up next 14:30

Was können Automatisierungstechniker konkret unternehmen, um für die neuen Cyber Security Gesetze und Normen gewappnet zu sein?

Hermann Obermair | MaximatioN GmbH

Was können Automatisierungs-techniker konkret unternehmen, um für die neuen Cyber Security Gesetzte und Normen gewappnet zu sein?

1. **Welche Cyber Security standards und Rechtsakte sind zukünftig für Maschinen- und Anlagenbauer relevant?**
2. Wie kann ich den „Cyber Security Status Quo“ meiner Maschine/Anlage transparent machen?
3. Wie entwickle ich einen optimalen „IEC62443 Compliance Zustand“ meiner Maschine/Anlage?
4. Wie sieht die komplette “Cyber Security Customer Journey” für einen Maschinenbauer aus?
5. Welche Business Modelle (Aftersales SLA) kann der Maschinenbauer seinem Kunden anbieten?

Welche Cyber Security Standards und Rechtsakte sind zukünftig relevant

Unternehmen können folgende Schritte unternehmen, um ihre Maschinen auf die neue Maschinenrichtlinie/Verordnung vorzubereiten:

Überprüfung der Maschinen:
- Identifizieren Sie alle Maschinen, die von der Verordnung betroffen sind. Berücksichtigen Sie auch digitale Komponenten wie Software und Schnittstellen.

Risikobewertung:
- Führen Sie eine Risikobewertung durch, um potenzielle Sicherheitslücken zu erkennen. Berücksichtigen Sie die gesamte Lebensdauer der Maschinen.

Anpassung der Konformitätsdokumentation:
- Aktualisieren Sie die technischen Unterlagen, um den neuen Anforderungen zu entsprechen.

Schulung der Mitarbeiter:
- Sensibilisieren Sie Ihre Mitarbeiter für die neuen Vorschriften und die Bedeutung der Cybersicherheit.

Inkrafttreten/Umsetzung/Gültigkeit:
- Inkraft: 14.06.2023, Gültigkeit: 14.01.2027

Welche Cyber Security Standards und Rechtsakte sind zukünftig relevant

Der Cyber Resilience Act (CRA) zielt darauf ab, Verbraucher und Unternehmen zu schützen, die Produkte oder Software mit einer digitalen Komponente kaufen oder verwenden. Hier sind die wichtigsten Punkte:

Harmonisierte Regeln beim Inverkehrbringen:

- Produkte oder Software mit digitalen Elementen auf dem EU-Markt müssen weniger Schwachstellen aufweisen. Hersteller bleiben während des gesamten Produktlebenszyklus für die Cybersicherheit verantwortlich.

Verbesserte Transparenz bei Sicherheit von Hardware und Software:

- Der CRA stellt sicher, dass Verbraucher und Unternehmen fundierte Entscheidungen treffen können.

Vorteile für Geschäftsanwender und Verbraucher durch besseren Schutz

- Der Cyber Resilience Act (CRA) wird voraussichtlich Anfang 2024 in Kraft treten

Inkrafttreten/Umsetzung/Gültigkeit:

- Inkraft: noch offen, Gültigkeit: vermutlich 24 nach Inkrafttreten

Welche Cyber Security Standards und Rechtsakte sind zukünftig relevant

Die NIS2-Richtlinie (Richtlinie (EU) 2022/2555) zielt darauf ab, ein hohes gemeinsames Cybersicherheitsniveau in der EU sicherzustellen. Hier sind einige wichtige Punkte:

Erweiterter Anwendungsbereich:

- NIS2 gilt für öffentliche und private Einrichtungen, die bestimmte Mitarbeiter- und Finanzschwellenwerte erreichen und Dienstleistungen in der EU erbringen.

Verschärfte Cybersicherheitsanforderungen:

- Unternehmen müssen angemessene Sicherheitsmaßnahmen gemäß den Risiken und der Art der verarbeiteten Daten umsetzen.

Meldepflicht für Sicherheitsvorfälle:

- Betroffene Einrichtungen müssen Sicherheitsvorfälle melden.

Grenzüberschreitende Zusammenarbeit:

- Kooperation und Informationsaustausch auf EU-Ebene sind erforderlich.

Strafen bei Nichteinhaltung:

- Unternehmen, die gegen die Richtlinie verstoßen, können mit Sanktionen rechnen

Welche Cyber Security Standards und Rechtsakte sind zukünftig relevant

Die IEC 62443 ist eine internationale Normenreihe, die sich mit der IT/OT-Sicherheit für industrielle Kommunikationsnetze und Systeme befasst. Hier sind einige wichtige Punkte:

Ganzheitlicher Ansatz:

Die Norm berücksichtigt nicht nur technische Aspekte, sondern auch Arbeitsprozesse, Gegenmaßnahmen und Mitarbeiterqualifikationen.

Rollenbasierte Sicherheitsansätze:

Betreiber, Integratoren und Hersteller verfolgen risikobasierte Ansätze zur Vermeidung und Behandlung von Sicherheitsrisiken.

Teile der Normenreihe:

- **General:** Grundbegriffe, Konzepte und Modelle.
- **Policies and Procedures**: Management industrieller IT-Sicherheit.
- **System:** Sicherheitsvorgaben für Steuerungs- und Automatisierungssysteme.
- **Components and Requirements:** Anforderungen an Produktentwicklung von Automatisierungskomponenten

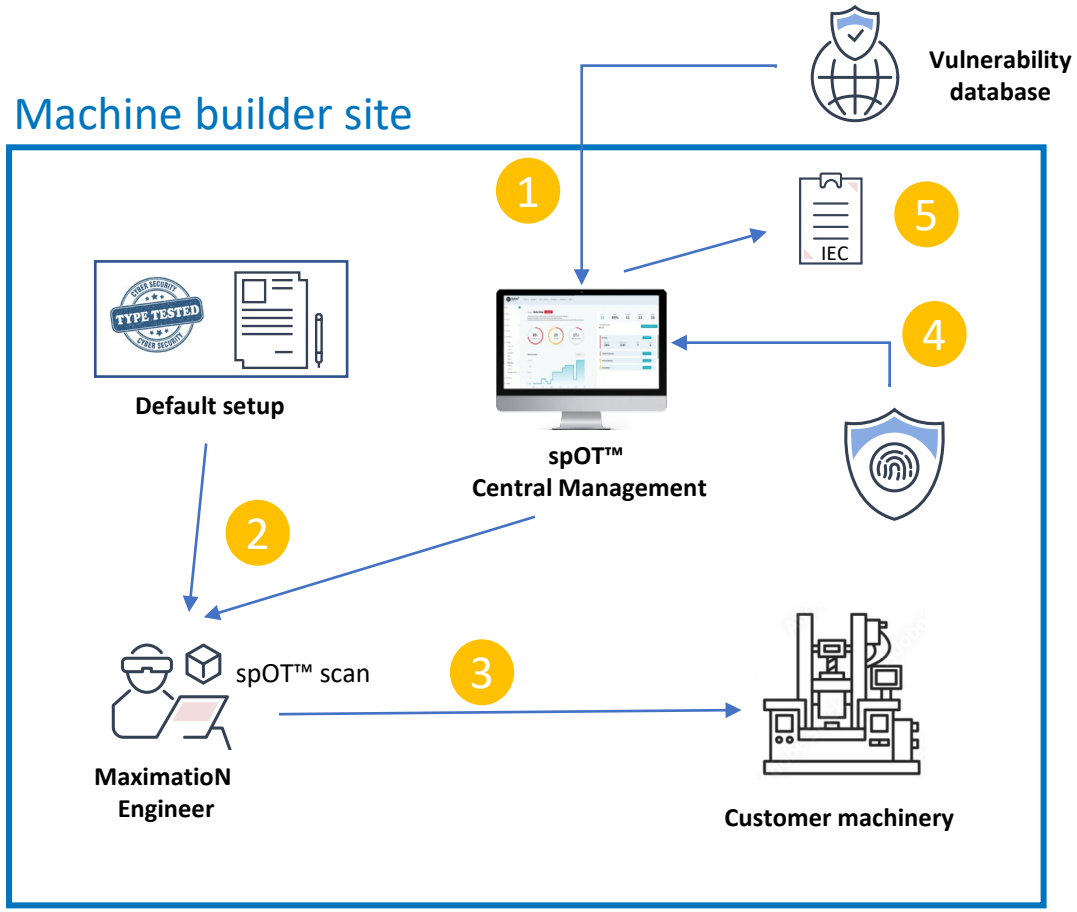
Teil	Stand	Titel
General	Edition 1.0, Juli 2009	Terminologie, Konzepte und Modelle
Policies and Procedures	Edition 1.0, November 2010	Anforderungen an Sicherheitsprogramme für IACS-Betreiber
System	Edition 1.0, Januar 2018	Sicherheitstechnologien für industrielle Automatisierungs- und Steuerungssysteme (IAC)
Components and Requirements	Edition 1.1, August 2017	Anforderungen an IACS-Komponenten
Components and Requirements	Edition 2, Dezember 2023	Anforderungen an IACS-Dienstleister

Was können Automatisierungs-techniker konkret unternehmen, um für die neuen Cyber Security Gesetzte und Normen gewappnet zu sein?

1. Welche Cyber Security standards und Rechtsakte sind zukünftig für Maschinen- und Anlagenbauer relevant?
2. **Wie kann ich den „Cyber Security Status Quo“ meiner Maschine/Anlage transparent machen?**
3. Wie entwickle ich einen optimalen „IEC62443 Compliance Zustand“ meiner Maschine/Anlage?
4. Wie sieht die komplette “Cyber Security Customer Journey” für einen Maschinenbauer aus?
5. Welche Business Modelle (Aftersales SLA) kann der Maschinenbauer seinem Kunden anbieten?

„Status Quo“ Cyber Security Risk Assessment

powered by MaximatioN



1. Update spOT™ with latest known vulnerabilities
2. Commissioning Engineer uses spOT™ expert setup + predefined parameters data set as basis for cyber security FAT test
3. Run spOT™ - Test scan and generate finger-print for each delivered machine
4. Transfer fingerprint dataset in machine builders spOT™ central management
5. Generate automatically IEC compliant report for each delivery / machine

„Status Quo“ Cyber Security Risk Assessment

powered by MaximatioN

Sequence of „Risk Assessment Checks“

1) **Secure Asset Scan – SAQ**
   - Identifizierung aller OT-Assets (PLCs, Antriebe, Switches usw.) innerhalb der dedizierten Netzwerkbereiche
   - Identifizierung aller Computer-Assets (WIN, Linux usw.) innerhalb der zugewiesenen Netzwerkbereiche

2) **Secure Compliant Machinery check – SCM**
   - RDP oder VNC verbundene Computer können zentral gescanned werden
   - Eine manuelle Prüfung per USB Stick ist für nicht erreichbare Computer verfügbar

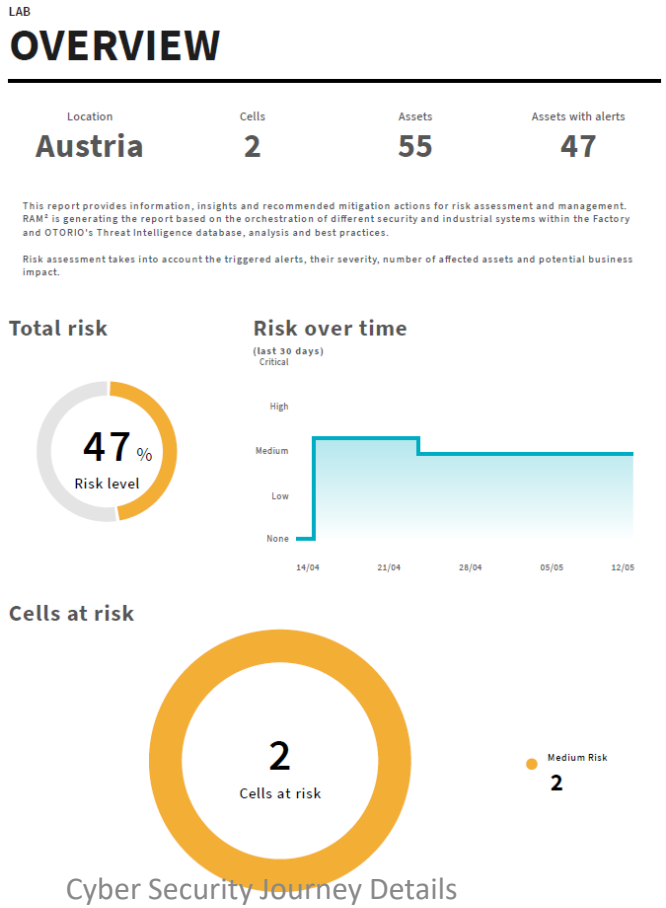
3) **Microsoft Active Directory check – wenn verwendet**
   - Die Diagnose des WIN Active Directory (AD) und die Compliance pro Benutzer wird mitgeprüft

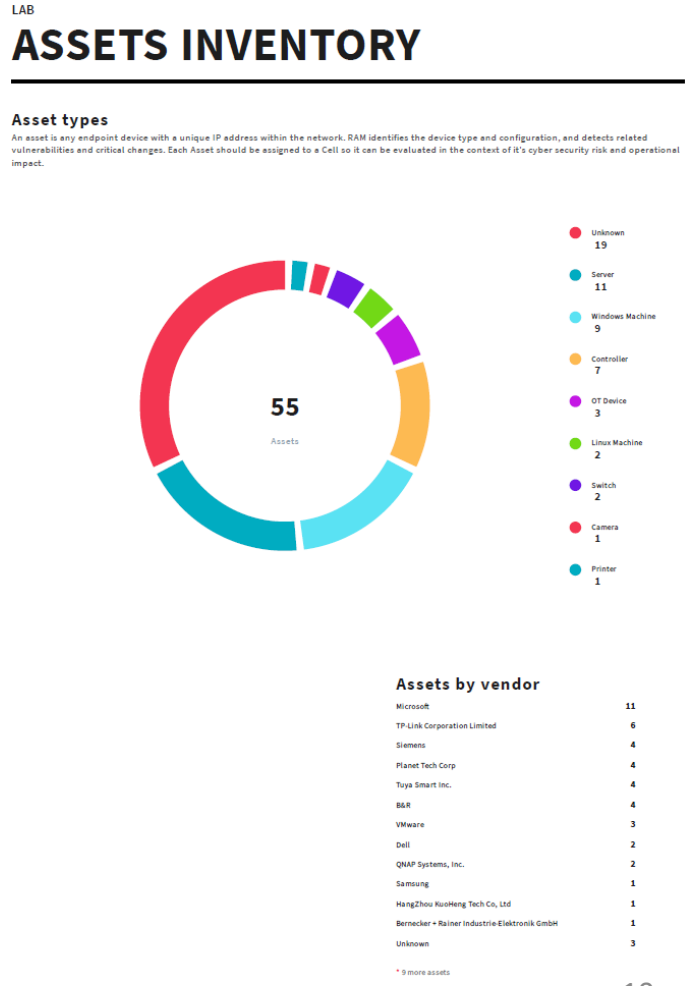
„Status Quo“ Cyber Security Risk Assessment

powered by MaximatioN

RESULTS of „Risk Assessment SCAN“

1) **RISK Overview of complete Machine**
   - OVERVIEW complete Machine
   - THREAT CATEGORIES
   - ASSETS INVENTORY
   - ALERTS
   - VULNERABILITIES





„Status Quo“ Cyber Security Risk Assessment

powered by MaximatioN

RESULTS of „Risk Assessment SCAN“

2) Operational Security Posture Assessment

- TECHNICAL Summary
- Key Findings
- Steps Forward
- Appendixes

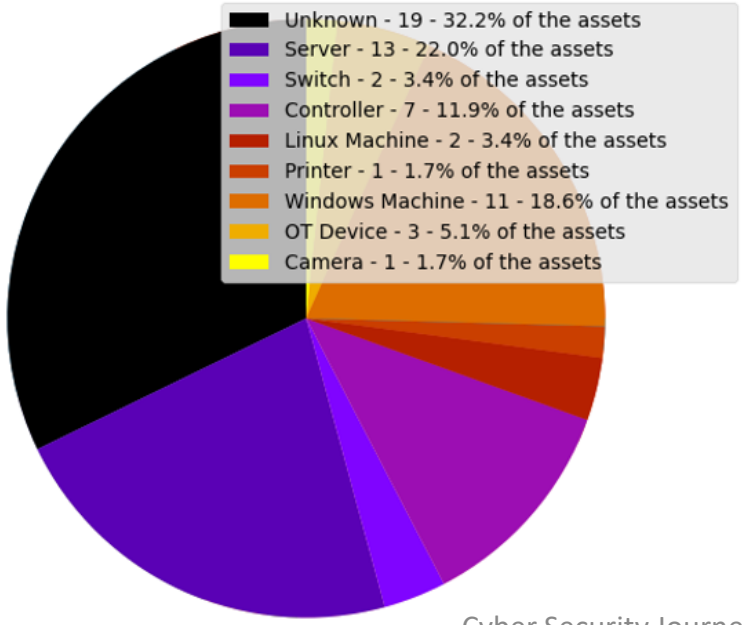


Table of Contents

„Status Quo“ Cyber Security Risk Assessment

powered by MaximatioN

RESULTS of „Risk Assessment SCAN“

3) ASSET Inventory in HTML or EXCEL format

- Detailed information to all assets scanned

ID	Name	Type	External ID	Mac	IP address	Subnet	Interface index	Shop	Cell	Owner	Impact level	Risk level	IEC 62443 Compliance Level	NERC Compliance Level	Location	State	First Seen	Last Seen	Alerts	Vulnerabilities	Vendor
108	Stratix 5700 108	Network Device			192.168.2.13		1 out of 1			admin		Low				Operational	26/08/23 04:55	26/08/23 06:56	29	28	Rockwell
46	Stratix 5700 46	Network Device			192.168.1.26		1 out of 1			admin		Low				Operational	26/08/23 03:52	26/08/23 04:06	28	28	Rockwell
45	Stratix 5700 45	Network Device			192.168.1.12		1 out of 1			admin		Low				Operational	26/08/23 03:52	26/08/23 04:06	28	28	Rockwell
44	_8626_TXL	Controller		08:61:95:d7:33:e6	192.168.1.1	192.168.1.0/24	1 out of 4			admin		Low				Operational (Slot 0: REMOTE RUN, Slot 1: REMOTE PROGRAM)	26/08/23 03:52	26/08/23 06:56	6	5	Rockwell
44	_8626_TXL	Controller		08:61:95:d8:75:1b	192.168.1.2	192.168.1.0/24	2 out of 4			admin		Low				Operational (Slot 0: REMOTE RUN, Slot 1: REMOTE PROGRAM)	26/08/23 03:52	26/08/23 06:56	6	5	Rockwell
44	_8626_TXL	Controller		08:61:95:dd:94:b7	192.168.3.1	192.168.3.0/24	3 out of 4			admin		Low				Operational (Slot 0: REMOTE RUN, Slot 1: REMOTE PROGRAM)	26/08/23 03:52	26/08/23 06:56	6	5	Rockwell
44	_8626_TXL	Controller		08:61:95:dd:95:06	192.168.2.1	192.168.2.0/24	4 out of 4			admin		Low				Operational (Slot 0: REMOTE RUN, Slot 1: REMOTE PROGRAM)	26/08/23 03:52	26/08/23 06:56	6	5	Rockwell
159	ABB Field Device 159	OT Device		00:1c:01:42:ab:39	192.168.2.206		1 out of 1			admin		No risk				Operational	26/08/23 04:58	26/08/23 06:58	1	0	ABB
155	ABB 155	OT Device		00:1c:01:42:a9:20	192.168.2.232		1 out of 1			admin		No risk				Operational	26/08/23 04:57	26/08/23 06:59	1	0	ABB
154	ABB 154	OT Device		00:1c:01:42:ab:12	192.168.2.231		1 out of 1			admin		No risk				Operational	26/08/23 04:57	26/08/23 06:59	1	0	ABB

Was können Automatisierungs-techniker konkret unternehmen, um für die neuen Cyber Security Gesetzte und Normen gewappnet zu sein?

1. Welche Cyber Security standards und Rechtsakte sind zukünftig für Maschinen- und Anlagenbauer relevant?

2. Wie kann ich den „Cyber Security Status Quo“ meiner Maschine/Anlage transparent machen?

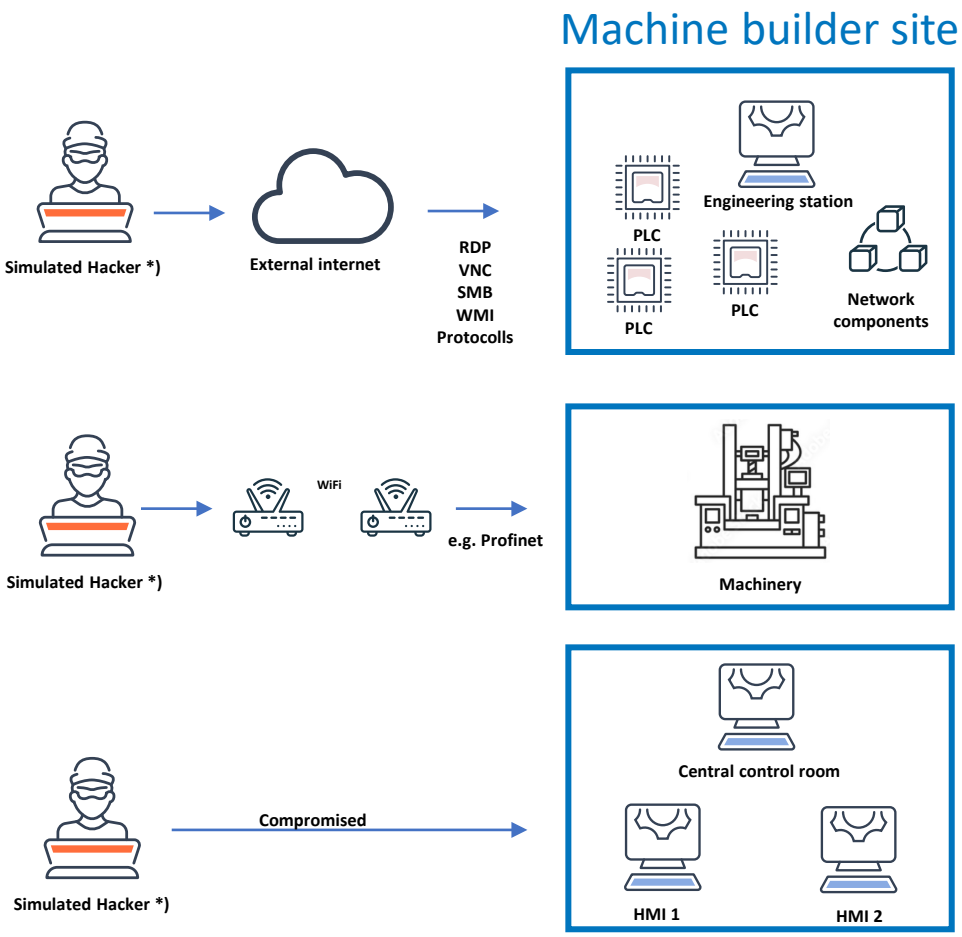
3. **Wie entwickle ich einen optimalen „IEC62443 Compliance Zustand“ meiner Maschine/Anlage?**

4. Wie sieht die komplette “Cyber Security Customer Journey” für einen Maschinenbauer aus?

5. Welche Business Modelle (Aftersales SLA) kann der Maschinenbauer seinem Kunden anbieten?

Cyber Security Expert Consulting

powered by MaximatioN



Cyber Security Expert Consulting

powered by MaximatioN

Individuelles EXPERT Consulting um die IEC62443 compliance zu erzielen

1) **FIXING der Hardware und Software Vulnerabilities**
   - Handlungsanleitungen, um Vulnerabilities zu beheben
   - Vorschläge für Security updates
   - Empfehlungen für „best practice“ Automation design (managed Switches, Segmentation, etc.)

2) **Hardening von Windows Computers**
   - Gemeinsame Entwicklung der kundenspezifischen Windows GROUP POLICIES
   - Gemeinsame Entwicklung von MASTER IMAGE(s) per Machinenkonfiguration

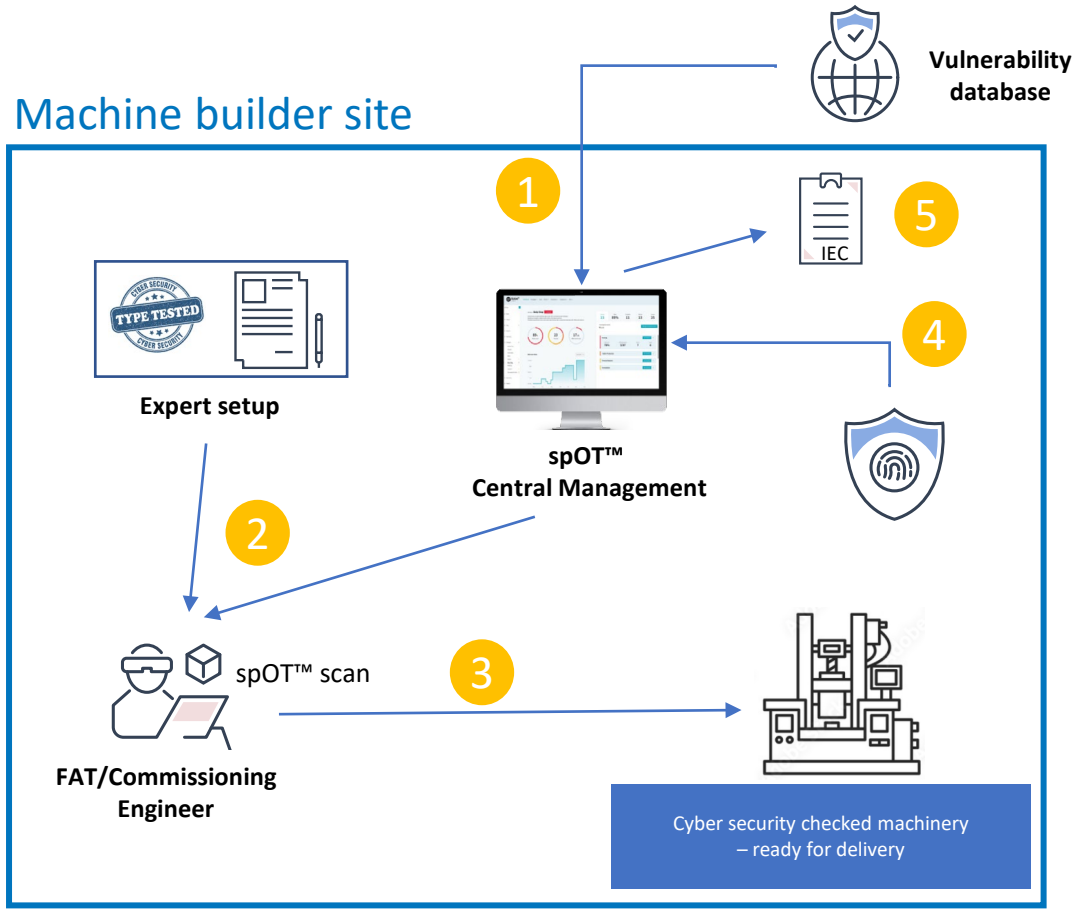
3) **Finalisierung der *SpOT* Test settings (Typenschein dieser Maschinentype)**
   - IEC62443 Compliance report pro Windows Computer
   - SBOM report (Software Bill of Material) pro Windows Computer
   - RISK Overview Report dieser Maschinentype

Was können Automatisierungs-techniker konkret unternehmen, um für die neuen Cyber Security Gesetzte und Normen gewappnet zu sein?

1. Welche Cyber Security standards und Rechtsakte sind zukünftig für Maschinen- und Anlagenbauer relevant?
2. Wie kann ich den „Cyber Security Status Quo“ meiner Maschine/Anlage transparent machen?
3. Wie entwickle ich einen optimalen „IEC62443 Compliance Zustand“ meiner Maschine/Anlage?
4. **Wie sieht die komplette “Cyber Security Customer Journey” für einen Maschinenbauer aus?**
5. Welche Business Modelle (Aftersales SLA) kann der Maschinenbauer seinem Kunden anbieten?

Cyber Security FAT Check / Customer hand over

powered by MaximatioN



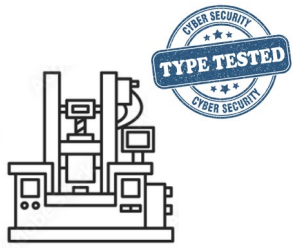
1. Update spOT™ with latest known vulnerabilities
2. Commissioning Engineer uses spOT™ expert setup + predefined parameters data set as basis for cyber security FAT test
3. Run spOT™ - Test scan and generate finger-print for each delivered machine
4. Transfer fingerprint dataset in machine builders spOT™ central management
5. Generate automatically IEC compliant report for each delivery / machine

Cyber Security FAT Check / Customer hand over

powered by MaximatioN

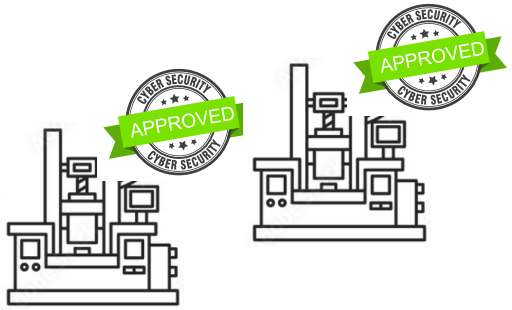
Machine builder site

Cyber security by „expert design“



Type test - once per machine type

spOT™ cyber security SCAN @ FAT



Automated CHECK for all CUSTOMER deliveries

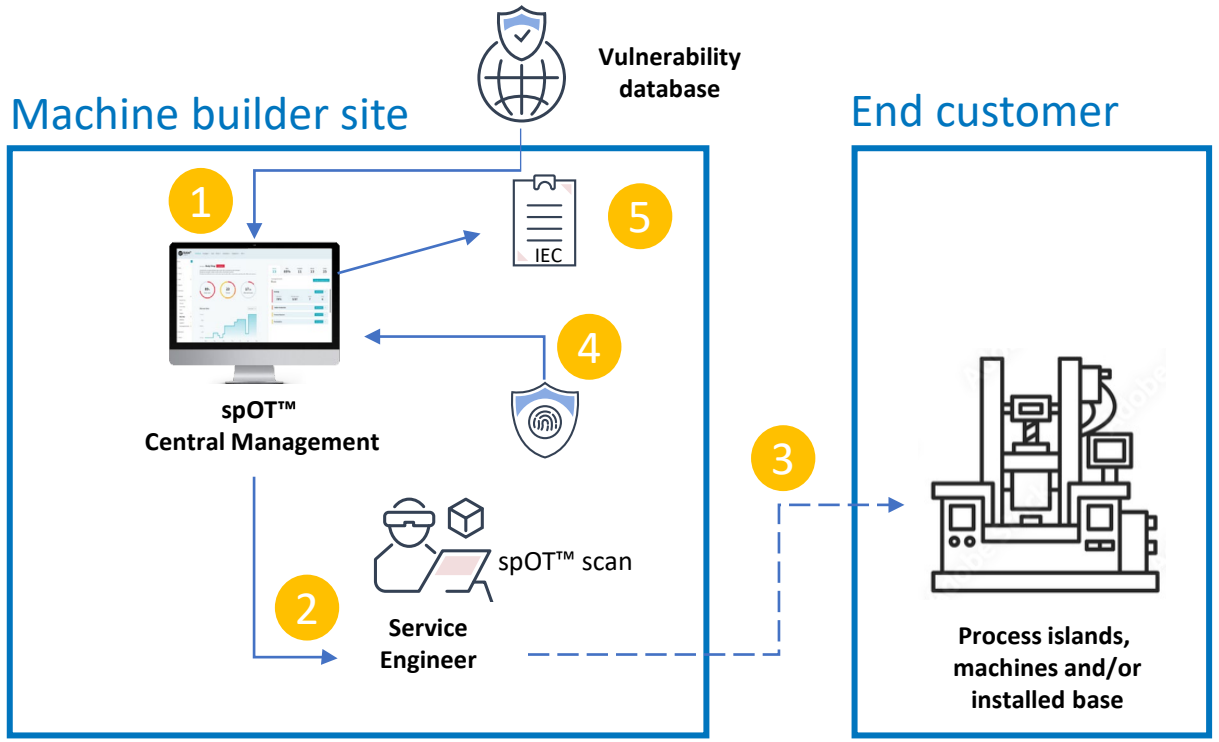
END Customers production sites

Was können Automatisierungs-techniker konkret unternehmen, um für die neuen Cyber Security Gesetzte und Normen gewappnet zu sein?

1. Welche Cyber Security standards und Rechtsakte sind zukünftig für Maschinen- und Anlagenbauer relevant?
2. Wie kann ich den „Cyber Security Status Quo“ meiner Maschine/Anlage transparent machen?
3. Wie entwickle ich einen optimalen „IEC62443 Compliance Zustand“ meiner Maschine/Anlage?
4. Wie sieht die komplette “Cyber Security Customer Journey” für einen Maschinenbauer aus?
5. **Welche Business Modelle (Aftersales SLA) kann der Maschinenbauer seinem Kunden anbieten?**

Cyber Security Aftersales Services

powered by MaximatioN



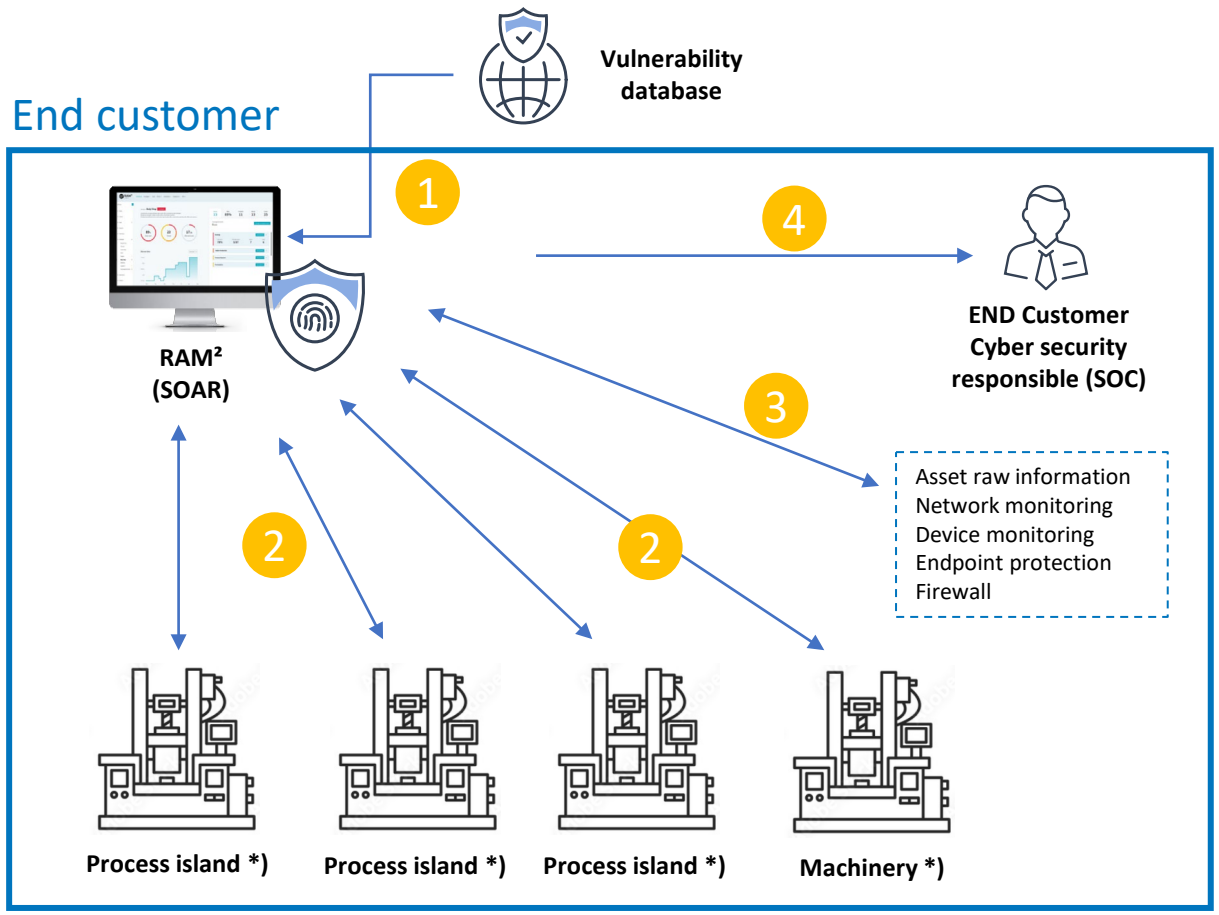
1. **Automatic update** of spOT™ with latest known vulnerabilities
2. Service Engineer uses spOT™ Central Management to check **stored fingerprints** for **new threats and vulnerabilities**
3. Optional **Fingerprint update** could be handled via remote connection or directly on premise with spOT™ scan
4. Store updated fingerprint dataset in machine builder's spOT™ Central management
5. Generate updated IEC compliance report including new risks or exposures for each updated machine

Result:

- CUSTOMER offers periodic cyber security checks **as a aftersales service**
- **Alerting end customer,** in case new threats or vulnerabilities arise.

24/7 Cyber Security orchestration platform - RAM2

powered by MaximatioN



1. Continuous update of RAM² (SOAR) with latest known vulnerabilities
2. Continuous real-time supervision of all heterogeneous plant-floor components
3. Continuous real-time supervision of the installed Network components
4. In case of vulnerability and threat detection Automatic Alarming to SOC (Security operations center)

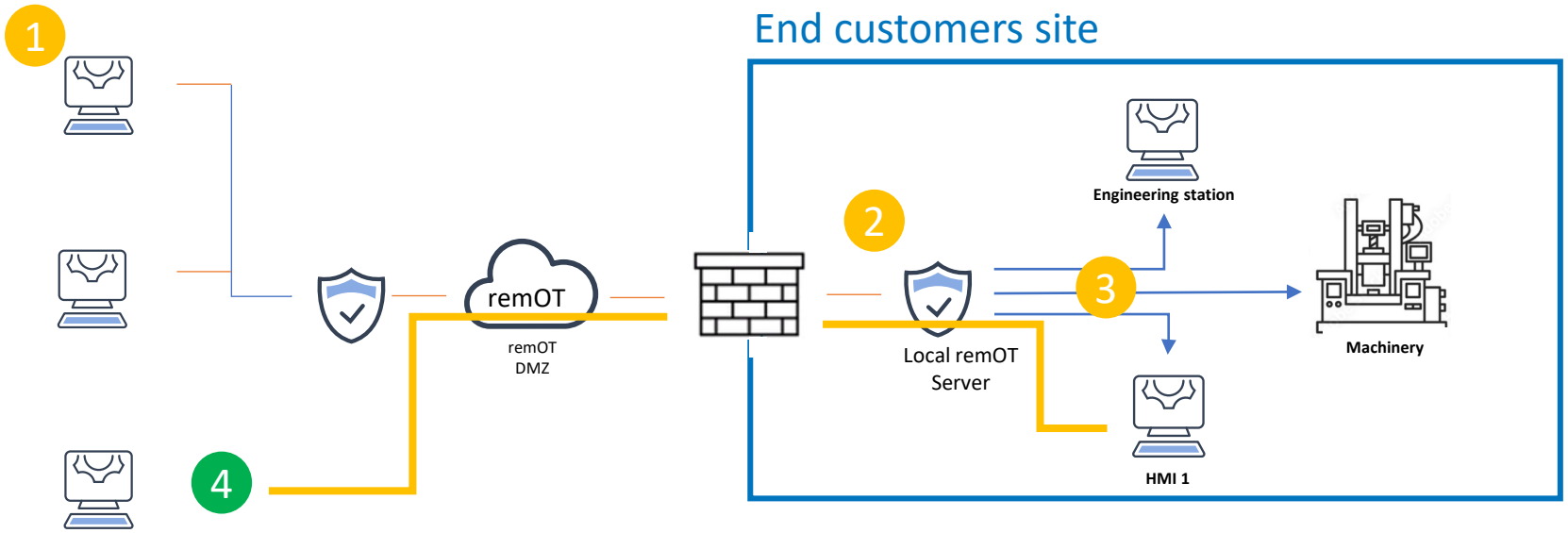
Result:

- Continuous cyber security supervision on-site
- Real-time network supervision
- Highest cyber security protection

*) Multi-vendor equipment, Multi-supplier

Cyber Security REMOTE ACCESS - remOT

powered by MaximatioN



1 Request connection via **remOT** using MFA (Multi factor authentication)

2 **remOT** local server responses with dedicated credentials and priviledges for each user

3 **remOT** Forwarding to allowed devices with dedicated functionalities

4 Managed and governed connection for employees

Result:

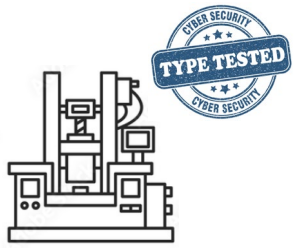
- Secured, managed and documented remote connection

Cyber Security Customer Journey

powered by MaximatioN

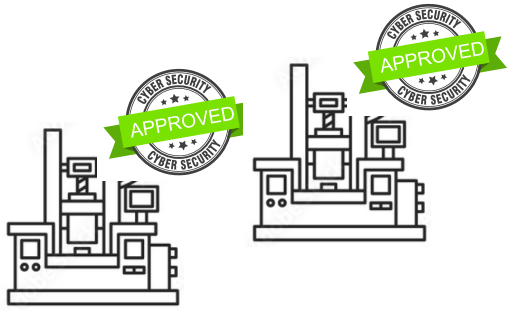
Machine builder site

Cyber security by „expert design“



Type test - once per machine type

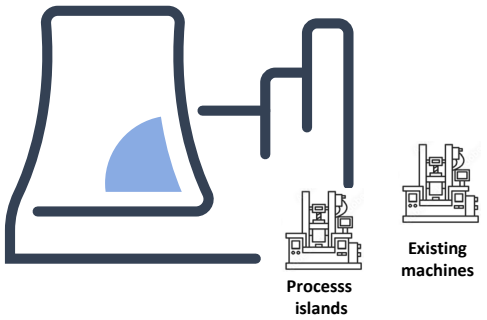
spOT™ cyber security SCAN @ FAT



Automated CHECK for all CUSTOMER deliveries

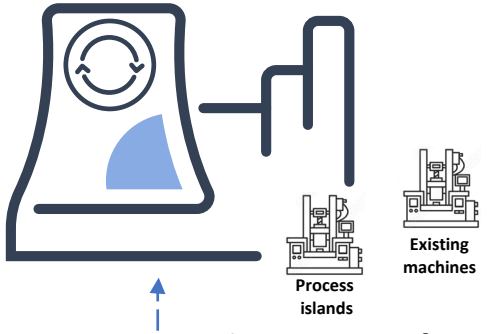
END Customers production sites

CUSTOMER Aftersales service based on **spOT™**



Periodic cyber security CHECK as a Service

RAM² Plant wide – 24/7 cyber security orchestration platform



Cyber security for a heterogeneous plant

remOT™ Secure remote connectivity management system

Was können Automatisierungs-techniker konkret unternehmen, um für die neuen Cyber Security Gesetzte und Normen gewappnet zu sein?

- **Danke für Ihre Aufmerksamkeit!**

Hermann Obermair
Geschäftsführer

MaximatioN GmbH
Neubaugasse 24
8020 Graz

M: +43 664 6317012
hermann.obermair@maximation.at

Bei Interesse: Live Präsentation am MaximatioN Stand