SIEMENS
Ingenuity for life

Industrial Security by SIEMENS

Ganzheilich Sicherheitskonzepte für industrielle Netzwerke

Industrial Security Services | 01/ 2020

siemens.com/industrial-security-services

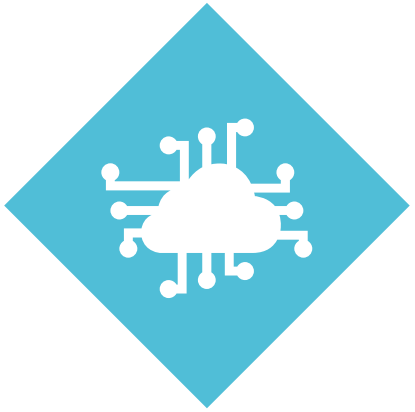
Eine sich ständig wandelnde Bedrohungslandschaft

SIEMENS
Ingenuity for life

Professionelle
Hacker

Schwach-
stellen

Internet of
Things



Cybersecurity Gesetze und
Vorschriften

Entwicklung der Cybersecurity Bedrohungslandschaft

SIEMENS
Ingenuity for life

Digital Information Processing | **Digital Connectivity** | **Digital Automation and Intelligence**

1950s – 1960s – Militär, Regierungen und andere Organisationen implementieren Computersysteme

1970s – Der Heimcomputer wird eingeführt

1980s – Computer halten Einzug in Schulen, Haushalten, Büros und die Industrie

1990s – Digitale Weiterentwicklung durch Elektrifizierung und Automatisierung

1991 – Das World Wide Web wird geboren

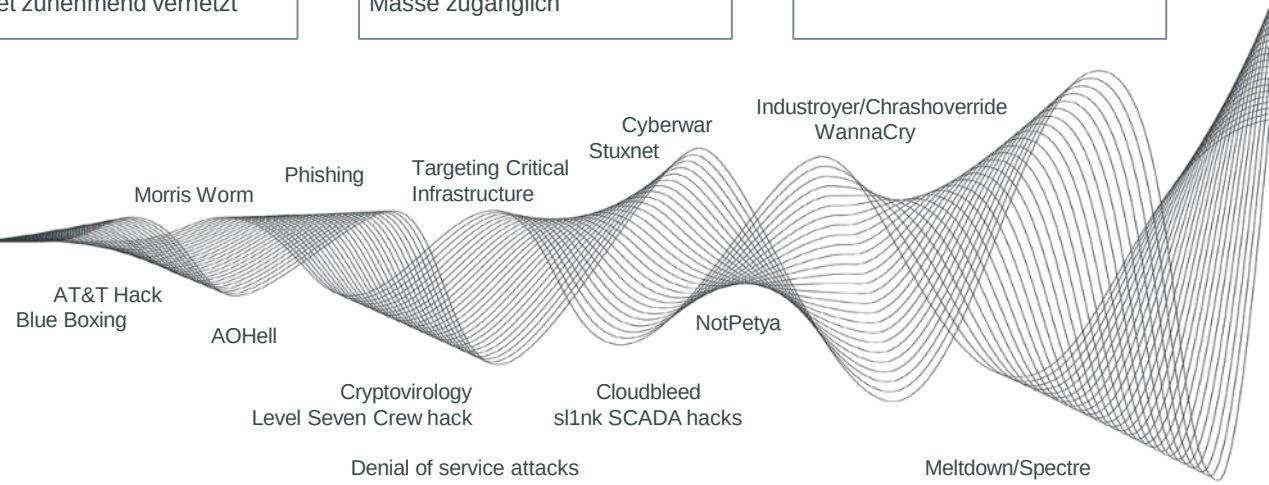
1999 – Die Welt wird durch das Internet zunehmend vernetzt

2000s – Mobile Endgeräte verbreiten sich

2010s – Cloud Computing wird der breiten Masse zugänglich

2015 – Internet of Things, Smarte und autonome Systeme, Artificial Intelligence, Big Data

2020s – Industrie 4.0



Die **Bedrohungslandschaft wächst** und **verändert** sich kontinuierlich – Attacken **adressieren** auch **industrielle** und **kritische Infrastrukturen**

Herausforderungen und Treiber
Die kritischsten Bedrohungen für industrielle Steuerungen

SIEMENS
Ingenuity for life

Industrial Control System Security
Top 10 Bedrohungen und Gegenmaßnahmen[1]

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- (D)DoS Angriffe
- Internet-verbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Produktionsumfeld

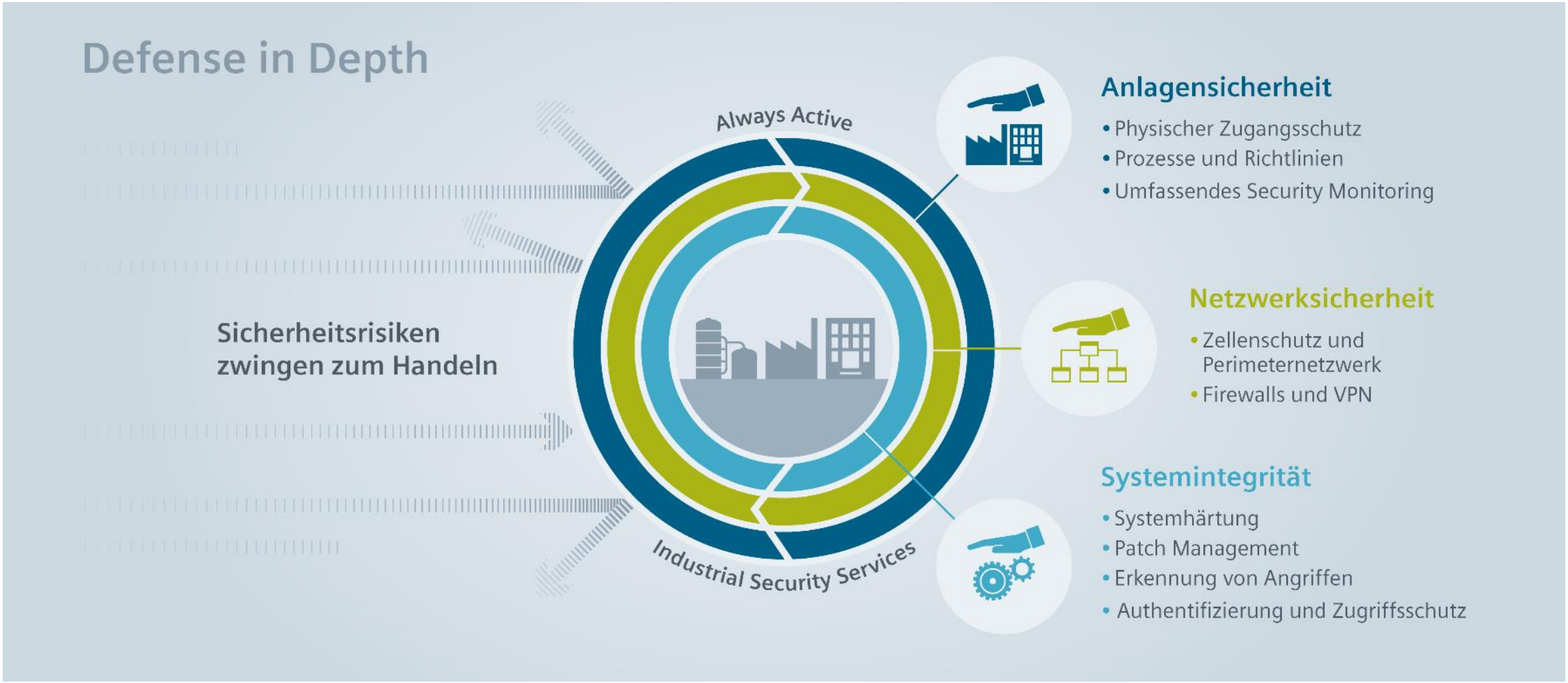
Abgekündigte Betriebssysteme[2]

Windows NT 4.0	30. June 2004
Windows XP	08. April 2014
Windows 7	14. January 2020
Windows 10	14. October 2025

1 Quelle © BSI-Veröffentlichungen zur Cyber-Sicherheit | Industrial Control System Security 2019
2 Quelle © Microsoft

Industrial Security Konzept von Siemens
Defense in Depth

SIEMENS
Ingenuity for life



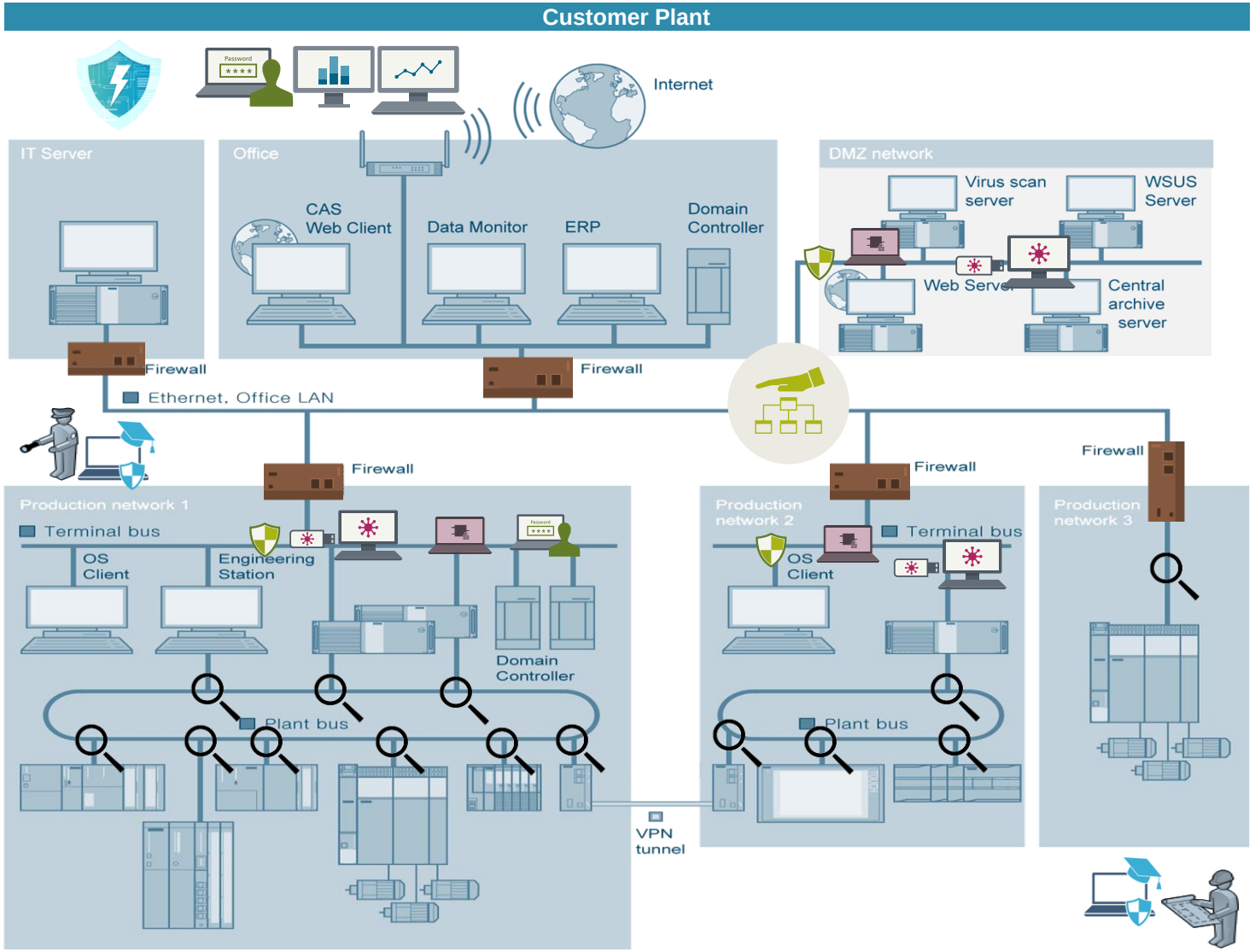
IT Security und Industrial (OT) Security haben ähnliche Herausforderungen – aber eine ganz andere Realität

SIEMENS
Ingenuity for life

IT Security		Industrial Security
Vertraulichkeit		**Verfügbarkeit**
3-5 Jahre	**Asset-Lebenszyklus**	20-40 Jahre
Erzwungene Migration (z.B. neuer PC, Smartphone)	**Software-Lebenszyklus**	Nutzung solange Ersatzteile verfügbar
Hoch (> 10 Security-Programme auf Büro-PCs)	**Möglichkeit, zusätzliche Security-Software aufzuspielen**	Gering (alte Systeme ohne freien Arbeitsspeicher)
Gering (~2 Generationen, Windows 7/10)	**Heterogenität der Systeme**	Hoch (von Windows 95 bis zu 10)
Standardansatz (zentralisiertes und erzwungenes Patchen)	**Schutzstrategie**	Fall- und risikobasiert

Best Practise – Realization of Security Measures

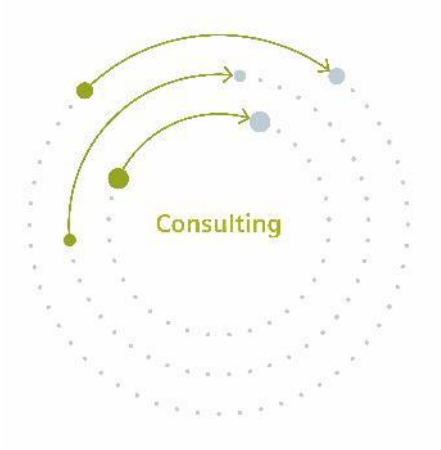
SIEMENS
Ingenuity for life



Implementierungselemente

- Industrial Anomaly Detection
- Security Vulnerability Information
- Security Monitoring
- Identity & Access Management
- Training and Processes
- Security Zones and DMZ
- Firewalls and VPN
- System hardening
- Patch Management
- Malware-Detection and -Prevention

Industrial Security Angebot von Siemens



Security Consulting

Evaluierung des aktuellen Security-Status in industriellen Anlagen

- Security Assessments
  - Industrial Security Check
  - IEC 62443 Assessment
  - ISO 27001 Assessment
  - Risk & Vulnerability Assessment
- Scanning Services
- Industrial Security Consulting

Security Implementation

Risikominderung durch die Implementierung von Security-Maßnahmen

- Security Awareness Training
- Automation Firewall
- Endpoint Protection

Security Optimization

Umfassender Schutz durch Managed Services

- Industrial Anomaly Detection
- Industrial Security Monitoring
- Remote Incident Handling
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC Security Service Packages

Frühes Erkennen von Cyber-Bedrohungen dank Industrial Anomaly Detection

SIEMENS
Ingenuity for life

Industrial Anomaly Detection

- Die Fertigungslandschaft verändert sich von isolierten Inseln zu hochkomplexen Netzwerken ohne Transparenz über den “normalen” Kommunikationsfluss und ein automatisiertes Erkennen von Cyber-Bedrohungen.
- Industrial Anomaly Detection schafft Transparenz über Assets und deren Datenverkehr sowie gesteigerte Security durch ein kontinuierliches und proaktives Erkennen von Veränderungen (Anomalien) im System.

Wie funktioniert es?

- Fortschrittliche Technik durch maschinelles Lernen
- Korrelation des aktuellen Datenverkehrs gegen eine Baseline des Normalbetriebs
- 100% passives Monitoring ohne Einfluss auf die Produktion
- Planung, Implementation und Inbetriebnahme durch geschulte Experten

Ihr Nutzen

Transparenz über den Datenverkehr in industriellen Netzwerken

Frühes Erkennen von Anomalien und Cyber-Bedrohungen

Automatisierte Asset-Identifizierung

Industrial Anomaly Detection
Transparenz über die Kommunikation innerhalb der Produktion

SIEMENS
Ingenuity for life

Transparenz über den Datenaustausch innerhalb der Anlage ermöglicht eine kontinuierliche und proaktive Identifikation von Veränderungen (Anomalien) im System

Korrelation des aktuellen Datenverkehrs mit einer selbst generierten Baseline aus normalem Datenverkehr ermöglicht die Erkennung von Anomalien im Netzwerk, inkl. erweiterter „Deep Packet Inspection“

Automatisierte **Asset Identifikation** unterstützt bei Risikoanalyse und bei der Umsetzung von Maßnahmen

Industrial Anomaly Detection
Transparenz über die Kommunikation innerhalb der Produktion

SIEMENS
Ingenuity for life

Herausforderung
- Fertigungslandschaft verändert sich von isolierten Inseln zu hochkomplexen Netzwerken
- Keine Erkennung von bösartiger Kommunikation in der Fertigung

Übliche Herangehensweise
- Perimeterschutz zur Office-IT mit „Deep Packet Inspection“
- Endpoint Firewalls

Schwachpunkte der üblichen Herangehensweise
- Keine Transparenz der „normalen“ Kommunikation in der OT
- Perimeterschutz in Richtung der Office-IT erkennt kein bösartiges Verhalten im Anlagennetzwerk selbst
- Automatisierungslösungen benutzen proprietäre Protokolle
- Keine Erkennung von neuen/geänderten Komponenten

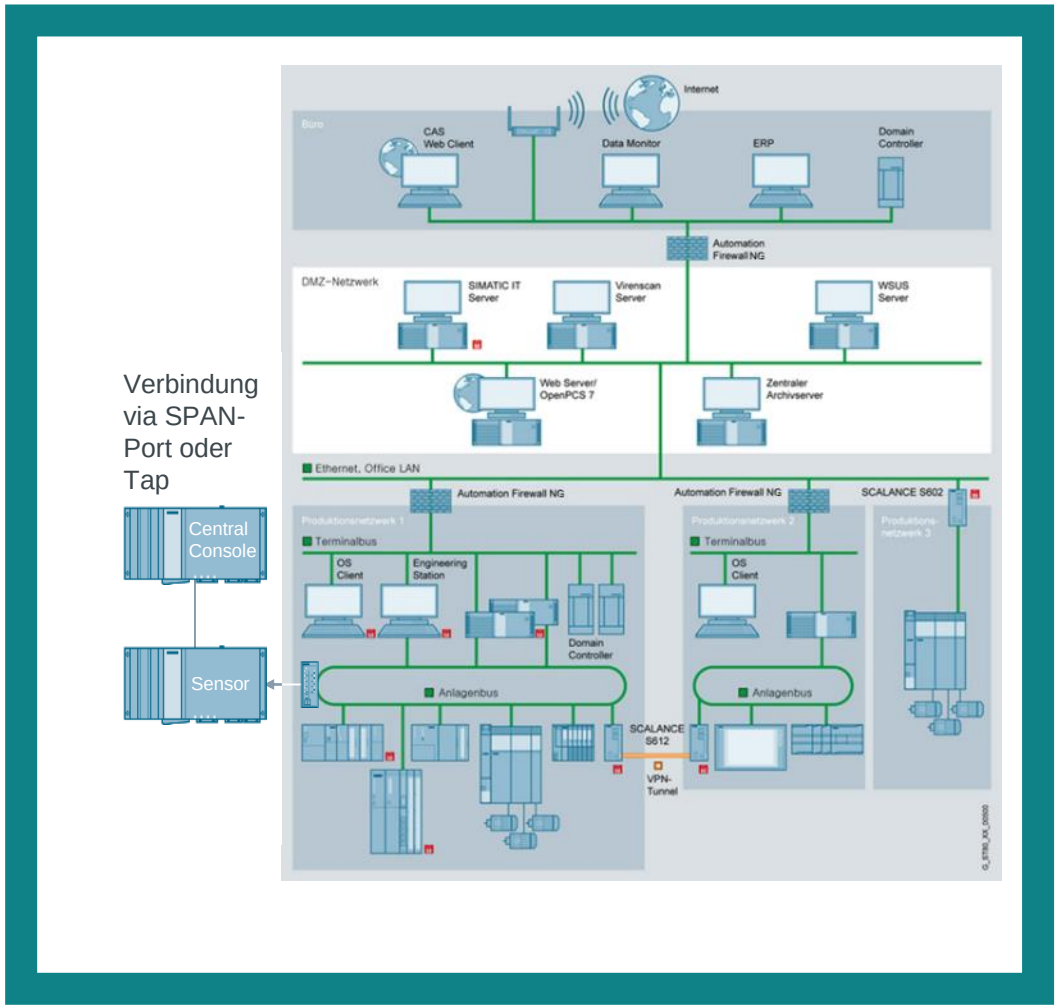
Ziel

Unterstützung des Kunden mittels Anomalie-Erkennung generiert Transparenz, „Situational Awareness“ und Nachvollziehbarkeit im Anlagennetzwerk

Industrial Anomaly Detection
Lösungsarchitektur

SIEMENS
Ingenuity for life

- Verbindung zum IAD-Sensor über einen SPAN[1]-Port
- Ein Sensor kann mit Daten aus mehreren SPAN-Ports arbeiten
- Zentrale Konsole überwacht den Betrieb der Sensoren
- Visualisierung und Analyse in der zentralen Konsole
- Sensor und zentrale Konsole sind auf einem Siemens IPC installiert
- Events können von der zentralen Konsole einfach weitergeleitet werden z.B. an ein SIEM-System

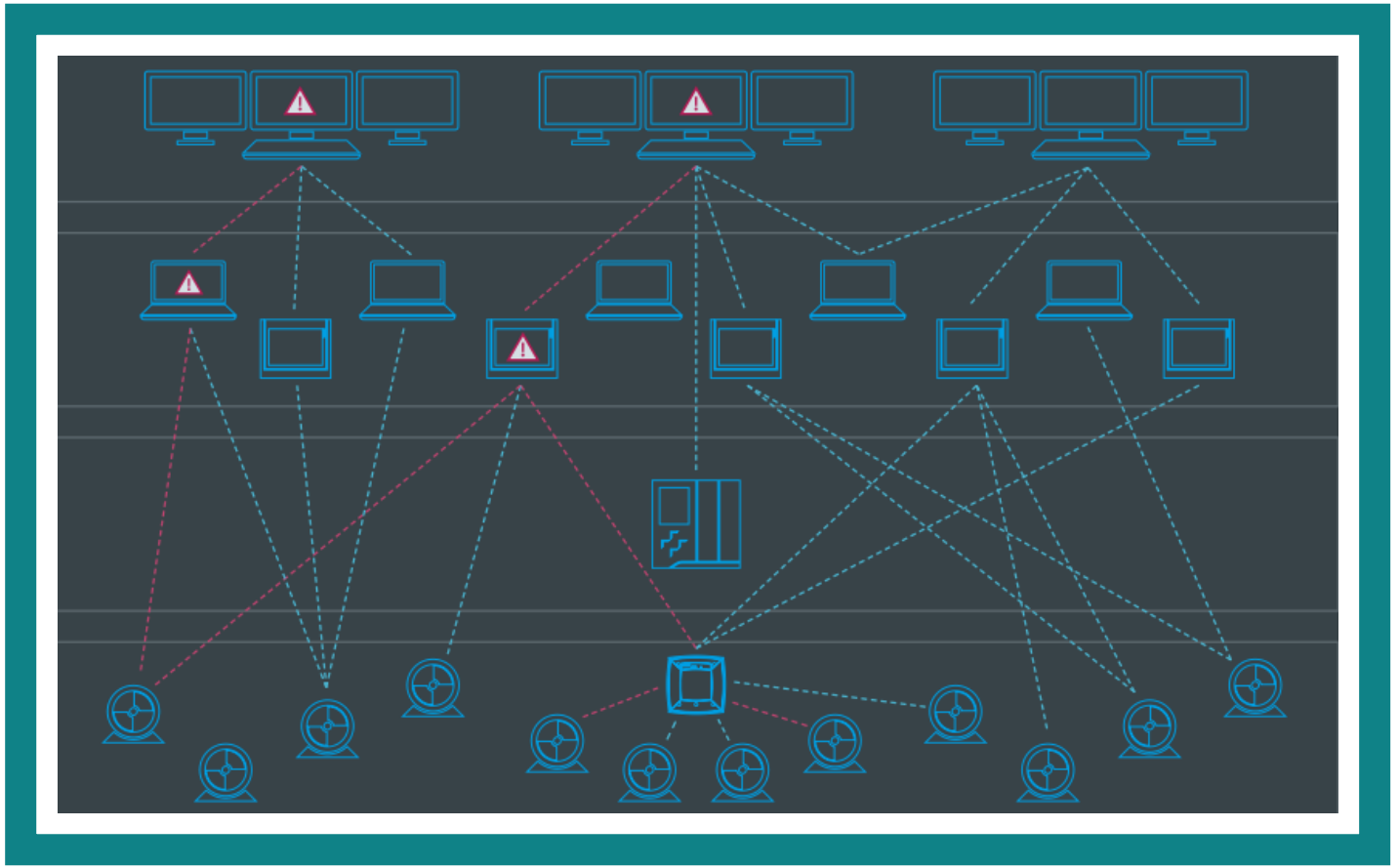


1 Switched Port Analyzer (Mirror Port)

Industrial Anomaly Detection
Kommunikationsansicht

SIEMENS
Ingenuity for life

- Automatische Erkennung von Systemen und Darstellung von Kommunikationsbeziehungen
- Leistungsstarkes und einfaches Dashboard ermöglicht Überwachung und Ereignisverwaltung mit minimaler Konfiguration
- Enthält Informationen zu Schwachstellen
- Unterstützt Geräte von Drittanbietern



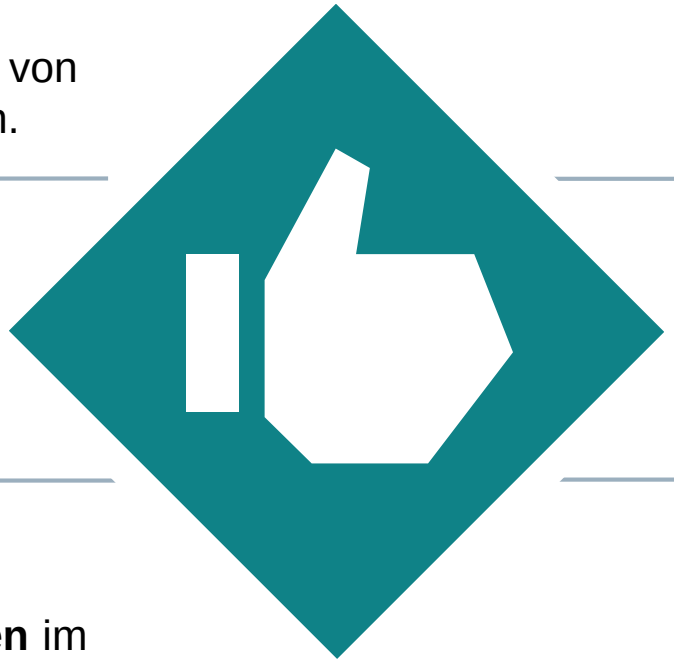
Industrial Anomaly Detection
Vorteile

SIEMENS
Ingenuity for life

Transparenz über die Kommunikation innerhalb der Produktion

Transparenz über den Datenverkehr innerhalb der Produktionsnetzwerke ermöglicht die **kontinuierliche** und **proaktive** Erkennung von Änderungen (Anomalien) an den Systemen.

Ermöglicht die **Einhaltung** von Anforderungen aus den Standards und **der Gesetzgebung** und dient so als Schutz der **kritischen Infrastruktur**



Automatisierte **Asset Identifikation** zur Unterstützung der Risikoanalyse und -minimierung

Nutzung von **maschinellem Lernen**, um eine **Verbesserung** der **Erkennungsrate** zu ermöglichen

Korrelation des aktuellen Datenverkehrs **gegen** eine Baseline des Normalbetriebs ermöglicht eine **Erkennung von Anomalien** im Netzwerk inclusive erweiterter **„Deep Packet Inspection“**

100% passives Monitoring stellt die Überwachung des Produktionsnetzwerk **ohne Beeinflussung** der überwachten Systeme sicher

Lassen Sie uns wissen, wie wir Sie unterstützen können!

SIEMENS
Ingenuity for life

Stefan Turi

Siemens AG

Niederlassung Essen
RC-DE DF CS 2

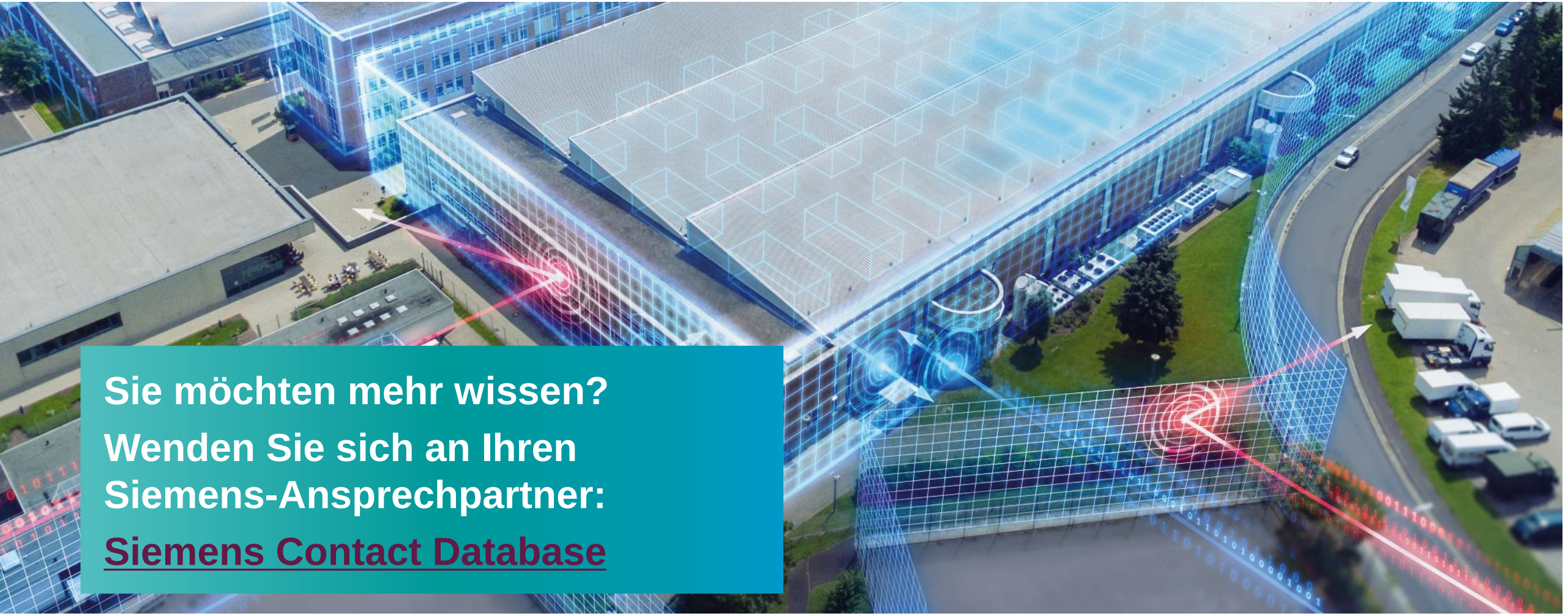
Kruppstr. 16
45128 Essen

E Mail: stefan.turi@siemens.com
Tel: +49 172 69 20 849

siemens.com/industrial-security-services

Lassen Sie uns wissen, wie wir Sie unterstützen können!

SIEMENS
Ingenuity for life



Sie möchten mehr wissen?

Wenden Sie sich an Ihren Siemens-Ansprechpartner:

Siemens Contact Database

Security-Hinweise

SIEMENS
Ingenuity for life

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen.

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen einen Bestandteil eines solchen Konzepts.

Die Kunden sind dafür verantwortlich, unbefugten Zugriff auf ihre Anlagen, Systeme, Maschinen und Netzwerke zu verhindern. Diese Systeme, Maschinen und Komponenten sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn und soweit dies notwendig ist und nur wenn entsprechende Schutzmaßnahmen (z.B. Firewalls und/oder Netzwerksegmentierung) ergriffen wurden.

Weiterführende Informationen zu möglichen Schutzmaßnahmen im Bereich Industrial Security finden Sie unter https://www.siemens.com/industrialsecurity.

Die Produkte und Lösungen von Siemens werden ständig weiterentwickelt, um sie noch sicherer zu machen. Siemens empfiehlt ausdrücklich, Produkt-Updates anzuwenden, sobald sie zur Verfügung stehen und immer nur die aktuellen Produktversionen zu verwenden. Die Verwendung veralteter oder nicht mehr unterstützter Versionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Produkt-Updates informiert zu sein, abonnieren Sie den Siemens Industrial Security RSS Feed unter https://www.siemens.com/industrialsecurity.

Disclaimer

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Erzeugnisbezeichnungen können geschützte Marken oder sonstige Rechte des Siemens Konzerns oder Dritter enthalten, deren unbefugte Benutzung die Rechte der Inhaber verletzen kann.