SIEMENS

Unterstützungen und Lösungen für die **NIS2-Richtlinie**

siemens.de/nis2-richtlinie

Lösungen zur Erfüllung der Anforderungen von NIS2

Machen Sie sich bereit für NIS2! Hier finden Sie einen kurzen Überblick über unser Beratungs-, Hardware- und Softwareangebot. Darüber hinaus bieten wir Ihnen ausführliche Informationen zur Cybersecurity, die darauf abzielen, Netzwerk- und Informationssysteme sowie deren physische Umgebung vor Vorfällen zu schützen. Zusätzlich zu dieser Auswahl finden Sie weitere nützliche Lösungen in unserem Portfolio.

↗ **Weitere Informationen zu NIS2, einschließlich Artikel 20 (Governance) und Artikel 21 (Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit)**

LÖSUNG

Entwicklung geeigneter Sicherheits-richtlinien für Ihre Kunden

Neben technischen Maßnahmen sind Richtlinien und Abläufe obligatorischer Bestandteil eines Sicherheitskonzepts. Ebenso wichtig sind Richtlinien für die Einhaltung der in Normen und Vorschriften für Cybersecurity festgeschriebenen Anforderungen. Unbedingt erforderlich ist die Entwicklung geeigneter Richtlinien für die jeweiligen OT-Anwendungen und die Festlegung von Richtlinien, die den Anforderungen der OT-Umgebung Ihres Kunden entsprechen. Richtlinien müssen mehrere Lösungen unterschiedlicher Hersteller und unterschiedlicher Stakeholder abdecken (Asset-Eigner, Integratoren, Lieferanten, Wartungspartner usw.).

Unterstützung durch Experten zur Erfüllung der speziellen Anforderungen Ihrer Kunden

Policy Consulting durch erfahrene Berater von Siemens gewährleistet, dass Ihr Kunde die passende Richtlinie für sein Unternehmen und seine OT-Umgebung erhält. Dafür sorgen unsere Erfahrungen aus unterschiedlichen Projekten. Unser Security Consulting nutzt das globale Fachwissen von Siemens, um den Aufwand für unsere Kunden zu begrenzen und die erforderliche Qualität sicherzustellen.

Im Rahmen von Industrial Security Consulting bieten erfahrene Berater Unterstützung im Bereich Sicherheits-Richtlinien, -Beratung und -Engineering für die unterschiedlichen Cybersecurity-Maßnahmen, die Bestandteil eines ganzheitlichen Cybersecurity-Ansatzes sind. Ziel ist es dabei, die Einhaltung der relevanten Normen und Rechtsvorschriften sicherzustellen.

LÖSUNG 1

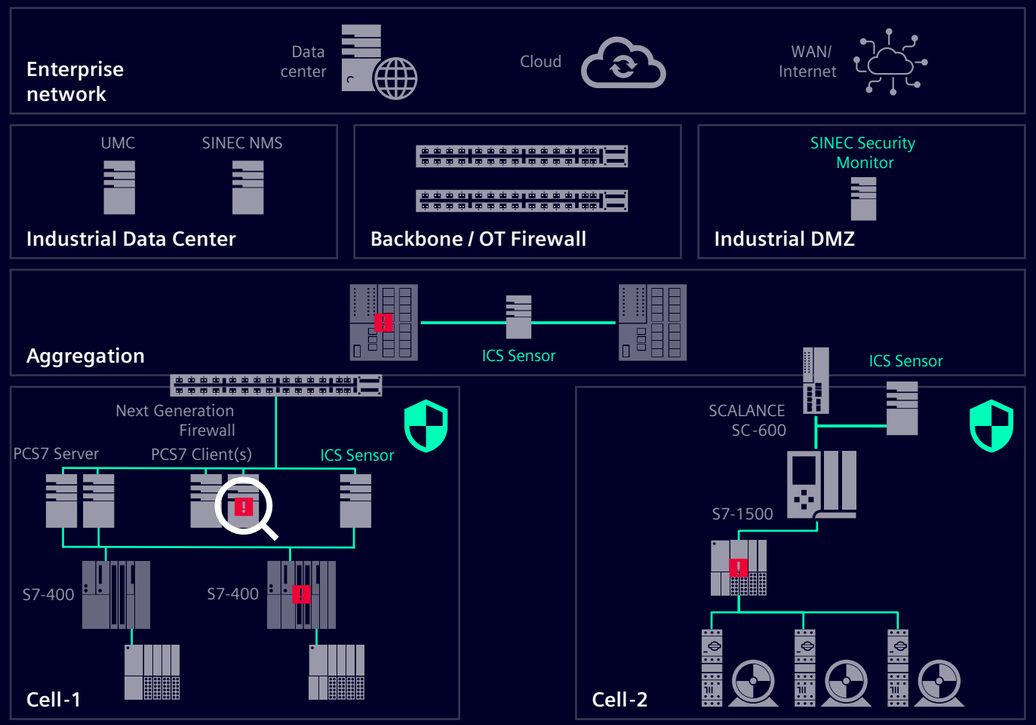
Höhere Sicherheit und Verfügbarkeit durch frühzeitige Erkennung von Bedrohungen

Cyber-Angriffe auf Industrieunternehmen nehmen zu. Doch die mangelnde Transparenz des Sicherheitsstatus industrieller Steuerungssysteme lässt das Cyber-Risiko weiter ansteigen. Werden Cybersecurity-Vorfälle erst spät erkannt, sind Anlagenstillstände und zusätzliche Wiederherstellungskosten die Folge. Regulierte Industrien sind zudem verpflichtet, Sicherheitsvorfälle zu melden.

Anomaly Detection ermöglicht dem Betreiber schnelleres Eingreifen

SINEC Security Monitor überwacht den Datenverkehr im Netzwerk, erstellt eine Baseline, die den Normalbetrieb abbildet, und erkennt Abweichungen mit integrierten KI-Mechanismen. Dies ermöglicht es dem Betreiber, schnell zu reagieren und frühzeitig gegen Bedrohungen anzugehen. Die Software analysiert automatisch den Netzwerkverkehr und gleicht den aktuellen Datenverkehr mit einer Baseline bzw. Bedrohungsdatenbank ab. Auf diese Weise lassen sich Anomalien, z. B. Hacker-Angriffe, Datendiebstahl usw., erkennen.

Die Überwachungslösung kann zu 100 Prozent passiv konfiguriert und nahtlos in industrielle Netzwerke und Steuerungssysteme integriert werden. Lokale Sensoren erfassen die Daten in den verschiedenen Netzwerken durch Spiegelung des Netzwerkverkehrs. Die Daten werden vorverarbeitet und anschließend an die zentrale Instanz in der Industrial DMZ weitergeleitet. SINEC Security Monitor verbessert mithilfe eines Agenten für Windows-basierte Endpoints die Datenqualität.



LÖSUNG 2

Erfassen und Teilen sicherheitsrelevanter Ereignisdaten von OT-Geräten

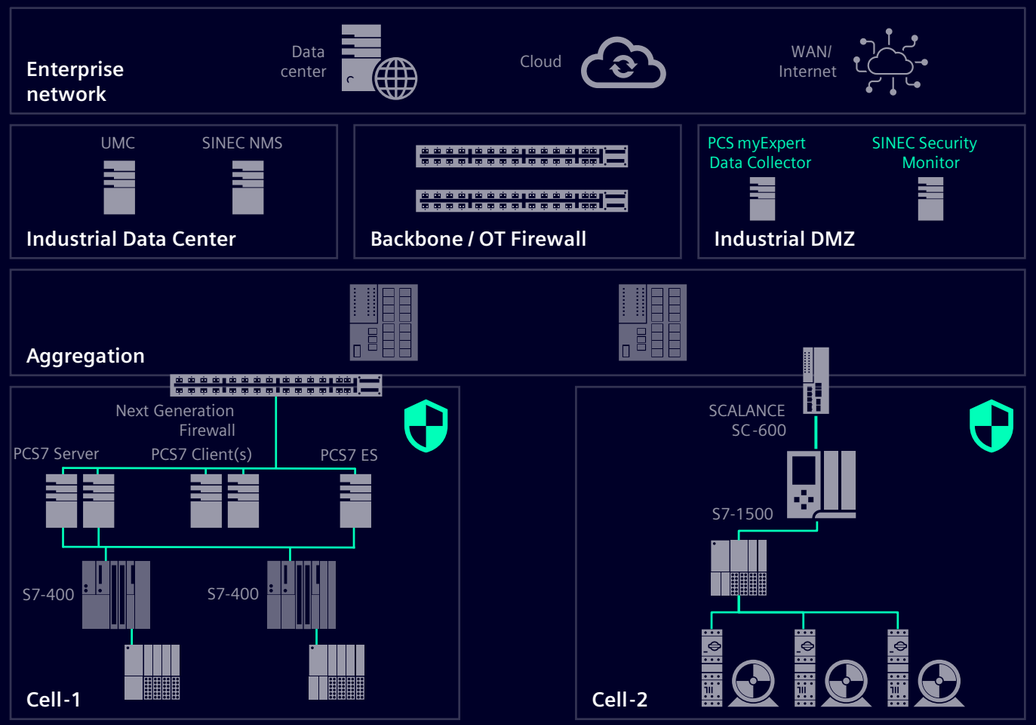
Wachsende regulatorische Anforderungen oder die Erfüllung internationaler Standards wie z. B. IEC 62443-3-3, machen die Erfassung und Analyse sicherheitsrelevanter Ereignisdaten erforderlich. Die Kundenanforderungen an die IT-OT-Integration erfordern keine spezielle Lösung, sondern die Integration von OT-Sicherheitsereignissen in die vorhandene Überwachungslösung.

OT-Systeme ohne direkte Anbindung an übergeordnete Netzwerke müssen dem Top-Level-SIEM (Security Information and Event Management) Sicherheitsereignisdaten zur weiteren Untersuchung übermitteln. Das gilt auch für Systeme, die kein Systemprotokoll (syslog) erstellen können. IT-Abteilungen sind mit dem Abrufen von Sicherheitsereignissen aus OT-Systemen häufig nicht im Detail vertraut.

Integration von OT-Systemen in ein vorhandenes IT-SIEM

SIMATIC PCS myExpert ist eine webbasierte Anwendung, die Sicherheitsereignisse, z. B. in einer SIMATIC PCS 7-Umgebung, überwacht und an ein vorhandenes IT-SIEM-System auf höchster Ebene weiterleitet. Sicherheitsereignisse werden an einen zentralen Anlagen-Collector in der OT-DMZ übertragen.

SINEC Security Monitor ist eine lokal installierte Softwarelösung, die Sicherheitsereignisse im Netzwerk überwacht, diese in der SINEC Security Monitor-Serverinstanz visualisiert und Sicherheitsereignisse an ein bestehendes IT/OT-SIEM-System weiterleiten kann.



LÖSUNG 3

Schnelle Reaktion auf Sicherheitsvorfälle durch Vorfallanalyse im Rahmen von Industrial Security Consulting

Bei einem Sicherheitsvorfall ist eine schnelle und fachkundige Untersuchung von entscheidender Bedeutung.

Oftmals fehlen Unternehmen jedoch die internen Kapazitäten und das Fachwissen, um effektiv zu reagieren. Dadurch bleiben wichtige Fragen häufig unbeantwortet: Was ist passiert? Warum ist es passiert? Welche Maßnahmen verhindern eine Wiederholung?

Um diese Herausforderungen zu meistern, ist spezialisiertes Fachwissen und die Fähigkeit, schnell zu reagieren, erforderlich.

Schnelle und fachkundige Untersuchung bei Vorfällen

Mit unserer Incident Analysis bieten wir Ihnen sofortige fachkundige Unterstützung bei der Untersuchung von Vorfällen und liefern Ihnen klare Ergebnisse.

Was wir bieten:

- Standardisierte Erfassung von Vorfällen und Koordination der Protokollsammlung
- Ursachenanalyse durch einen Cybersicherheitsexperten von Siemens
- Einen umfassenden Bericht mit Ergebnissen, Zeitachse und Empfehlungen zur Risikominderung.

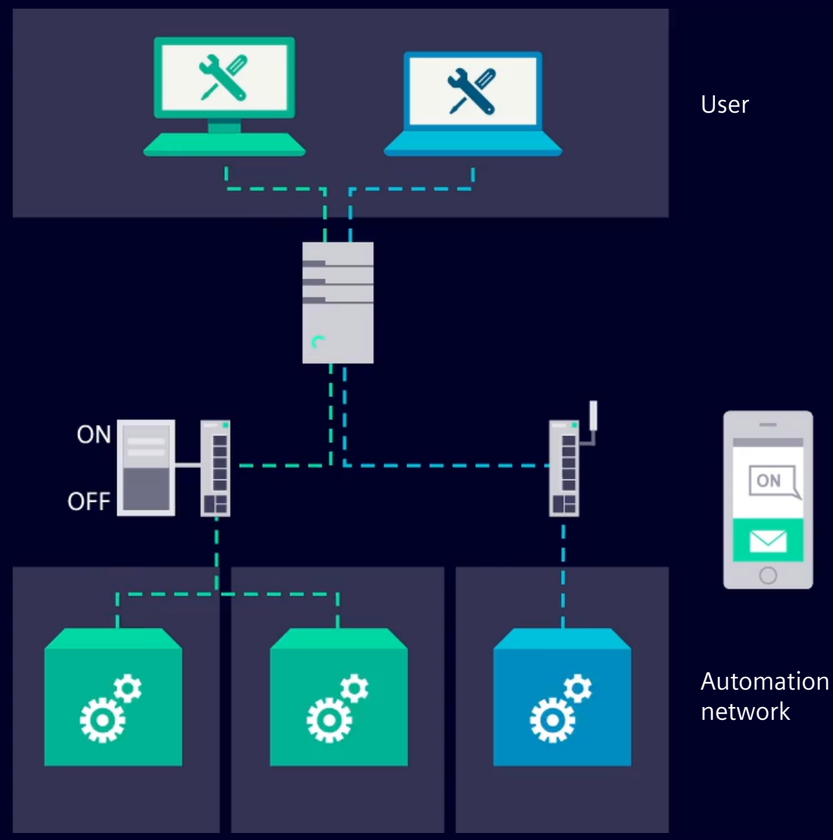
LÖSUNG 1

Geschäftskontinuität durch Backup-Management und sicheren Fernzugriff für die Wiederherstellung

Industrieanlagen sind oft verteilt, teils über Landesgrenzen hinweg. Während der Betriebs- und Optimierungsphase müssen die Wartung und die Wiederherstellung nach Störfällen in verteilten Industrieanlagen und Maschinen im laufenden Betrieb ohne Verzögerung erfolgen, um Betriebs- und Serviceunterbrechungen zu vermeiden. Disaster-Recovery-Systeme und Fernwartungs-Support begegnen diesen Herausforderungen. Bei Siemens bieten wir Disaster-Recovery-Systeme mit Online-/Offline-Backup-Optionen mit einer Vielzahl von lokalen und Offsite-Backup-Optionen, z. B. SIMATIC DCS SCADA Infrastructure.

So stellen Sie sichere Fernverbindungen her

Der Verbindungsaufbau ist mit unserer VPN-Management-Plattform SINEMA Remote Connect oder der common Remote Service Plattform cRSP sehr einfach. Servicetechniker verwenden einen SINEMA Remote Connect Client oder cRSP. Die Anlage oder Maschine ist mit einer SCALANCE S Industrial Security Appliance, einem SCALANCE M Industrie-Router oder Industrial Next Generation Firewalls ausgestattet.



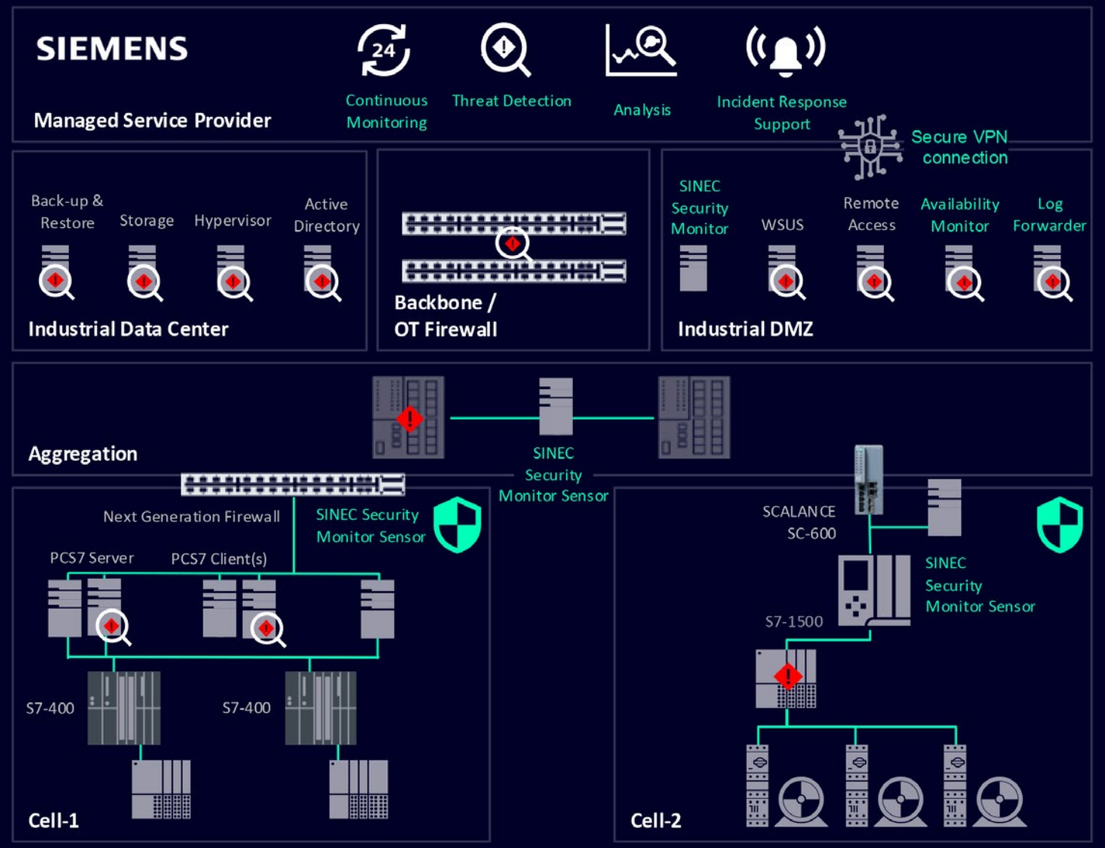
LÖSUNG 2

Setzen Sie für Bedrohungserkennung und Incident Response auf OT SOC as a Service

Das OT Security Operations Center (SOC) as a Service (OT-SOCaaS) bietet eine 24/7-Cybersecurity-Überwachung für industrielle Umgebungen und kritische Infrastrukturen an. Im Gegensatz zu IT-zentrierten SOC-Anbietern kombiniert Siemens kontinuierliche Sicherheitsüberwachung mit fundierter Expertise in der industriellen Automatisierung und der Einhaltung gesetzlicher Vorschriften. Das ist besonders in OT-Umgebungen entscheidend, in denen Cybervorfälle Auswirkungen auf die Sicherheit, Produktionskontinuität und Compliance haben können. Aufbauend auf unserer langjährigen Erfahrung beim Schutz unserer eigenen Werke hilft OT-SOCaaS Unternehmen dabei, widerstandsfähiger gegen fortschrittliche OT-Cyberbedrohungen zu werden und unterstützt gleichzeitig die Einhaltung von Sicherheitsvorschriften.

Stärkung der Cyber-Resilienz in der Industrie mit OT SOC as a Service

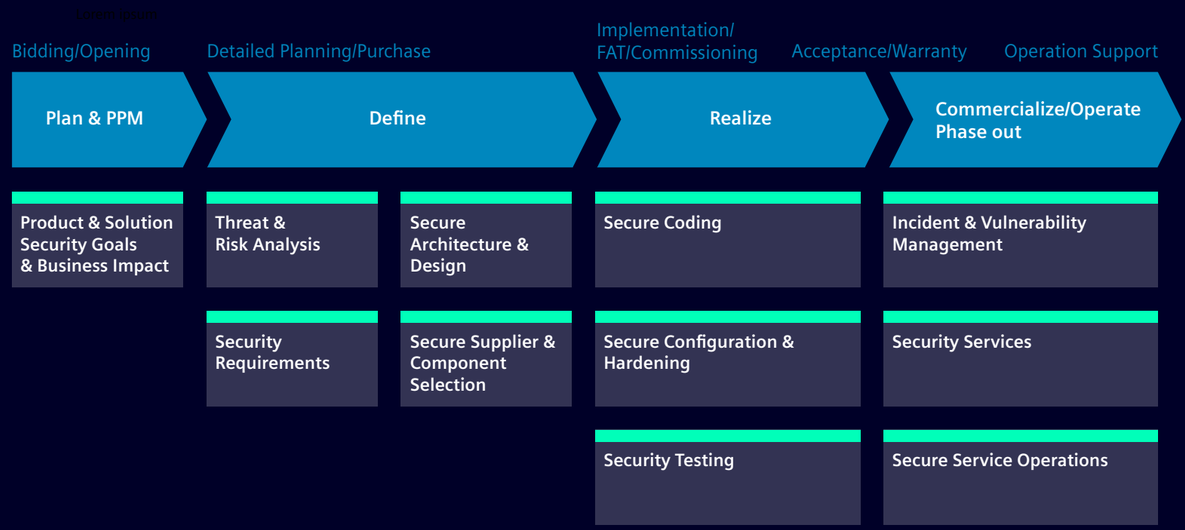
Der Service umfasst eine 24/7-Überwachung, Bedrohungserkennung und -analyse zur Identifikation verdächtiger Aktivitäten sowie Unterstützung bei der Reaktion auf Vorfälle und Wiederherstellung. Unsere Experten erkennen Bedrohungen durch die Triage und Korrelation mehrerer Indikatoren in Ihrer Umgebung. OT-SOCaaS hilft dabei, die Kosten von Sicherheitsvorfällen zu reduzieren – von Ausfallzeiten, Produktionsausfällen und Sanktionen bis hin zu Reputationsschäden.



LÖSUNG 1

Sichere Produkte und Services über den gesamten Lebenszyklus

Für eine robuste Lieferkette sind mehrere Faktoren entscheidend. Neben der Integration cybersicherer Komponenten in Ihre Produkte muss gewährleistet sein, dass alle an dem Prozess beteiligten Anwendungen den Sicherheitsnormen entsprechen, und dass Sie sich im Problemfall auf Ihre Service Provider verlassen können. Da auch die Hersteller Teil der Lieferkette sind, muss mit Maßnahmen, die zur Cyber-Resilienz führen, eine durchgängige Vertrauensbasis geschaffen werden. Die Integration robuster Sicherheitsmaßnahmen für Lieferkette und Produkte über den gesamten Lebenszyklus kann bei der Einhaltung neuer Gesetze und Vorschriften helfen und hohe Standards setzen.



Berücksichtigung des gesamten Produktlebenszyklus

Experten für Automatisierung, Digitalisierung und Cybersecurity identifizieren Schwachstellen und Risiken in Product Lifecycle Management, Projektmanagement und Engineering und entwickeln gemeinsam mit Ihnen eine Sicherheits-Roadmap mit spezifischen Sicherheitsmaßnahmen für die Lieferkette. Im Rahmen unserer Consulting Services für Sicherheit in der Lieferkette greifen die Berater auf unsere eigenen Erfahrungen aus der Produktion zurück und verfolgen einen ganzheitlichen Risikomanagement-Ansatz für Product Lifecycle Management, Projektmanagement und Engineering.

LÖSUNG 2

Schwachstellen laufend ermitteln und bewerten

Die Cybersecurity von Anwendungen erfordert eine strukturierte Software Bill of Materials wie CycloneDX, um Schwachstellen zu identifizieren, die Einhaltung von Lizenzbestimmungen zu gewährleisten und die Software-Lieferkette zu überwachen. Während des gesamten Cybersecurity-Lebenszyklus werden das Risiko und die Anwendbarkeit der identifizierten Schwachstellen überprüft. Dies erfordert jedoch ein Verständnis der Cybersecurity-Risiken und -Auswirkungen während des gesamten Lebenszyklus von Softwareanwendungen.

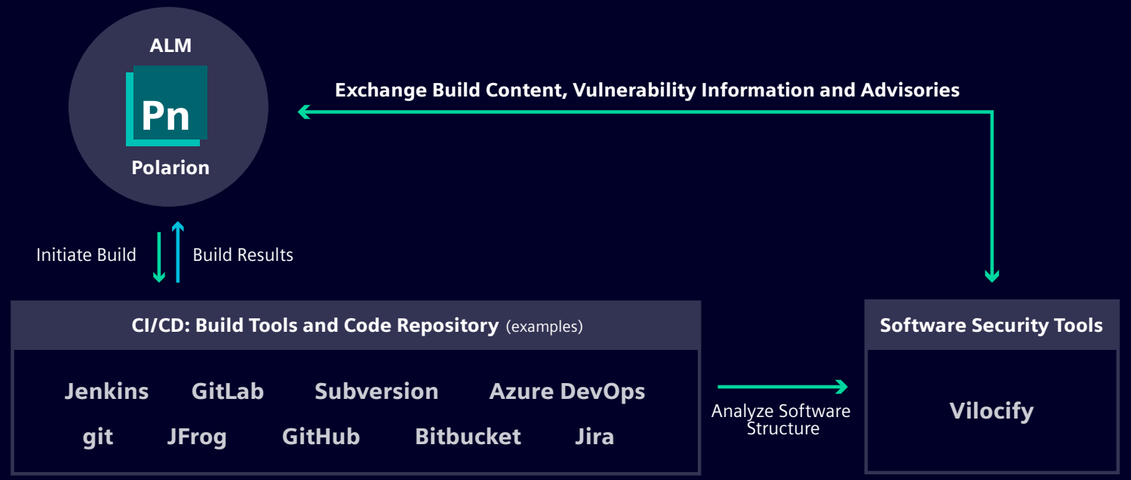
Entwickeln, Steuern und Pflegen einer cybersicheren Anwendung

Unsere umfassende Lösung gewährleistet eine vollständige Rückverfolgbarkeit des Produkts nach Industrieanforderungen mit Bedrohungs- und Risikoanalyse und Dokumentation von Sanierungsmaßnahmen und Produktänderungen.

Polarion orchestriert das Software-Cybersecurity-Ökosystem, das Build-Tools (CI/CD), Code-Repositories und Testumgebungen miteinander verknüpft.

Software-Sicherheits-Tools wie Vilocify Vulnerability Services identifizieren und bewerten kontinuierlich Schwachstellen und überwachen die Software-Lieferkette.

Die Integration von Polarion in diesen Prozess ermöglicht ein automatisiertes Schwachstellenmanagement und Compliance-Tests von Softwarekomponenten.



LÖSUNG 1

Umgang mit Schwachstellen und Patches zur Erhöhung der Sicherheit und Verfügbarkeit

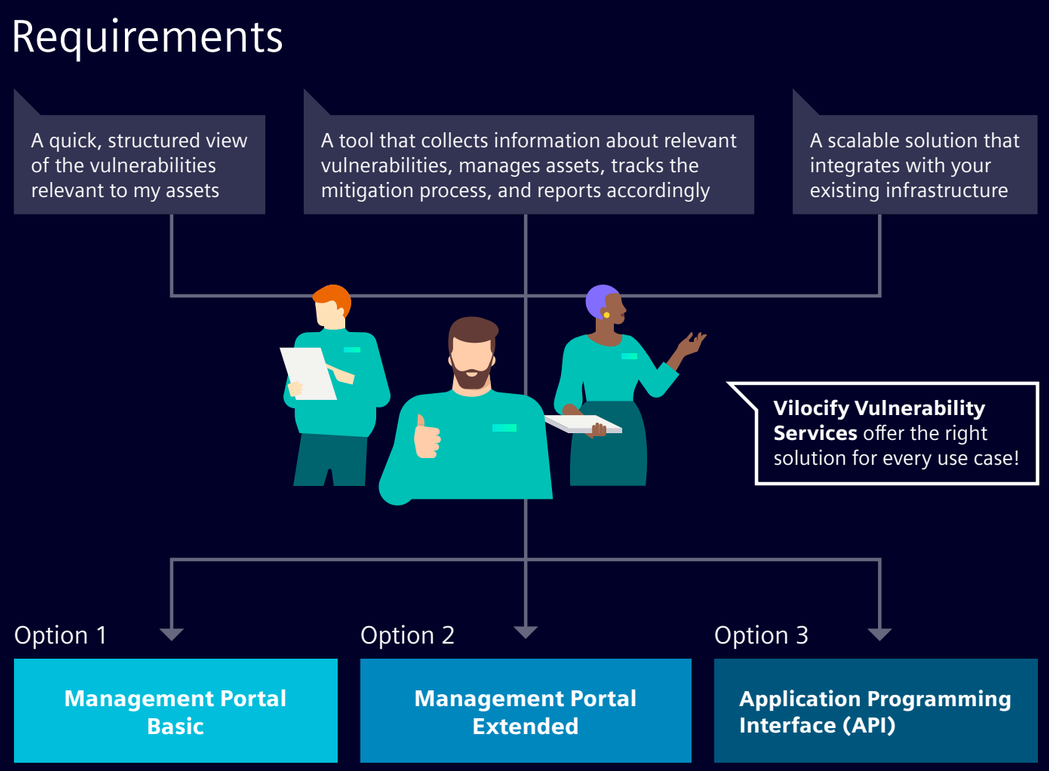
Während der Betriebs- und Optimierungsphase müssen die Systeme regelmäßig aktualisiert werden. Für viele Systeme werden täglich neue Schwachstellen gemeldet, die Angreifer ausnutzen können. Darum müssen neue Schwachstellen so schnell wie möglich identifiziert und die Zeit bis zum Patch minimiert werden. Eine der Verpflichtungen des NIS2-Cyber-Risikomanagements (CRM) sind der Umgang mit und die Offenlegung von Schwachstellen.

Sichern Sie Ihre Infrastruktur und Ihr Produktportfolio

Mit Vilocify Vulnerability Services sichern Sie Ihre Infrastruktur und Ihr Portfolio durch relevante, umsetzbare Schwachstelleninformationen. Diese erhalten Sie über:

- Management-Portal: Webbasierte Anwendung, die einen strukturierten Überblick über relevante Schwachstellen für Ihre Komponenten bietet
- Anwendungsprogrammierschnittstelle (API): Nahtlose Schnittstelle zur Integration der Schwachstellen-Informationen in Ihre Tools und Prozesse

Nutzen Sie SINEC Security Guard als cloudbasierte Software-as-a-Service-Lösung (SaaS), um Sicherheitslücken automatisch zu erfassen und das Sicherheitsmanagement für Nicht-Sicherheitsexperten im Bereich OT zu übernehmen. Patch Management unterstützt Sie bei der Verwaltung wichtiger Microsoft-Produkt-Updates.



LÖSUNG 2

Mehr Sicherheit und Transparenz durch Management von OT-Anlagen

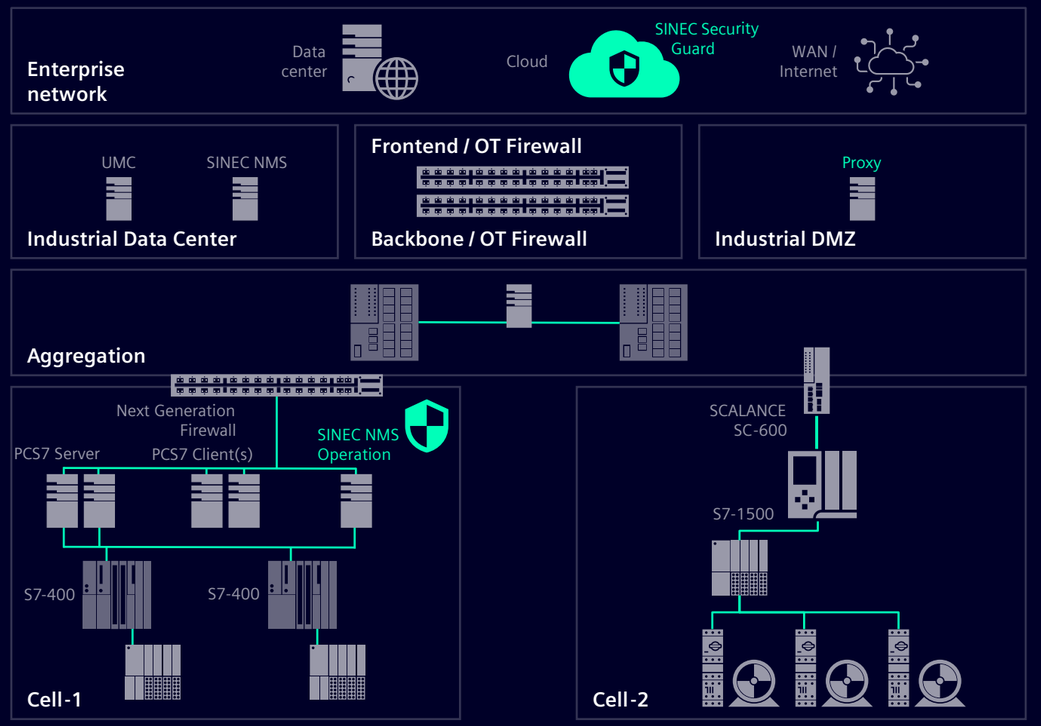
In der Betriebsphase müssen die Industrieunternehmen den reibungslosen und sicheren Betrieb der OT-Anlagen in den Werkshallen gewährleisten. Sie müssen neue Schwachstellen, die laufend gemeldet werden, überwachen, um mit geeigneten Abhilfemaßnahmen reagieren zu können. Darüber hinaus müssen die Anlagenbetreiber die staatlichen Vorschriften (z. B. NIS2, NERC-CIP) einhalten.

Einfacher Abgleich, Bewertung und Schadensbegrenzung mit SINEC Security Guard

Die Identifizierung und das Management von Schwachstellen können zeitaufwändig sein und erfordern spezielle Fachkenntnisse in den Bereichen Cybersicherheit und Automatisierung. Standard-Risiko-Levels sind jedoch nicht die beste Lösung für die Betriebsumgebung einer Anlage. Aus diesem Grund nutzt SINEC Security Guard bestehende digitale Anlageninventare (z. B. SINEC NMS, Industrial Asset Hub) und ordnet diese den Schwachstellen zu:

- Abgleich der Sicherheitshinweise des Herstellers mit dem Anlageninventar
- Bewertung des Risikos von Schwachstellen im Kontext der Betriebsumgebung der Anlage, Priorisierung von Abhilfemaßnahmen auf Basis ihrer Kritikalität
- Abhilfemaßnahmen können über das integrierte Aufgabenmanagement definiert und geplant werden

IT-spezifische Anwendungen von Drittanbietern können über eine öffentliche API angebunden werden (für Anwendungen wie Anlageninventar und Workflow-Anwendungen).



LÖSUNG

Unterstützung für Vorstand und CEO bei der Umsetzung der NIS2-Richtlinie

Führungsteam und Mitarbeiter müssen sich das Wissen und die Kompetenzen aneignen, um Risiken erkennen und die Maßnahmen zum Risikomanagement im Bereich Cybersecurity sowie deren Auswirkungen auf die vom Unternehmen erbrachten Services bewerten zu können. Vorstand und CEO müssen zudem beurteilen, ob und wie Informationen über einen Cyber-Angriff intern sowie extern an Kunden und Investoren weitergegeben werden sollten. Es ist jedoch nicht leicht, einen Trainingsanbieter zu finden, der über entsprechendes Wissen zu Prozessen, Abläufen und Cybersecurity-Lösungen in IT und OT verfügt. Es ist wichtig, ein modulares Schulungsangebot zu finden, dass die Anforderungen Ihres Unternehmens erfüllt, und mit einem Schulungsanbieter zusammenzuarbeiten, der Sie auf dem langen Weg der Umsetzung von NIS2 begleitet.

Aufbau von Cyber-Resilienz im Unternehmen

Schulungen zur Cybersecurity mit erfahrenen Beratern von Siemens vermitteln Ihnen die richtigen Schulungsinhalte, die sorgfältig auf die Anforderungen Ihres Unternehmens und die IT- und OT-Umgebung abgestimmt werden. Das gewährleisten unsere Erfahrungen aus verschiedenen Projekten. Mit unserem Schritt-für-Schritt-Ansatz begleiten wir Unternehmen von der ersten NIS2-Sensibilisierungsschulung bis zur Erreichung der NIS2-Compliance. Unsere erfahrenen Schulungsleiter sind gerne bereit, auf Ihre individuellen Anforderungen einzugehen.

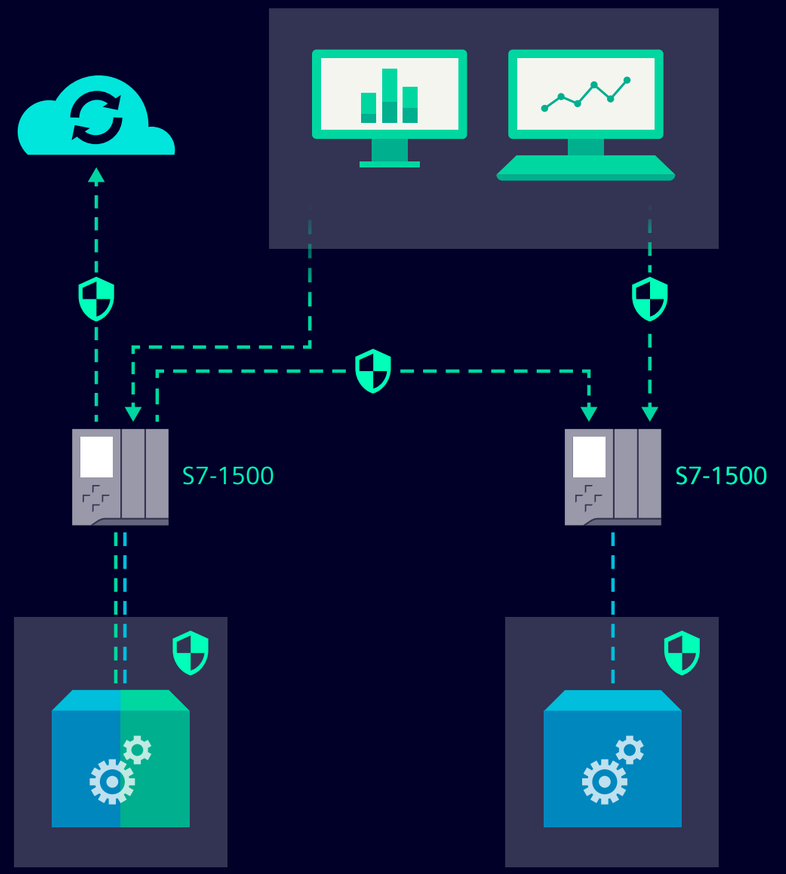
LÖSUNG

Minderung von Cyber-Risiken durch verschlüsselte Kommunikation für OT

Da die Fertigung immer dynamischer wird, wird der Datenzugriff während des gesamten Produktlebenszyklus immer wichtiger. Geräte, Systeme und Benutzer tauschen fortlaufend oder bei Bedarf Daten aus, ohne dass eine angemessene Datenzugriffsverwaltung oder Identifizierungsmechanismen vorhanden sind. Ohne diese Mechanismen kann jeder eine Verbindung zum Netzwerk herstellen, was das System anfällig für Man-in-the-Middle-Angriffe macht. Da die Daten im Klartext vorliegen, sind sie anfällig für Diebstahl, Manipulation, Spionage und Sabotage. Eine der Verpflichtungen im Rahmen des NIS2-Cybersicherheits-Risikomanagements (CRM) ist der Einsatz von Kryptographie und gegebenenfalls Verschlüsselung.

Faktoren für sichere Kommunikation und Systemintegrität

Stellen Sie die Systemintegrität durch Authentifizierung und Verschlüsselung sicher, z. B. mit einer Ende-zu-Ende-Verschlüsselung zwischen TIA Portal, S7-1500/1200 Steuerungen und HMI-Stationen dank modernster gesicherter Kommunikation auf Basis von Transport Layer Security (TLS) V1.3.



LÖSUNG 1

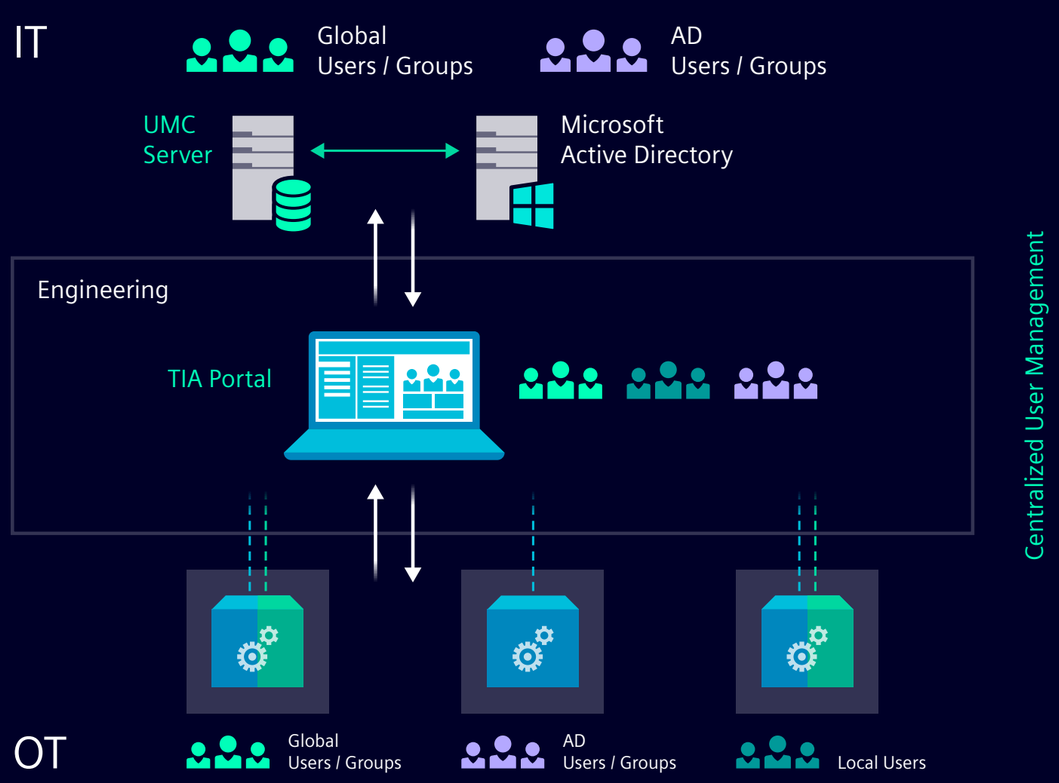
Einfache und zentrale Verwaltung von Benutzern, Rollen und Zugriffsrechten

Um den unbefugten Zugriff auf Benutzerprogramme, das Automatisierungssystem und Daten während der Projektierungs- und Wartungsphase zu verhindern, ist eine granulare Konfiguration der Benutzerrechte und der Zugriffsverwaltung erforderlich. Häufig ist die Benutzerverwaltung während der Entwicklung und insbesondere während des Betriebs nicht zentralisiert.

Engineering-Projekte erfordern eine Benutzerverwaltung und Zugriffskontrolle, um unbefugte Zugriffe zu verhindern, was zu einem erhöhten Aufwand führt. Die individuellen Zugriffsrechte für jeden Benutzer sollten sich an seiner Rolle orientieren. Daraus resultiert ein noch höherer Aufwand, um jedes Projekt konsistent zu halten und die Projekte entsprechend den Benutzeränderungen zu aktualisieren.

Effiziente Benutzerverwaltung auf OT-Ebene

Die Umsetzung einer zentralisierten Benutzerverwaltung erfordert nur wenige Schritte. Importieren Sie Benutzer und Gruppen aus Microsoft Active Directory auf den UMC Server und verbinden Sie die TIA Portal Engineering Station mit dem UMC-Server. Importieren Sie Benutzer und Gruppen vom UMC-Server in TIA Portal und weisen Sie dann lokal Rechte und Rollen zu.



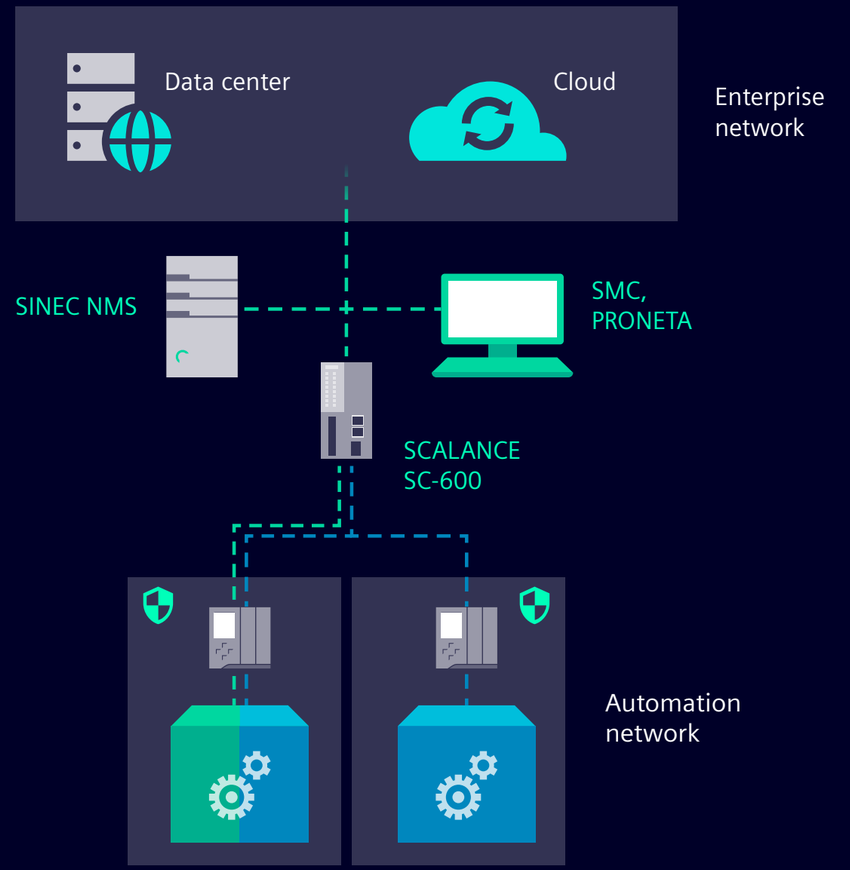
LÖSUNG 2

Verbessern Sie die Sicherheit durch Erkennung und Verwaltung von Assets

Unternehmen, die eine Vielzahl von physischen und virtuellen Assets verwalten, benötigen eine Asset-Erkennung, um genaue Bestandsaufzeichnungen zu führen, Wartungspläne zu optimieren (z. B. zur Behebung von Schwachstellen), die Einhaltung von Vorschriften sicherzustellen und den Verlust oder Diebstahl von Assets zu verhindern. Eine kontinuierliche und genaue Bestandsaufnahme ist die Grundlage für alle weiteren Sicherheitsmaßnahmen! Um einen umfassenden Überblick über das Anlageninventar zu erhalten, wird der Einsatz verschiedener Tools empfohlen. Eine der Maßnahmen des NIS2-Cybersecurity-Risk-Managements (CRM) ist die Umsetzung eines Asset Managements.

Verschaffen Sie sich einen umfassenden Überblick über alle Ihre Assets

Unsere Lösung nutzt das zentralisierte SINEC NMS (Network Management System), SMC (SIMATIC Management Console) und PRONETA, um Netzwerküberwachung, Topologieerkennung, Diagnose und Firmware-Management zu ermöglichen. Darüber hinaus bietet SINEC Security Inspector leistungsstarke, nicht-intrusive, herstellerunabhängige Scans zur Erstellung einer einfach zu verwaltenden Installationsübersicht.



LÖSUNG 3

Überblick über alle Netzwerk-Assets in Ihren Anlagen

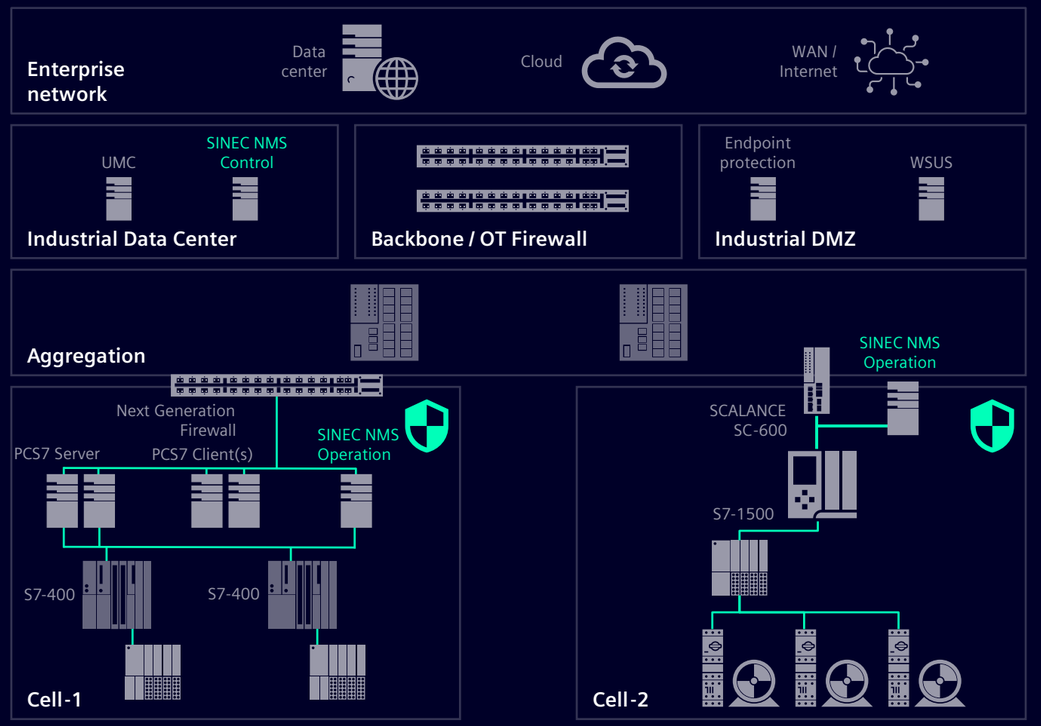
Ein ganzheitlicher Cybersecurity-Ansatz setzt die Fähigkeit voraus, alle – auch kritische – OT-Assets zu erkennen, zu überwachen, zu bedienen und zu verwalten. Ein jederzeit detaillierter Überblick über die OT-Assets ist nötig, um sie effektiv verwalten und ihre Angriffsfläche reduzieren zu können.

Eine besondere Herausforderung ist, dass Anlagen eine Vielzahl an Netzwerk-Assets unterschiedlicher Hersteller sowie auch Alt-Assets enthalten. Modernisierungen der Ausrüstung und die neuesten Firmware-Updates sind in der Liste der Netzwerk-Assets nicht enthalten. Netzwerk-Assets mit veralteter Firmware stellen ein besonderes Cybersecurity-Risiko dar.

Unterstützung bei der Erkennung Ihrer Netzwerk-Assets

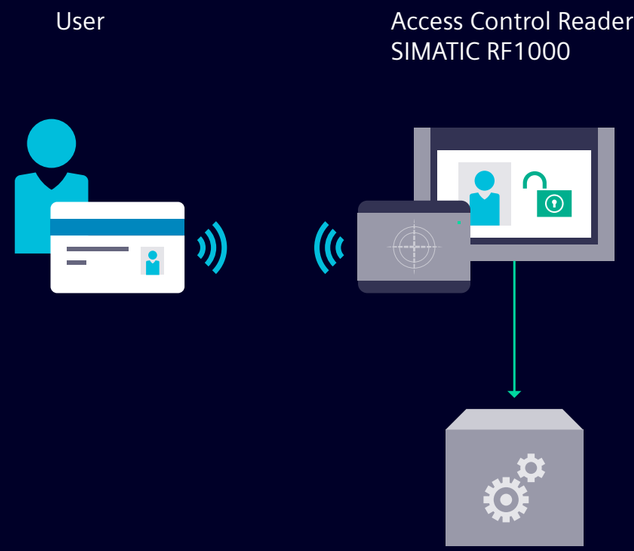
Unsere Lösung unterstützt Kunden nahtlos und umfassend bei der Erkennung und Verwaltung von Netzwerk-Assets:

- Bestand und Transparenz: Verfolgen Sie Ihren Bestand an Geräten, Ausrüstung und Software im Anlagennetzwerk.
- SINEC NMS erkennt automatisch Ihre Netzwerk-Assets und verwaltet sie in einer jederzeit vollständigen, aktuellen Bestandsliste oder Netzwerktopologie-Ansicht.
- Zusätzlich können verschiedene Netzwerkbereiche überwacht werden. Das gilt auch für Automatisierungsprodukte wie PCS 7/neo, SPS, PROFINET-IO und Drittanbieter-Assets.



LÖSUNG

Prüfung und Verifizierung einer Benutzer-ID gegenüber einem System



Anwendungen sind wichtige Unterelemente einer Produktion oder eines Prozesses, die nur für autorisierte Personen zugänglich sein sollten. Stellen Sie sicher, dass zu jeder Zeit nur autorisierte und geschulte Personen Zugang haben, da der unbefugte Zugriff auf Maschinen zu Stillstandszeiten führen kann.

Brownfield-Umgebungen stellen häufig ein Hindernis dar, und die Stakeholder schenken der Authentifizierung nicht genügend Aufmerksamkeit. Es ist nicht ausreichend transparent, wo eine Multi-Faktor-Authentifizierung in der Produktion sinnvoll ist. Zudem verfügen Unternehmen vielfach weder über Prozesse, die eine Multi-Faktor-Authentifizierung ermöglichen, noch kennen sie die verfügbaren Lösungen. Außerdem ist für den Betrieb der Maschine lokaler und Fernzugriff auf das HMI erforderlich.

Zugangskontrolle schützt die Systemintegrität

Die Lösung besteht in der expliziten Identifizierung der Bediener von Maschinen und Anlagen einschließlich Zugangskontrolle und Audit-Trail.

Die SIMATIC RF1000R Access Control Reader unterstützen die Anmeldung mit einmalig und wiederholt nutzbaren RFID-Karten sowie die Anmeldung via RFID-Karte mit Anmeldedaten:

- Einmaliges Lesen der ID-Karte
- Wiederholtes Lesen der ID-Karte
- Einmaliges Lesen der ID-Karte mit zusätzlicher Authentifizierung über ein benutzerspezifisches Passwort

LÖSUNG

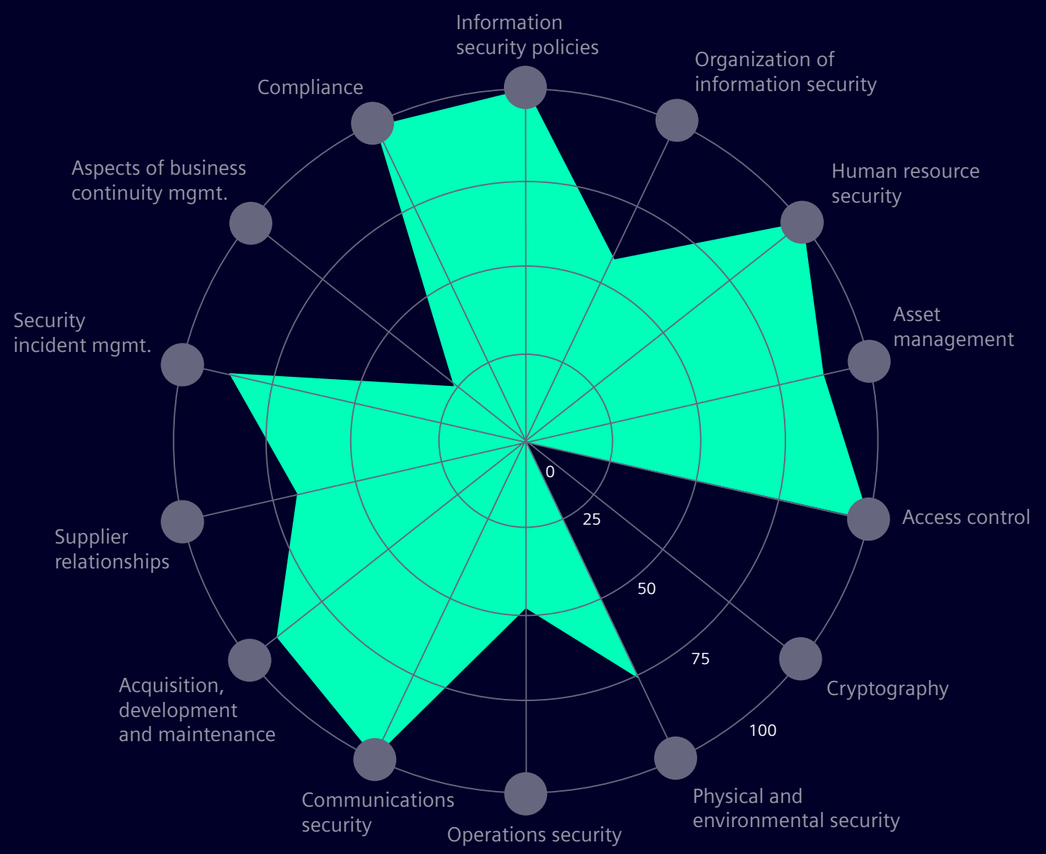
Erhalten Sie Transparenz und entwickeln Sie eine Sicherheits-Roadmap

Die Umsetzung wirksamer Sicherheitsmaßnahmen ist von entscheidender Bedeutung. Industrieunternehmen stehen zunehmend unter Druck, nationale Gesetze und Vorschriften wie NIS2 und NIST sowie Normen wie IEC 62443 und ISO 27001 umzusetzen. Aufgrund des Mangels an Kompetenz und Fachwissen im Bereich industrieller Cybersecurity ist die IT jedoch auf die Unterstützung von Sicherheitsexperten mit Automatisierungs-Fachwissen angewiesen. Neue Compliance-Anforderungen und Gesetze erhöhen den Zeitdruck. Hinzu kommt, dass die Durchführung umfassender Assessments und die Entwicklung individueller Sicherheitspläne keine einfache Aufgabe ist und häufig fundierte Kenntnisse der OT und IT erfordert.

Nutzung des Fachwissens von Cybersecurity- und Industrie-Experten

Security Assessments enthalten eine ganzheitliche Analyse möglicher Bedrohungen und Schwachstellen, die Identifizierung von Risiken und Empfehlungen zur Schließung identifizierter Sicherheitslücken. Sie maximieren die Transparenz und bieten einen vollständigen Überblick über den aktuellen Sicherheitsstatus Ihrer Automatisierungsanlagen. Sie haben die Wahl zwischen einem kompakten, eintägigen Assessment vor Ort (Industrial Security Check) und einer gründlichen Bewertung der Einhaltung von IEC 62443 (IEC 62443-3-3/NIS2 und IEC 62443-2-1 Assessment).

Industrial Security Consulting bietet Vor-Ort-Support durch erfahrene Berater zu Sicherheitsrichtlinien und zum anlagenspezifischen Netzwerkdesign. Hinzu kommt maßgeschneiderte Implementierungs-Unterstützung für das Industrial-Security-Portfolio.



Kontakt

Herausgeber

Siemens AG
Digital Industries
Postfach 4848
90026 Nürnberg
Deutschland