
SIEMENS
Ingenuity for life
Produktivität umfassend schützen mit Industrial Security Services
Schwachstellen und Bedrohungen frühzeitig erkennen. Proaktive Maßnahmen ergreifen. Langfristig optimalen Anlagenschutz erreichen.
siemens.de/industrial-security-services

Umfassend vor Cyberangriffen geschützt

Industriespezifisch und skalierbar: optimales Schutzniveau für Ihre Anlagen

Schnell wachsende und ständig neue Sicherheitsrisiken und Cyberbedrohungen erfordern schnelle Reaktionen. Besonders Produktionsprozesse bieten immer wieder neue Angriffsflächen und benötigen daher ein besonders hohes Schutzniveau. Mit Siemens Industrial Security Services profitieren Industrieunternehmen vom umfassenden Know-how sowie von der Fachkompetenz eines weltweiten Expertennetzwerks für Automatisierung und Cyber Security.

Der ganzheitliche Ansatz des kundenspezifischen Konzepts basiert auf modernsten Technologien und erfüllt dabei die aktuell geltenden Security-Normen und -Standards. Bedrohungen oder Schadsoftware werden frühzeitig erkannt, die Schwachstellen im Detail analysiert und geeignete Sicherheitsmaßnahmen sofort eingeleitet.

Das skalierbare Angebot enthält umfassende Beratung, die technischen Implementierungen und kontinuierlichen Service.
Das Portfolio steht sowohl für bestehende Siemens-Automatisierungstechnik als auch für Komponenten von Drittanbietern zur Verfügung.

Langfristiger Schutz von Industrieanlagen: Transparenz dank Überwachung und Analyse

Tritt ein Cyber Security Vorfall ein, können folglich die Kunden informiert und geeignete Gegenmaßnahmen eingeleitet werden. Egal für welche Industriebranche: Ein anlagenspezifischer Security-Fahrplan gewährleistet auf der Grundlage von Risikomanagement das bestmögliche, kostenoptimierte Sicherheitsniveau für Ihre Industrieanlage.

Kontinuierliche Überwachung gibt Anlagenbetreibern größtmögliche Transparenz über die Sicherheit ihrer Industrieanlage und somit jederzeit einen besonders guten Investitionsschutz. Die integrierten, leistungsfähigen Global-Threat-Intelligence-Datenbanken analysieren und erkennen neu auftretende Bedrohungen. Die entsprechenden Anpassungen erfolgen direkt und kontinuierlich. Das industriespezifische, umfassende und modular aufgebaute Portfolio bietet passgenaues und budgetgerechtes Engineering.

Industrieunternehmen vertrauen auf Siemens Industrial Security Services, denn dank des transparenten Überblicks zum Sicherheitsstatus können sich Anlagenbetreiber jederzeit auf ihr Kerngeschäft in Ihrer Produktionsumgebung konzentrieren. Das sensible Thema Cyber Security gehört in die Hände von versierten Experten mit Automatisierungskompetenz: Siemens Industrial Security Services.

Assess Security für einen risikobasierten Security-Fahrplan

Assess Security beinhaltet die umfassende, auf Normen und Standards basierende Analyse von Bedrohungen. Risiken werden identifiziert und konkrete Empfehlungen von Security-Maßnahmen werden dem Kunden an die Hand gegeben.

Ihr Vorteil:

Ein anlagenspezifischer und risikobasierter Security-Fahrplan gewährleistet ein durchgängig konsistentes Sicherheitsniveau.

Industrial Security Assessment

- **Basierend auf dem Siemens Defense-in-Depth Konzept**
- **Abgeleitet aus IEC 62443**
- **Beruht auf Siemens Industrial Security Erfahrungen**
- **Kompaktes eintägiges Assessment**

IEC 62443 Assessment

- **Gemäß IEC 62443 Normen**
- **Verfügbar für Anlagen von Siemens und von Drittanbietern**
- **Fragenbasiert**
- **Empfehlungen zur Risikominderung (Bericht umfasst bis zu 30 Seiten)**

ISO 27001 Assessment

- **Gemäß ISO 27001 Normen**
- **Verfügbar für Anlagen von Siemens und von Drittanbietern**
- **Fragenbasiert**
- **Empfehlungen zur Risikominderung (Bericht umfasst bis zu 30 Seiten)**

Risk & Vulnerability Assessment

- **Datenbasierte Analyse von Bedrohungen, Schwachstellen und Lücken**
- **Risikoklassifizierung und -auswertung unter Berücksichtigung der Systemkritikalität**
- **Empfehlungen von Risikominderungsmaßnahmen (Bericht umfasst über 100 Seiten)**
- **Basis für einen risikobasierten, anlagenspezifischen Security-Fahrplan**

Implement Security zur Umsetzung von Maßnahmen, die Risiken minimieren

Implement Security bedeutet die lokale Umsetzung von Schutzmaßnahmen, um das Sicherheitsniveau von Anlagen und Produktionsstätten zu erhöhen.

Ihr Vorteil:

Vermeidung von Sicherheitslücken und besserer Schutz vor Cyberbedrohungen dank technischer und organisatorischer Maßnahmen.

Security Awareness Training

- **Web-basierte SITRAIN-Schulungen**
- **Schaffung eines Security-Bewusstseins des Anlagenpersonals: zur aktuellen Lage und im Umgang mit Bedrohungen, Risiken, Erkennung von Sicherheitsvorfällen**

Industrial Security Consulting

- **Kundenspezifische Beratung zu Cyber Security-Prozessen und -Richtlinien in der Produktion**
- **Beratung zur Auslegung von Automatisierungsnetzwerken**

Automation Firewall

- **Automation Firewall classic, basierend auf SecureGUARD Firewalls (PCS7 getestet)**
- **Automation Firewall-NG, basierend auf Palo Alto Firewalls mit next-generation Funktionalität (insb. deep-package inspection)**
- **Festlegung und Überprüfung der Anlagenperimeter-Firewall-Regeln**

Windows Patch Installation

- **Installation von Microsoft-Betriebssystem-Patches mithilfe eines kundeneigenen WSUS-Servers[2]**
- **Kompatibilitätsbetrachtung: Installation von Hersteller empfohlenen und kundengenehmigten Patches**

Application Whitelisting

- **Installation und Konfiguration einer Whitelisting-Software: McAfee Application Control**
- **Installation einer zentralen Management-Konsole: McAfee ePO[1] (empfohlen bei mehr als 10 Whitelisting-Agenten)**
- **Kompatibilitätsbetrachtung für SIMATIC PCS 7 Systeme**

Anti Virus Installation

- **Installation und Konfiguration von Virenschutzsoftware: McAfee Virusscan Enterprise**
- **Installation einer zentralen Managementkonsole: McAfee ePO[1] (empfohlen bei mehr als 10 Antivirus-Agenten)**
- **Kompatibilitätsbetrachtung für SIMATIC PCS 7 Systeme**

System Back-up

- **Durchführung eines einmaligen Back-ups kritischer Anlagen-systeme durch Symantec System Recovery Software (wird vom Kunden bereitgestellt)**

Industrial Anomaly Detection

- **Transparenz über die in einer Anlage kommunizierenden Assets**
- **Erkennung von Anomalien im Kommunikationsverhalten**
- **100% passiv und damit rückwirkungsfrei für die Produktion**
- **Verfügbar für Anlagen von Siemens und von Drittanbietern**
- **Basierend auf Siemens IPCs 427E**

Industrial Security Monitoring

- **Kontinuierliche Überwachung von industriespezifischen Security Monitoring Szenarien, basierend auf SIEM-Technologien[3]**
- **Locale Installation der Erfassungskomponente**
- **Betrachtung der kundenspezifischen Anwendungen, z. B. Justierung des Intrusion Detection/Prevention Systems (IDS/IPS)**

[1] ePO – McAfee ePolicy Orchestrator
[2] WSUS – Microsoft Windows Software Update Server
[3] SIEM - Security Information und Event Management

Manage Security für kontinuierlichen Schutz und Transparenz

Manage Security heißt regelmäßige Überwachung und Aktualisierung der implementierten Maßnahmen durch unsere zentralisierte Services.

Ihr Vorteil:

Sie erhalten größtmögliche Transparenz über den Sicherheitsstatus Ihrer Anlagen und vermeiden potenzielle Bedrohungsfälle proaktiv dank unserer weltweiten Security-Experten und unserer skalierbaren Infrastruktur.

Security Vulnerability Information

- **Informationen zu bekannten Schwachstellen von verwendeten Software-Versionen**
- **Bereitstellung über die Security Vulnerability Information App, auch verfügbar als MindSphere-App**

Patch Management

- **Systemspezifische Informationen über bekannte Schwachstellen und Patch-Verfügbarkeiten**
- **Empfehlungen zur anlagenspezifischen Patch-Strategie**
- **Verfügbar für SIMATIC PCS 7 Software, Microsoft Betriebssysteme, Adobe Reader und Flash**

Anti Virus Management

- **Aktualisierung der Virensignaturen und periodische Virenscans gemäß den Empfehlungen der Softwarehersteller**
- **Erkennung möglicher Fehlalarme[2] durch enge Zusammenarbeit mit Herstellern von Virenschutz-Software**
- **Regelmäßige Berichte über den Anlagenzustand bzgl. der Erkennung und Vermeidung von Malware**
- **Zentrales Management durch ePO-Konsole[1] möglich**

Industrial Security Monitoring

- **Kontinuierliche Analyse und Korrelation der Log-Daten sowie Abgleich mit »Global Threat Intelligence«-Datenbanken**
- **Erkennung, Klassifizierung sowie unmittelbare Benachrichtigung beim Erkennen von Sicherheitsbedrohungen und -vorfällen**
- **Übersicht zum aktuellen Sicherheitsstatus der Anlage durch regelmäßige Statusberichte**

Remote Incident Handling

- **Schnelle Reaktionen durch Cyber Security Experten von Siemens mit Industrieerfahrung**
- **Informationssammlung, Ursachenanalyse sowie Kritikalitätsanalyse u. a. mit Threat-Intelligence-Mechanismen, Malware Sandboxing sowie Schwachstellenüberwachung**
- **Empfehlungen zur Behebung eventueller Folgeschäden**

[1] ePO – McAfee ePolicy Orchestrator
[2] »False positive«, ausschließlich für Siemens-Produkte

Die Sicherheitsstrategie mit Wirkung

Defense in Depth

Mit zunehmender Digitalisierung wird umfassende Sicherheit in der Automatisierung immer wichtiger. Deshalb ist Industrial Security ein Kernelement von Digital Enterprise, dem Lösungsansatz von Siemens auf Ihrem Weg zu Industrie 4.0. Mit Defense in Depth bietet Siemens ein vielschichtiges Konzept, das Ihre Anlage sowohl rundum als auch in die Tiefe schützt. Das Konzept basiert auf Anlagensicherheit, Netzwerksicherheit und Systemintegrität nach den Empfehlungen der ISA 99/IEC 62443.

Anlagensicherheit

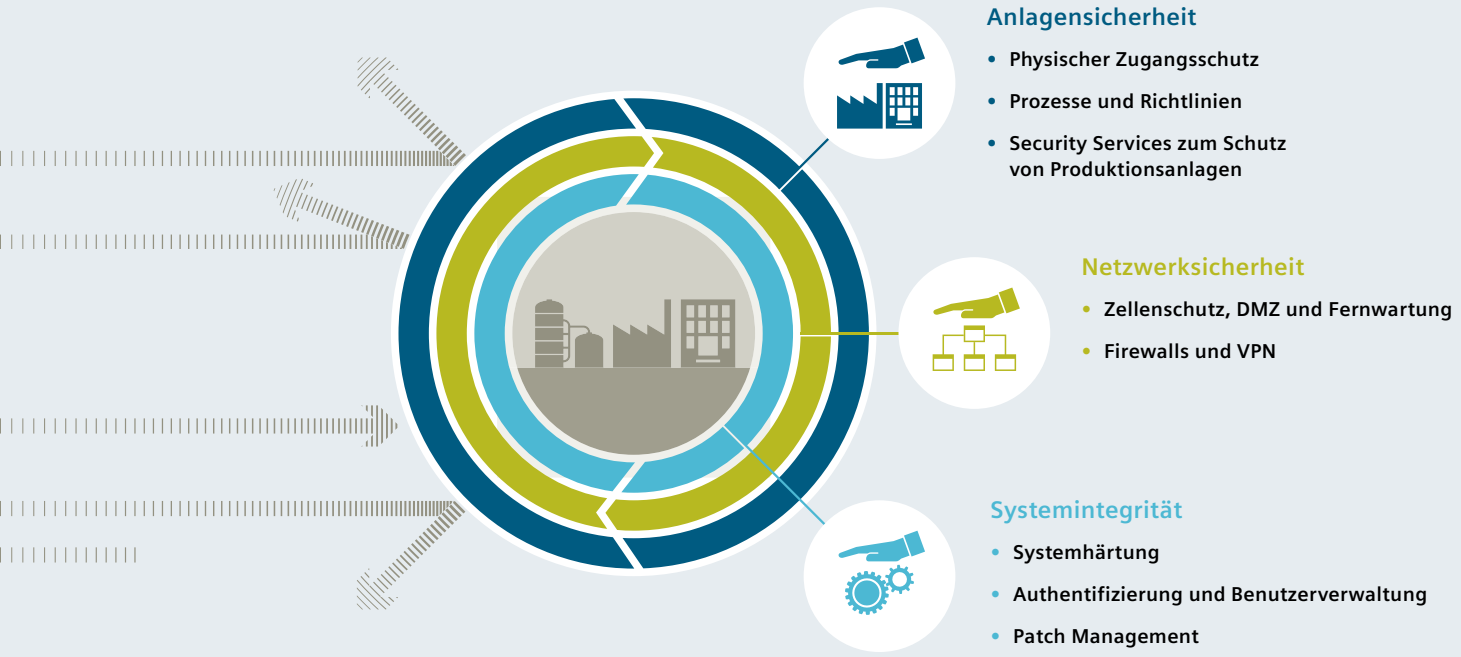
Anlagensicherheit sichert mit verschiedenen Methoden den physischen Zugang von Personen zu kritischen Komponenten. Dies beginnt mit dem klassischen Gebäudezutritt und reicht bis zur Sicherung sensibler Bereiche mittels Codekarten. Die maßgeschneiderten Industrial Security-Services umfassen Prozesse und Richtlinien für einen umfassenden Anlagenschutz. Das reicht von der Risikoanalyse über die Implementierung geeigneter Maßnahmen und deren Überwachung bis zu regelmäßigen Updates.

Netzwerksicherheit

Produktionsnetze vor unberechtigten Zugriffen zu schützen ist heute insbesondere an den Verbindungsstellen zu anderen Netzen (z. B. Office oder Internet) unabdingbar. Zusätzliche Sicherheit bietet hier die Segmentierung einzelner Teilnetze wie das Zellenschutzkonzept mit SCALANCE S oder den Security-Kommunikationsprozessoren für SIMATIC. Die Datenübertragung kann zudem mit VPN geschützt werden, etwa für weltweite Fernzugriffe auf entlegene Anlagen über Internet oder Mobilfunknetze mit SCALANCE M. Das Firewall-Portfolio wird ergänzt durch Automation Firewall classic oder NG, die schwerpunktmäßig an Perimeter zwischen Office-IT und dem Produktionsnetz zur Anwendung kommen.

Systemintegrität

Die dritte tragende Säule von Defense in Depth ist die Sicherung der Systemintegrität. Dies beinhaltet, Automatisierungssysteme und Steuerungen wie SIMATIC S7 Steuerungen sowie SCADA- und HMI-Systeme gegen unbefugte Zugriffe abzusichern oder darin enthaltenes Know-how zu schützen. Weiterhin geht es um die Authentifizierung von Benutzern und deren Zugriffsrechte sowie um die Systemhärtung gegenüber Angriffen.



Anlagensicherheit

- **Physischer Zugangsschutz**
- **Prozesse und Richtlinien**
- **Security Services zum Schutz von Produktionsanlagen**

Netzwerksicherheit

- **Zellenschutz, DMZ und Fernwartung**
- **Firewalls und VPN**

Systemintegrität

- **Systemhärtung**
- **Authentifizierung und Benutzerverwaltung**
- **Patch Management**
- **Erkennung von Angriffen**
- **Integrierter Zugangsschutz in der Automatisierung**

Assess Security

- Industrial Security Assessment
- IEC 62443 Assessment
- ISO 27001 Assessment
- Risk & Vulnerability Assessment

Manage Security

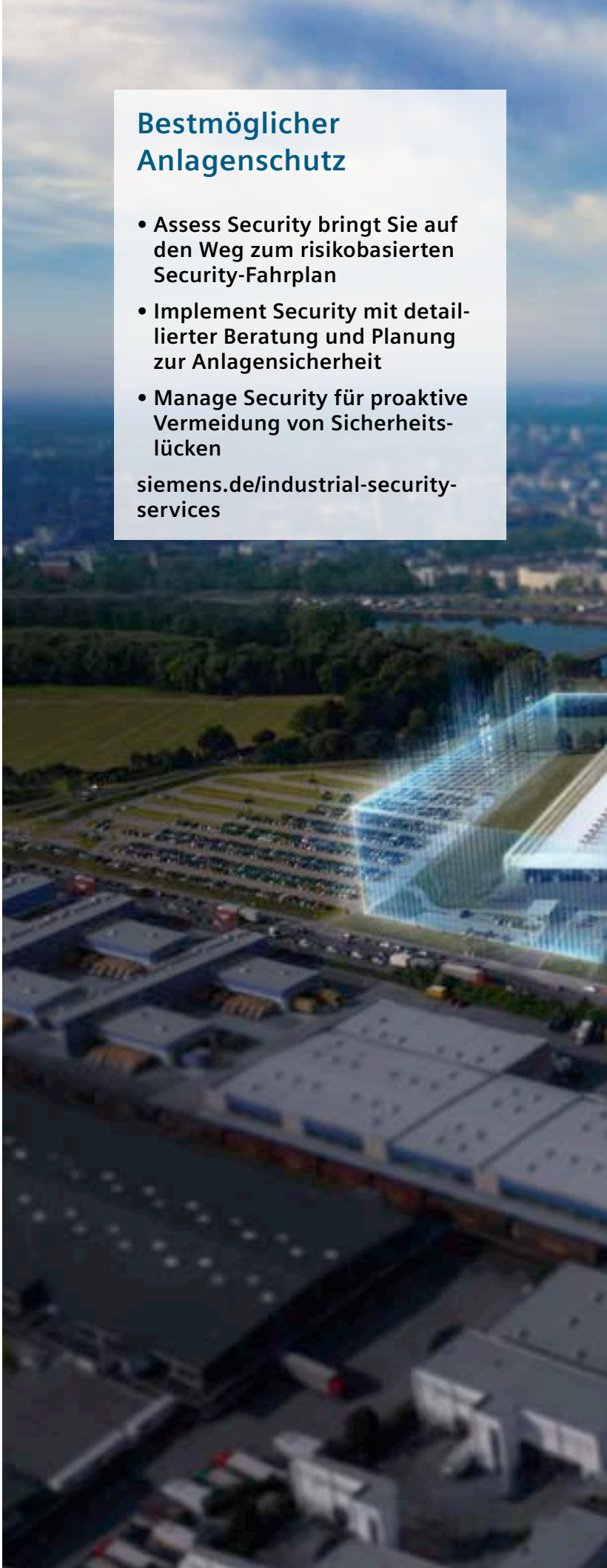
- Security Vulnerability Information
- Patch Management
- Anti Virus Management
- Industrial Security Monitoring
- Remote Incident Handling

Implement Security

- Security Awareness Training
- Industrial Security Consulting
- Automation Firewall
- Windows Patch Installation
- Application Whitelisting
- Anti Virus Installation
- System Back-up
- Industrial Anomaly Detection
- Industrial Security Monitoring

Siemens AG
Digital Factory
Postfach 48 48
90026 Nürnberg
Deutschland

Änderungen vorbehalten
Artikel-Nr.: DFPL-B10009-01
WS 04180.3
Gedruckt in Deutschland



Bestmöglicher Anlagenschutz

- **Assess Security bringt Sie auf den Weg zum risikobasierten Security-Fahrplan**
- **Implement Security mit detaillierter Beratung und Planung zur Anlagensicherheit**
- **Manage Security für proaktive Vermeidung von Sicherheitslücken**

siemens.de/industrial-security-services