SIEMENS

Preis-vorteil über 40 %

Angebot gültig bis 30.09.2021

Sichere industrielle Netzwerke mit SINEC NMS

Netzwerk-Management-System, Industrial Security Appliances SCALANCE SC-600 und Industrial Ethernet Switch SCALANCE XC-200

Testen Sie jetzt unser Aktionspaket!

Unser Netzwerk-Management-System SINEC NMS erfüllt zuverlässig prozessuale und technische Sicherheitsanforderungen gemäß der Norm IEC 62443. Die Kombination aus Industrial Security Appliances SCALANCE SC-600 und SINEC NMS erhöht die Sicherheit des gesamten Netzwerks im Operational Technology (OT)-Bereich.

Um diese Anforderungen zu erfüllen und Ihr industrielles Netzwerk abzusichern, generiert SINEC NMS z. B. hunderte von Firewall-Regeln. Sie können grafisch und regelbasiert Kommunikationsbeziehungen zwischen zwei Gruppen kreieren und Richtlinien für automatisch generierte Firewall-Regeln für Industrial Security Appliances festlegen.

Anforderungen gemäß IEC 62443	Ihre Vorteile
Identifizierung und Authentifizierung	Eine rollenbasierte Zugriffskontrolle ermöglicht eine präzise Verwaltung der Zugriffe und Rechte verschiedener Nutzer inklusive existierender Nutzer von RADIUS oder Active Directory auf einem zentralen User Management Component (UMC)-Server
Systemintegrität	Verschlüsselte Datenkommunikation zwischen den zwei Ebenen des Systems, SINEC NMS Control und SINEC NMS Operation (über Zertifikate und Passwörter) sowie zwischen SINEC NMS und Netzwerkkomponenten (via SNMPv3, HTTPS, SSH)
Eingeschränkter Datenfluss mit Netzwerksegmentierung und Schutz der Zonengrenzen	Fehlerfreie, regelbasierte Konfiguration von Access Control-Listen (ACL) für die Zugriffskontrolle in mehreren Switches und Routern, Visualisierung von Redundanz oder VLANs, um segmentierte Netzwerkarchitekturen inklusive Netzwerke hinter NAT-Routern zu diagnostizieren
Zugang zu Inventarliste, Statistiken und Audit-Log-Einträgen	Netzwerkinformationen sind jederzeit auf einen Blick verfügbar (z. B. Inventarliste der Geräte und Netzwerkstatistiken), um Security-Audits zu bestehen und über standardisierte Schnittstellen Informationen an unterschiedliche IT-Systeme zu senden bzw. diese zu empfangen
Verfügbarkeit der Ressourcen	Sicherung / Wiederherstellung der Konfiguration von Netzwerkgeräten in variablen Zeitabständen, zentrale Verwaltung der Firmwarestände, um z. B. sicherheitsrelevante Updates einzuspielen
Geräte- und Systemhärtung	Zentrales Blockieren von physischen Ports und ungenutzten Anschlüssen, Deaktivierung unsicherer Protokolle wie TELNET oder HTTP an allen unterstützten Netzwerkgeräten via Richtlinien

siemens.de/sinec-nms

Bestellen Sie jetzt Ihr Aktionspaket![1)]

SINEC NMS & SCALANCE SC632-2C

- 1x SINEC NMS 50 Lizenz (DVD)
- 2x Industrial Security Appliance SCALANCE SC632-2C

Artikel-Nr.: 6GK8781-1AP02
Preis: 2500€

SINEC NMS, SCALANCE SC632-2C & SCALANCE XC208G

- 1x SINEC NMS 50 Lizenz (DVD)
- 1x Industrial Security Appliance SCALANCE SC632-2C
- 1x Industrial Ethernet Switch SCALANCE XC208G

Artikel-Nr.: 6GK8781-1AP01
Preis: 2400€

Zusätzliche SINEC-Softwaretools zur Kombination mit den Aktionspaketen

SINEC INS (Infrastructure Network Services)

Software für zentrale Netzwerkdienste, z. B.:

- Verwaltung dynamischer IP-Adressen (DHCP-Server)
- Bereitstellung von Firmware-Upgrade-Dateien (TFTP-Server)
- Senden / Empfangen von Syslog-Nachrichten (Sicherer Syslog-Server)
- Zeitsynchronisation (Sicherer NTP-Server)
- Authentifizierung von Nutzern und Geräten (RADIUS-Server)

Zum kostenlosen Download:
support.industry.siemens.com/cs/ww/de/view/109781022

SINEC PNI (Primary Network Initialization)

Software zur Initialisierung von Netzwerkkomponenten von Siemens

- Netzwerkscan von SCALANCE-, RUGGEDCOM- und PROFINET-Geräten
- Masseninitialisierung der Parameter von Netzwerkgeräten, z. B.:
  - IP-Adresse, Subnetz und Gateway, PROFINET-Name
  - Änderung des initialen Passworts (SCALANCE)
- Reset zu Werkseinstellungen und PROFINET-Standard-Einstellungen

Zum kostenlosen Download:
support.industry.siemens.com/cs/ww/de/view/109776941

Security information

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

[1)] Je Kunde kann ein Aktionspaket bestellt werden. Es gelten die Allgemeinen Zahlungsbedingungen sowie die Allgemeinen Lieferbedingungen für Erzeugnisse und Leistungen der Elektroindustrie. Für Softwareprodukte gelten die Allgemeinen Bedingungen zur Überlassung von Software für Automatisierungs- und Antriebstechnik an Lizenznehmer mit Sitz in Deutschland. Die Preise (ohne Mehrwertsteuer) gelten in Euro ab Werk, ausschließlich Verpackung.

Siemens AG
Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Deutschland

PDF
BR 0820 2. De
Produced in Germany

siemens.de/sinec-nms