Industrial Cybersecurity Services

Portfolioübersicht

SIEMENS

Digitalisierung verändert alles

Cybersecurity ist essenziell für OT-Umgebungen – doch der Mangel an Expertise hat weitreichende Konsequenzen

Operative Herausforderungen

- Durch die Digitalisierung und die zunehmende Vernetzung von Maschinen und Industrieanlagen steigt auch das Risiko von Cyberangriffen. Täglich werden neue cyberkriminelle Vorfälle bekannt. Daher ist Cybersecurity essenziell in heutigen Automatisierungsumgebungen.
- Es gibt zahlreiche Cybersecurity-Normen sowie länderspezifische Gesetze und Reguliarien, insbesondere für kritische Infrastrukturen, z.B. IEC 62443, oder die NIS-2-Richtlinie in der EU.
- Trotz der Relevanz des Themas fehlt es an Expertise im Bereich IT und Cybersecurity für OT-Umgebungen. Dies führt zu mangelnder Transparenz über potenzielle Risiken und zu einem unzureichenden Schutz der Anlage.

Durch die fortschreitende Digitalisierung der Industrie wächst auch das Risiko für Cyberangriffe – aber es besteht ein Mangel an Experten und Schutz.

Mögliche Konsequenzen

Erhöhtes Risiko von Cyberangriffen

Störungen, ungeplante Ausfallzeiten, Datendiebstahl und Erpressung oder sogar Sabotage und Produktschäden

Erheblicher finanzieller Verlust oder Reputationsschaden

SIEMENS

Herausforderungen und Treiber für Security
Produktivität, Kostendruck und Regulierungen

Produktivität schützen

Schutz gegen

- extern verursachte Vorfälle durch steigende Konnektivität
- internes Fehlverhalten
- sich entwickelnde Bedrohungslage

Kosten senken

Kosten

- für qualifiziertes Personal
- für essentielle Sicherheitstechnologien

Regulierungen erfüllen

Erfüllen von

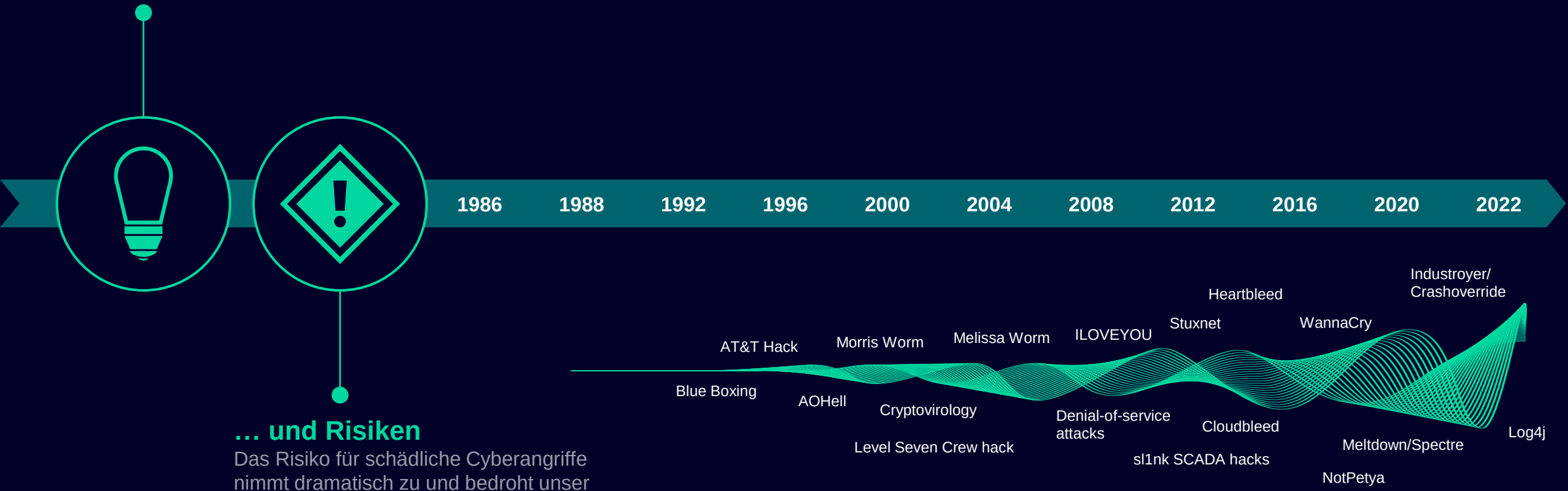
- Meldepflichten
- Mindeststandards
- Security-Know-how

SIEMENS

Entwicklung der Cybersecurity Bedrohungslandschaft

Chancen

Milliarden von Geräten werden durch das Internet der Dinge miteinander verbunden und bilden das Rückgrat unserer Infrastruktur und Wirtschaft.



… und Risiken

Das Risiko für schädliche Cyberangriffe nimmt dramatisch zu und bedroht unser Leben und die Stabilität unserer Gesellschaft.

SIEMENS

Die Security-Anforderungen eines industriellen Steuerungssystems unterscheiden sich deutlich von denen der Office IT

IT Security		Industrial Security
Vertraulichkeit		**Verfügbarkeit und Sicherheit**
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 (hauptsächlich Windows 10)	**Heterogenität der Systeme**	Hoch (von Windows 95 bis zu 10)
Standardansatz (zentralisiertes und erzwungenes Patchen)	**Schutzstrategie**	Fall- und risikobasiert

SIEMENS

Siemens ist Ihr verlässlicher Partner für sichere Digitalisierung

Wir sind die Experten für Automatisierung und haben spezifisches Branchen-Know-how

Wir treiben die Digitalisierung voran

Wir verstehen Industrial Security

Wir bieten State-of-the-Art-Technologie und ganzheitliche Services aus einer Hand

Unsere Prozesse und Produkte sind geprüft und zertifiziert

„Wir sorgen dafür, dass Sie sich auf Ihr Kerngeschäft konzentrieren können.“

SIEMENS

Siemens setzt auf ein ganzheitliches Cybersecurity-Konzept: Defense in Depth

Sicherheitsrisiken zwingen zum Handeln

Defense in Depth

basierend auf IEC 62443

- Anlagensicherheit
- Netzwerksicherheit
- Systemintegrität

Industrial Cybersecurity Services

SIEMENS

Cybersecurity for Industry: Angebot von Siemens

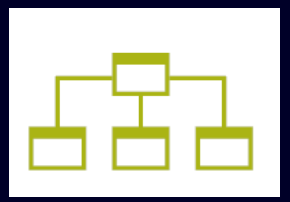
Defense in Depth

basierend auf IEC 62443

Siemens Produkte und Systeme mit integrierter Security

Know-how und Kopierschutz

Authentifizierung und Nutzerverwaltung



Firewall und VPN

System-Härtung und kontinuierliche Überwachung mit Anomalie Erkennung

Siemens Industrial Cybersecurity Services

- Transparenz über den aktuellen Security-Status
- Erhöhtes Security-Level durch das Schließen von Sicherheitslücken
- Langfristiger Schutz durch kontinuierliches Security-Management

SIEMENS

Industrial Cybersecurity Services: Ein ganzheitlicher Ansatz

Plant Security Services

- Security Assessments
- Scanning Services
- Industrial Security Consulting
- Cybersecurity Trainings
- Remote Industrial Operations Services

Network Security Services

- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Remote Platform Software as a Service

System Integrity Services

- Endpoint Protection
- Vulnerability Services
- Patch Management
- Backup and Restore

SIEMENS

Anlagenspezifische Security-Roadmap
mit Security Assessments

Security Assessments

- Anlagenbetreiber können es sich heutzutage nicht leisten, auf wirksame Security-Maßnahmen zu verzichten.
- Kapazitäten für die industrielle Cybersicherheit sind nur selten verfügbar, und es herrscht Zeitdruck aufgrund neuer Compliance-Anforderungen und Gesetze wie der NIS 2 Richtlinie.
- Mit Security Assessments erhalten Sie einen vollständigen Überblick über den tatsächlichen Security-Status Ihrer Automatisierungssysteme.

Wie funktioniert es?

- Unsere Security Assessments beinhalten eine ganzheitliche Analyse möglicher Bedrohungen und Schwachstellen, die Identifizierung von Risiken und Empfehlungen zur Schließung identifizierter Sicherheitslücken.

Benötigen Sie ein **Assessment** basierend auf dem bekanntesten Sicherheits-standard für **Automatisierungssysteme**?	**IEC 62443 / NIS 2 Assessment**
Genügt ein **kompaktes Ein-Tages-Assessment vor Ort**?	**Industrial Security Check**

Vorteile auf einen Blick

Bewertung des aktuellen Security-Status

Anlagenspezifische und risikobasierte Security-Roadmap

Basis für transparente Kostenschätzungen

SIEMENS

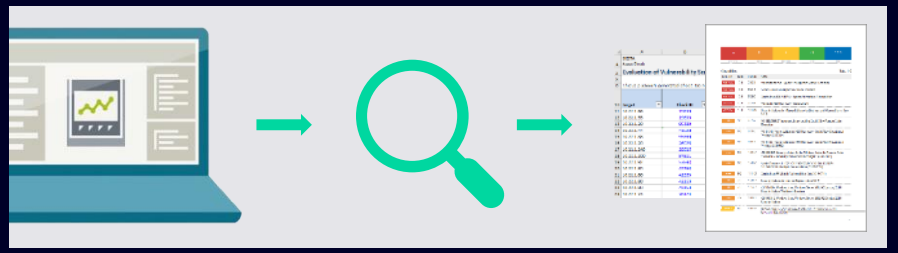
Schnelle Transparenz über Assets und Schwachstellen
dank Scanning Services

Scanning Services

- Die wachsende Anzahl von Assets und steigende Komplexität in Automatisierungsumgebungen führt zu einer unvollständigen Inventarisierung, ausbleibendem Patching und zur Nutzung veralteter Hard- und Software, was das Risiko von Cyber-Vorfällen erhöht.
- Scanning Services bieten eine effiziente Evaluation für industriellen Anlagen – basierend auf einer Kombination von Scanning-Tools und Industrial Security Expertise.

Wie funktioniert es?

- Option 1: Active Asset Inventory Scan
- Option 2: Vulnerability Detection Scan



Vorteile auf einen Blick

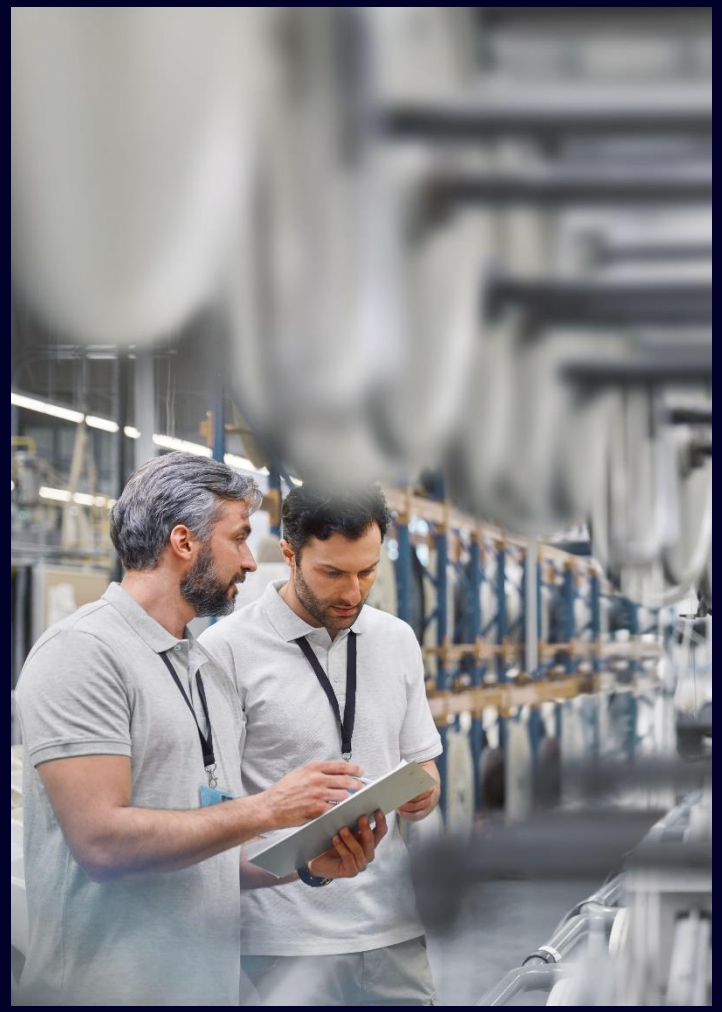
Transparenz über eingesetzte Assets

Erkennen von Schwachstellen

Verständlicher Leitfaden zur Steigerung des Security-Levels

SIEMENS

Sofortiger Zugang zu Industrial Security Expertise
dank Industrial Security Consulting



Industrial Security Consulting

Anlagenbetreiber können es sich heutzutage nicht leisten, auf wirksame Security-Maßnahmen zu verzichten. Allerdings sind selten Kapazitäten im Bereich „Industrial Security“ vorhanden.

Industrial Security Consulting bietet Vor-Ort-Support durch erfahrene Consultants in Bezug auf Security-Richtlinien und das anlagenspezifische Netzwerklayout sowie maßgeschneiderte Implementierungsunterstützung für das Industrial Security Portfolio.

Wählen Sie aus unseren Optionen:

- **Incident Analysis:** Sofortige Unterstützung bei Security-Vorfällen (Ursachenanalyse, Sanierungsstrategie)
- **Policy Consulting:** Prüfung und Integration von Richtlinien, Prozessen und Abläufen
- **Network Consulting:** Support bei Zellsegmentierung, Netz-werkdesign u. Firewall-Regeln
- **Implementation Support:** Reibungslose Integration des Portfolios inkl. Training

Vorteile auf einen Blick

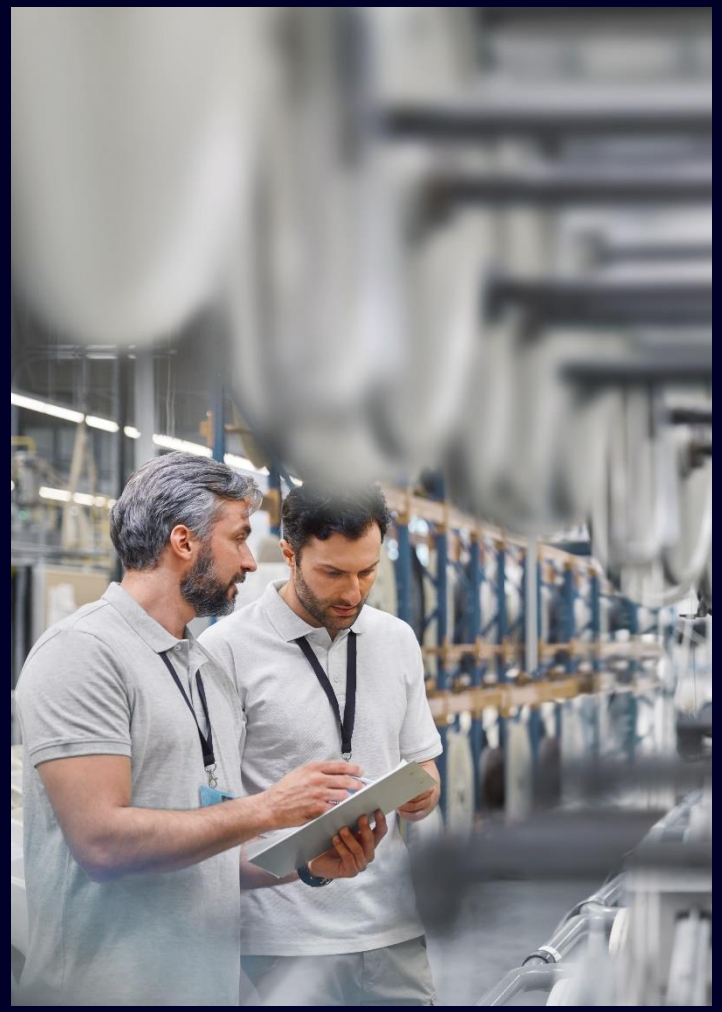
Maßgeschneiderte Security-Richtlinien und -Konzepte

Sofortiger Zugang zu Industrial Security Know-How

Keine Investition für die Entwicklung eigener Security-Kapazitäten

SIEMENS

Schnelle Reaktion bei Security-Vorfällen
mit Incident Analysis als Teil von Industrial Security Consulting



Incident Analysis

Bei Cybersecurity-Vorfällen ist schnelle Reaktion gefragt, um Lücken zu schließen und Schäden gering zu halten. Doch fachliche Expertise ist selten vorhanden. Wer kann helfen?

Mit Incident Analysis unterstützen unsere Experten für Industrial Security dabei, Sicherheitslücken zu schließen, die Produktion wiederaufzunehmen und zukünftige Vorfälle zu verhindern.

Wie funktioniert es?

- Sammlung forensischer Informationen
- Umfassende Analyse der Grundursache und Kritikalität
- Empfehlung einer geeigneten Sanierungsstrategie

1. Erkennen
2. Analysieren
3. Eindämmen
4. Ausmerzen
5. Wiederherstellen
6. Abschluss-Aktivitäten

Vorteile auf einen Blick

Sofortiger Zugang zu Expertenwissen

Unterstützung bei schneller Wiederaufnahme der Produktion

Reduzierte Ausfallkosten

SIEMENS

Industrial Security erhöhen durch Wissen
mit dem Cybersecurity Training Curriculum als Teil von SITRAIN access

Cybersecurity Training Curriculum

Industrielle Sicherheit spielt eine zentrale Rolle beim Schutz kritischer Infrastrukturen. Um diese Komplexitäten zu bewältigen, ist Bildung von entscheidender Bedeutung.

Das Curriculum von SITRAIN access vermittelt Ihnen das Wissen, das Sie zur Verbesserung der industriellen Sicherheit benötigen. Es konzentriert sich darauf, Wissen über die folgenden Schlüsselkomponenten zu vermitteln.

Inhalt

- **Bewusstsein und Schwachstellen**: Identifizieren Sie potenzielle Bedrohungen speziell für Automatisierungs-systeme und ergreifen Sie proaktive Maßnahmen.
- **EU-Richtlinie (NIS 2)**: Halten Sie die EU-Richtlinie für einen robusten Schutz vor Cyberbedrohungen ein.
- **IEC 62443-Normen**: Machen Sie sich mit den internationalen Normen für IT-Sicherheit in industriellen Kommunikationsnetzwerken vertraut.

Holen Sie sich die Mitgliedschaft für die digitale Lernplattform SITRAIN access und lernen Sie rund um die Uhr, überall und jederzeit. Erweitern Sie Ihr Wissen in kleinen Schritten oder auf einmal.

Vorteile auf einen Blick

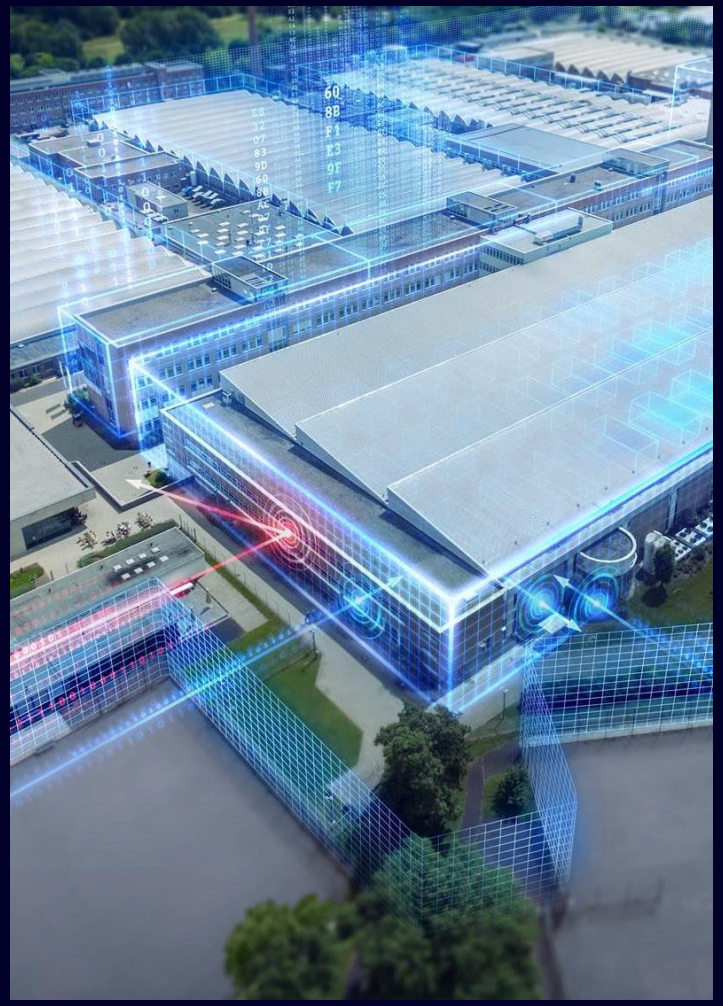
Situationsbewusstsein hinsichtlich Security

Empfehlungen zur Reaktion auf Cyberrisiken

Hilfe bei der Identifizierung von Security-Vorfällen

SIEMENS

Das „schwächste Glied“ Ihre Anlage sichern
mit Industrial Security Training



Industrial Security Training

Die Digitalisierung und die zunehmende Vernetzung von Maschinen und Industrieanlagen erhöhen das Risiko von Cyberangriffen. Insbesondere für kritische Infrastruktur sind entsprechende Schutzmaßnahmen zwingend erforderlich.

Industrial Security Trainings erhöhen das Situations-bewusstsein, um industrielle Security-Vorfälle durch menschliches Versagen zu vermeiden. Buchen Sie Ihr Learning Event als Training im realen oder virtuellen Klassenzimmer oder vor Ort in Ihrem Werk.

Wie funktioniert es?

Die Trainings basieren auf typischen Alltagssituationen und Beispielszenarien sowie gesetzlichen Anforderungen und Richtlinien. Die Teilnehmer werden mit den Gefahren in der Fertigungs- und Prozessindustrie vertraut gemacht, lernen mögliche Schwachstellen zu analysieren, Risiken zu bewerten und Anlagen vor Angriffen zu schützen. Es stehen verschiedene Trainings zur Verfügung:

- Grundlagen Cybersecurity für die diskrete Industrie
- Grundlagen Cybersecurity für die Prozessindustrie
- Cybersecurity in industriellen Netzwerken

Vorteile auf einen Blick

Situationsbewusstsein hinsichtlich Security

Empfehlungen zur Reaktion auf Cyberrisiken

Hilfe bei der Identifizierung von Security-Vorfällen

SIEMENS

24/7 Managed Services für Ihre IT/OT-Infrastruktur
mit Remote Industrial Operations Services

Remote Industrial Operations Services

Die zunehmende Komplexität von IT/OT Systemen, fehlende Ressourcen und Cyberbedrohungen stellen erhebliche Risiken für Produktivitätsverluste in der Betriebstechnologie dar. Mit Remote Industrial Operations Services steht Ihnen ein Team erfahrener Experten zur Seite, das Ihre IT/OT-Infrastruktur rund um die Uhr aus der Ferne überwacht und verwaltet – so können Sie sich auf Ihr Kerngeschäft konzentrieren.

Wie funktioniert es?

Das modulare Vertragsmodell ermöglicht es Ihnen, genau die Services auszuwählen, die Sie benötigen:

- **24/7 Überwachung** der IT/OT Infrastruktur zur Vermeidung von Ausfallzeiten
- **Managed Security Services und SOC as a Service** (inkl. SIEM) für kontinuierlichen Schutz vor Cyberbedrohungen
- **Proaktive Identifikation von Wartungsbedarf** in Ihrer IT/OT-Infrastruktur und Bereitstellung von Ersatzteilen zur Maximierung der Betriebszeit
- **Technischer Experten-Support** für IT und OT aus einer Hand zur schnellen Lösung von Problemen

Nutzen

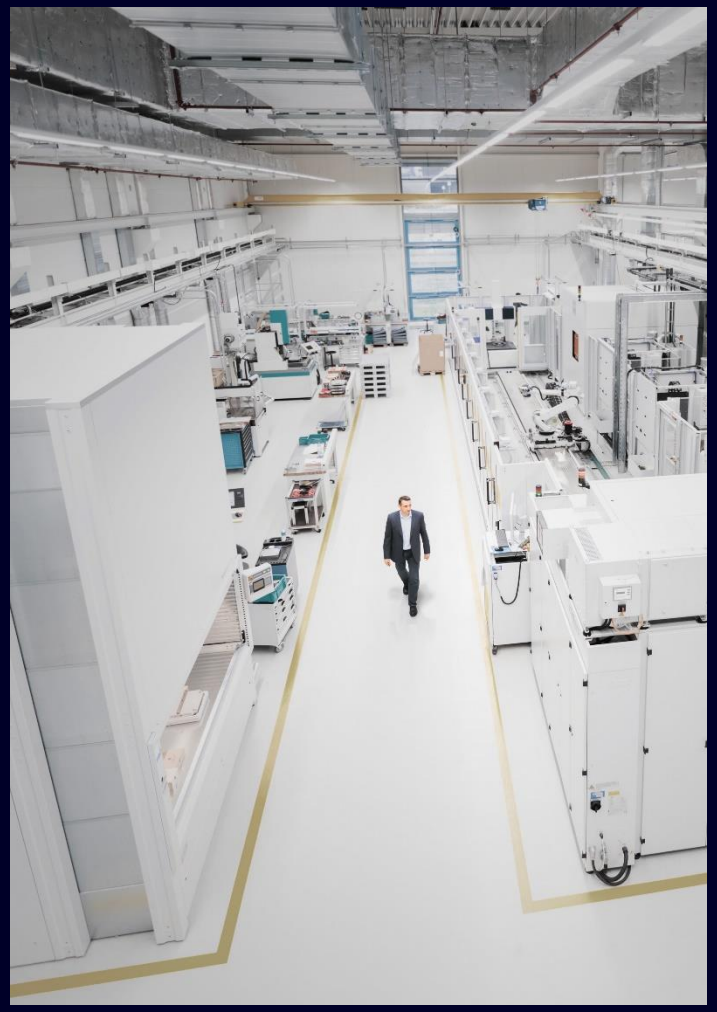
Bewährte IT/OT-Expertise unseres Teams

Betriebskontinuität durch 24/7 fernverwaltete IT/OT-Infrastruktur

Einhaltung von Cybersicherheits-vorschriften (z.B. NIS 2)

SIEMENS

Kontinuierlicher Schutz des Netzwerks
mit Industrial Next Generation Firewall



Industrial Next Generation Firewall

- Automatisierungsumgebungen haben sich von isolierten Inseln zu hochkomplexen Netzwerken verändert – oft ohne Segmentierung von nicht-vertrauenswürdigen Cybernetzwerken (z.B. Büro oder Internet).
- Industrial Next Generation Firewall ist ein Perimeterschutz gemäß der Security-Anforderungen für die industrielle Automatisierung, geprüft und freigegeben für die Nutzung mit dem Siemens Prozessleitsystem.

Wie funktioniert es?

- State-of-the-Art Next Generation **Firewall Appliances**
- Zusätzliche **Security Subscriptions** für Threat Prevention, URL Filtering und WildFire
- **Support Package** (3 oder 5 Jahre) mit Premium Supprt

Vorteile auf einen Blick

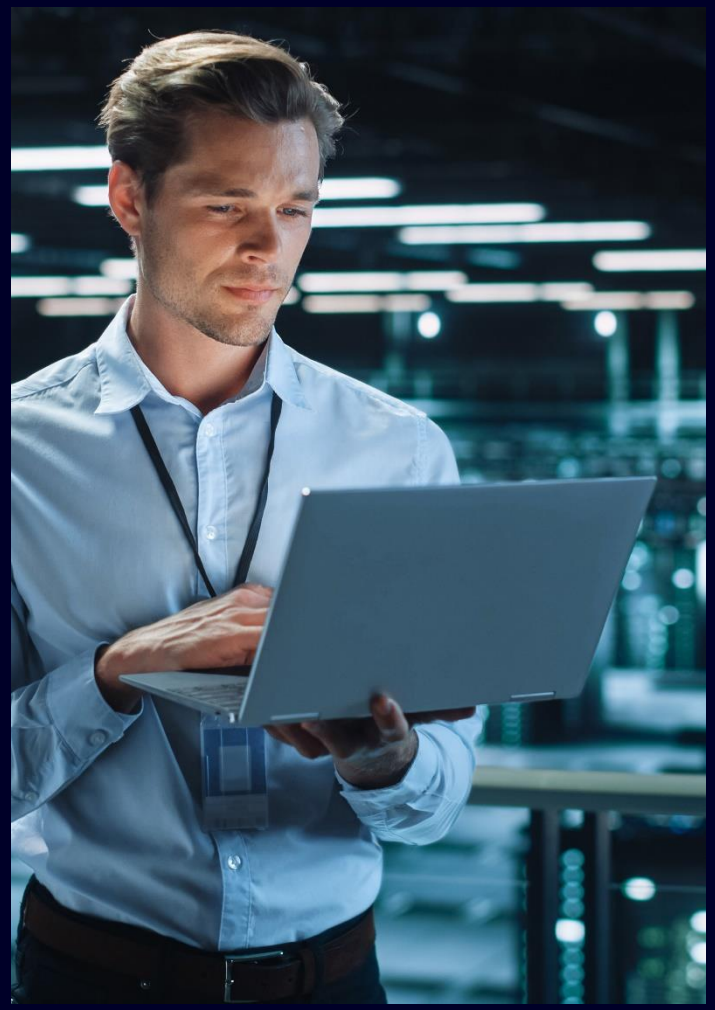
Kontinuierlicher Schutz vor bekannten und unbekannten Bedrohungen

Geprüft und freigegeben für SIMATIC PCS 7 und SIVaaS

Sehr gutes Preis-Leistungs-Verhältnis

SIEMENS

Sicherer Datenaustausch zwischen IT und OT
mit Industrial DMZ Infrastructure



Industrial DMZ Infrastructure

Um sich vor Cyberangriffen zu schützen, empfiehlt der internationale Security-Standard IEC 62443 eine tief gestaffelte Verteidigung, u.a. mit Netzwerksegmentierung.

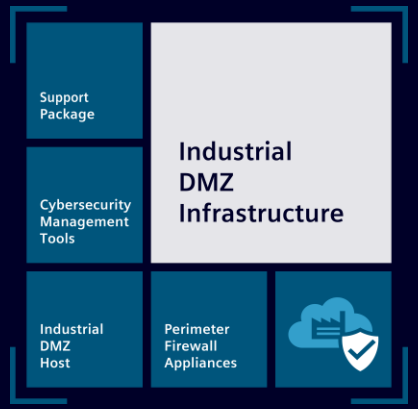
Industrial DMZ Infrastructure ist ein betriebsfertiges Konzept zur Segmentierung von IT- und OT-Netzwerken mit integrierten Security-Features in mehreren Verteidigungsebenen.

Wie funktioniert es?

Das Konzept basiert auf dem Prinzip der demilitarisierten Zone (DMZ). Die eingesetzten Next Generation Firewalls schützen die Automatisierungsebene vor unautorisiertem Zugriff von außen.

Zusätzliche Highlights:

- Inklusive weiterer Hardware, Software und Services für Netzwerksicherheit und Systemintegrität
- Implementierung auf der hyperkonvergenten IT-Plattform Industrial Automation DataCenter



Vorteile auf einen Blick

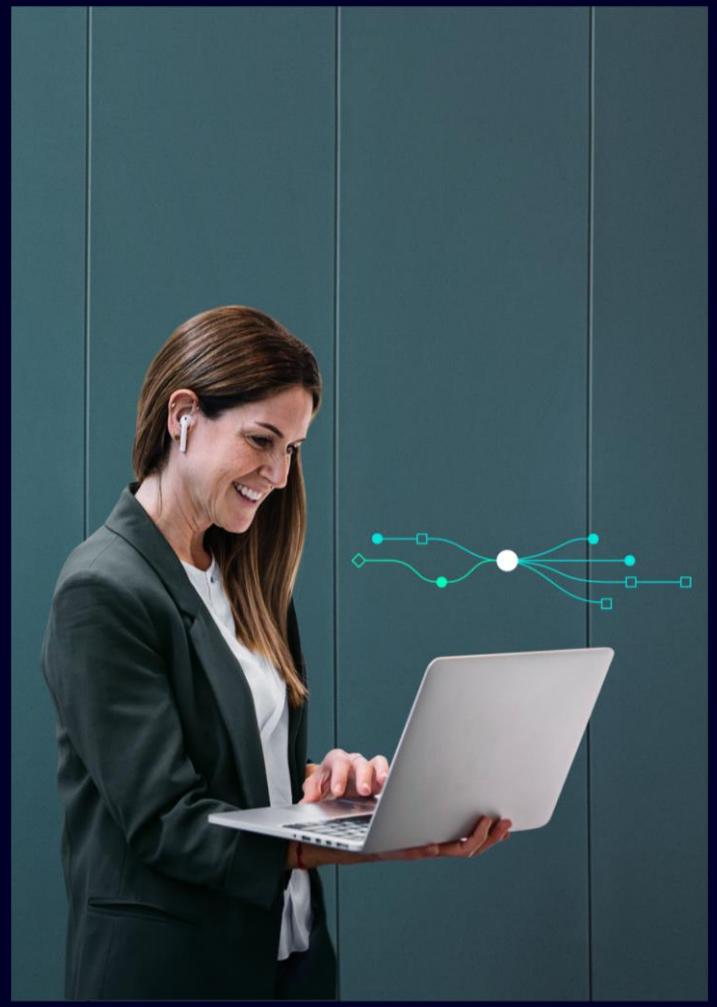
Segmentierung von IT/OT-Netzwerken gemäß IEC 62443

Defense in Depth mit Security-Features „out of the box“

Hyperkonvergente IT-Infrastruktur für High Performance Computing

SIEMENS

Sicherer Zguriff auf Industriegeräte
mit Remote Platform SaaS

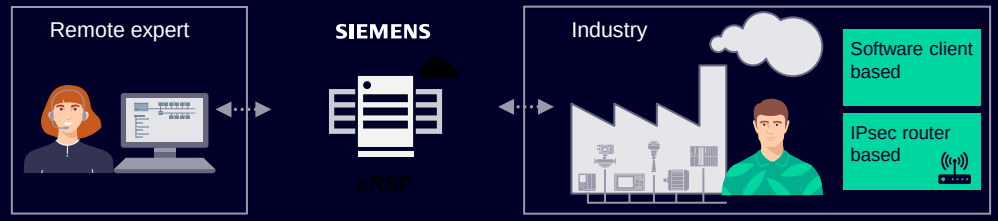


Remote Platform SaaS

Remote Platform Software as a Service (Remote Platform SaaS) bietet eine hoch skalierbare und sichere Fernzugriffsinfrastruktur, die von Siemens betrieben und gewartet wird. Die Common Remote Service Platform (cRSP) ist nach Branchenanforderungen gemäß IEC 62443 konzipiert und konzentriert sich auf den Zugriff auf Industriegeräte.

Wie funktioniert es?

cRSP wird für die Implementierung des Fernzugriffs und die Übertragung von Daten an IP-basierte Geräte verwendet. Die Administration und Konfiguration der Remote-Plattform erfolgt selbstverwaltet oder wird von Siemens verwaltet. Vordefinierte Anwendungsvorlagen sorgen für einfache Arbeitsabläufe für Remote-Experten. Nach der Ersteinrichtung kann ein autorisierter Remote-Experte über einen Software-Client oder einen IPsec-Router über einen sicheren VPN-Tunnel eine Remote-Verbindung zu den angeschlossenen Geräten herstellen.



Vorteile auf einen Blick

Weniger Reisen und geringere Ausfallzeiten führen zu Kosten-senkungen und tragen zur CO_2-Neutralität bei

Einsatz der bewährten und weltweit verfüg-baren Remote-Plattform cRSP von Siemens

State-of-the-Art Industrial Security

SIEMENS

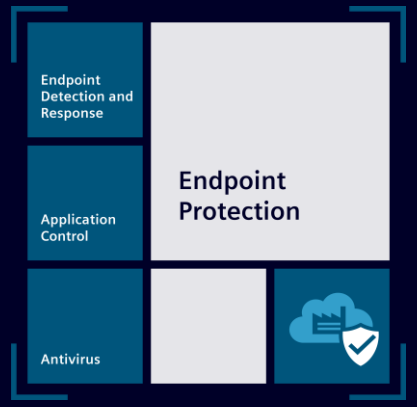
Kontinuierlicher Schutz vor Schadsoftware
dank Endpoint Protection

Endpoint Protection

- Die Bedrohung durch Malware in Form von Viren, Rootkits und Trojanern wächst exponentiell – auch für Endgeräte in industriellen Umgebungen (z.B. IPC)
- Endpoint Protection bietet unterschiedliche Ansätze – jeder hat seine Vorteile je nach Use-Case.

Wie funktioniert es?

- **Antivirus:** Blockiert die Ausführung bekannter schadhafter Anwendungen auf Basis kontinuierlich aktualisierter Signaturdateien
- **Application Control:** Erlaubt nur die Ausführung ertrauenswürdiger Anwendungen auf Basis einer Positivliste
- **Endpoint Protection and Response:** Interoperatibilitätstest für die spezifische Konfiguration von PCS 7 Versionen und EDR-Lösungen von Drittanbietern



Vorteile auf einen Blick

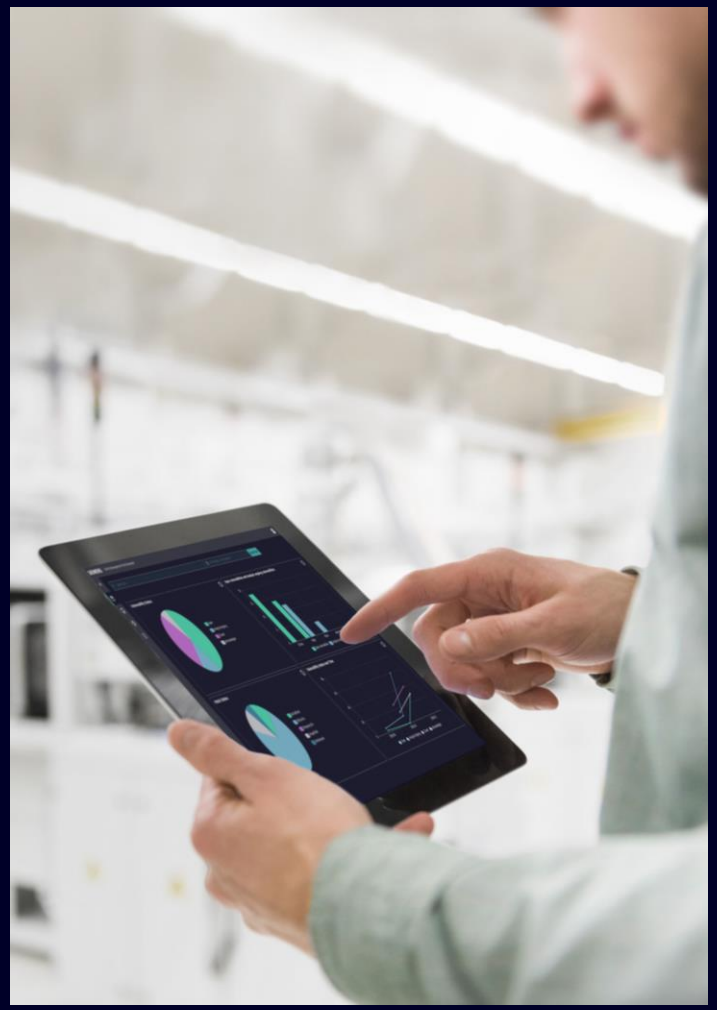
Schutz vor bekannten und unbekannten durch Malware verursachten Gefahren

Einfache, zentralisierte Verwaltung über einen Managementserver

Freigegebene Versionen mit maßgeschneiderten Konfigurationen für Siemens Produkte

SIEMENS

Effizientes Management von Schwachstellen
mit Vulnerability Services



Vulnerability Services

- Angesichts der wachsenden Zahl von Cyberbedrohungen müssen Unternehmen Schwachstellen so schnell wie möglich identifizieren und die Patchzeiten minimieren.
- Vulnerability Services helfen bei der Absicherung Ihrer gesamten Infrastruktur und Ihres Produktportfolio durch relevante, umsetzbare Schwachstellenintelligenz.

Wie funktioniert es?

Basierend auf einem einzigartigen Monitoring-Ansatz erhalten Sie Warnungen über Schwachstellen für Ihr individuelles System. Es gibt mehrere Optionen – je nach Anforderung:

- **Management Portal:**
  Tool inkl. Asset-Import, Tracking und Reporting
- **API:**
  Nahtlose Integration in bestehende Tools/Prozesse
- **Managed Service:**
  Wir kümmern uns!

Vorteile auf einen Blick

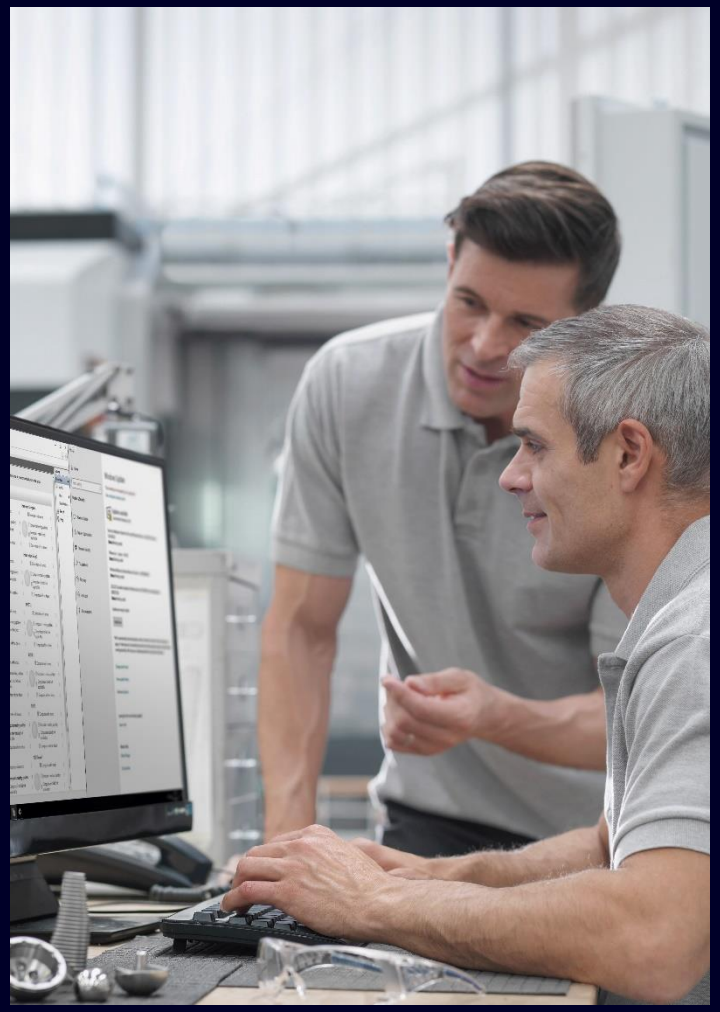
Sofortige Transparenz über Schwachstellen und minimierte Patchzeiten

Proaktives Management von Cyber-Risiken – mit einfacher Integration in Ihren Workflow

Vermindertes Risiko von kostspieligen Angriffen

SIEMENS

Verwalten von Schwachstellen und kritischen Updates
mit Patch Management



Patch Management

- Die Installation von Patches ist die gängige Lösung, um Schwachstellen in Software zu schließen. Patches tragen somit zu einem stabilen Anlagenbetrieb bei. Allerdings ist Patching manuelle Arbeit und ein inkompatibles Patch kann zu ungeplanten Ausfallzeiten führen.
- Siemens bietet Patch Management von Security-Patches und wichtigen Updates in Microsoft-Produkten für SIMATIC PCS 7 und vereinfacht so den Prozess.

Wie funktioniert es?

- **Schritt 1:** Die monatlich veröffentlichten Security-Patches für Microsoft-Produkte werden getestet und auf Kompatibilität mit SIMATIC PCS 7 überprüft.
- **Schritt 2:** Diese Informationen werden als Metadaten über den zentralen Update-Server (WSUS1) veröffentlicht, der die Informationen automatisch an den lokalen WSUS-Server in der Anlage sendet.
- **Schritt 3:** Sie erhalten eine Benachrichtigung und laden die genehmigten Patches direkt von Microsoft herunter.

1 Windows Software Update Services

Vorteile auf einen Blick

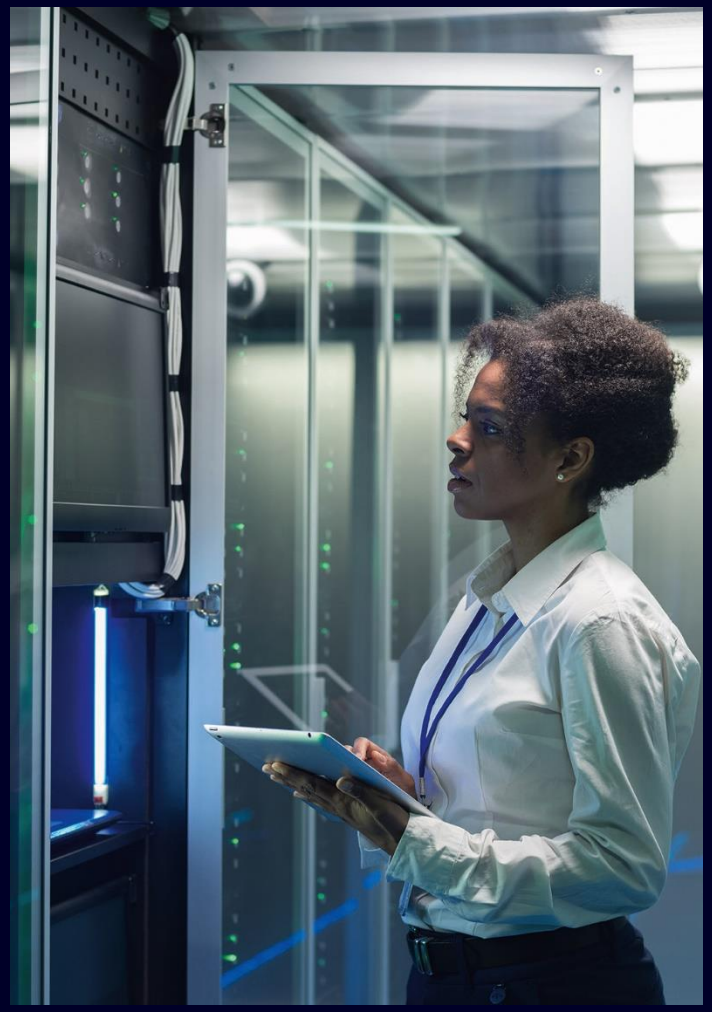
Zeit und Kosten sparen durch die Reduzierung manueller Arbeit

Minimierung des Risikos für Fehler

Gesteigerte Anlagenverfügbarkeit

SIEMENS

Vorkonfigurierte IT-Infrastruktur für Notfallwiederherstellung
mit Backup and Restore (SIMATIC DCS/SCADA Infrastructure)



Backup and Restore

Die richtige Disaster Recovery-Strategie ist ein wichtiger Faktor, um die Produktion nach einem Ausfall wieder aufzunehmen und Datenverluste zu verhindern. Insbesondere in Zeiten von steigenden Cyberangriffen und neuen Richtlinien, z.B. NIS 2, ist eine vollständig unterstützte Backuplösung unverzichtbar.

Backup and Restore (als Teil von SIMATIC DCS / SCADA Infrastructure) bietet eine leistungsstarke und vorkonfigurierte IT-Infrastruktur zur Notfallwiederherstellung in industriellen Umgebungen.

Wie funktioniert es?

Backup and Restore:
Einsatz der besten Disaster-Recovery-Lösung am Markt, adaptiert auf industrielle Umgebungen

Support Package:
Servicevertrag (3 oder 5 Jahre)

Vorteile auf einen Blick

- Erhöhte Verfügbarkeit dank schneller Wiederherstellung und Vermeidung von Datenverlust
- Einhaltung von Cybersecurity-Regularien und gesteigerte Datensicherheit
- Betriebsfertige Infrastruktur mit vorkonfigurierten Komponenten

SIEMENS

Industrial Cybersecurity Services @ Industrial Automation DataCenter

SIEMENS

Die Lücke zwischen IT und OT schließen
mit Industrial Automation DataCenter

Industrial Automation DataCenter

Die Systemkomplexität steigt und die Cybersecurity-Bedrohungen nehmen zu, gleichzeitig mangelt es an Know-how und Ressourcen bei der IT/OT-Integration.

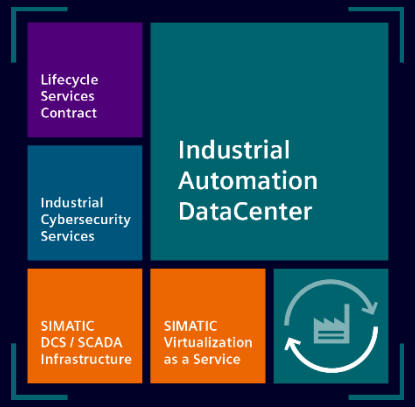
Das Industrial Automation DataCenter ist eine betriebsbereite maßgeschneiderte IT-Infrastruktur für OT-Umgebungen – entwickelt von Experten mit Expertise in beiden Bereichen.

Wie funktioniert es?

Alle Kernelemente eines Rechenzentrums sind enthalten:

- High Performance Computing
- IT/OT-Netzwerke
- Backup & Disaster Recovery
- Prozessdatenarchivierung
- unterbrechungsfreie Stromversorgung
- Security-Architektur gemäß IEC 62443

Der ganzheitliche Ansatz umfasst die Beratung, die Konfiguration sowie die passenden Managed Services über den gesamten Lebenszyklus – aus einer Hand.



Vorteile auf einen Blick

Betriebsbereite hochverfügbare IT/OT-Infrastruktur

Hohe Energieeffizienz und Platzeinsparungen

Cybersecurity by Design

SIEMENS

Lassen Sie uns wissen, wie wir Sie unterstützen können!

Sie möchten mehr wissen?

siemens.de/icss

SIEMENS

Ausschlusshinweis

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 Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

SIEMENS

Sicherheitsinformation

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

Zum Schutz von Anlagen, Systemen, Maschinen und Netzwerken vor Cyberangriffen ist es notwendig, ein ganzheitliches industrielles Sicherheitskonzept nach dem neuesten technologischen Stand zu implementieren und kontinuierlich zu pflegen.
Die Produkte und Lösungen von Siemens stellen dabei nur einen Teil dieses Konzepts dar.

Es liegt in der Verantwortung der Kunden, den unberechtigten Zugang zu ihren Werken, Anlagen, Maschinen und Netzwerken zu verhindern. Diese Anlagen, Maschinen und Komponenten sollten nur bei Bedarf, nur im erforderlichen Umfang und nur bei Vorhandensein geeigneter Sicherheitsmaßnahmen (z.B. Firewalls und/oder Netzwerk-Segmentierung) an ein Unternehmensnetzwerk oder das Internet angebunden werden.

Weitere Informationen zur Umsetzung industrieller Sicherheitsmaßnahmen finden Sie unter https://www.siemens.com/industrialsecurity .

Die Produkte und Lösungen von Siemens werden kontinuierlich weiterentwickelt, um ihre Sicherheit zu verbessern. Es wird von Siemens dringend empfohlen, verfügbare Produkt-Updates sofort durchzuführen und nur die aktuellen Produktstände zu verwenden.
Die Verwendung von nicht mehr unterstützten Produktständen und die Nichtdurchführung der neuesten Updates können die Gefahr von Cyberangriffen für Kunden erhöhen.

Für aktuelle Informationen über Produkt-Updates abonnieren Sie bitte den Siemens Industrial Security RSS Feed unter
https://www.siemens.com/industrialsecurity

SIEMENS