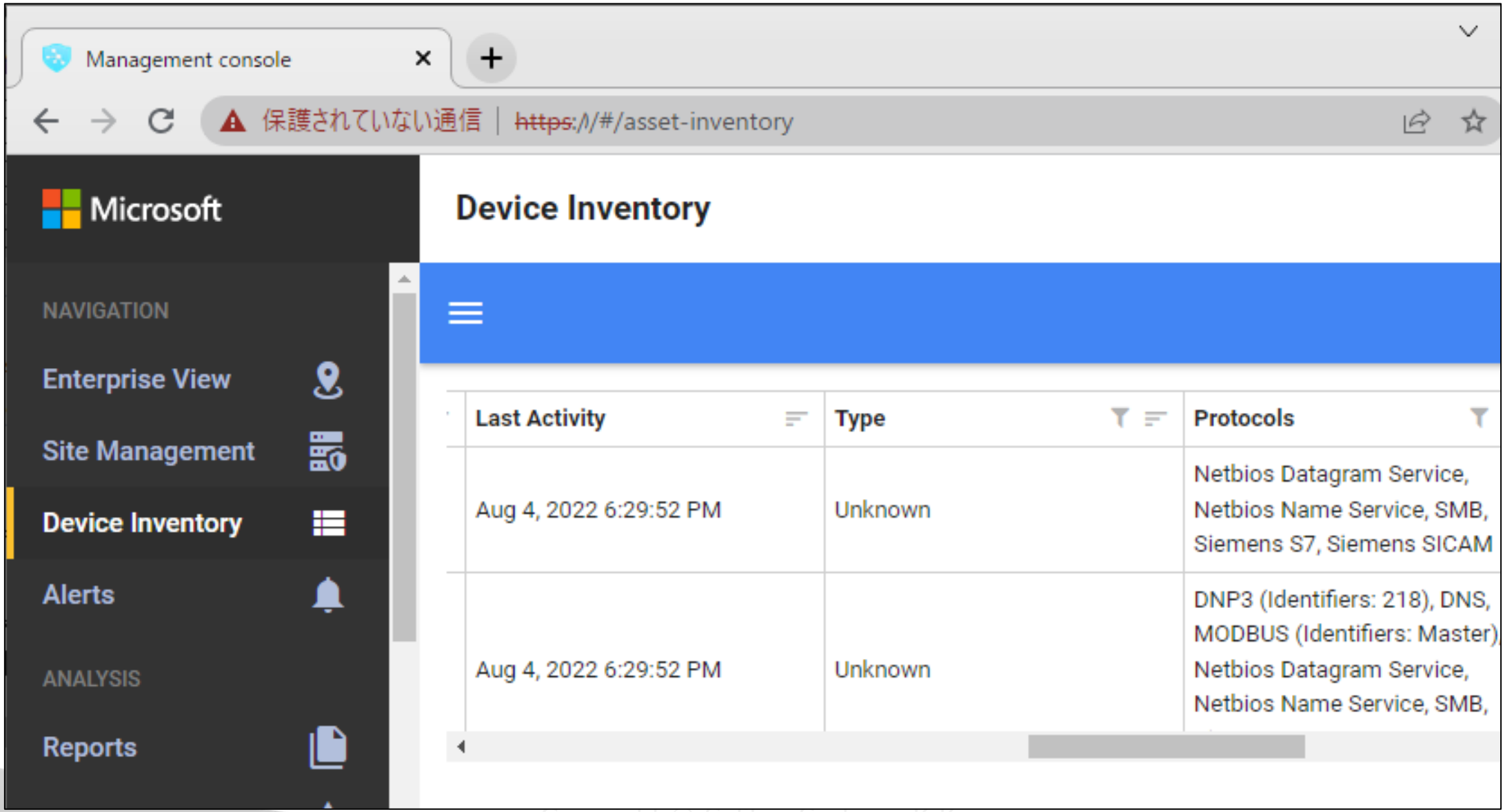

Defender for IoT
センサー
管理コンソール
• デバイス情報
• リスク分析結果
• アラート
SCADA/HMI
OTトラフィック
MES (製造実行システム)
ネットワーク監視
（ミラーポート）
PLC
ネットワーク
スイッチ
OT ネットワーク

機能：操作方法：ログイン



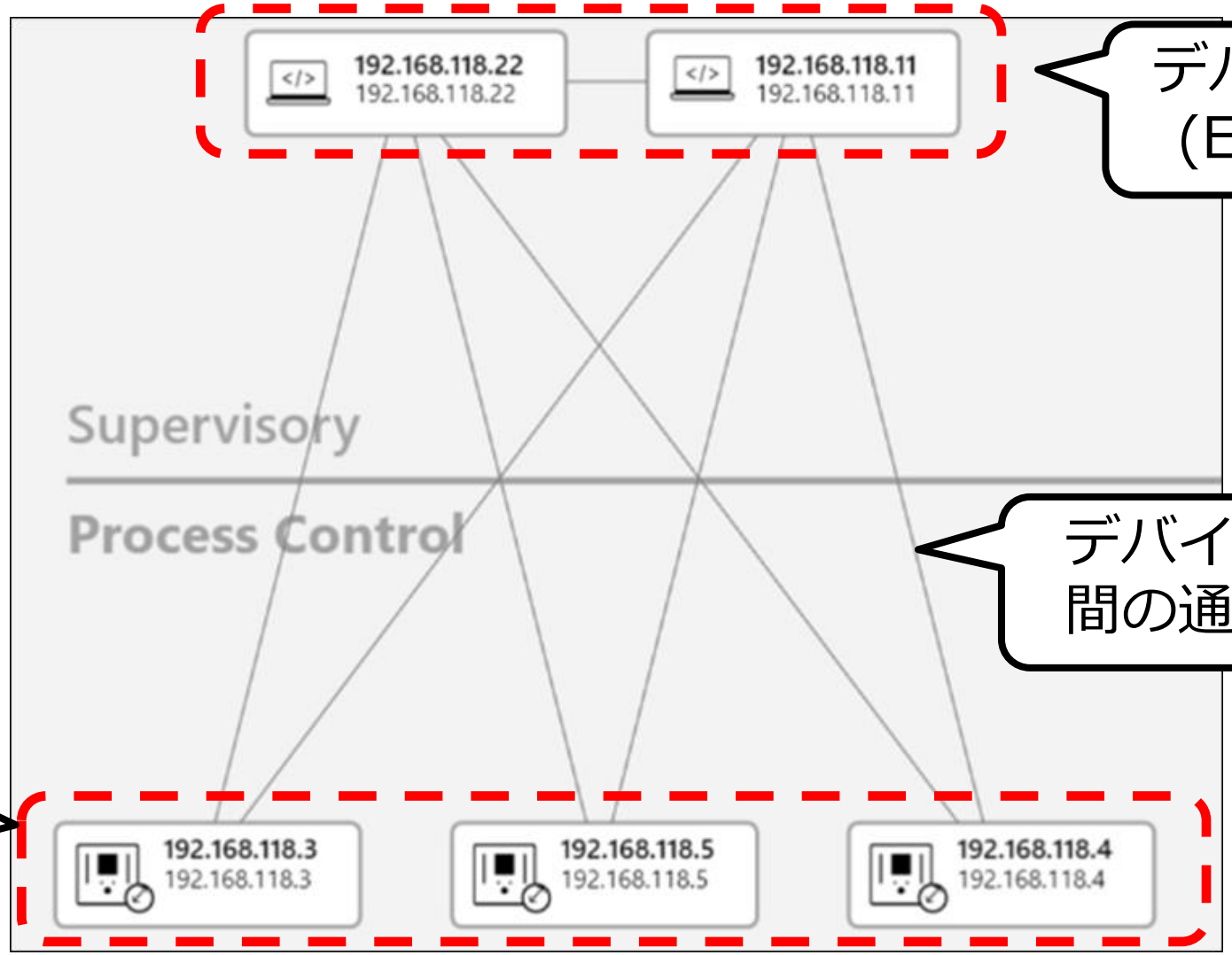
13

機能：操作方法：メニュー画面



14

機能：可視化：ネットワーク構成図



デバイス
(EWS)

デバイス
間の通信

デバイス
(PLC)

機能：可視化：デバイス一覧

Device Inventory

IPアドレス

稼働状況

デバイス
タイプ

通信
プロトコル

デバイス
ベンダー

IP Address	Last Activity	Type	Protocols	Vendor
192.168.123.10	Aug 4, 2022 6:29:49 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7 Plus	VMWARE INC.
192.168.118.22	Aug 4, 2022 6:29:50 PM	Engineering Station	Netbios Datagram Service, SMB, Siemens S7	
172.30.35.255	Aug 4, 2022 4:49:03 PM	Multicast/Broadcast	Netbios Datagram Service, Netbios Name Service, SMB	
192.168.117.7	Aug 4, 2022 6:29:52 PM	PLC	Netbios Name Service, SMB, Siemens S7, Siemens SICAM	SAT GMBH & CO.
192.168.117.8	Aug 4, 2022 6:29:51 PM	PLC	ICMP, Netbios Datagram Service, SMB, Siemens SICAM	SAT GMBH & CO.

機能：異常検知：アラート一覧

機能：他のセキュリティ製品との連携

連携可能製品

- Aruba ClearPass
- Axonics
- CyberArk PSM
- Forescout
- Fortinet
- IBM QRadar
- LogRhythm
- Micro Focus ArcSight
- Microsoft Defender for EndPoint
- Micosorft Sentinel
- Palo ALto
- RSA NetWitness
- ServiceNow
- Skybox
- Splunk

アラート転送方式

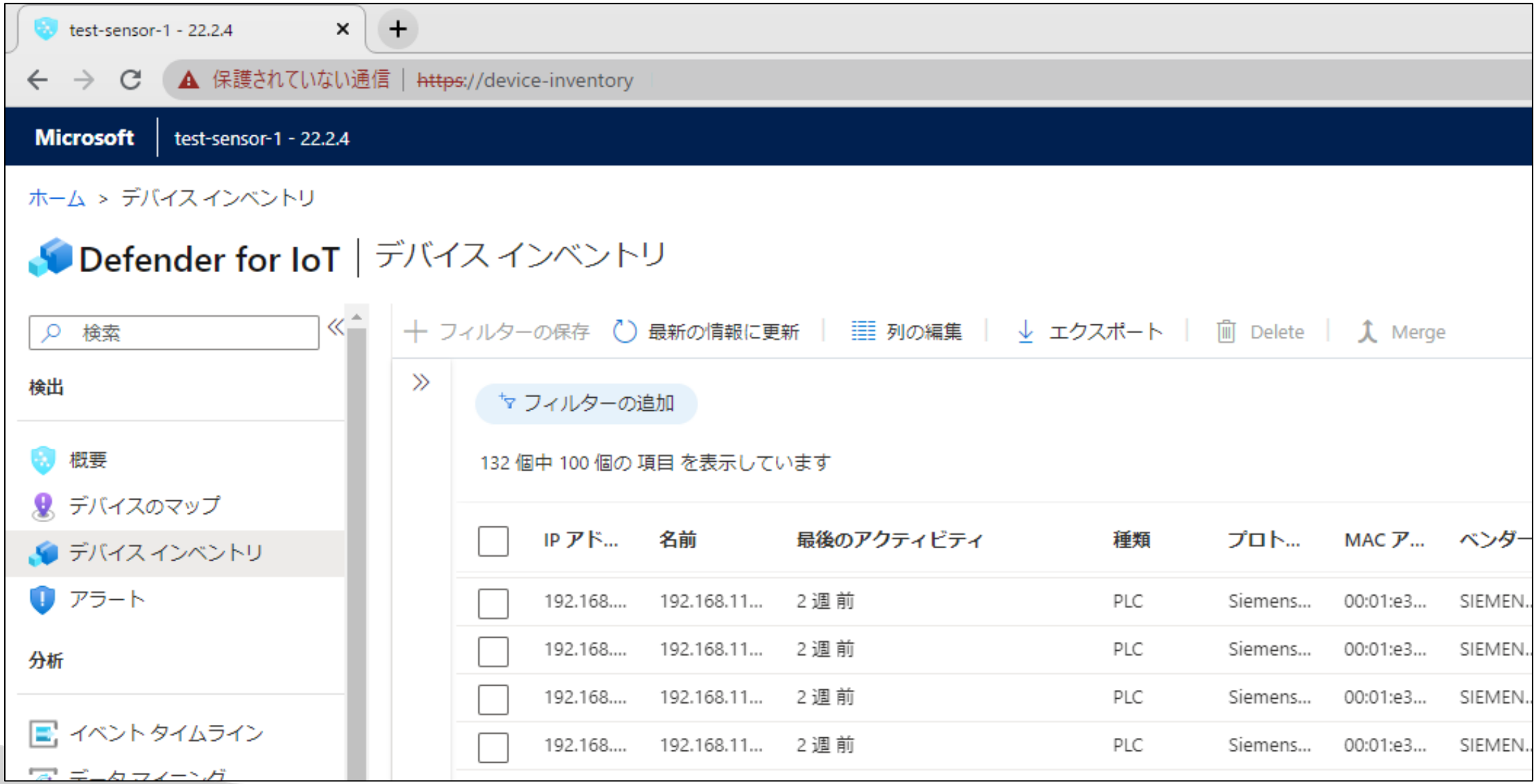
- Syslog (TEXT/CEF/LEEF)
- 電子メール
- Webhook

外部制御

- WEB API
- SSH

18

機能：日本語対応



19

II. まとめ

Microsoft Defender for IoT とは、

- OT 対応の行動分析と脅威インテリジェンス、多数の制御機器ベンダーのプロトコル対応により「可視化」と「異常検知」を実現
- 稼働中のシステムの可用性やパフォーマンスを損なうことなく、導入・運用が可能。
- 他のセキュリティ製品と連携して「防御」も可能。OT システムのセキュリティ対策に重要な三要素を全てカバー

OT システムのセキュリティ対策に最適なソリューション

ソリトンのサービス

- サービス概要
- システム導入例
- 運用体制
- 平時のタスク
- インシデント対応
- Soliton コールセンターのご紹介
- 無償 PoC のご案内

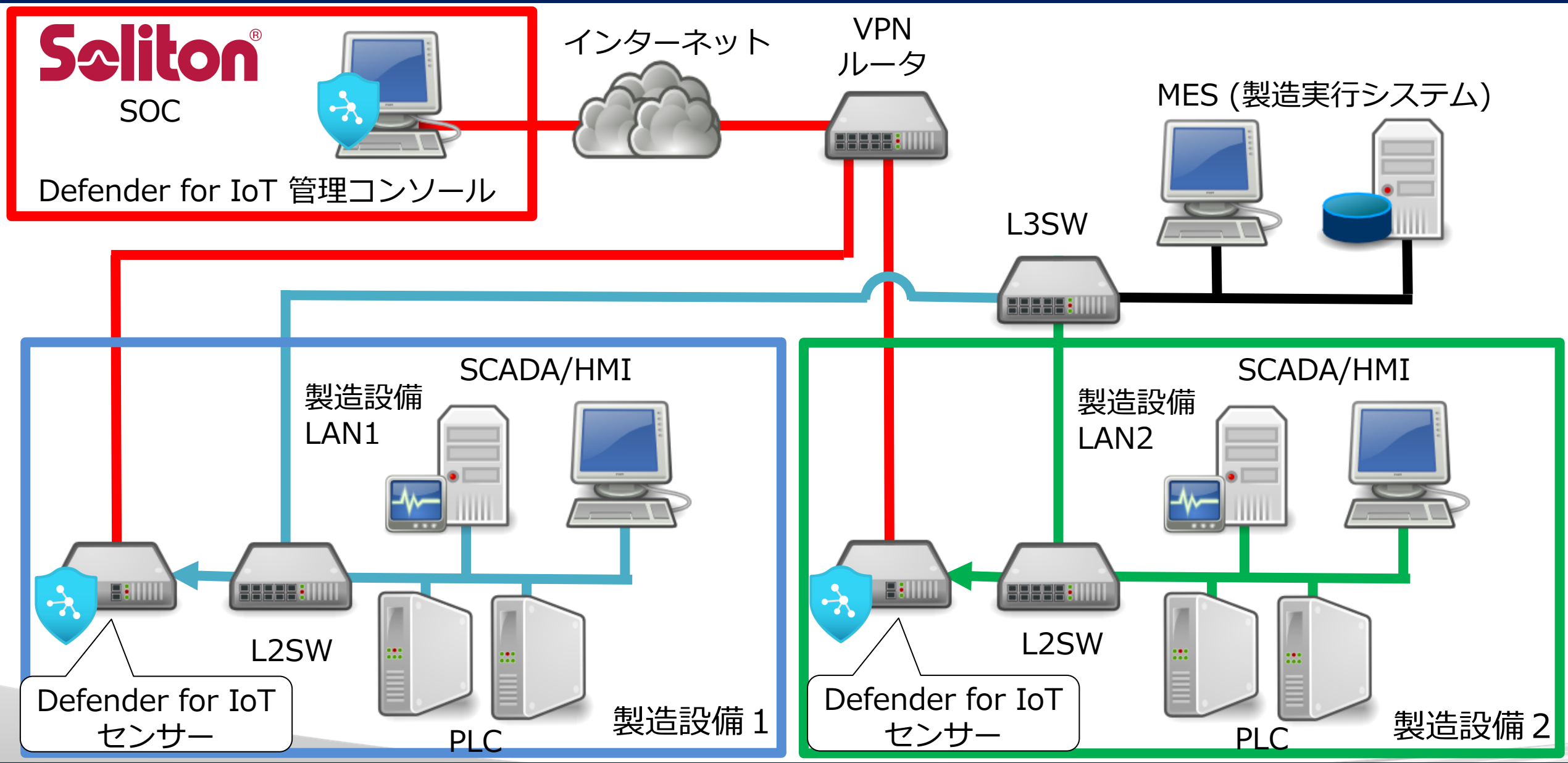
サービス概要

「OT セキュリティの専門家がいない！」「24時間監視体制の構築は難しい！」といった課題を解決

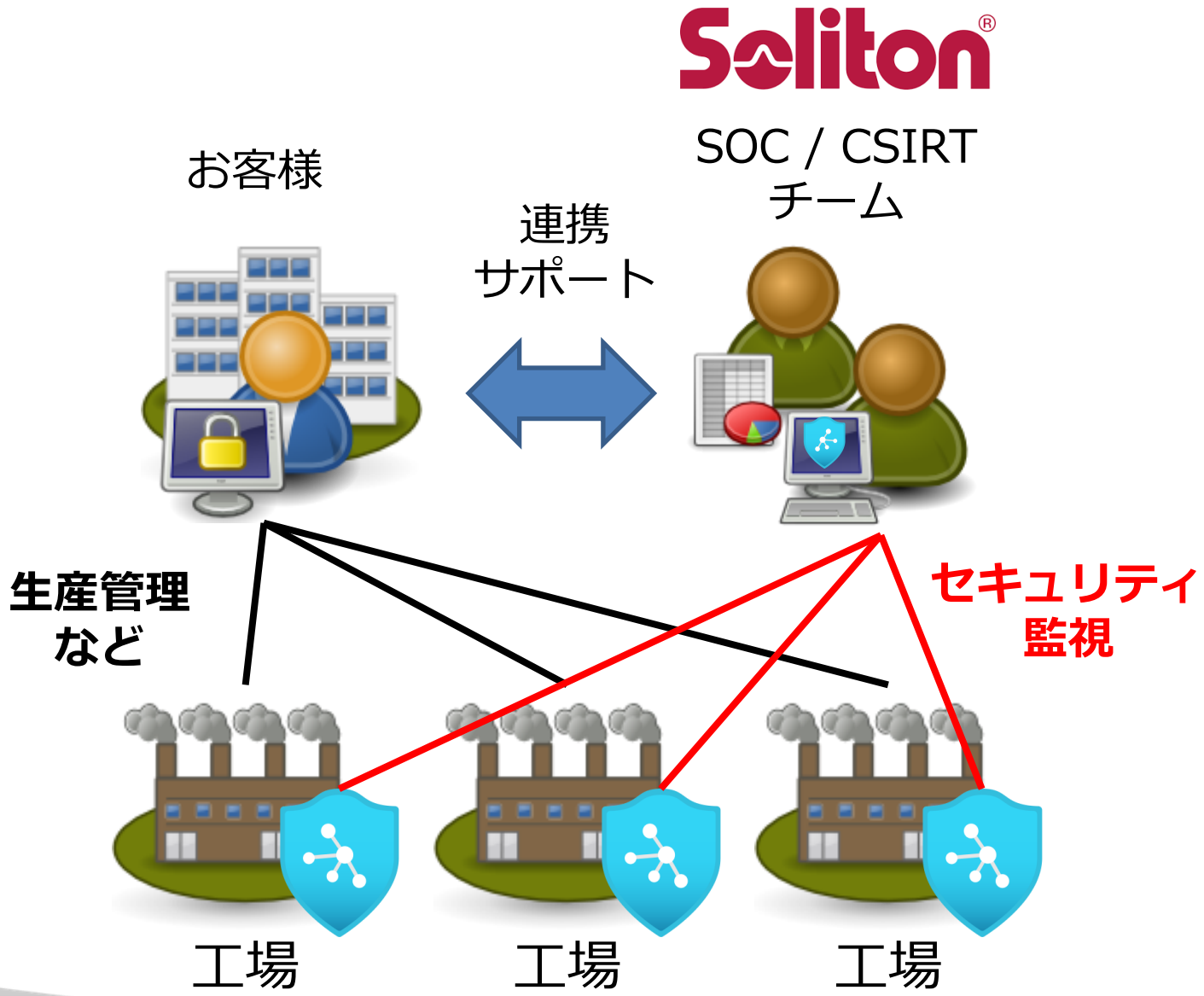
Microsoft Defender for IoT を使った OT SOC & CSIRT サービス

- 稼働中の OT システムへの影響を極力抑えたサービス導入
- OT セキュリティの専門家による SOC / CSIRT チーム
- 24時間365日 受付・対応可能なサービス運用体制
- インシデント発生時の現場急行サービスをオプションで用意

システム導入例


SOC
Defender for IoT 管理コンソール
インターネット
VPN
ルータ
MES (製造実行システム)
L3SW
SCADA/HMI
製造設備
LAN1
L2SW
Defender for IoT
センサー
PLC
製造設備 1
SCADA/HMI
製造設備
LAN2
L2SW
Defender for IoT
センサー
PLC
製造設備 2

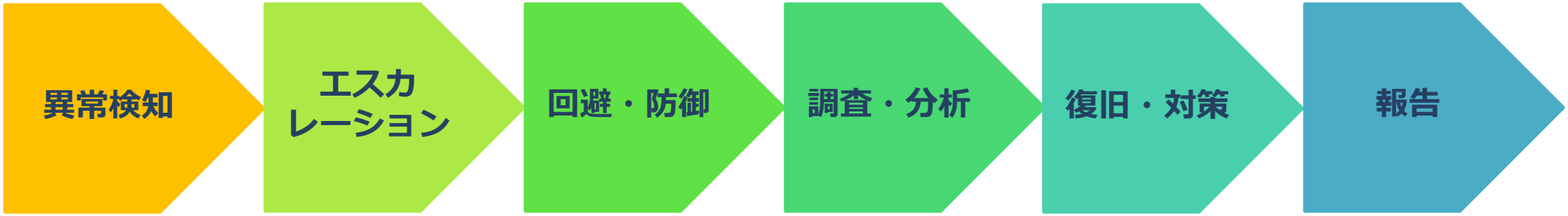
運用体制



平時の業務

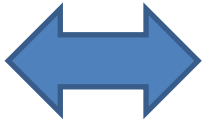
- アラート監視
- お客様からのお問い合わせ対応
- 脆弱性情報をはじめとするサイバーセキュリティ関連情報の収集と注意喚起
- サービス運用レポートの作成
  - 定期リスクアセスメント結果（脆弱性情報、対応状況など）
  - お問い合わせ内容分析（問い合わせ件数、対応状況など）
  - インシデント対応分析（発生件数、発生傾向、対応状況など）
- 監視システムメンテナンス

インシデント対応



お客様
OT セキュリティ
担当部署

連携
サポート



Soliton®
SOC / CSIRT
チーム

OT 現場との調整・連携

インシデント対応中心の業務

Soliton コールセンター

- 24時間365日問い合わせ対応
- 電話、メール、WEB、各種メッセージングサービス（オプション）による受付
- アラート対応
  - 緊急度の高いアラートは即座にエスカレーション
  - オプションで現場駆けつけサービスもご用意
- ISMS 認証、プライバシーマーク取得

ICMS-SR0315 / JIS Q 27001

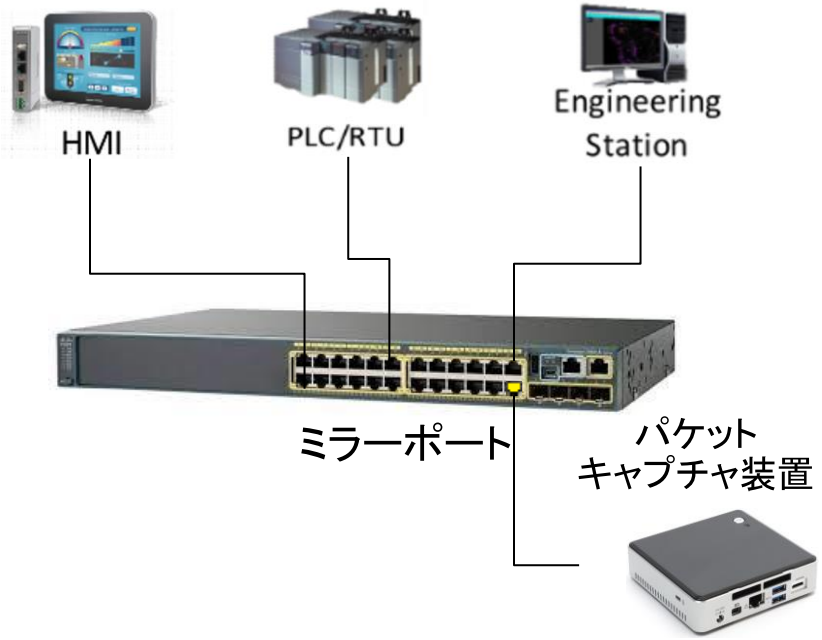
無償 PoC のご案内

- 簡易アセスメントを実施いたします

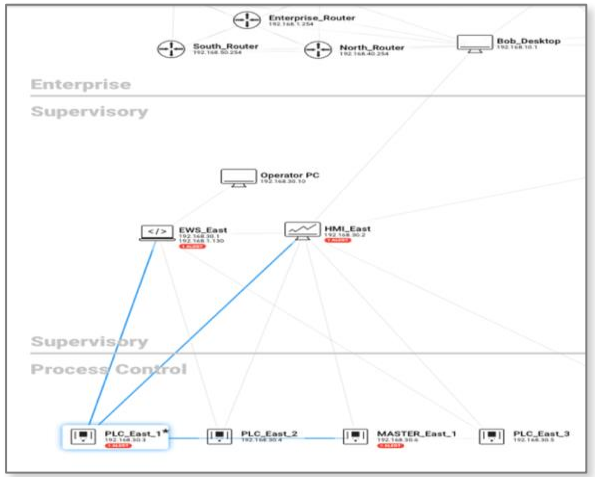
  1.PLCやHMIが接続されている
  　スイッチにミラーポートを設定

  2.ミラーポートにパケットキャプチャ装置を接続

  3.30分から数時間分のPCAPを保存



- 下記の情報をご確認いただけます
  - どのようなデバイスが接続されているか
  - それらのデバイスはどのようなプロトコルで通信をしているか
  - 脆弱性や潜在的な脅威は存在しないか



リポート

Microsoft Defender for IoT を使った OT SOC & CSIRT サービス

- 稼働中の OT システムへの影響を極力抑えたサービス導入
- OT セキュリティの専門家による SOC / CSIRT チーム
- 24時間365日 受付・対応可能なサービス運用体制
- インシデント発生時の現場急行サービスをオプションで用意

OT セキュリティ対策の導入から運用までフルサポート

ソリトン セキュリティ監視サービス for IoT/OT と Trend Micro EdgeIPS を組み合わせ OT セキュリティ対策の三要素を実現

セッション全体のまとめ

- OT セキュリティ対策の重要な三要素
  「可視化」「異常検知」「防御」

  三要素の実現で効果的な OT セキュリティ対策

- 三要素を実現するソリューション Microsoft Defender for IoT

  OT システムのセキュリティ対策に最適なソリューション

- Microsoft Defender fot IoT を使った OT SOC / CSIRT サービス
  「セキュリティ監視サービス for IoT/OT」

  OT セキュリティ対策の導入から運用までフルサポート