SIEMENS
Ingenuity for life

Produktivität umfassend schützen mit Plant Security Services

Schwachstellen und Bedrohungen frühzeitig erkennen. Proaktive Maßnahmen ergreifen. Langfristig optimalen Anlagenschutz erreichen.

siemens.de/plant-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 Plant 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 (Manage Security). Das Portfolio steht sowohl für bestehende Siemens-Anlagen als auch für technische Anlagen von Drittanbietern zur Verfügung.

Langfristiger Schutz von Industrieanlagen: Transparenz dank Überwachung und Analyse

Tritt ein Sicherheitsfall ein, können folglich schnelle Reaktionen eingeleitet, die Kunden informiert und geeignete Security Patches und Updates bereitgestellt werden. Darüber hinaus ist die Dienstleistung an die individuellen Kundenbedürfnisse optimal anpassbar. Egal für welche Industriebranche: Ein anlagenspezifischer Security-Fahrplan gewährleistet das bestmögliche Sicherheitsniveau bei maßgeblich reduziertem Risiko.

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 nicht nur passgenaues, sondern auch budgetgerechtes Engineering.

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

Assess Security

- IEC 62443 Assessment
- ISO 27001 Assessment
- SIMATIC PCS 7 & WinCC Assessment
- Risk & Vulnerability Assessment

Manage Security

- Industrial Security Monitoring
- Remote Incident Handling
- Perimeter Firewall Management
- Perimeter Firewall Review
- Anti Virus Management
- Whitelisting Management
- Patch & Vulnerability Management

Implement Security

- Security Awareness Training
- Security Policy Consulting
- Network Security Consulting
- Perimeter Firewall Installation
- Clean Slate Validation
- Anti Virus Installation
- Whitelisting Installation
- System Back-up
- Windows Patch Installation

Assess Security für einen risikobasierten Security-Fahrplan

Assess Security beinhaltet die umfassende Analyse von Bedrohungen, die Identifizierung der Risiken und die konkrete Empfehlung von Security-Maßnahmen.

Ihr Vorteil:

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

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)**

SIMATIC PCS 7 & WinCC Assessment

- **Gemäß SIMATIC PCS 7 und WinCC Sicherheitskonzept**
- **Speziell für SIMATIC PCS 7 und WinCC Anlagen**
- **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 für Maßnahmen zur Risikominderung

Implement Security bedeutet die 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**

Security Policy Consulting

- **Einführung neuer und Prüfung bestehender sicherheitsrelevanter Standards, Richtlinien und Prozesse für die Anlagensicherheit**
- **Integration in bestehende Büro-IT-Sicherheitsrichtlinie**
- **Umsetzung der Empfehlungen, z. B. Patch- und Back-up-Strategie, Umgang mit Wechselmedien**

Network Security Consulting

- **Unterstützung bei der Planung und Segmentierung des Automatisierungsnetzes in Sicherheitszellen gemäß IEC 62443 und dem SIMATIC PCS 7 & WinCC Sicherheitskonzept**
- **Planung eines DMZ-Netzwerks (Perimeter)**
- **Festlegung und Überprüfung der Anlagenperimeter-Firewall-Regeln**

Perimeter Firewall Installation

- **Installation, Konfiguration und Test der Firewall sowie der Firewall-Regeln**
- **Back-up der Konfiguration gemäß Automation Firewall Appliance**
- **Betrachtung der kundenspezifischen Anwendungen, z. B. Justierung des Intrusion Detection/Prevention Systems (IDS/IPS)**

Clean Slate Validation

- **Identifizierung von Sicherheitsrisiken mit zwei unterschiedlichen Virenscannern: McAfee Command Line Scanner und Kaspersky Rescue Disk**
- **Keine Installation nötig: Verwendung von USB-Sticks und Kommandozeile**

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**

Whitelisting Installation

- **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**

System Back-up

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

Windows® Patch Installation

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

[1] ePO – McAfee ePolicy Orchestrator
[2] WSUS – Microsoft Windows Software Update Server

Manage Security für umfassenden Schutz und Transparenz

Manage Security heißt regelmäßige Überwachung und Aktualisierung der implementierten Maßnahmen durch unsere Cyber Security Operation Center (CSOC).

Ihr Vorteil:

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

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**
- **Permanente Übersicht über den aktuellen Sicherheitsstatus der Anlage durch monatliche Statusberichte**

Remote Incident Handling

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

Perimeter Firewall Management

- **Überwachung, Alarmierung und monatliche Berichterstattung**
- **IDS/IPS Management der Einbruchmeldeanlage (Intrusion Detection/Prevention System)**
- **Anpassungen bestehender Firewall-Konfigurationen und -Regeln**
- **Back-ups/Upgrades von Firmware und Software**

Perimeter Firewall Review

- **Schwachstellenanalyse der Firmware**
- **Redundanzprüfung sowie semantische Analyse der Firewall-Regeln**
- **Validierung der Firewall-Konfiguration gegen die Netzwerkstruktur (Konsistenzprüfung)**
- **Unterstützung einer großen Vielfalt an Firewall-Technologien**

Anti Virus Management

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

Whitelisting Management

- **Aktualisierung und Verwaltung aktivierter Whitelisting-Richtlinien (Definition zugelassener und ausführbarer Softwarepakete)**
- **Monatliche Berichte über den Anlagenzustand bzgl. der Erkennung und Vermeidung von Malware**
- **Umsetzung der Regeln für die Applikationskontrolle durch Kundenzustimmung**
- **Zentrales Management durch ePO-Konsole[2] möglich**

Patch & Vulnerability Management

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

[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 dem 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

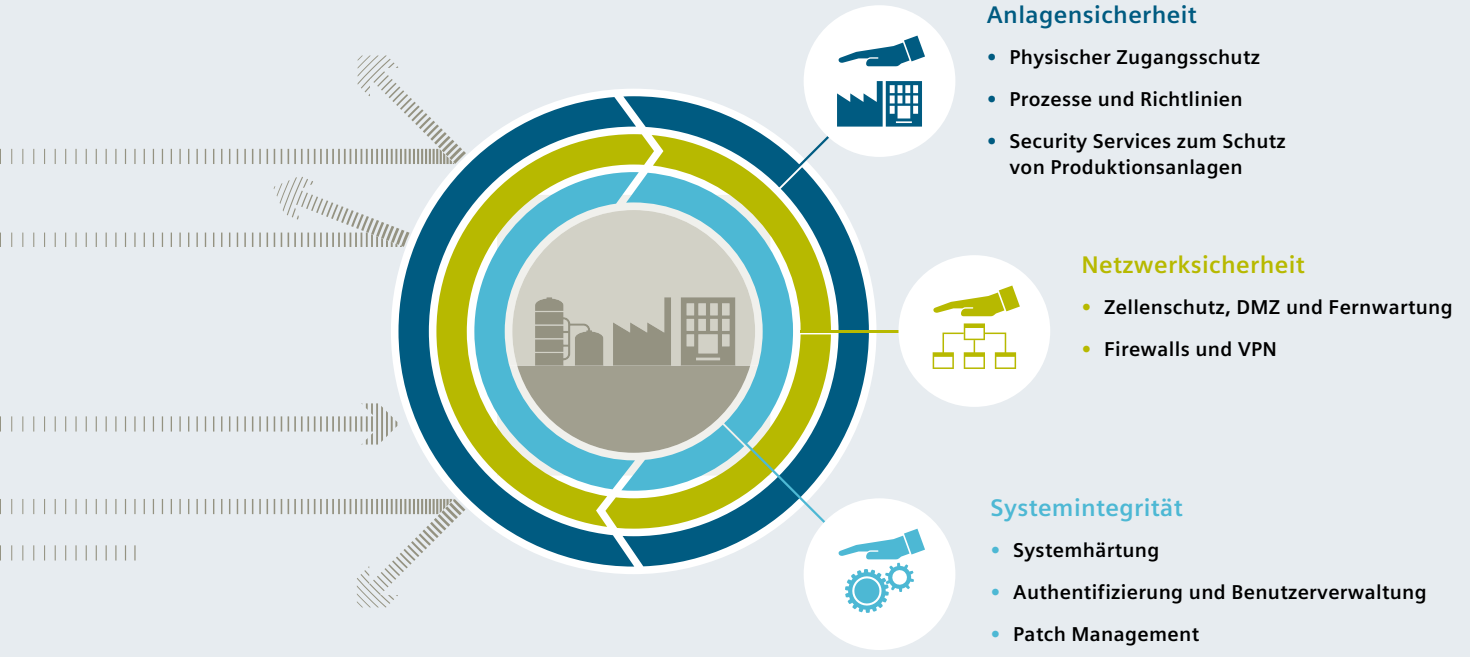
Anlagensicherheit sichert mit verschiedenen Methoden den physischen Zugang von Personen zu kritischen Komponenten. Dies beginnt mit dem klassischen Gebäudezutritt und reicht bis zur Sicherung sensibler Bereiche mittels Codekarten. Die maßgeschneiderten Industrial Security-Services umfassen Prozesse und 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.

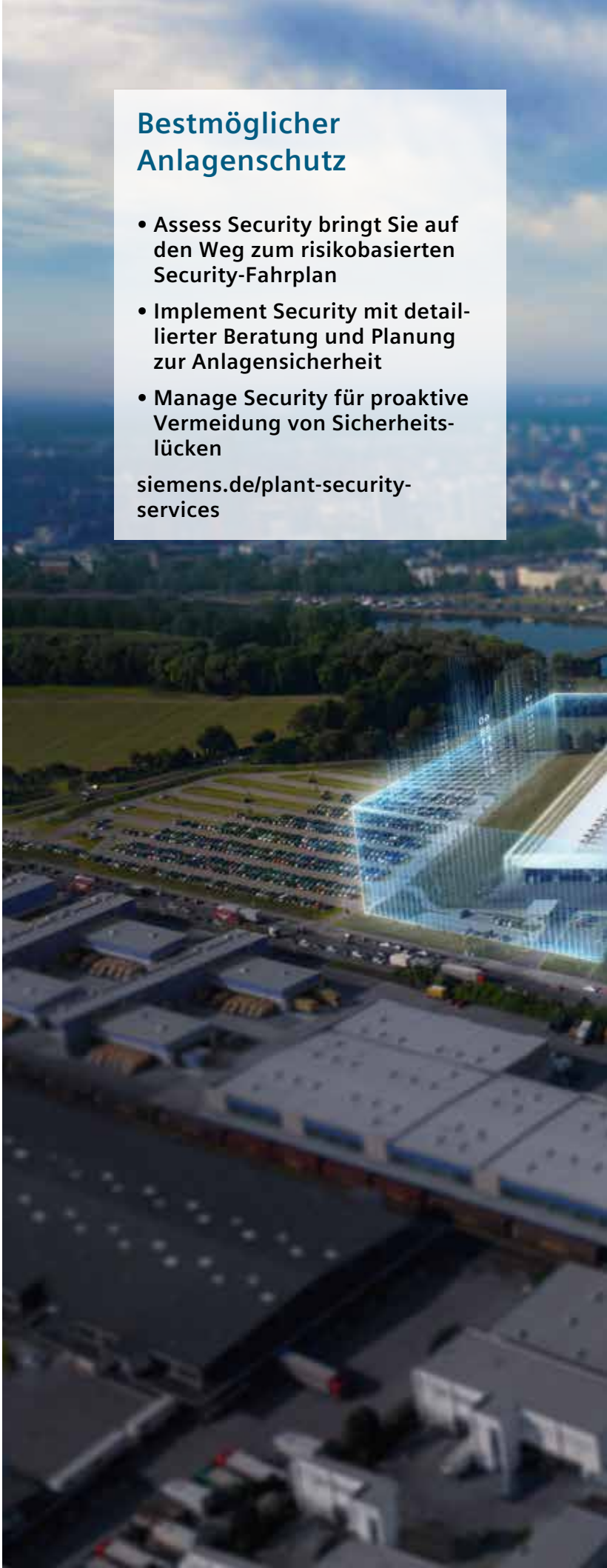
Systemintegrität

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.



Siemens AG
Digital Factory
Postfach 48 48
90026 Nürnberg
Deutschland

Änderungen vorbehalten
Artikel-Nr.: DFPL-B10009-00
Dispo 21639 WS 0416X.X
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/plant-security-services