OTサイバーセキュリティーの鍵を握る OT-SoCの重要性

2024 CIP&ICSサイバーセキュリティコンファレンス

シュナイダーエレクトリック
インダストリーソリューション & サービス
ダイレクター　森本　直幸

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

私たちは、**あらゆる人がエネルギーや資源を**
最大限活用することを可能にし、世界の進歩と
持続可能性を同時に実現することを目指しています。

私たちはこれを Life Is On と表現しています。

私たちのミッションは、**持続可能性と効率性を実現するための**
デジタルパートナーになることです。

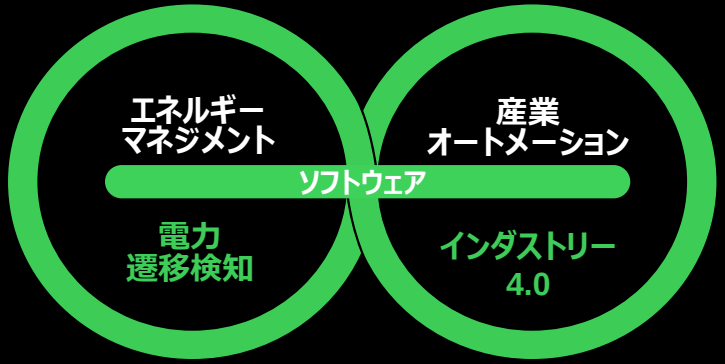
© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

エネルギーとオートメーションに効率性と持続可能性のためのデジタルソリューションを提供

€34bn グループ全体での2022年収益

135k+ 100以上の国・地域で働く従業員数



核となる2つのビジネス

バランスの取れた収益構造

サスティナビリティ ＋ 効率化

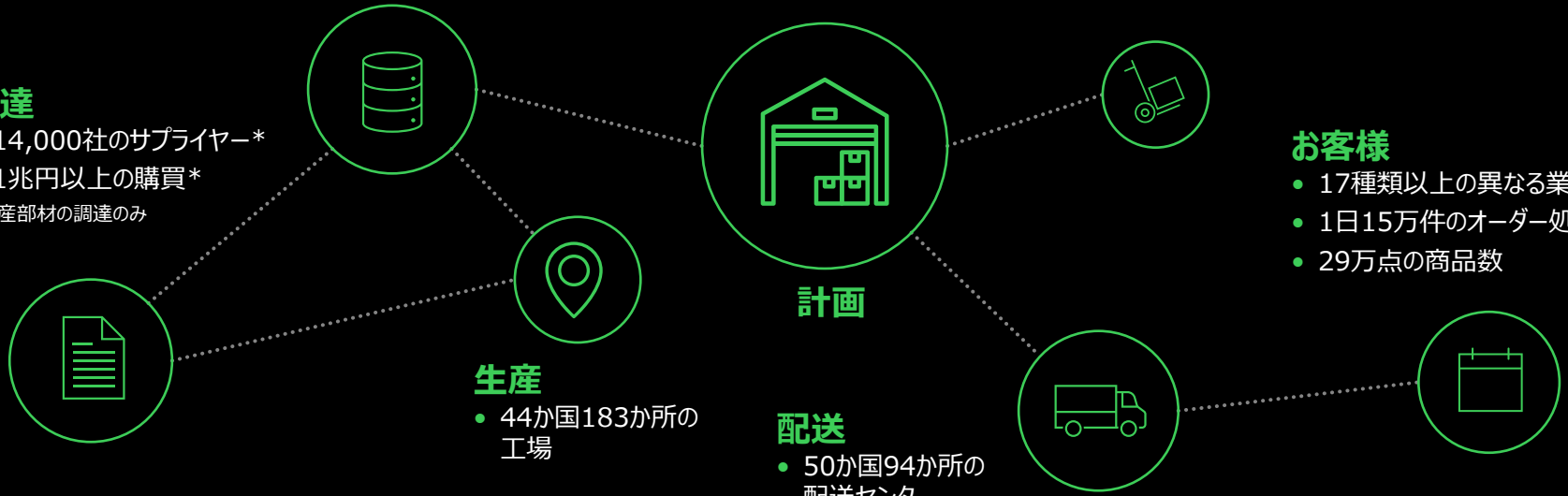
収益(グループ別)	製品 58%	システム 24%	ソフトウェア及びサービス 18%	
業界・市場別	データセンター 16%	ビルディング 37%	製造業 34%	インフラ 13%
地域別	ヨーロッパ 25%	北米 32%	アジア太平洋 30%	その他の地域 13%

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

進化したグローバルサプライチェーンの構築で安定した生産と物流

エンドツーエンドのバリューチェーンを実現するグローバルネットワークの実現



サプライチェーン全体で約8万人の従業員

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

デジタル化とサスティナビリティにおける実績と対外的な評価

世界最高のデジタル化とサステナビリティのソリューションプロバイダーであるために

運用実績

200か所
工場数

100か所
物流センター

400社以上
サプライヤーと業界エキスパートとのコラボ

100か所
スマート工場
スマート物流センター

30か所
ゼロカーボン施設

ETO、MTO、MTS*のさまざまな生産形態

Gartner
第1位
2023年
サプライチェーントップ25社

WORLD ECONOMIC FORUM
8認定
2023年
世界経済フォーラム
ライトハウス認定工場

Corporate Knights
1位
2021年
世界で最も持続可能性の高い企業

* ETO =特機生産、MTO =受注生産、MTS =在庫生産

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

エコシステム全体で
ESGの
模範的存在
となる

A Global 100
Most Sustainable Corporation
ダボス会議「世界で最も持続可能な100社」コーポレートナイツ社発表

13年連続ランクイン
2024年は7位

Moody's | ESG Solutions

全世界120 および **欧州**120 の indexに選出

---

ecovadis

評価対象 100,000 社の
上位1% にあたる
プラチナ評価を獲得

CDP

12年連続で
気候変動部門 A-list に選定

Dow Jones Sustainability Indices
Powered by the S&P Global CSA

全世界 および **欧州**
2つのindexで業界**1位**の評価

© 2024 Schneider Electric, All Rights Reserved

Life Is On | Schneider Electric

あらゆる人がエネルギーや資源を最大限活用することを可能にし世界の進歩と持続可能性を同時に実現することを目指す

2つの側面における方程式

自社の事業や
エコシステムの中で
模範となる

顧客のための
ソリューションの
一部となる

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

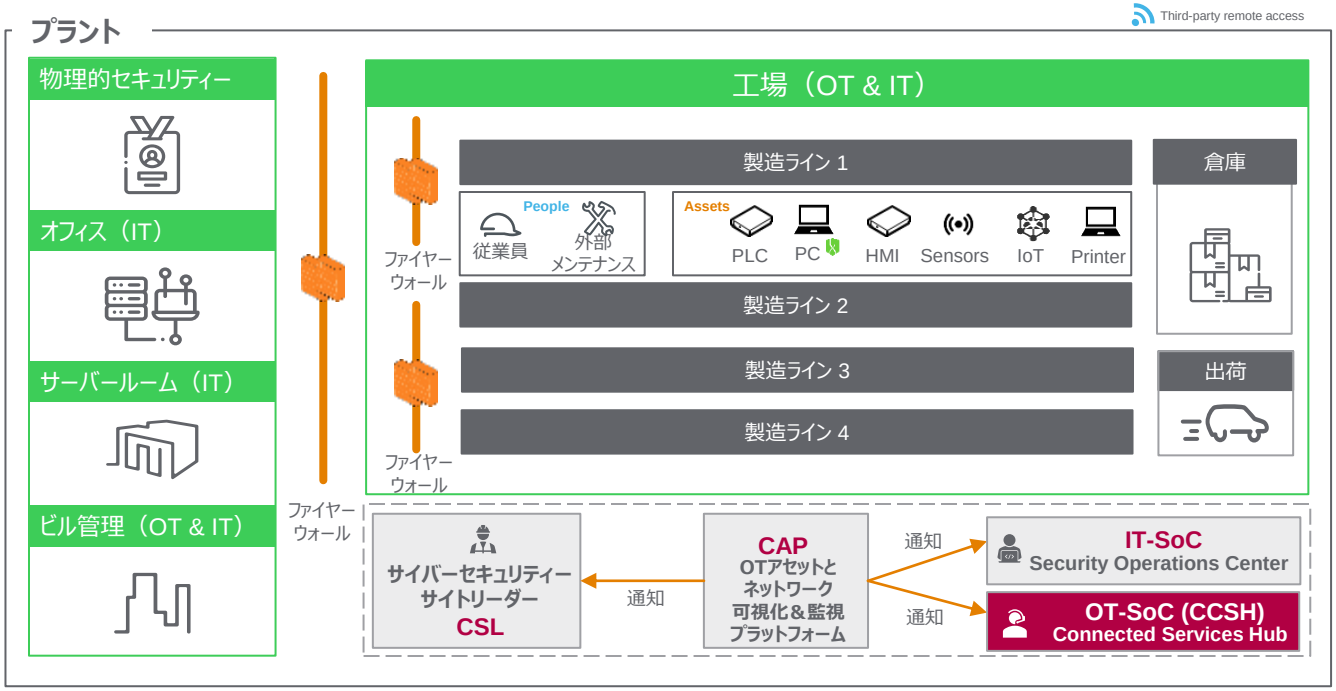
シュナイダーエレクトリックのサイバーセキュリティー

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

シュナイダーエレクトリックのサイバーセキュリティー

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



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

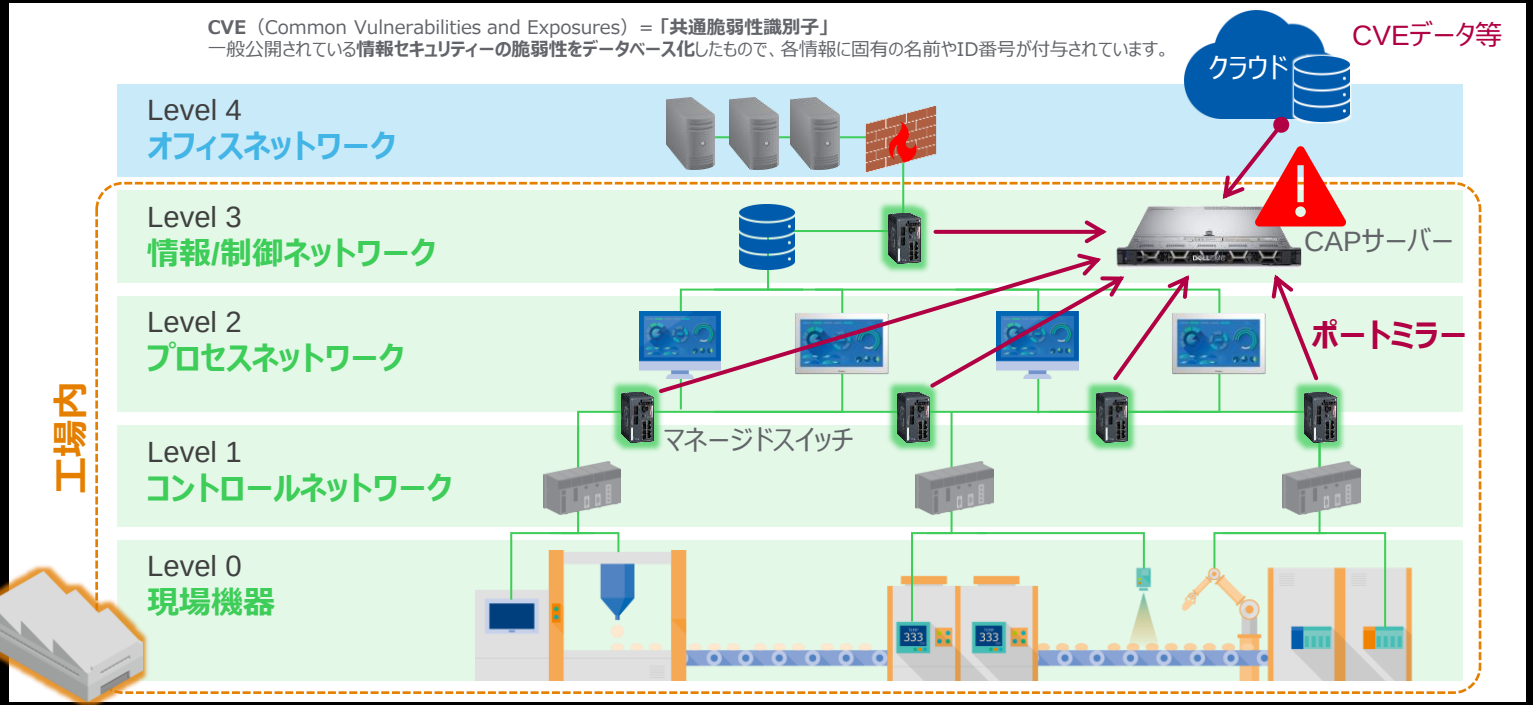
回復
- 事業継続計画
- 災害復旧計画

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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

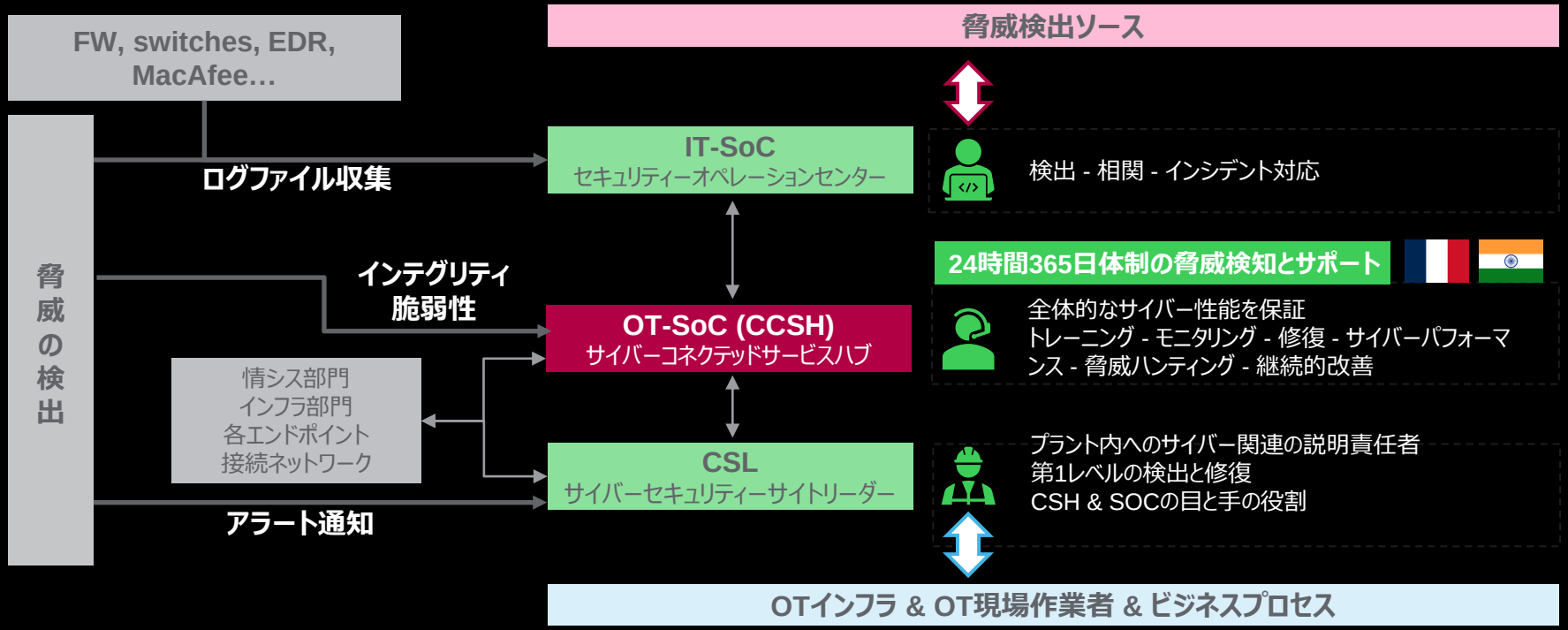


© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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



© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

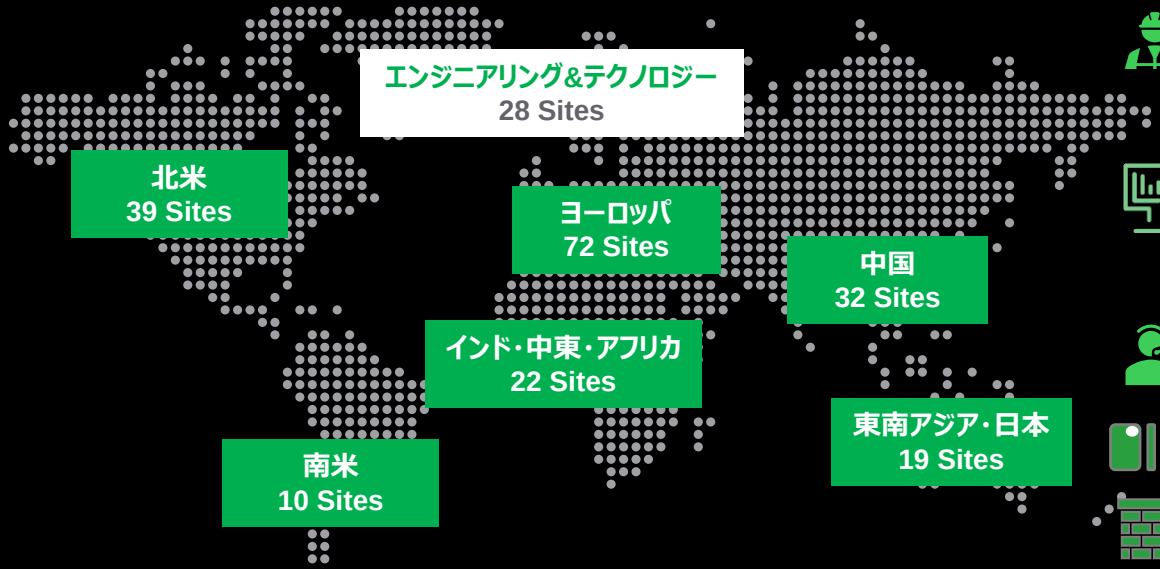
監視ハブOT-SoC (CCSH) の構造

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

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

シュナイダーのサイバーセキュリティー 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ーサイトリーダ（CSL）
各現場にサイバーセキュリティー説明責任者を配置
Compliancy 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 ファイヤーウォールによるセグメンテーション
100% の拠点に実装

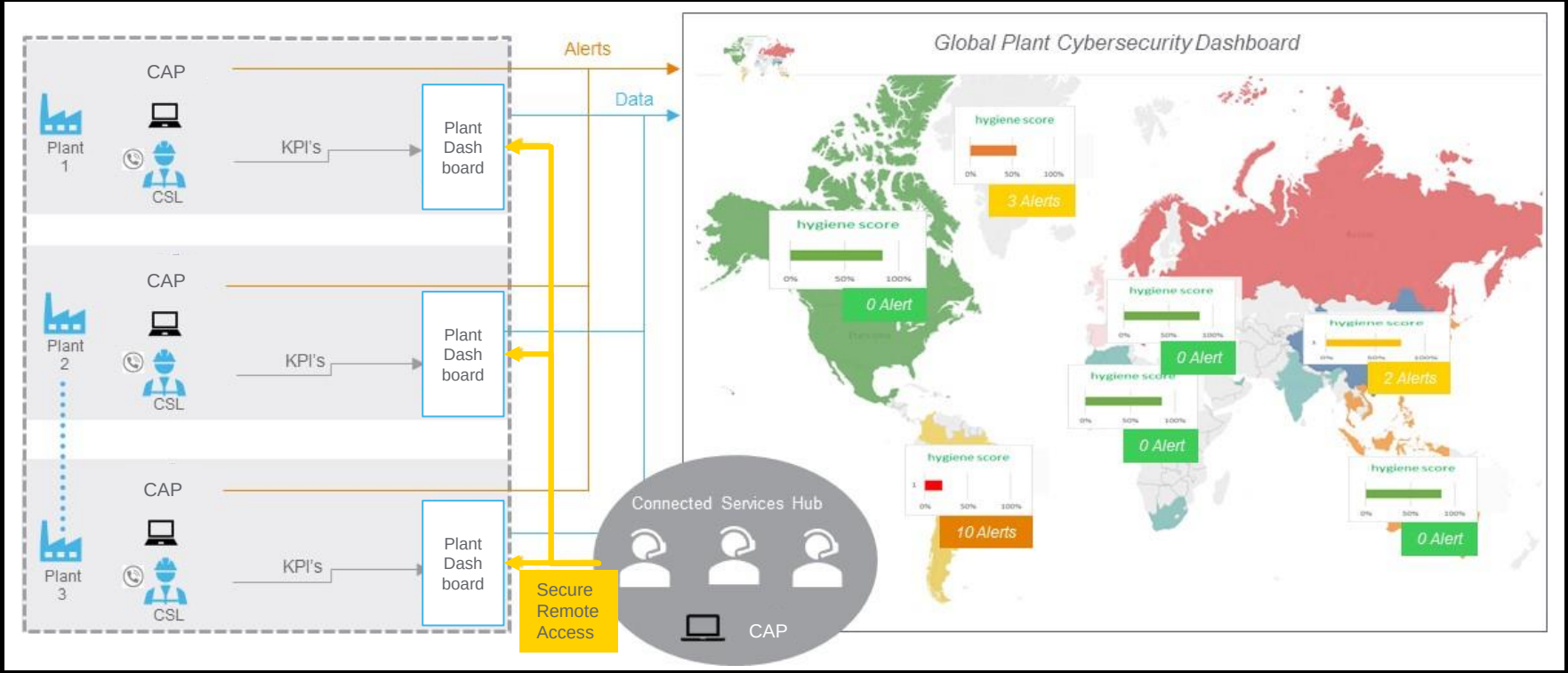
3 Productions Lines IEC62443
IEC62443 SL2に準拠

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

（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ー体制のイメージ



© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

顧客に提供する
サイバーセキュリティー

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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アタック
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11億円

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

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

立場によって異なるOTサイバーセキュリティーの捉え方

サイバーセキュリティーは
非常に重要で関心あり。
対応はITチームに一任。

サイバーセキュリティーについては
理解しており、対策は万全。
OT? ITネットワークは対策して
いるので問題ない。

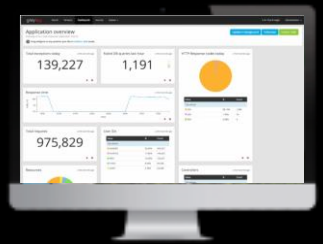
日々のメンテナンス業務で手一杯！
セキュリティー関連はITチームが対応
しているのでよく分からない。

マネジメント

IT

OT / ファシリティー

橋渡しが必要



© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

OTサイバーセキュリティー業界が抱える課題

IT/OTセキュリティー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ー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。

セキュリティー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、セキュリティーチームがセキュリティー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ーに割り当てられる予算の不足

セキュリティー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。

© 2024 Schneider Electric, All Rights Reserved

シュナイダーのサイバーセキュリティーソリューション

自社工場で採用し、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ーサービス（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ー
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ーアプリケー
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

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

1. 資産とネットワーク管理

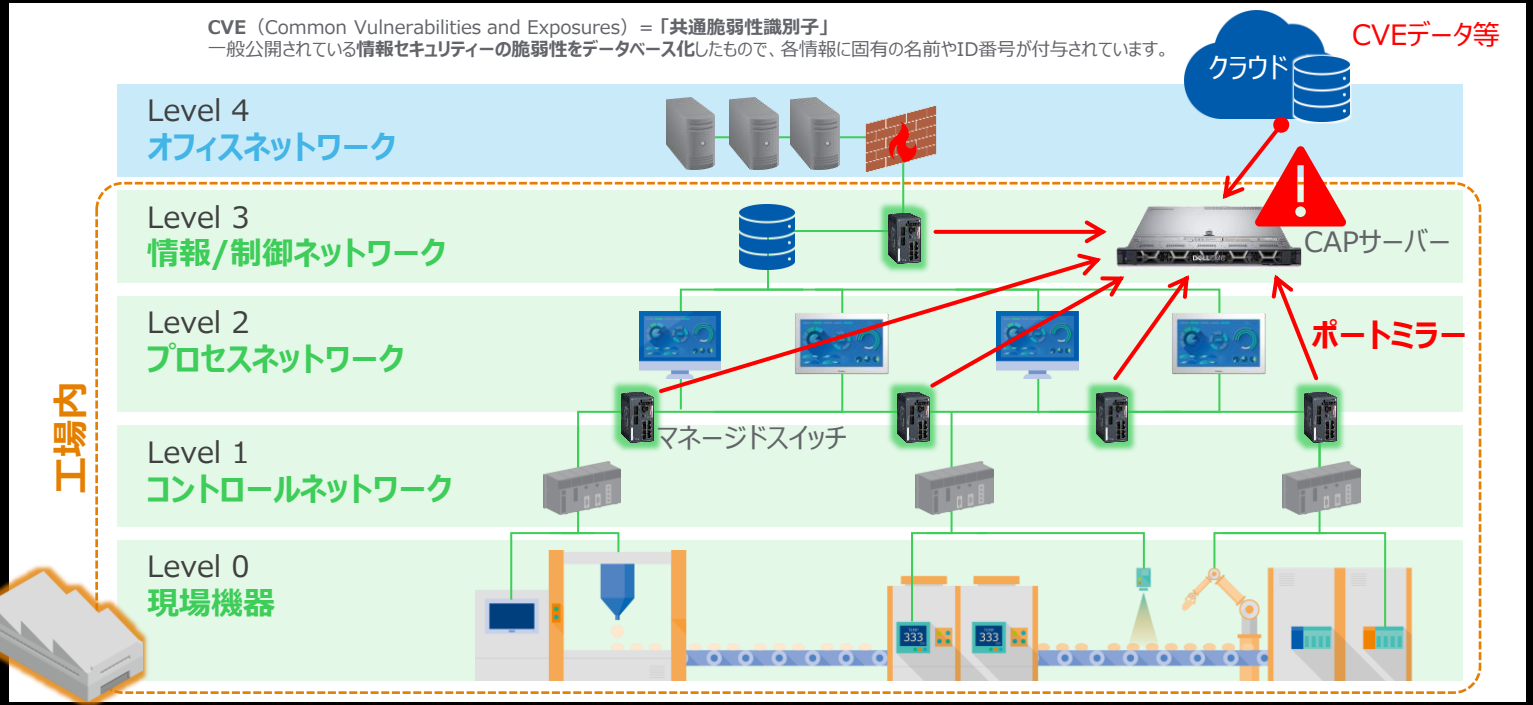
資産と資産間の通信を継続的に監視し、
プロセスの安定稼働を妨げる可能性のある
疑わしい変更や異常なアクティビティーの有無を
確認します。

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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



© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

2. 脆弱性とリスク管理

重要なパッチ、不要なオープンポート、

危険な構成設定など、

クライアントのインフラストラクチャー、資産、

システム内の脆弱性をプロアクティブに特定して、

攻撃者による悪用のリスクを最小限に抑えます。

© 2024 Schneider Electric, All Rights Reserved

3. 脅威とインシデント管理

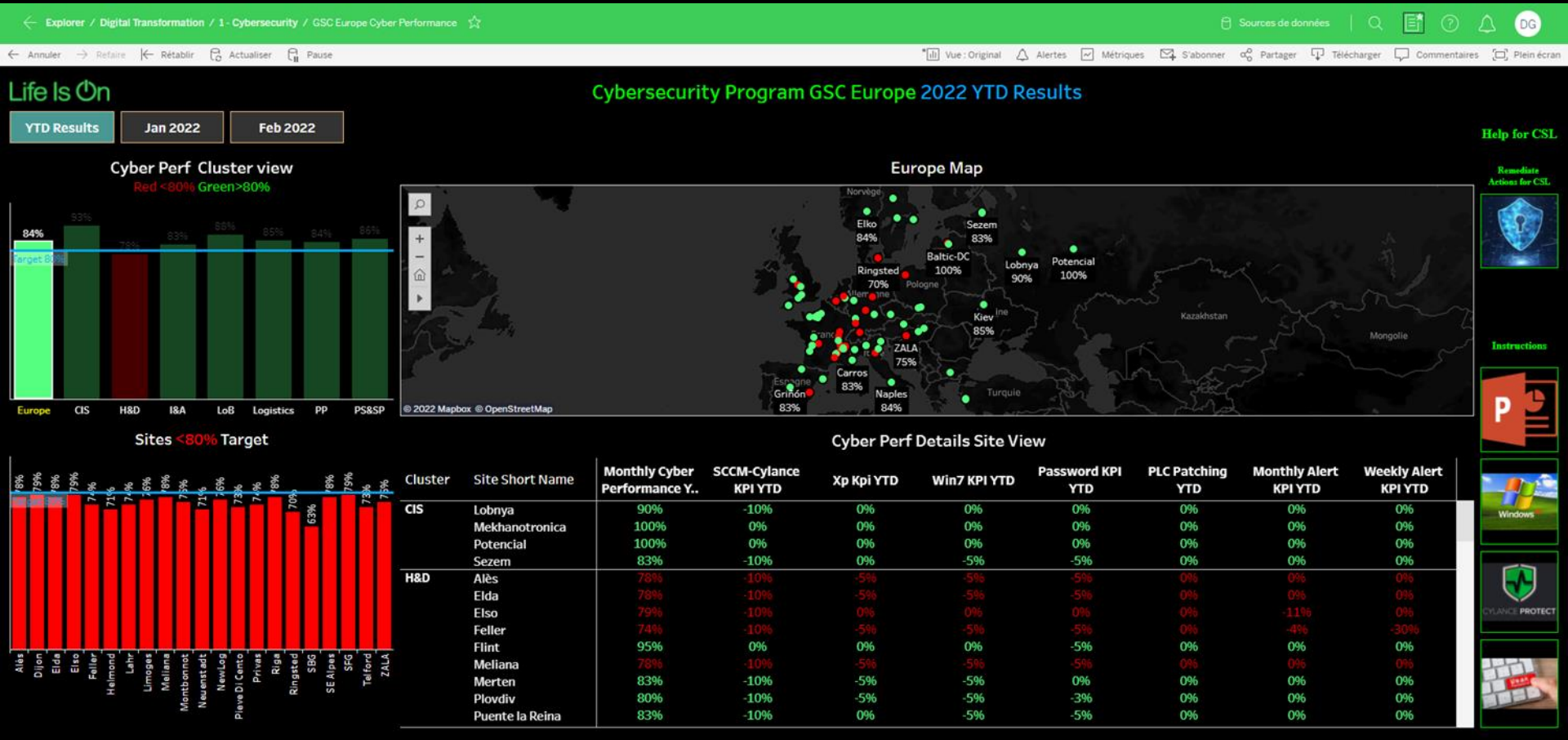
お客様の環境を24時間365日で監視して
疑わしいアクティビティーと潜在的な侵害を
特定します。
すべてのアラートは優先度のもと、迅速に対応し
必要に応じてインシデント対応手順
をお客様へ提供します。

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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。



3. 脅威とインシデント管理（様々なセキュリティー製品との連携）

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

ネットワーク保護

ファイヤーウォール
Cisco / Check Point / pololalto / Vmware NSX / Fortinet / FIREEYE

NAC
Cisco ISE / Aruba Clear Pass / FORESCOUT / Fortinet FortiNAC

脅威検知と対応

EDR
CROWDSTRIKE / Microsoft ATP / Vmwere / Sentinel One / TANIUM

SOAR
CORTEX XSOAR
SWIMLANE

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

アセットと変更管理

CMDB＆チケッティング
Bmc / ServiceNow
Cherwell

アセット管理
Accruent / Nuvolo
ServiceNow

バックアップとリカバリー＆変更管理
Octoplant / AUVESY-MDT/
Rockwell Automation

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

4. サイバーセキュリティー制御管理

サイバーセキュリティーデバイスの正常性と
安定稼働を継続的に監視し、
セキュリティー制御の最適なパフォーマンスを
保証して、最大限の保護を提供します。

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

4. サイバーセキュリティー制御管理

EMC の健全性ステータス

データを更新する

サーバーの状態

サーバーCPU	サーバーストレージ	サーバーメモリ
2.8%	41.2%	36.41%

アプリケーションの健全性

表示中: **6 つの健康要因**

健康要因	状態	ステータスの説明
重要なサービスは稼働中です	真実	CTD クリティカル サービスは稼働中です。
アラートが作成されます	間違い	過去 2 日間に CTD によって新しいアラートは作成されませんでした。
適切な資産データの収集	真実	資産はしきい値を超えませんでした。
適切なベースラインデータ収集	真実	ベースラインはしきい値を超えませんでした。
スケジュールされたバックア…	該当なし	構成された設定のため、またはスケジュールされた時間がまだ経過して…

サーバーの制御管理事項

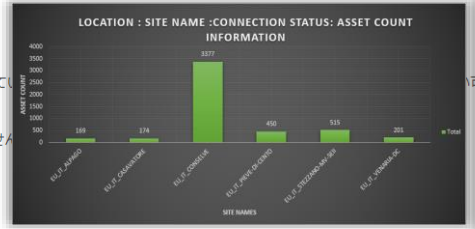
設置場所、ステータス、型式、OS Ver、シリアル、I/F、IP、MAC、連続稼働日数、認識したVLAN数、前週認識したVLAN数、過去1時間に認識したVLAN数、トラフィック前月平均(Mbps)、トラフィックの前週平均、トラフィックの過去1時間平均、未処理のインシデント数

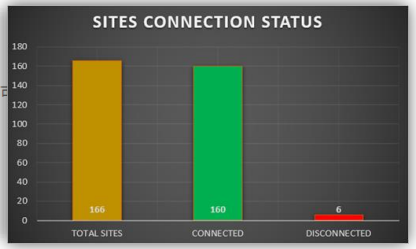
1.ヘルスモニタリング:

- 範囲内のCS制御の正常性、可用性、パフォーマンスを常時監視
- 発生した問題に対して24時間365日サポートサービス
- 検出された問題を修正するために必要な推奨事項を提供

2.メンテナンスとアップグレード:

- お客様の承認後、CSHはお客様に修正プログラム、更新プログラム、ナレッジベースを展開





5. コンプライアンス管理

シュナイダーエレクトリックは、

監査とレポートを定期的に行い

セキュリティー慣行が業界固有の規制と標準に

準拠していることを確認します。

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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ーマネジメントシステム

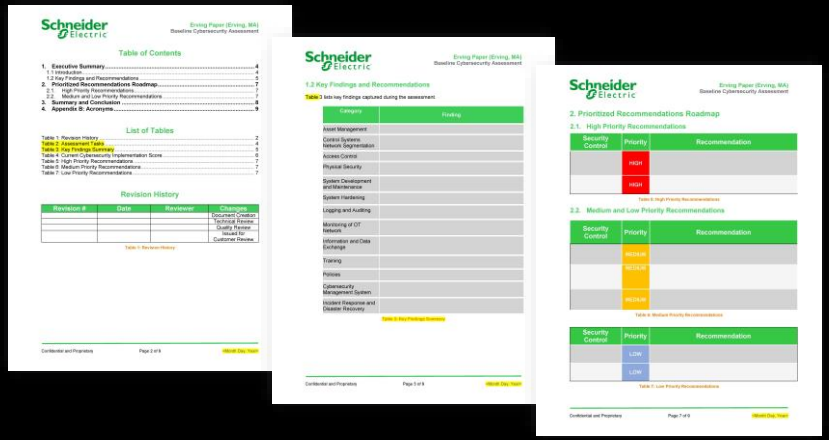
4.1 一般要求事項組織は、その組織の事業活動全般及び直面するリスクに対する考慮のもとで、文書化したCSMSを確立、導入、運用、監視、レビュー、維持及び改善しなければならない。CSMSに要求されている要素は、IACS（Industrial Automation and Control System）をサイバー攻撃から保護するためである。

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ー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ー上の脅威，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,saftyand 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ー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キスト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ー体制を示します。**

（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）



© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

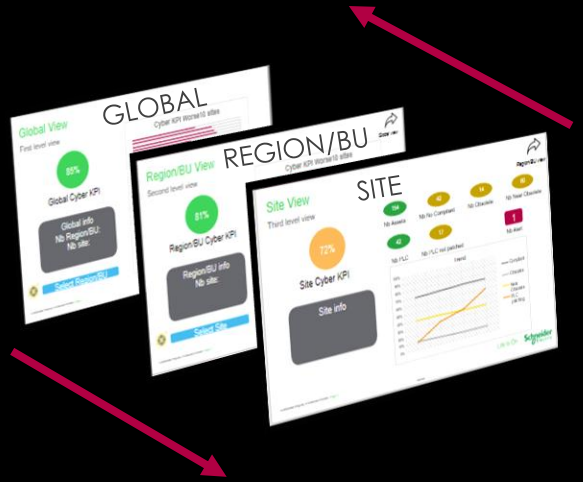
6. パフォーマンス管理

当社のCSエキスパートは、
主要なサイバーセキュリティーの指標と結果を
毎月レビューして、クライアントがセキュリティー
体制を継続的に評価及び改善できるよう
支援します。

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

提供予定のサービス

まずは「Core」からサービスを開始！

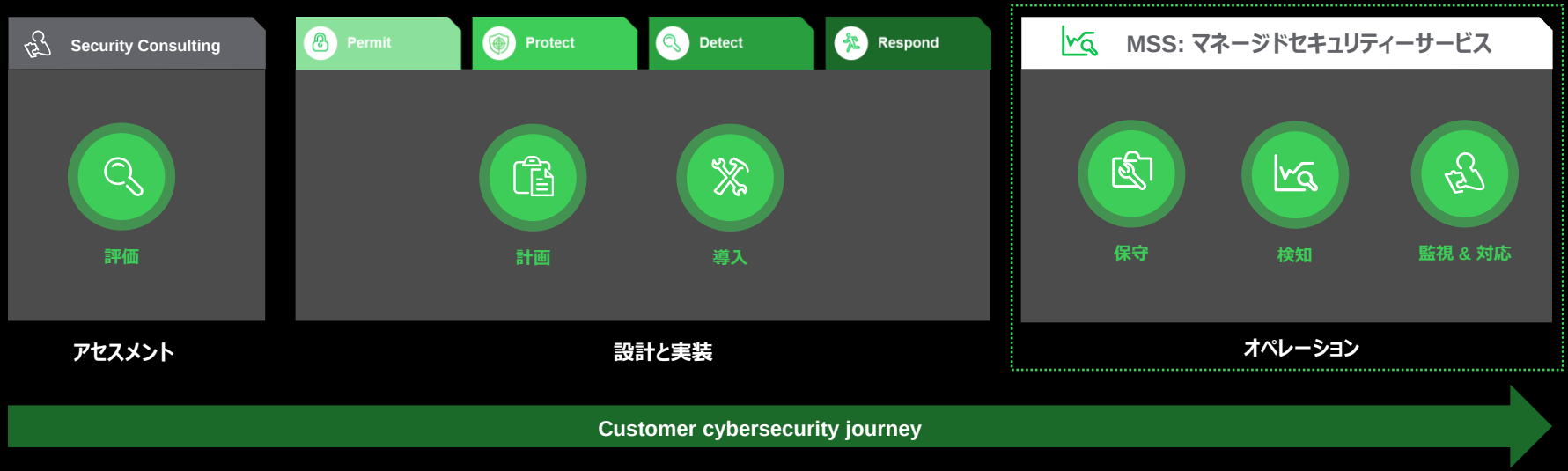
	Core	Enhanced（強化版）	Optimized（最適化版）
1: 資産とネットワーク管理	・資産及びネットワーク情報の可視化とマッピング	・ソフトウェア部品表の管理 ・攻撃対象資産の把握と管理	・資産のライフサイクル管理
2: 脆弱性とリスク管理	・脆弱性評価 ・セキュリティー更新アドバイス	・会社間経路全体の脆弱性管理 ・リスクの定量化	・リスクガバナンスサービス
3: 脅威とインシデントの管理	・P1インシデントへのアドバイス ・脅威の検出と優先順位付け ・脅威の速報	・P2-3インシデントへの対応 ・脅威インテリジェンスとハンティング	・攻撃と侵害のシミュレーション フォレンジック調査とマルウェア分析
4: CS制御管理	・サイバーセキュリティーデバイスとプラットフォームの健全性を管理	・サイバーセキュリティー制御管理 (IDM,PKI,B&R,FW)	・CSコントロールの有効性の監視
5: コンプライアンス管理	・規制と法令遵守報告書の作成	・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	・継続的なコンプライアンス監視と推奨事項
6: パフォーマンス管理	・KPI とレポート	・経営幹部レベルのKPIレポート ・業界のベンチマーク	・サービスとしての CISO

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

提供までの流れ

サポート対象範囲



© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

全世界のサイバーセキュリティーチームを活用

220

全世界220の
シュナイダー拠点をサポートする
セキュリティーエキスパート

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

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

セキュリティーパートナーとサイバーエコシステムを構築

Network segmentation

FORTINET
OWL CYBER DEFENSE
WATERFALL Stronger Than Firewalls
CISCO
paloalto NETWORKS
BELDEN
Extreme networks
MOXA
JUNIPER NETWORKS
STORMSHIELD

End point protection

Symantec
KUB
McAfee

Secure remote access

VERICLAVE YOUR CRITICAL ASSETS, SECURED.
WALLIX TRACE, AUDIT & TRUST

Patching, servers and network support

Microsoft
hp
GFI Software

Anomaly Detection

NOZOMI NETWORKS
CLAROTY

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

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

© 2024 Schneider Electric, All Rights Reserved

サイバーセキュアな工場とOT-SoC（CCSH）の見学を計画中

シュナイダーエレクトリックの自社工場で取り組んでいる
最新のサイバーセキュリティー対策ノウハウを直接ご紹介します。

© 2024 Schneider Electric, All Rights Reserved

Life Is On Schneider Electric

Life Is On | Schneider Electric

se.com