

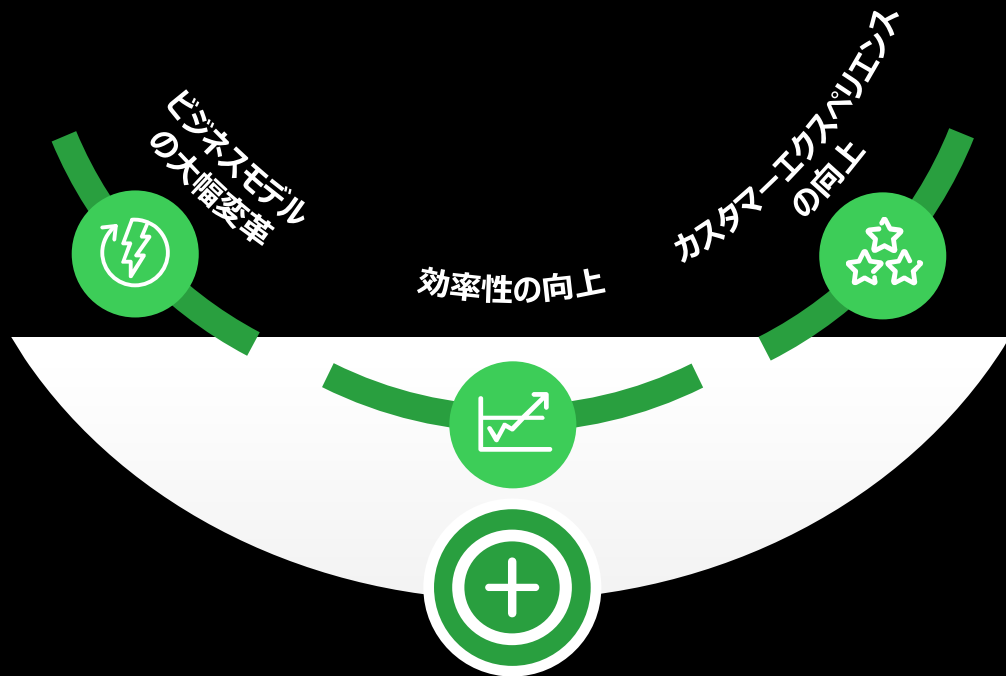
工場DXのためのサイバーセキュリティ OTサイバーセキュリティの鍵を握るIT・OTの融合

シュナイダーエレクトリック DXカンファレンス 2024

シュナイダーエレクトリック
インダストリアルオートメーション事業部 ソリューション営業部 森本 直幸

DXによる変革

デジタルトランスフォーメーション - デジタルテクノロジーの普及により…



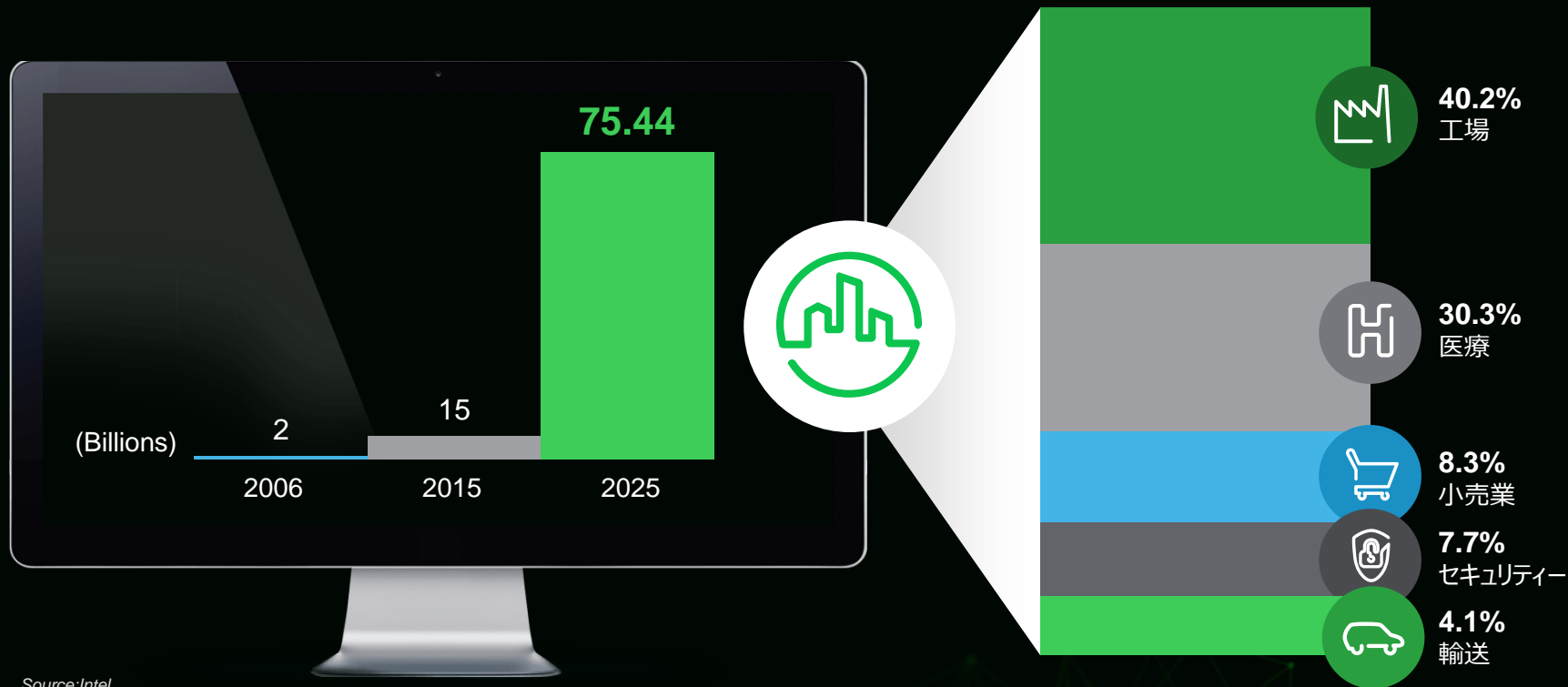
DXのメリットを**安全**に活用し、ビジネス価値を実現



世界はデジタル化された未来に向かっていきます。

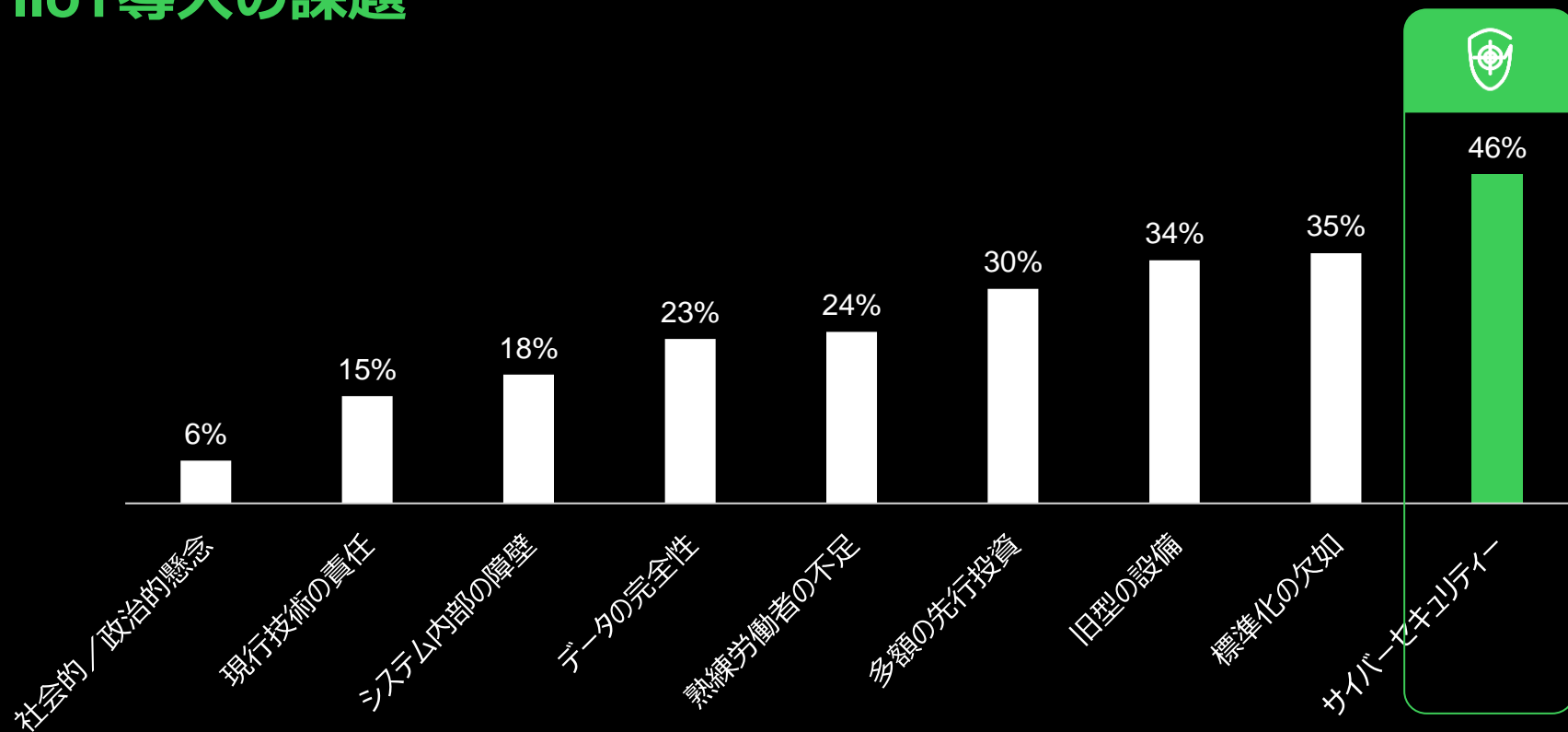
既に、誰もがデジタルの世界にどっぷり浸かって成長しています。

IoTコネクテッドデバイスの成長



Source: Intel

IIoT導入の課題



Source: Morgan Stanley

サプライチェーンを持つあらゆる製造事業者にとって サイバーリスクは現実的な課題

40%

40%のメーカーが自社の業務が
サイバーインシデントの影響を
受けたことがあると回答

Manufacturing

製造業は
最も頻繁にサイバー攻撃
のターゲットとされる業界

\$7,5 M

製造業におけるデータ侵害の
経済的影響は
1社平均：約12億円

Source: The rise of cyber threats to supply chains amid COVID-19, Deloitte.

OTサイバーセキュリティが抱える課題



IT/OTセキュリティの 経験を有する専門家不足

ICS環境は、需要の高い特定のサイバーセキュリティスキルセットと経験を必要とします。

競争の激しい市場では、人材の雇用と維持が困難です。



セキュリティ管理の 投資対効果の見えにくさ

テクノロジーの習熟度合いが高く、必要な時間投資が多いため、セキュリティチームがセキュリティ投資の価値を評価することが難しくなっています。



OTサイバーセキュリティに 割り当てられる予算の不足

セキュリティ要件は日々増加していますが、これらの要件に対応するための投資予算は、同じペースで増加していません。

サイバーセキュリティ対策を実施して得られる価値



シュナイダーエレクトリックの サイバーセキュリティ



シュナイダーエレクトリックのサイバーセキュリティ

サプライチェーンのサイバーリスクをいかに最小化するか - Supporting IT/OT convergence



プラント

物理的セキュリティ



オフィス (IT)



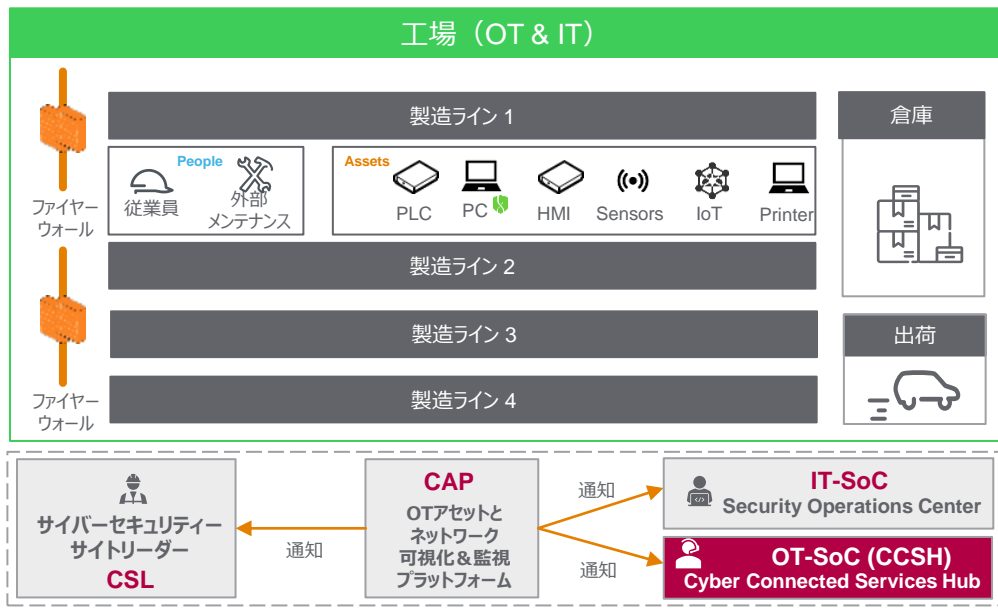
サーバールーム (IT)



ビル管理 (OT & IT)



ファイアーウォール



想定されるリスク

ビジネスの中断
流通・生産センター

お客様アセットへの損害
ソフトウェア/ファームウェアの不正使用

対策 (NIST Framework)

特定

- 人と資産

保護

- 意識すべきこととすべきでないこと
- 資産を含む製造現場と生産ライン

検知 & 対応

- 脆弱性とサイバーインシデント

回復

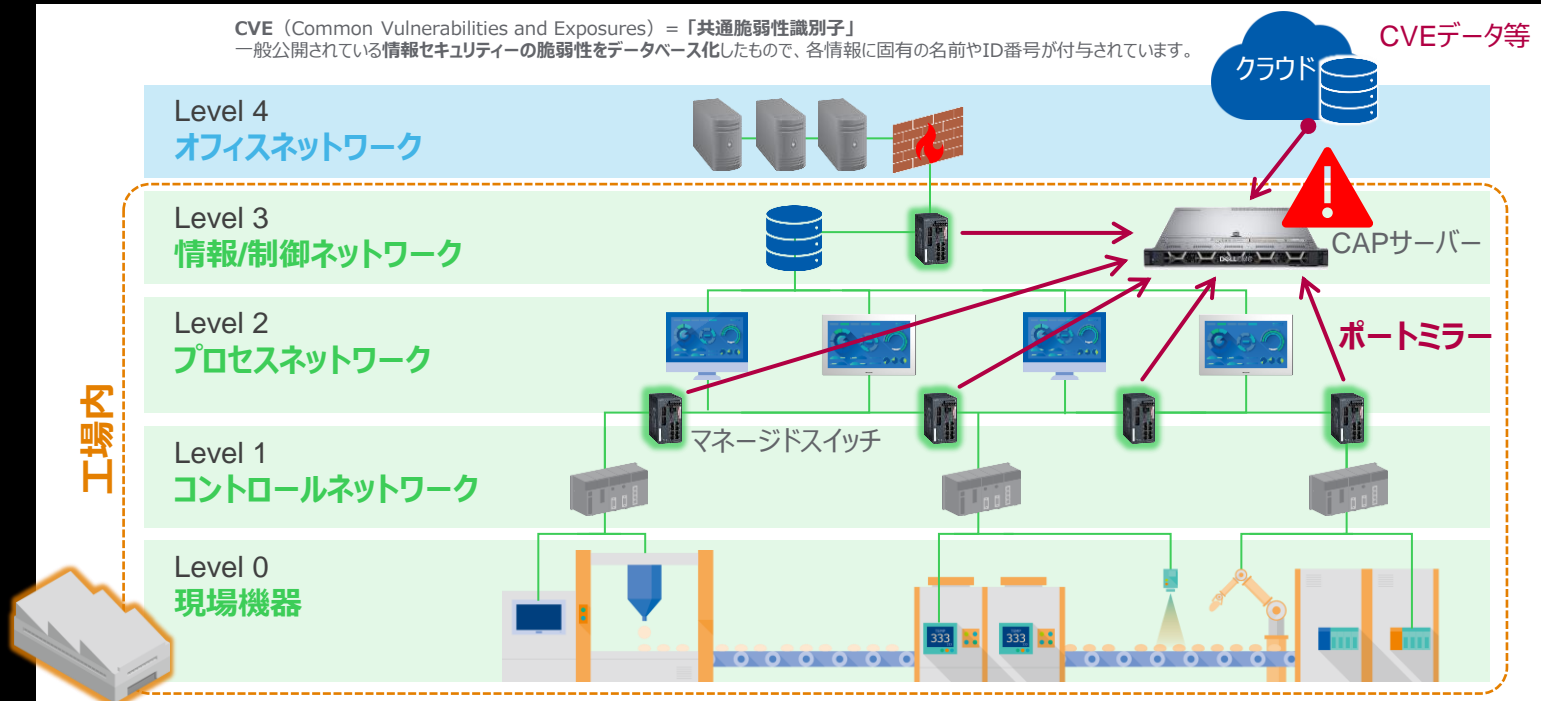
- 事業継続計画
- 災害復旧計画

実装構造イメージ

工場内の資産の見える化・ネットワークの見える化が第一ステップ

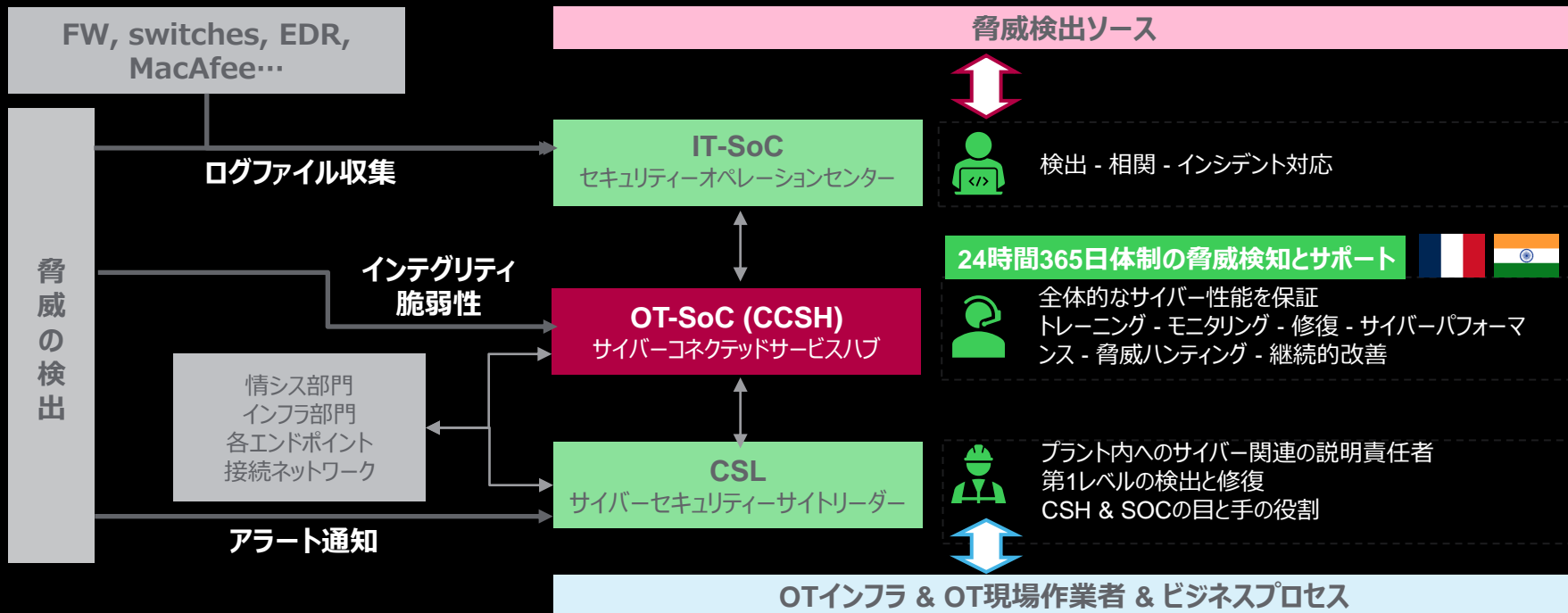
CVE (Common Vulnerabilities and Exposures) = 「共通脆弱性識別子」

一般公開されている情報セキュリティの脆弱性をデータベース化したもので、各情報に固有の名前やID番号が付与されています。



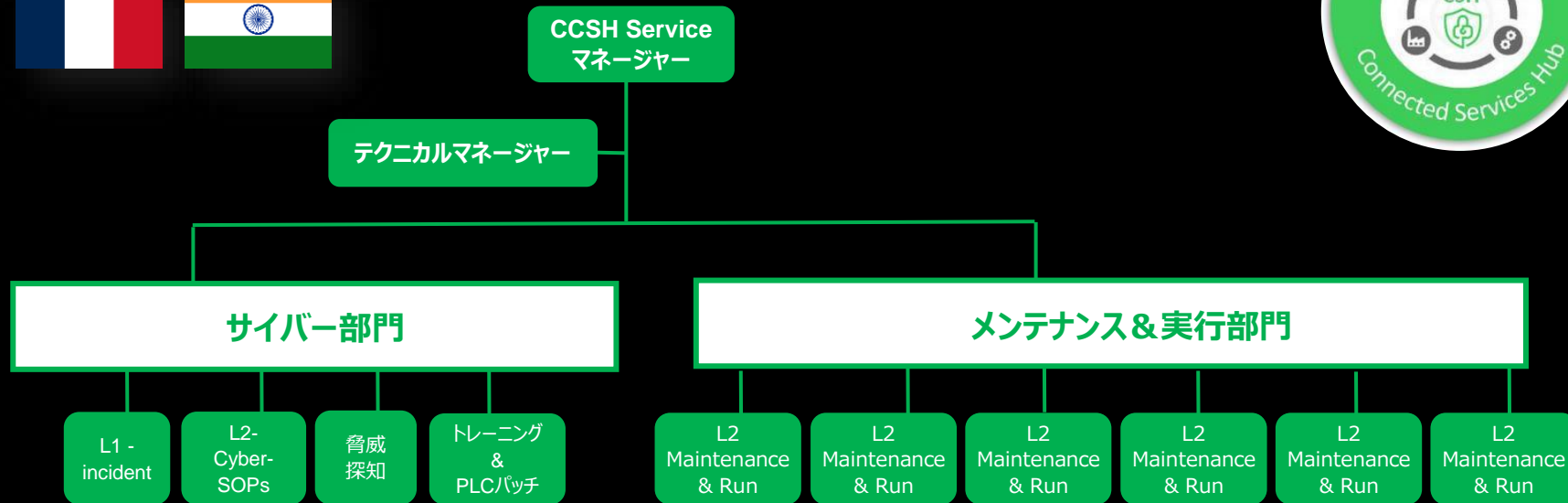
OTサイドのSoCを担うCCSH

社内にOT特化のSoCチームCCSHを組織

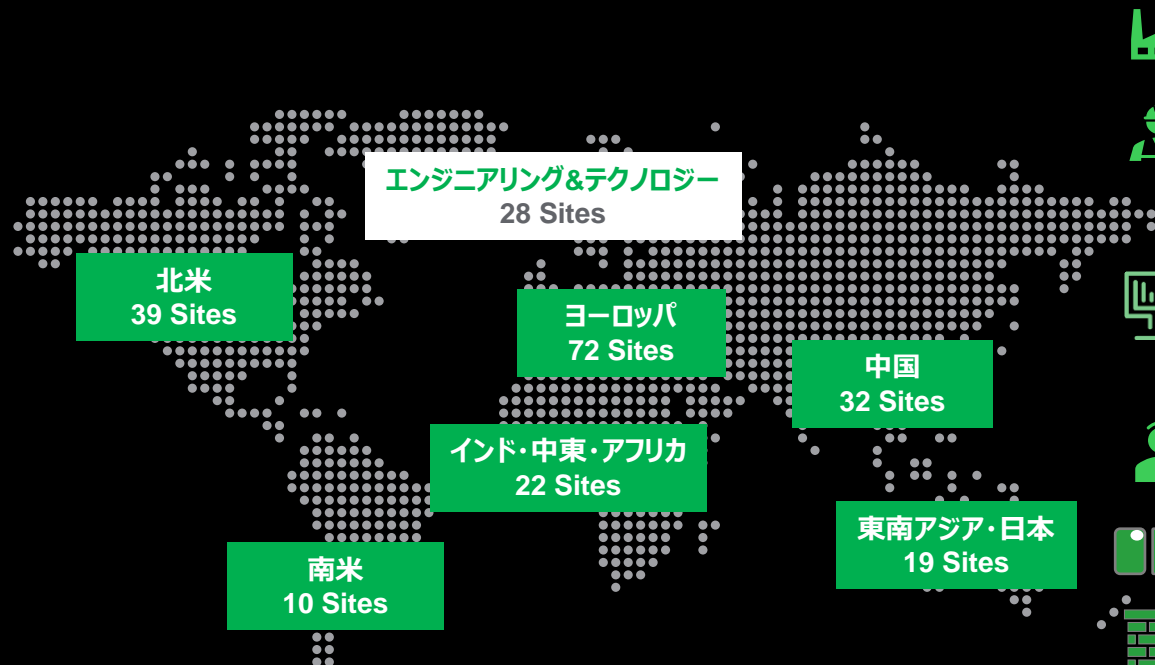


監視ハブOT-SoC (CCSH) の構造

24時間365日体制の脅威検知と対応をフランス、インドのCCSHが実践



サイバーセキュリティ サプライチェーン フットプリント



220拠点

プラント、エンジニアリング & テクノロジー



220人のサイバーセキュリティサイトリーダー (CSL)

各現場にサイバーセキュリティ説明責任者を配置
Compliance Security Policies



1 Cybersecurity Application Platform (CAP) / Plant

OT Threat Detection/Asset Inventory
Secure Remote Access



Incident Response Process

強固なオペレーティングモデル



PLCs Patching & Hardening

100%のPLCに最新のパッチ対応



IT/OT ファイアウォールによるセグメンテーション

100% の拠点に実装

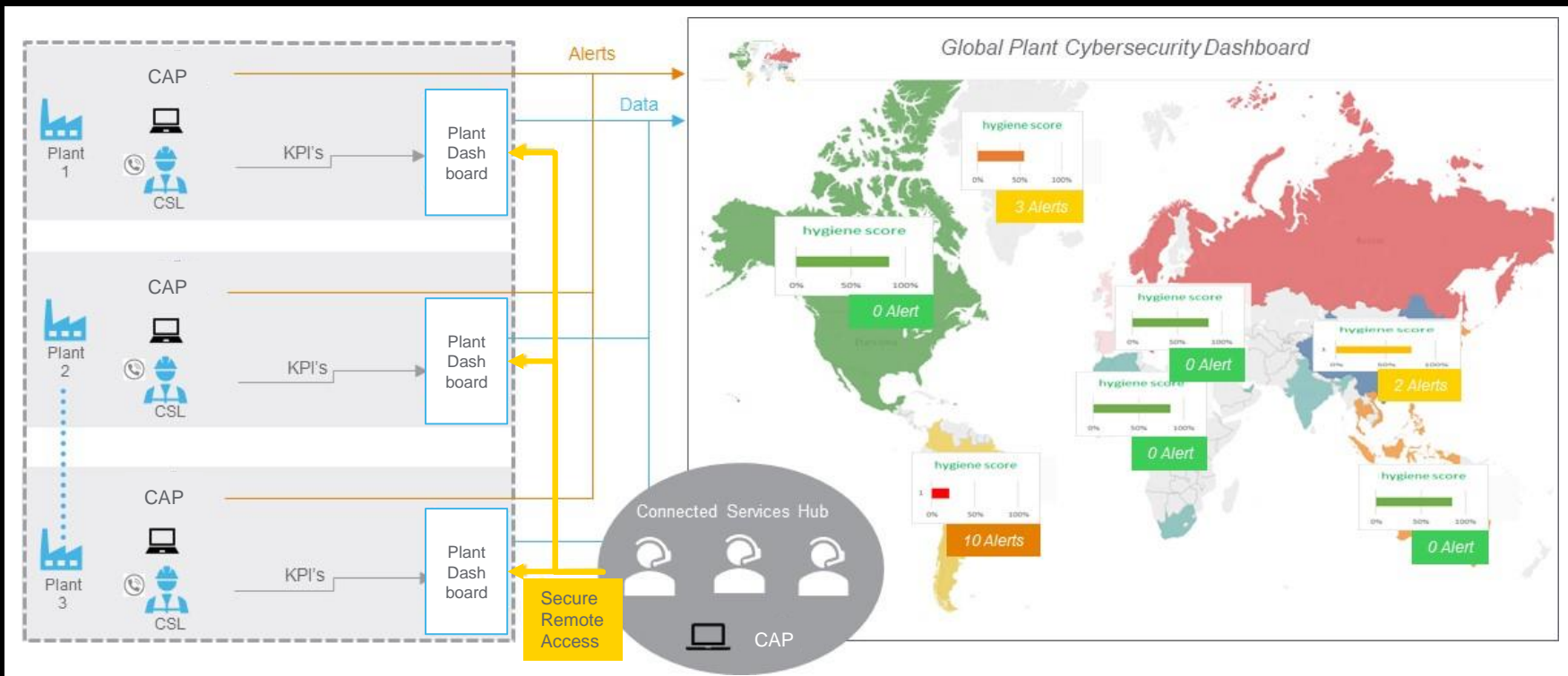


3 Productions Lines IEC62443

IEC62443 SL2に準拠

(サイバーコネクテッドサービスハブ)

CCSHで実現するサイバーセキュリティ体制のイメージ





顧客に提供する サイバーセキュリティ

シュナイダーエレクトリックのサイバーセキュリティソリューション

自社工場で構築して、培ったノウハウやソリューションをお客様にも提供

現状把握

監視

保全

マネージドセキュリティサービス (MSS)

シュナイダーが自社工場用に構築したCCSH (OT-SoC) の機能を
アセスメントから監視・対応まで一気通貫で顧客向けに提供



サイバーセキュリティ アセスメントサービス (CAS)

設備の現状把握/評価を行うサービス



サイバーセキュリティアプリケー ションプラットフォーム (CAP)

社内ネットワーク等に対する不正アクセ
ス等を防ぐサービスプラットフォーム
(不正侵入検知システム)



セキュアリモートアクセス (SRA)

資産へリモートアクセスする場合の管理
と操作記録を行うサービス

提供までの流れ

サポート対象範囲



マネージドセキュリティーサービス（MSS）の主な特長

シュナイダーエレクトリックが顧客に代わり 24時間365日体制で状況に応じた脆弱性管理、脅威のモニタリング、障害対応サポート等 OT-SoC としてのサービスを提供

- ・ 自社で培った知見、プロセス、テクノロジー、体制を採用
- ・ 日本国内のみでなくグローバルでMSSサービスを提供
- ・ グローバル及び各国のコンプライアンスを遵守
- ・ 自社での体制構築と維持にかかる顧客のコストと労力を節約
- ・ IT-OTセキュリティーの連携をサポート



セキュリティー体制を
即座に改善・構築



価値実現までの
時間を短縮



検出と対応の
平均時間を短縮

MSS 6つの管理項目軸

1. 資産とネットワーク管理



2. 脆弱性とリスク管理



3. 脅威とインシデント管理



4. CS制御管理



5. コンプライアンス管理



6. CSパフォーマンス管理

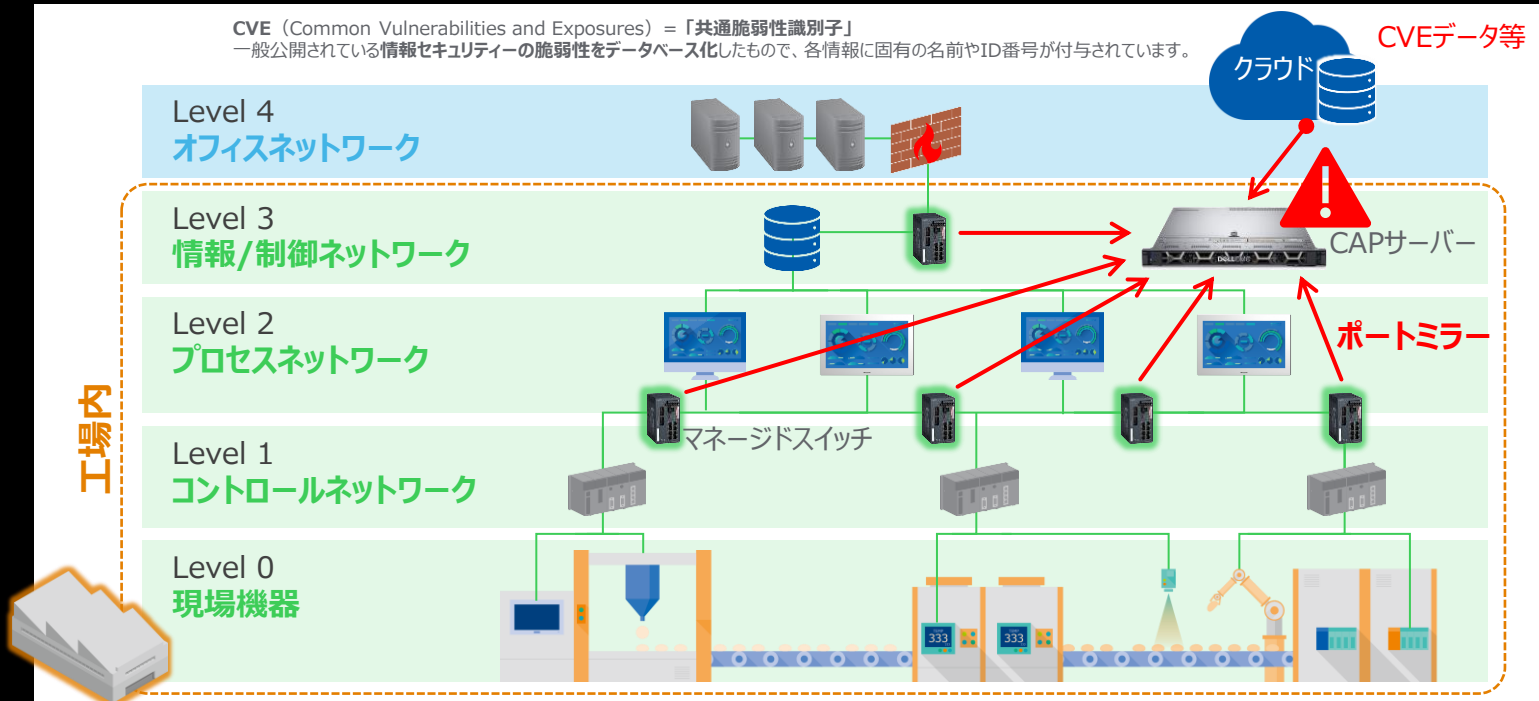


1. 資産とネットワーク管理（実装構造イメージ）

工場内の資産の見える化・ネットワークの見える化が第一ステップ

CVE (Common Vulnerabilities and Exposures) = 「共通脆弱性識別子」

一般公開されている情報セキュリティの脆弱性をデータベース化したもので、各情報に固有の名前やID番号が付与されています。



2. 脆弱性とリスク管理（脆弱性可視化 - 総合リスク）

サイト名 ▾

ネットワーク ▾

カテゴリ ▾

サブカテゴリ ▾

メーカー ▾

デバイスタイプ ▾

モデル ▾

リスクスコア ▾

有効可能性サブスコア ▾

インパクトサブスコア ▾

総合リスク

可能性とインパクト

補正制御

リスク推奨事項

総合リスク

システム内のデバイス総数



デバイス総数

デバイス
950

モデル
119



高リスク以上のデバイス数

重大リスクと高リスク

332

34.9%



過去1週間で高リスク以上になったデバイス数

新たな重大および高リスク

332

34.9%



過去1週間でリスクが増加したデバイス数

最近増加

0

0%



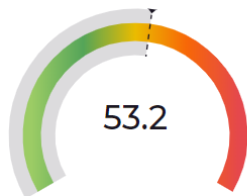
過去1週間でリスクが減少したデバイス数

最近減少

0

0%

総合リスクスコア ①



リスクスコアの分布

リスクスコア

デバイス

%

- Critical
- High
- Medium
- Low
- Very Low

92
240
550
59
9

9.7%
25.3%
57.9%
6.2%
0.9%



有効可能性とインパクトのヒートマップ ①

重大度・致命度・影響度

インパクト

	非常に低い	低い	中	高い	非常に高い
非常に低い	37	12	57	7	154
低い	8	37	67	4	58
中	94	1	8	4	45
高い	1	80	52	5	14
非常に高い	24	34	117	22	8

発生確率

有効の可能性

早急に対応検討すべきところ

3. 脅威とインシデント管理

クライアントの環境を24時間365日で監視して、
疑わしいアクティビティーと潜在的な侵害を特定します。

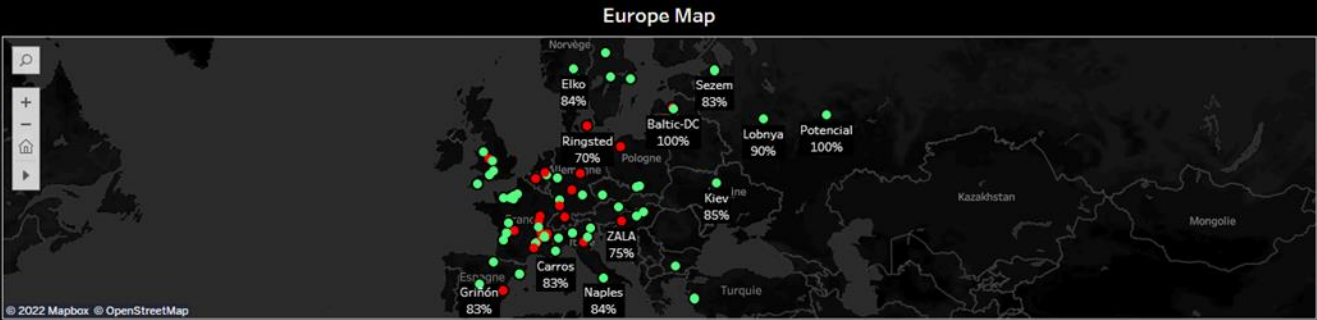
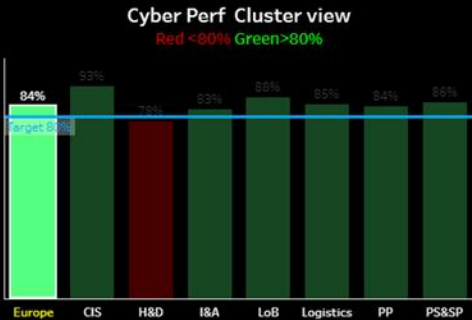
Life Is On

Cybersecurity Program GSC Europe 2022 YTD Results

YTD Results

Jan 2022

Feb 2022



Cluster		Site Short Name	Monthly Cyber Performance Y..	SCCM-Cylance KPI YTD	Xp Kpi YTD	Win7 KPI YTD	Password KPI YTD	PLC Patching YTD	Monthly Alert KPI YTD	Weekly Alert KPI YTD
CIS		Lobnya	90%	-10%	0%	0%	0%	0%	0%	0%
		Mekhanotronica	100%	0%	0%	0%	0%	0%	0%	0%
		Potencial	100%	0%	0%	0%	0%	0%	0%	0%
		Sezem	83%	-10%	0%	-5%	-5%	0%	0%	0%
H&D		Alès	78%	-10%	-5%	-5%	-5%	0%	0%	0%
		Eida	78%	-10%	-5%	-5%	-5%	0%	0%	0%
		Elso	79%	-10%	0%	0%	0%	0%	-11%	0%
		Feller	74%	-10%	-5%	-5%	-5%	0%	-4%	-30%
		Flint	95%	0%	0%	0%	-5%	0%	0%	0%
		Melliana	78%	-10%	-5%	-5%	-5%	0%	0%	0%
		Merten	83%	-10%	-5%	-5%	0%	0%	0%	0%
		Plovdiv	80%	-10%	-5%	-5%	-3%	0%	0%	0%
		Puente la Reina	83%	-10%	0%	-5%	-5%	0%	0%	0%

Help for CSL

Remediate Actions for CSL

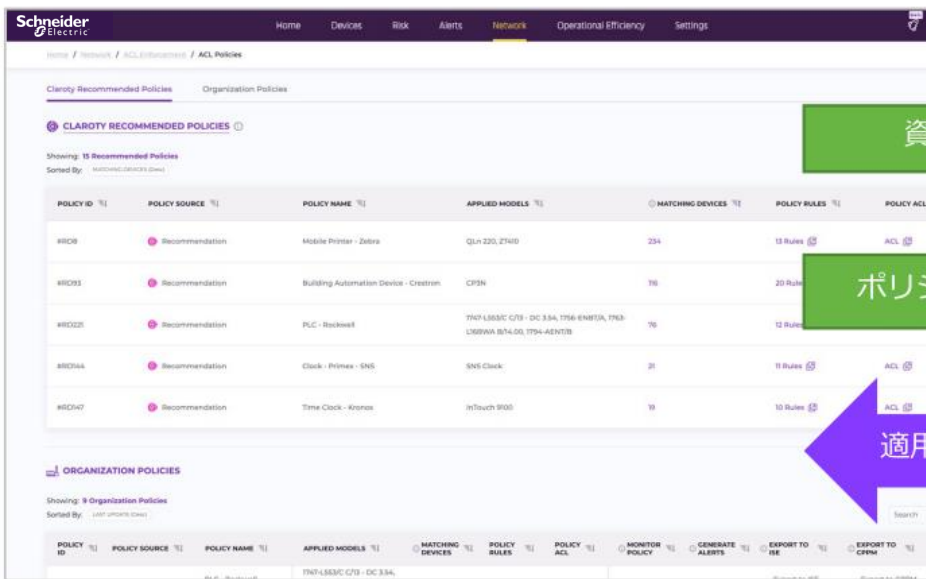


Instructions



3. 脅威とインシデント管理（ITダッシュボードとの連携）

CAP



The CAP interface displays a table of recommended policies. The table has columns for Policy ID, Policy Source, Policy Name, Applied Models, Matching Devices, Policy Rules, and Policy ACL. Below the table, there is a section for Organization Policies.

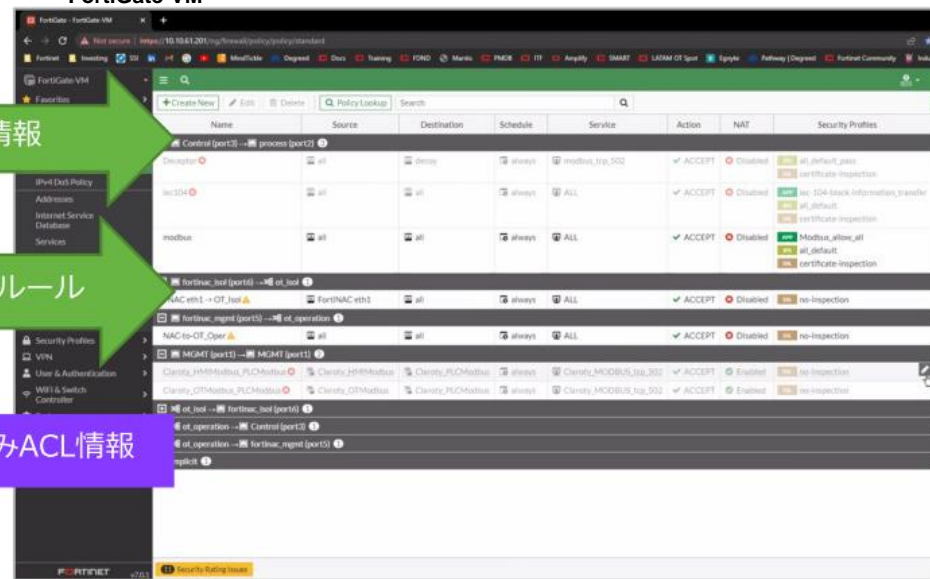
POLICY ID	POLICY SOURCE	POLICY NAME	APPLIED MODELS	MATCHING DEVICES	POLICY RULES	POLICY ACL
#B08	Recommendation	Mobile Printer - Zebra	QLA-220, Z740	234	13 Rules	ACL
#B093	Recommendation	Building Automation Device - Crestron	CP5N	76	20 Rules	ACL
#B0225	Recommendation	PLC - Beckhoff	7747-LS53C-C73 - DC 334, 1756-EN8T4, 1763-LS6RWA-B74-00, 1754-AEN70B	76	12 Rules	ACL
#B0344	Recommendation	Clock - Primex - SNS	SNS Clock	31	11 Rules	ACL
#B0407	Recommendation	Time Clock - Kronos	inTouch 900	19	10 Rules	ACL

ORGANIZATION POLICIES

POLICY ID	POLICY SOURCE	POLICY NAME	APPLIED MODELS	MATCHING DEVICES	POLICY RULES	POLICY ACL	MONITOR POLICY	GENERATE ALERTS	EXPORT TO IEE	EXPORT TO CPDM
#B0 - Beckhoff		7747-LS53C-C73 - DC 334								

FortiGate-VM

NAC/FW



The FortiGate-VM interface shows a table of policy rules. The table has columns for Name, Source, Destination, Schedule, Service, Action, NAT, and Security Profiles. Below the table, there is a section for Organization Policies.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
Control (port1) -> procmo (port1)	all	all	always	modbus_top_503	ACCEPT	Disabled	all, default, pass
inc504	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
modbus	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
fortinac_inet (port1) -> ot_inet	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
NAC-to-OT_inet	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
NAC-to-OT_Oper	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
Client_HIPModbus_RCMModbus	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
Client_OTModbus_RCMModbus	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
ot_inet -> fortinac_inet (port1)	all	all	always	ACL	ACCEPT	Disabled	all, default, pass
ot_inet -> fortinac_inet (port1)	all	all	always	ACL	ACCEPT	Disabled	all, default, pass

資産情報

ポリシールール

適用済みACL情報

1. CAPにてOT機器などの資産情報を可視化
2. CAP推奨ポリシーによる通信ポリシーを作成
3. 作成したポリシーをNAC/FWへエクスポートし、実際に通信を制限
4. NAC/FWから適用済みACL情報インポートし、資産のリスク評価に使用

3. 脅威とインシデント管理（様々なセキュリティ製品との連携）

Open APIにより新たな連携作成も可能

アセット検出&情報拡充化

DHCP/DNS

Infoblox
Microsoft
BLUECAT
BT

ネットワーク管理

Cisco
Aruba AirWave
SolarWinds
Microsoft Active Directory
VMware

バッチ管理

Microsoft SCCM
Quest

MDM

VMware Workspace ONE
Jamf
Microsoft Intune
MOBILETRON

ネットワークインフラ

Cisco Aruba Juniper

脆弱性とリスク管理

脆弱性スキャナ&自動化

Qualys / RAPID
tenable

脅威検知と対応

EDR

CROWDSTRIKE / Microsoft ATP
/ VMware / Sentinel One /
TANIMUM

アセットと変更管理

CMDB&チケットینگ

Bmc / ServiceNow
Cherwell

ネットワーク保護

ファイヤーウォール

Cisco / Check Point /
Palo Alto / VMware NSX /
Fortinet / FIREEYE

NAC

Cisco ISE / Aruba Clear
Pass / FORESCOUT /
Fortinet FortiNAC

SOAR

CORTEX XSOAR
SWIMLANE

SIEM

Splunk RSA / LogRhythm /
Tripwire / IBM QRadar /
graylog / MICRO Focus /
sumo logic

アセット管理

Accruent / Nuvolio
ServiceNow

バックアップとリカバリー&変更管理

Octoplat / AUVESY-MDT/
Rockwell Automation

5. コンプライアンス管理

IEC 62443 2-1

4. サイバーセキュリティマネジメントシステム

4.1 一般要求事項組織は、その組織の事業活動全般及び直面するリスクに対する考慮のもとで、文書化したCSMSを確立、導入、運用、監視、レビュー、維持及び改善しなければならない。CSMSに要求されている要素は、IACS（Industrial Automation and Control System）をサイバー攻撃から保護するためである。

4.2 リスク分析

4.2.1 概要組織は次の事項を実行しなければならない。

4.2.2 事業上の根拠

4.2.2.1 事業上の根拠の策定組織は、IACSのサイバーセキュリティを管理するための組織の取り組みの基礎として、IACSに対する組織の固有の依存性に対処する、上位レベルの事業上の根拠を策定しなければならない。

4.2.3 リスクの識別、分類及びアセスメント

4.2.3.1 リスクアセスメント方法の選択組織は、組織のIACS資産に関連するセキュリティ上の脅威、ぜい弱性及び結果に基づいてリスクの識別とその優先順位付けを行う、リスクのアセスメント及び分析のための特定のアプローチ及び方法を選択しなければならない。

4.2.3.2 リスクアセスメントの背景情報の提供組織は、リスクの識別を開始する前に、リスクアセスメント活動の参加者に対して、方法に関する訓練などの適切な情報を提供しなければならない。

4.2.3.3 上位レベルのリスクアセスメントの実行IACSの可用性、完全性又は機密性が損なわれた場合の財務的結果及びHSE（health,safetyand environment）に対する結果を理解するために、上位レベルのシステムリスクアセスメントが実行されなければならない。

4.2.3.4 IACSの識別組織は、各種のIACSを識別し、装置に関するデータを収集してセキュリティリスクの特性を識別し、それらの装置を論理的システムにグループ化しなければならない。

4.2.3.5 単純なネットワーク図の策定組織は、論理的に統合されたシステムのそれぞれについて、主要装置、ネットワークの種類及び機器の一般的な場所を示す単純なネットワーク図を策定しなければならない。

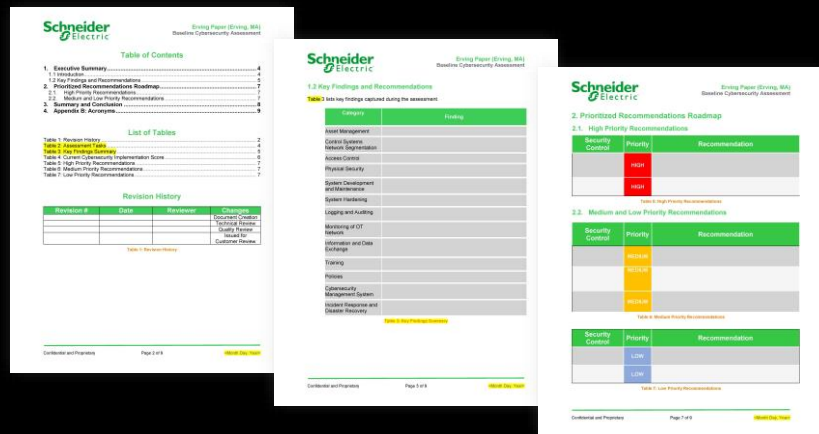
4.2.3.6 システムの優先順位付け組織は、各論理制御システムのリスクを軽減するため、基準を策定して優先順位を割り当てなければならない。

4.2.3.7 詳細なぜい弱性アセスメントの実行組織は、組織の個々の論理IACSの詳細なぜい弱性アセスメントを実行しなければならない。このアセスメントは、上位レベルのリスクアセスメントの結果及びそれらのリスクにさらされるIACSの優先順位付けに基づいて適用範囲を決定してもよい

- NISTフレームワーク又はIEC62443コンプライアンス要件に沿ったコンテンツ化されたコンプライアンス及び規制レポートを提供。
- 脅威検出プラットフォームから受信及び分析されたデータに基づいて主要なサイバーKPIに関するレポートを作成し、OT環境のセキュリティ体制を示します。

(IEC 62443パート2-1、2-3、3-3への評価と適合状況)

(NISTフレームワークに対する評価と適合状態)



6. パフォーマンス管理



月次報告書の主な内容

～導入時に決めたKPIに対する報告～

- 最高情報セキュリティ責任者へのパフォーマンス指標
- お客様のセキュリティ体制を強化するための提案
- セキュリティ体制を改善するための推奨事項



提供予定のサービス

まずは「Core」からサービスを開始！

1: 資産とネットワーク管理

2: 脆弱性とリスク管理

3: 脅威とインシデントの管理

4: CS制御管理

5: コンプライアンス管理

6: パフォーマンス管理



Core

- ・資産及びネットワーク情報の可視化とマッピング
- ・脆弱性評価
・セキュリティ更新アドバイス
- ・P1インシデントへのアドバイス
・脅威の検出と優先順位付け
・脅威の速報
- ・サイバーセキュリティデバイスとプラットフォームの健全性を管理
- ・規制と法令遵守報告書の作成
- ・KPI とレポート



Enhanced（強化版）

- ・ソフトウェア部品表の管理
・攻撃対象資産の把握と管理
- ・会社間経路全体の脆弱性管理
・リスクの定量化
- ・P2-3インシデントへの対応
・脅威インテリジェンスとハンティング
- ・サイバーセキュリティ制御管理 (IDM, PKI, B&R, FW)
- ・内部ポリシーコンプライアンスレポート
・ポリシーの推奨事項カスタマイズ
- ・経営幹部レベルのKPIレポート
・業界のベンチマーク



Optimized（最適化版）

- ・資産のライフサイクル管理
- ・リスクガバナンスサービス
- ・攻撃と侵害のシミュレーション
フォレンジック調査とマルウェア分析
- ・CSコントロールの有効性の監視
- ・継続的なコンプライアンス監視と推奨事項
- ・サービスとしての CISO

全世界のサイバーセキュリティチームを活用

220

全世界220の
シュナイダー拠点をサポートする
セキュリティエキスパート

100

認定資格を持つ
OTサイバーコンサルタント

3500

認定サイバートレーニングを受けた
サービスエンジニア



セキュリティパートナーとサイバーエコシステムを構築

Network segmentation



End point protection



Secure remote access



Patching, servers and network support



Anomaly Detection



シュナイダーエレクトリックが 提供できる価値

シュナイダー自らが取り組んできた
実績とノウハウ



OTサイバーエコシステム構築の
最大のボトルネックとなるIT/OT
融合の橋渡し



世界的なパートナーとともに提供
するサービス



Life Is On | **Schneider**
Electric

se.com

