

SIEMENS

Support and solutions for the **NIS 2 Directive**

siemens.com/nis2-directive



POLICIES ON RISK ANALYSIS

INCIDENT HANDLING

BUSINESS CONTINUITY

SUPPLY CHAIN SECURITY

NETWORK AND INFORMATION SYSTEMS / VULNERABILITY HANDLING

CYBERSECURITY TRAINING

CRYPTOGRAPHY AND ENCRYPTION

ACCESS CONTROL POLICIES / ASSET MANAGEMENT

MULTI-FACTOR AUTHENTICATION

POLICIES AND PROCEDURES



Solutions to meet the requirements of NIS 2

Get ready for NIS 2! Here, you'll find a brief overview of our consulting, hardware, and software offerings. Additionally, we provide in-depth information on cybersecurity that aims to protect network and information systems and their physical environment from incidents. In addition to this selection, you will find other useful solutions in our portfolio.

➔ **Further information on NIS 2, including Article 20, Governance and Article 21 Cybersecurity risk-management measures**



POLICIES ON RISK ANALYSIS

INCIDENT HANDLING

BUSINESS CONTINUITY

SUPPLY CHAIN SECURITY

NETWORK AND INFORMATION SYSTEMS / VULNERABILITY HANDLING

CYBERSECURITY TRAINING

CRYPTOGRAPHY AND ENCRYPTION

ACCESS CONTROL POLICIES / ASSET MANAGEMENT

MULTI-FACTOR AUTHENTICATION

POLICIES AND PROCEDURES



SOLUTION

Develop the right security policies for your customers

In addition to technical measures, policies and procedures are mandatory as part of a security concept. Policies are equally important to meet the requirements of cybersecurity standards and regulations. You need to ensure that you develop the right policies for specific OT applications and define a set of policies that meet your customer's needs for their OT environment. Policies need to cover multiple solutions from multiple vendors and multiple stakeholders (asset owners, integrators, suppliers, maintenance partners, etc.).

Expert support to meet the specific needs of your customers

[Policy Consulting](#), performed by experienced Siemens consultants, ensures that the customer gets the right policy that fits their organization and OT environment, based on our experience in various projects. The Security Consulting is based on Siemens' global experience to limit the effort for our customers and to get the required quality.

[Industrial Security Consulting](#) provides support from experienced consultants on security policies, consulting and engineering for the various cybersecurity measures that are part of a holistic cybersecurity approach to meet the requirements of cybersecurity standards and legislation.



SOLUTION 1

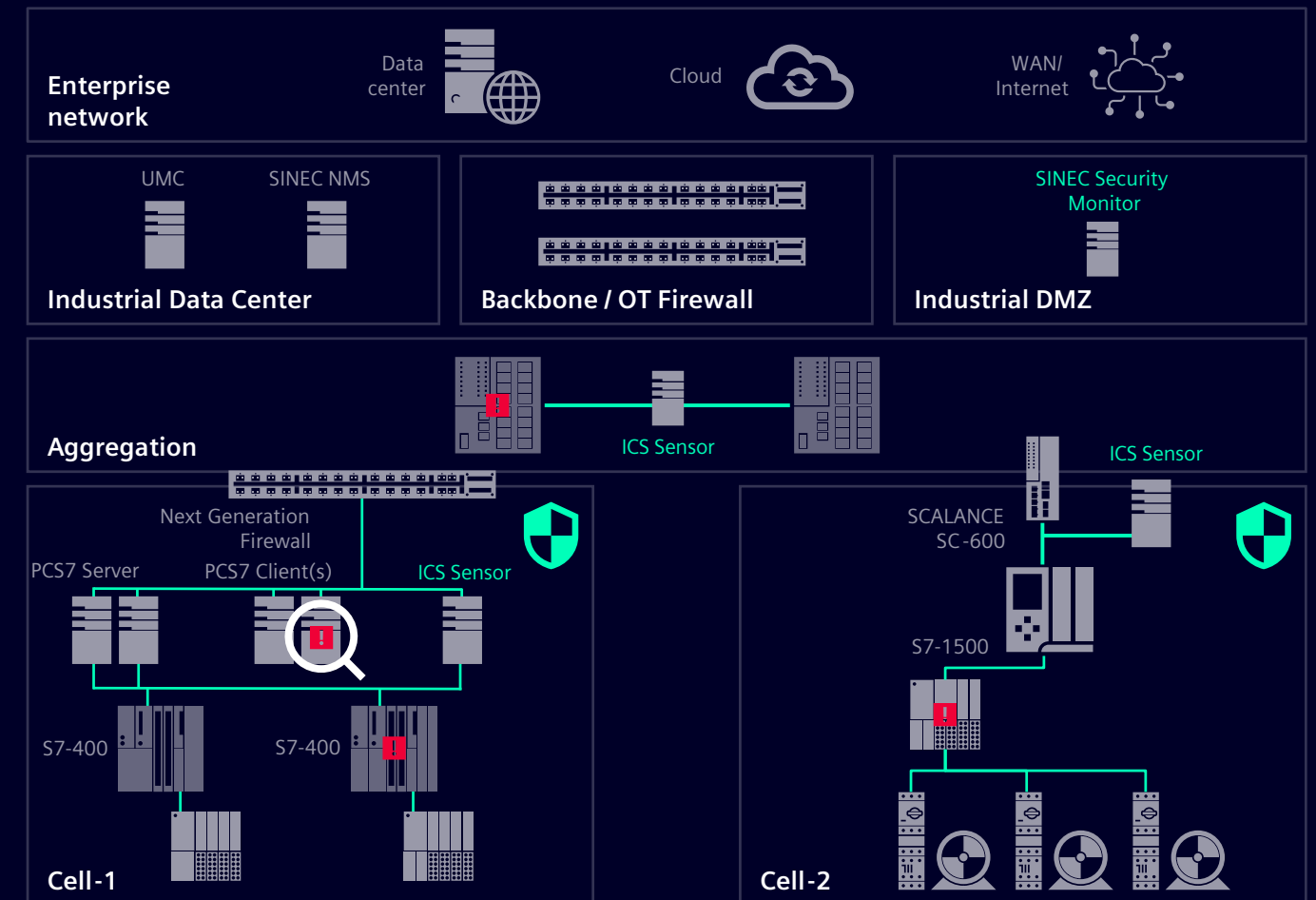
Detect threats at an early stage to increase security and availability

Cyber-attacks on industrial enterprises are on the rise. However, the lack of visibility into the security status of industrial control systems leads to increased cyber risk. Late detection of industrial cyber-security incidents results in plant downtime and additional recovery costs. In addition, regulated industries are required to report security incidents.

Anomaly detection helps operators to act earlier

[SINEC Security Monitor](#) monitors network traffic, creates a baseline of normal operations, and detects anomalies from that baseline. This enables operators to react quickly and address threats at an early stage. The software automatically analyzes network traffic and correlates current traffic against a baseline or threat database to detect anomalies, such as hacker intrusion, data theft, etc.

The monitoring solution can be configured as 100% passive and integrates seamlessly into industrial networks and control systems. Local sensors collect the data in the different networks by mirroring the network traffic, pre-processing it and forwarding it to the central instance in the industrial DMZ. SINEC Security Monitor enhances the data quality with an agent for Windows-based endpoints.



SOLUTION 2

Collect and share security-relevant event data from OT devices

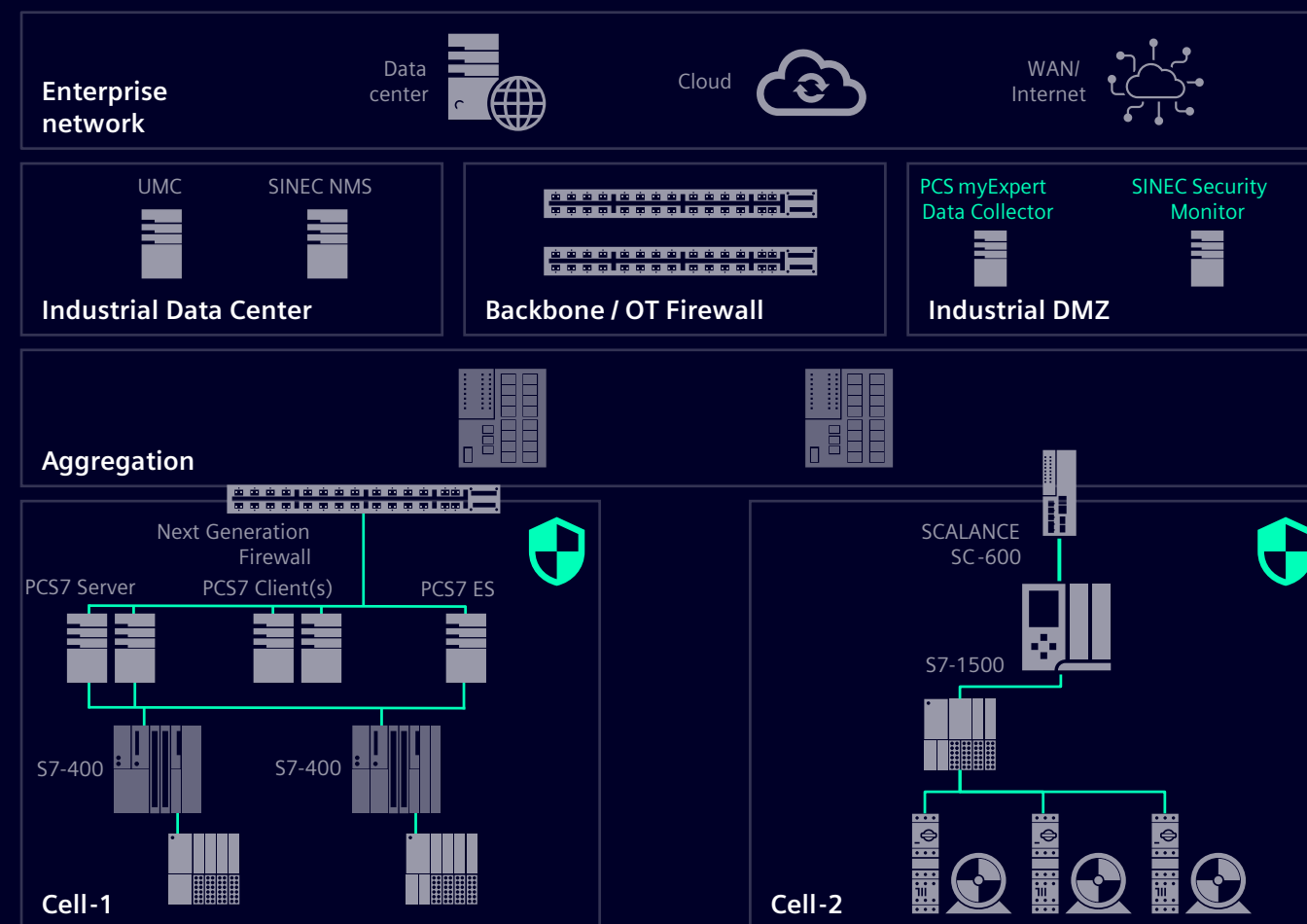
Due to increasing regulatory requirements or to comply to international standards like IEC 62443-3-3 security-related event data must be collected and analyzed. Customer requirements for IT-OT integration do not require a dedicated solution, but rather the integration of OT safety events into the existing monitoring solution.

OT systems without direct connection to higher-level networks are required to provide security event data to the top-level security information and event management (SIEM) for further investigation. Even systems that are not capable of syslog must provide security event data to the top-level SIEM. Often, IT departments lack knowledge about the details of extracting security events from OT systems.

Integrate OT systems into an existing IT SIEM

[SIMATIC PCS myExpert](#) is a web-based application that monitors security events in a e.g. SIMATIC PCS 7 environment and forwards them to an existing IT top-level SIEM system. Security events are transferred to a central plant collector in the OT DMZ.

[SINEC Security Guard](#) is a SaaS, that monitors security events in the network, visualizes them in the cloud and can forward security events to an existing IT/OT SIEM system. This approach collects all OT security events in one place, normalizes and sends consolidated data to the top-level SIEM, and meets all known regulatory and standards requirements.



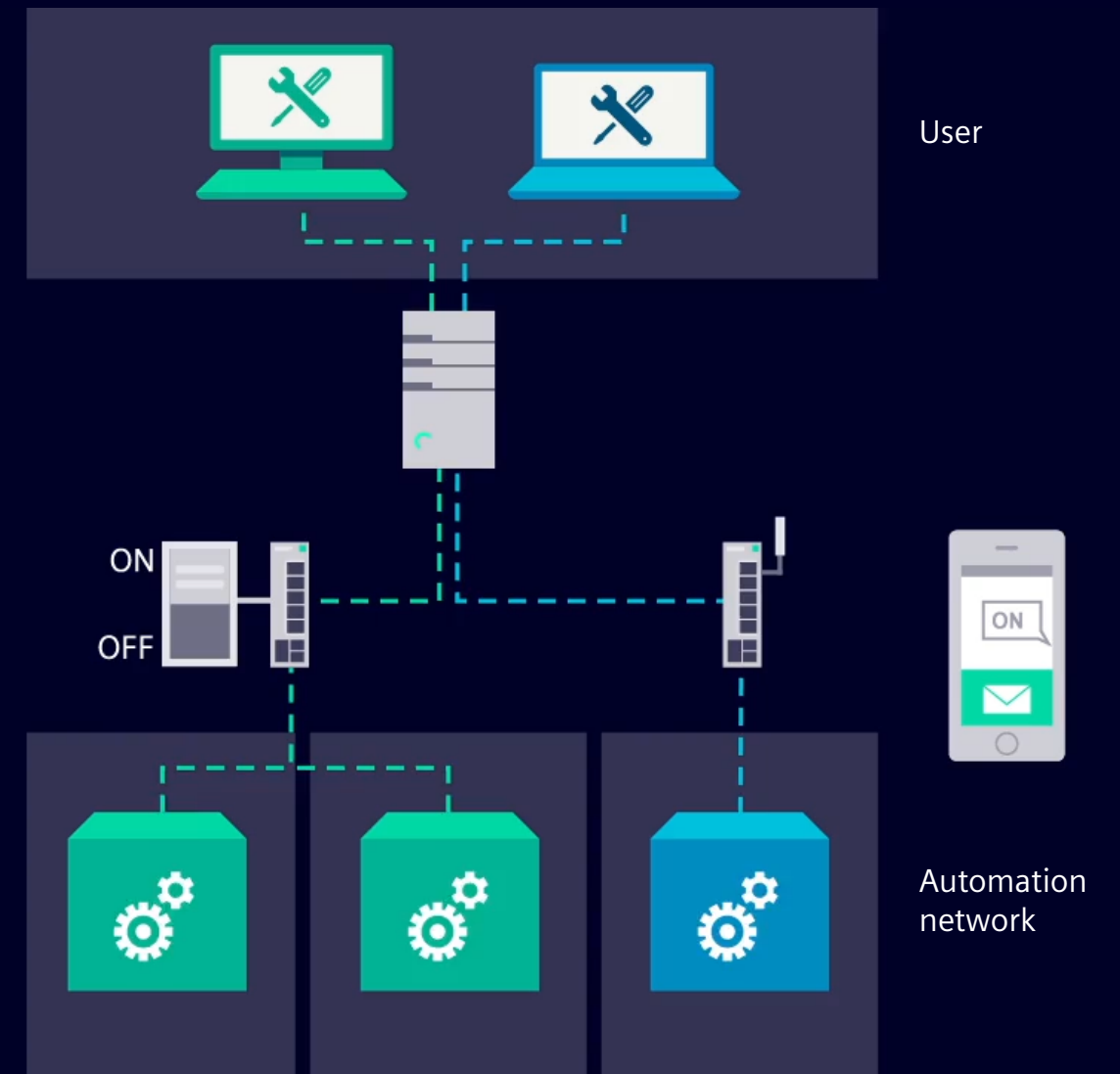
SOLUTION

Ensure business continuity with backup management and secure remote access for recovery

Industrial plants are typically distributed, sometimes across national boundaries. During the operation and optimization phases, maintenance and recovery from incidents in an operational distributed industrial plant and machinery must be performed without delay to avoid downtime for operations and services. Disaster recovery systems and remote recovery support address these challenges. At Siemens, we offer disaster recovery systems with online/offline backup options with a variety of local and offsite backup options, e.g. [SIMATIC DCS SCADA Infrastructure](#).

How to establish secure remote connections

Establishing the connection for secured remote access is very easy with our VPN management platform [SINEMA Remote Connect](#) or the common Remote Service Platform cRSP. The service technician uses a SINEMA Remote Connect Client or cRSP, the system or the machine to be serviced, is equipped with a [SCALANCE S](#) Industrial Security Appliance, a [SCALANCE M](#) industrial router or [Industrial Next Generation Firewalls](#). Secure remote access to the OT environment is also provided by the Zero Trust OT Access Service with the local processing platform [SCALANCE LPE](#).



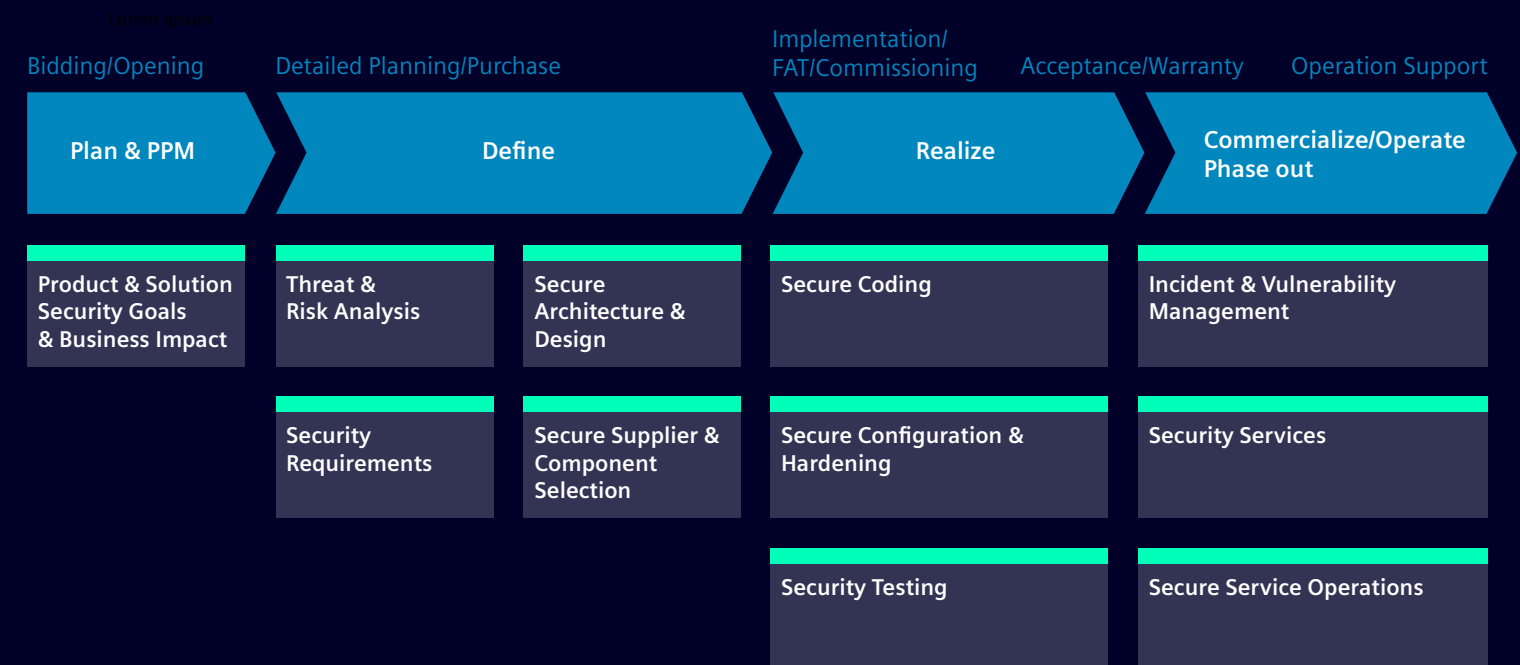
SOLUTION 1

Secure products and services along their lifecycle

A robust supply chain involves several key factors. It includes integrating cyber secure components into your products, ensuring that all applications involved in the process adhere to security standards, and being able to rely on your service providers in times of crisis. As manufacturers are also part of the supply chain, it's vital to establish a chain of trust through practices that lead to cyber resilience. Incorporating robust supply chain and product security measures throughout the lifecycle can help meet new laws and regulations and set high standards.

Consideration of the entire product lifecycle

Experts in automation, digitalization and cybersecurity identify vulnerabilities and risks in product lifecycle management, project management and engineering, and work with you to develop a security roadmap with specific supply chain security measures. Our [supply chain security consulting services](#) are delivered by consultants who draw on our own factory experience and take a holistic approach to risk management in product lifecycle management, project management, and engineering.



SOLUTION 2

Continually identify and evaluate vulnerabilities

Application cybersecurity requires a structured software bill-of-material (e.g. CycloneDX) to gain the ability to identify vulnerabilities, license compliance, and monitor the software supply chain. Throughout the application cybersecurity lifecycle, continuous assessment of risk and applicability of identified vulnerabilities is measured. However, this requires an understanding of cybersecurity risks and impacts throughout the lifecycle of software applications.

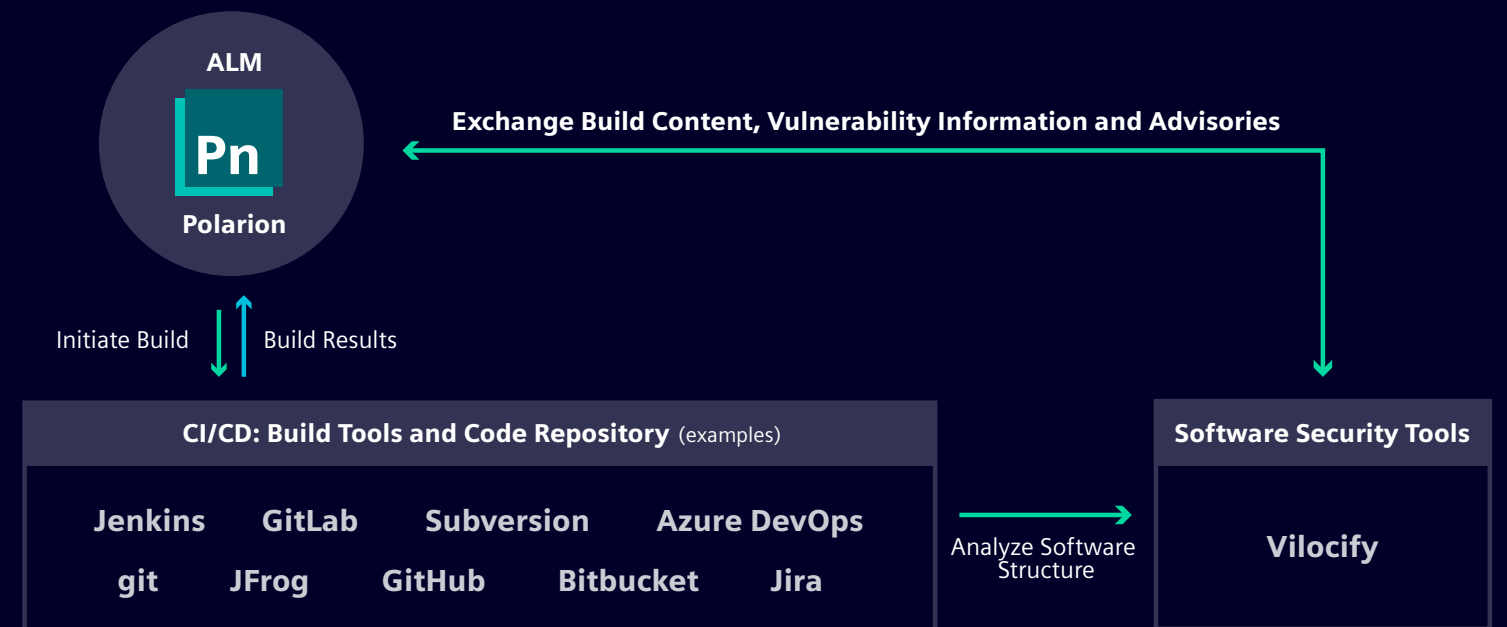
Control, manage, and maintain a cybersecurely developed application

Our comprehensive solution ensures complete product traceability by tracking industry requirements, performing threat and risk analysis, and documenting remediation efforts and product changes.

[Polarion](#) orchestrates the software cybersecurity ecosystem that connects build tools (CI/CD), code repositories, and test environments.

Software security tools such as [Vilocity Vulnerability Services](#) continuously identify and assess vulnerabilities and monitor the software supply chain.

Integrating Polarion into the process enables automated vulnerability management and compliance testing of software components



SOLUTION 1

Manage vulnerabilities and patches to increase security and availability

During the operations and optimization phase, systems must be updated on a regular basis. New vulnerabilities are reported daily for many systems. Vulnerabilities can be exploited by attackers if proper mitigation is not implemented. Identifying new vulnerabilities as soon as possible and minimizing the time to patch is critical. One of the NIS 2 Cybersecurity Risk Management (CRM) obligations is the handling and disclosure of vulnerabilities.

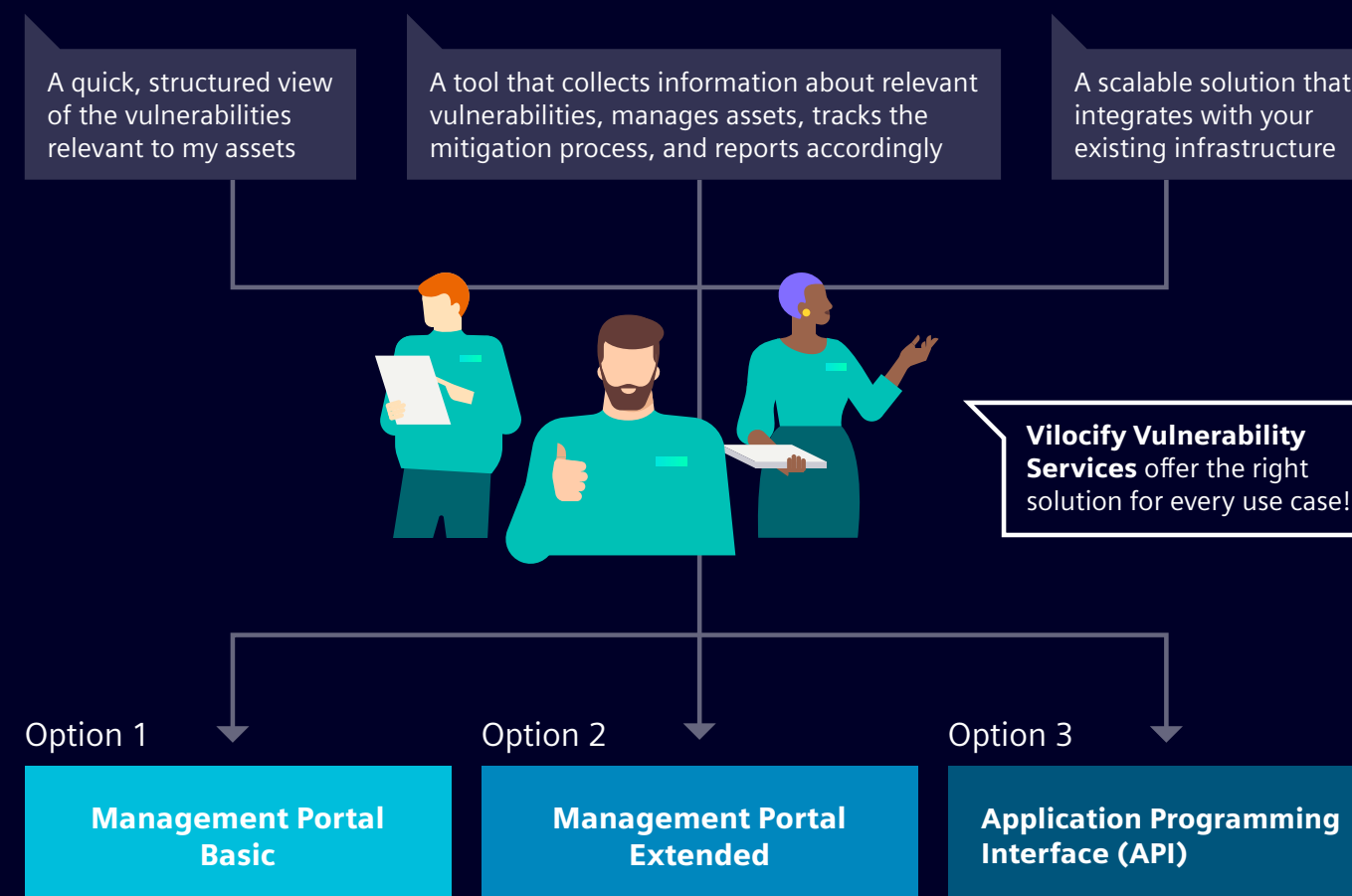
Secure your infrastructure and product portfolio

[Vilocity Vulnerability Services](#) empower you to secure your infrastructure and product portfolio by providing relevant, actionable vulnerability intelligence. You receive vulnerability alerts for your individual system via different options:

- Management Portal: Web-based application offering a structured overview of relevant vulnerabilities for your components
- Application Programming Interface (API): Seamless interface to integrate the vulnerability intelligence into your existing vulnerability management tools and processes

With its vulnerability scanner, [SINEC Security Inspector](#) also checks the network for potential gateways that could be used for cyber-attacks to compromise systems and data. [Patch Management](#) helps you manage critical Microsoft product updates.

Requirements



SOLUTION 2

Manage OT assets to increase security and transparency

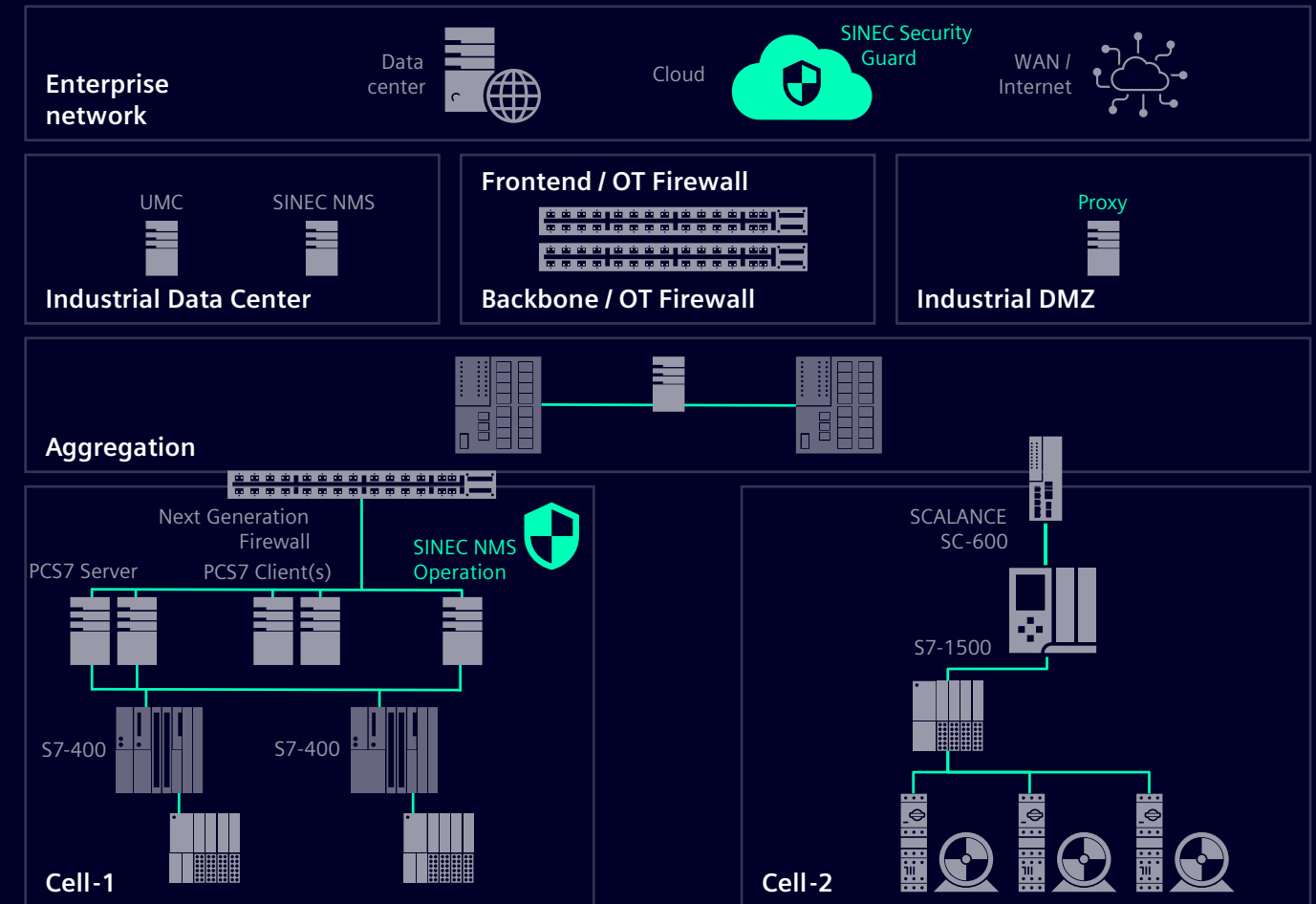
During the operational phase, industrial operators must ensure the smooth and secure operation of OT assets on the shop floor. They need to monitor new vulnerabilities that are continuously reported in order to respond with appropriate mitigation actions. In addition, industrial operators must comply with government regulations (e.g., NIS2, NERC-CIP).

Easily match, evaluate and mitigate with SINEC Security Guard

Identifying and managing vulnerabilities can be time-consuming and requires specialized cybersecurity and automation expertise. However, standard risk levels are not the best solution for a plant's operational environment. That's why [SINEC Security Guard](#) leverages existing digital asset inventories (e.g., [Industrial Asset Hub](#)) and maps them to vulnerabilities:

- Matching vendor security advisories to the asset inventory of the plant
- By assessing the risk of vulnerabilities in the context of the asset's operational environment, mitigation actions are prioritized based on criticality
- Mitigation actions can be defined and scheduled through integrated task management

3rd party IT specific applications can be connected via a public API (for applications such as asset inventories and workflow applications).



SOLUTION

Help the board and CEO deal with NIS 2 requirements

The executive team and employees must acquire sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the organization. The board and CEO must also evaluate whether and how to disclose a cyberattack internally and externally to customers and investors. However, finding the right training provider with appropriate knowledge of processes, procedures and cybersecurity solutions in IT and OT is challenging. It's important to find a modular training offering that fits your organization's unique needs, and to work with a training provider that will be with you for the long haul of the NIS 2 journey.



Build cyber resilience in your organization

[Cybersecurity Training](#) delivered by experienced Siemens consultants ensures that the organization receives the right training content, tailored to the needs of the organization and the IT and OT environment, based on our experience in various projects. Our step-by-step approach ensures that we guide organizations from the first NIS 2 awareness training to the implementation of NIS 2 compliance. Our experienced trainers are always responsive to your individual needs.

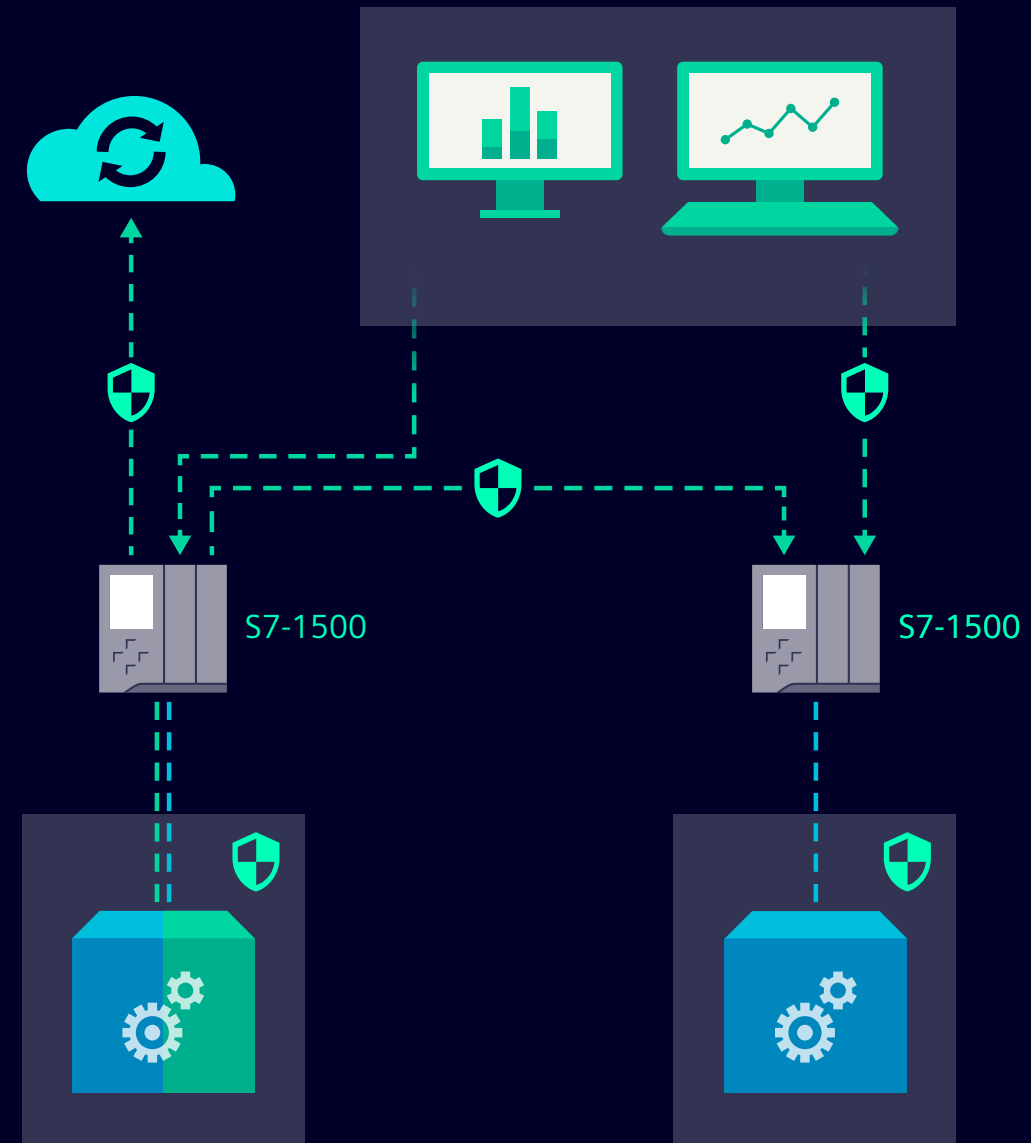
SOLUTION

Mitigate cyber risks with encrypted communication for OT

As manufacturing becomes more dynamic, data access throughout the product lifecycle becomes critical. Devices, systems, and users exchange data continuously or on demand without proper data access management or identification mechanisms. Without these mechanisms, anyone can connect to the network, making the system vulnerable to man-in-the-middle attacks. Because the data is in clear text, it is vulnerable to theft, manipulation, espionage, and sabotage. One of the NIS 2 Cybersecurity Risk Management (CRM) obligations is the use of cryptography and, where appropriate, encryption.

Secure communication and system integrity factors

Ensure system integrity through authentication and encryption, for example with end-to-end encryption between [TIA Portal](#), [S7-1500/1200 controllers](#), and [HMI stations](#) thanks to state-of-the-art secured communication based on Transport Layer Security (TLS) V1.3.



SOLUTION 1

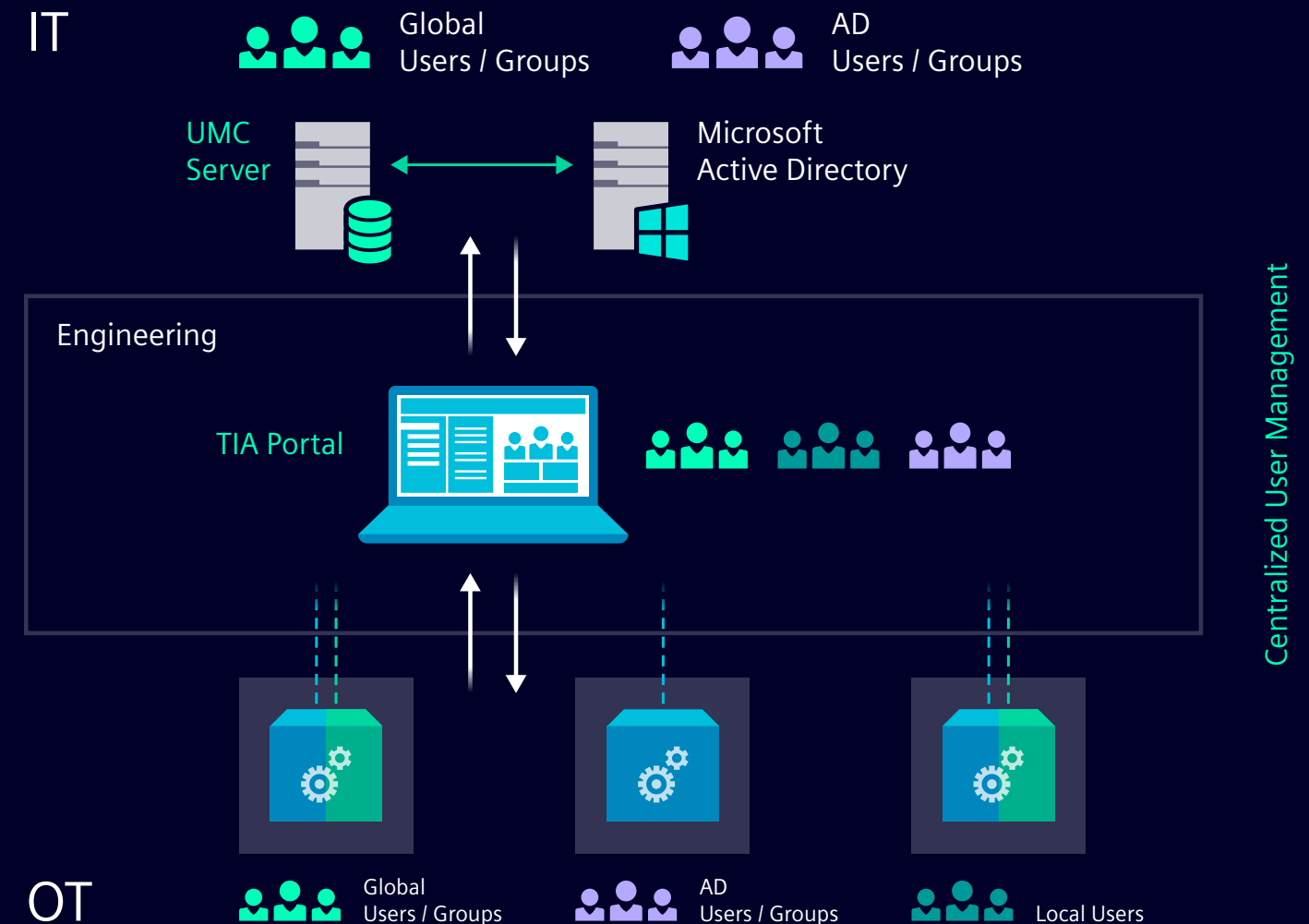
Easily and centrally manage users, roles and access rights

Preventing unauthorized access to user programs, the automation system, and data during the design and maintenance phases requires granular configuration of user privileges and access management. Often, user management is not centralized during engineering and especially during operations.

Engineering projects require user management and access control to prevent unauthorized access, resulting in increased effort. Individual access rights for each user should be based on their role. This results in even more effort to keep each project consistent and to update projects according to user changes.

Efficient user management at the OT level

Implementing a centralized user management requires just a few steps. Import users and groups from Microsoft Active Directory to the [UMC server](#) and connect the TIA Portal engineering station to the UMC server. Import users and groups from the UMC server to [TIA Portal](#), then assign rights and roles locally.



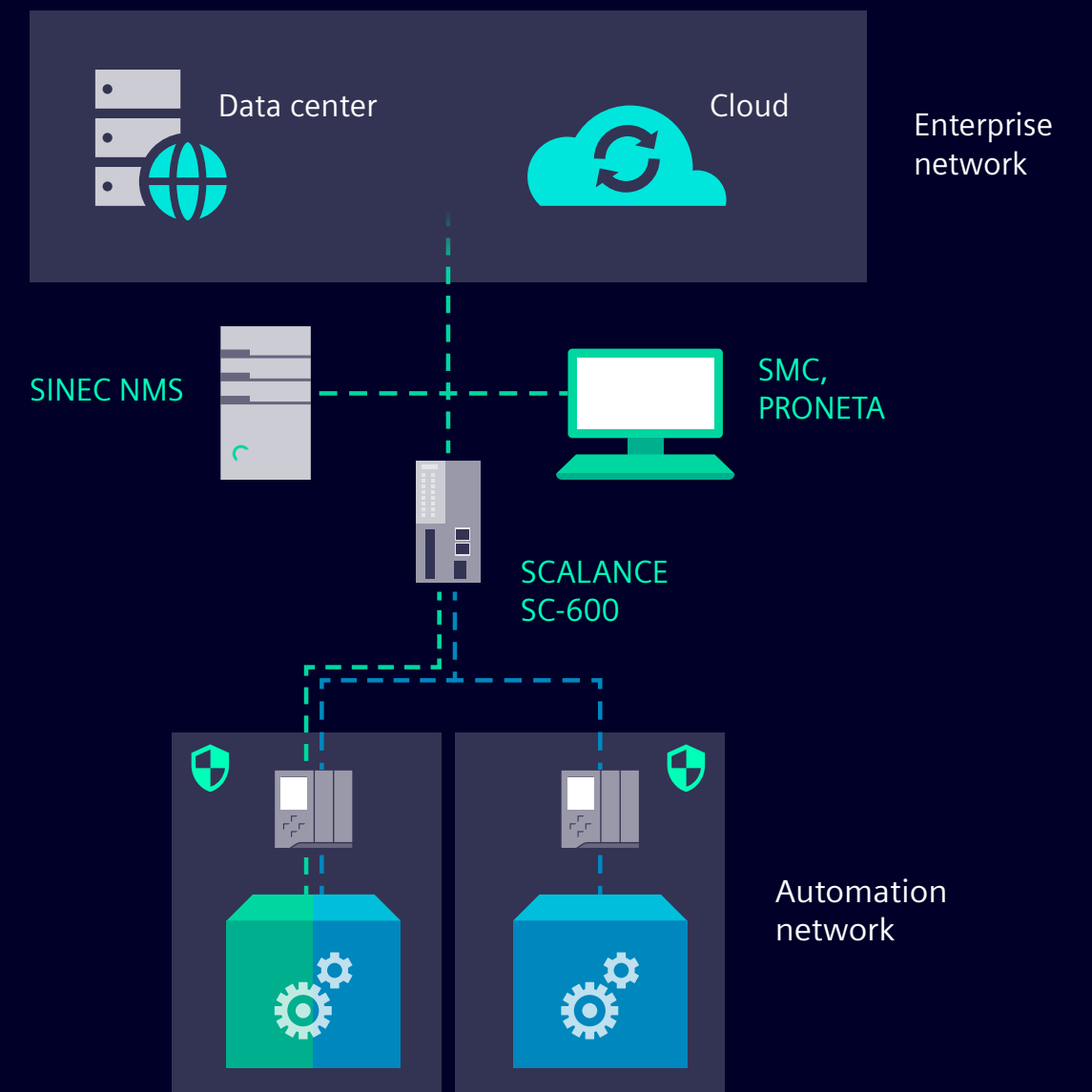
SOLUTION 2

Improve security with asset discovery and management

Organizations that manage a wide variety of physical and virtual assets need asset discovery to maintain accurate inventory records, streamline maintenance schedules (e.g., to address vulnerabilities), ensure compliance, and prevent loss or theft of assets. A continuously accurate asset inventory is the foundation for all other security measures! For a comprehensive view of the asset inventory, the use of different tools is recommended. One of the NIS 2 Cybersecurity Risk Management (CRM) measures is the implementation of asset management.

Get a comprehensive view of all your assets

Our solution makes use of the centralized [SINEC NMS](#) (Network Management System), [SMC](#) (SIMATIC Management Console), and [PRONETA](#) to provide network monitoring, topology discovery, diagnostics and firmware management. Additionally, [SINEC Security Inspector](#) features a high performance, nonintrusive, vendor independent scans to generate easy to manage installation overview.



SOLUTION 3

Gain a comprehensive view of all your network assets across the plants

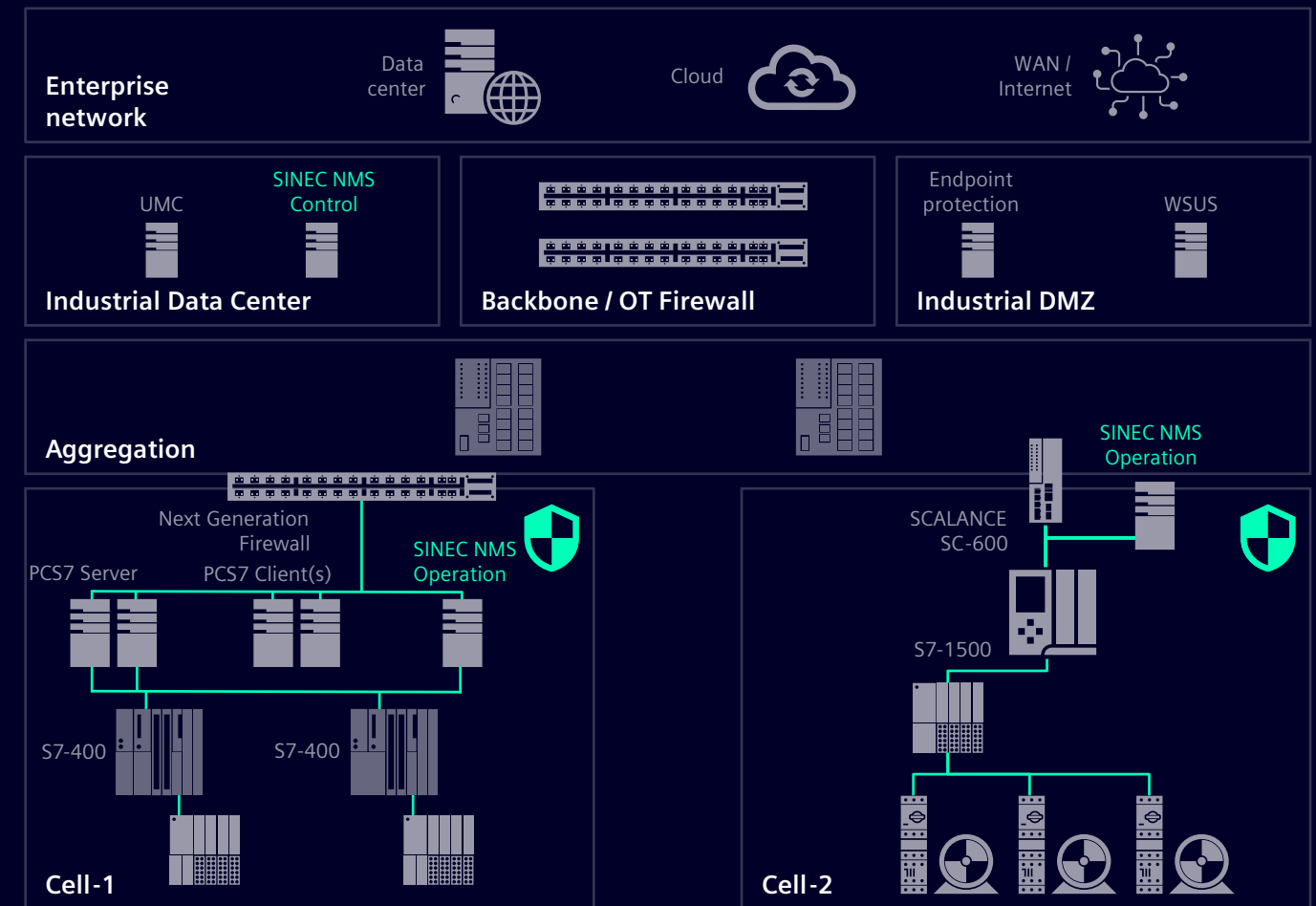
A holistic approach to cybersecurity requires the ability to discover, monitor, operate and manage all OT assets, including critical ones. Throughout the cybersecurity lifecycle, a detailed view of OT assets is required to effectively manage these assets and reduce their attack surface.

The challenge is that plants contain many network assets from many different vendors and may also contain legacy assets. Equipment upgrades and the latest firmware updates are not included in network asset lists. Network assets with outdated firmware are a particular cybersecurity risk.

Support for discovery of your network assets

Our solution seamlessly and comprehensively assist customers in network asset discovery and management:

- Inventory and visibility: Maintain an up-to-date inventory of all devices, equipment and software in your plant's network.
- [SINEC NMS](#) automatically discovers network assets and manages them in an inventory list or network topology view, providing a complete, up-to-date view of all components in the network, including their properties.
- In addition, various network areas can be monitored, including automation products such as PCS 7/neo, PLCs, PROFINET-IO and third-party assets.



SOLUTION

Prove and verify a user's ID to a system

A variety of applications are important sub-elements of a production or process. Different people have access to these applications. It must be ensured that only authorized persons have access to these applications. Availability of production systems is a top priority. Unauthorized access to machines can cause downtime. Ensure that only authorized and trained personnel have access at all times.

Brownfield environments are often an obstacle, and stakeholders don't pay enough attention to authentication. There is a lack of visibility into where multi-factor authentication makes sense in production, and many organizations haven't developed processes to enable multi-factor authentication and don't know what solutions are available on the market to help them implement it. In addition, local and remote access to the HMI is required to operate the machine.

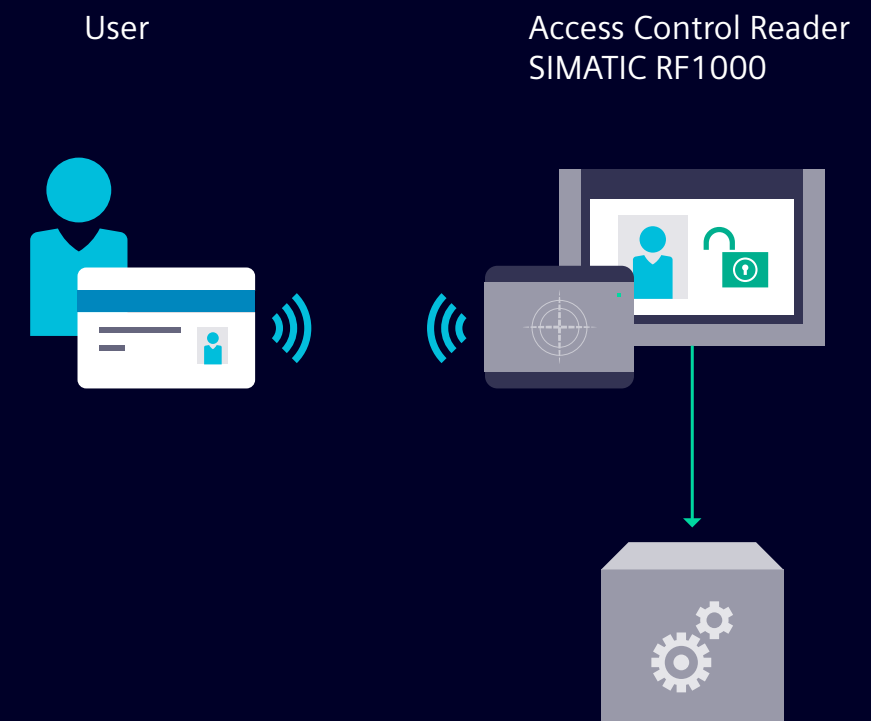
Reliable access control protects system integrity

The solution is the explicit identification of operators at machines and plants, including:

- Access control
- Audit trail

The [SIMATIC RF1000R](#) access control reader supports one-time and permanent RFID card logon, as well as [RFID card logon with user credentials](#):

- One-time reading of the ID card
- Permanent reading of the ID card
- One-time reading of the ID card [with additional user-specific password authentication](#)



SOLUTION

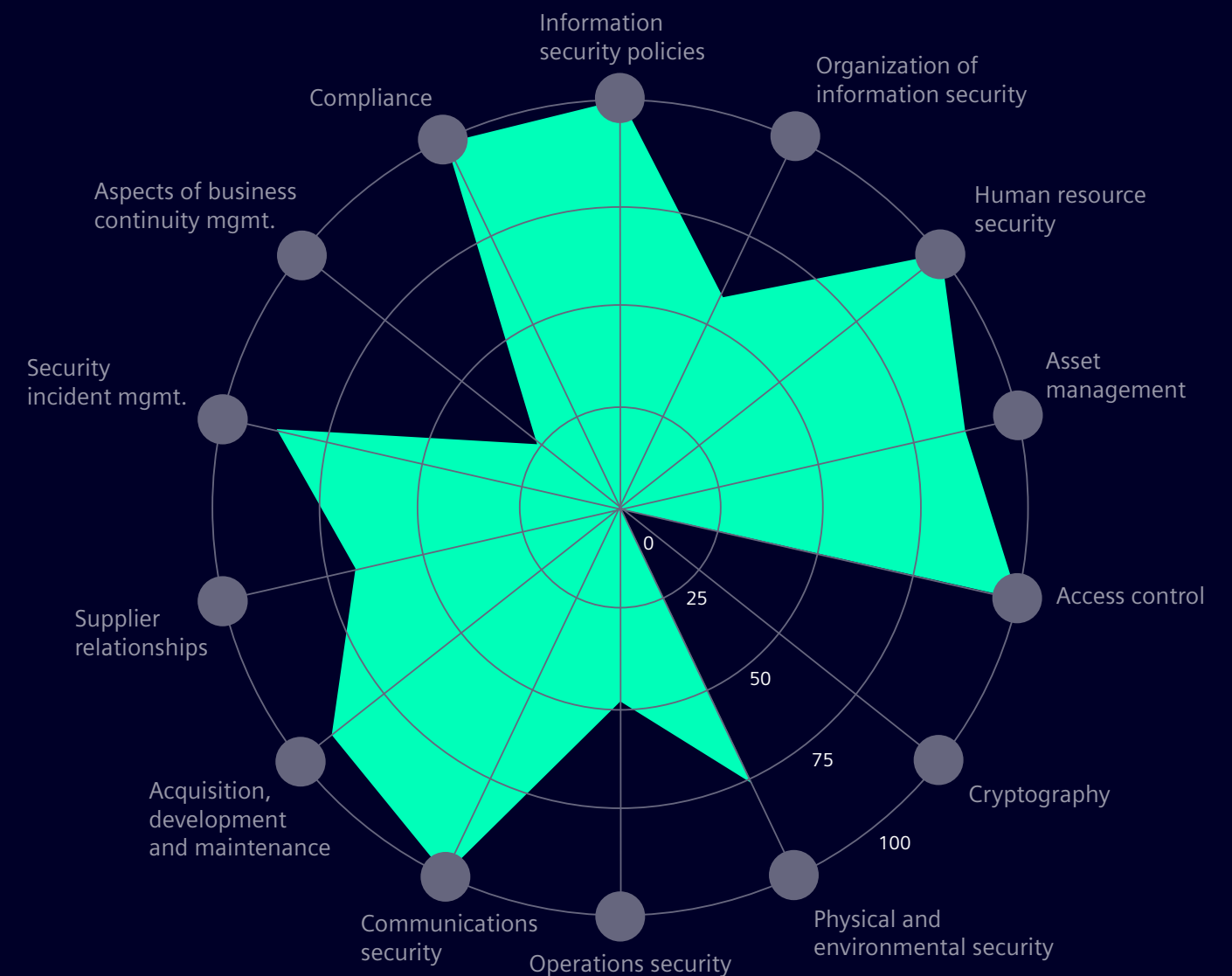
Gain transparency and develop a security roadmap

Implementing effective security measures is critical. The pressure on industrial companies to comply with national laws and regulations, such as NIS 2 and NIST, and standards, such as IEC 62443 and ISO 27001, is increasing significantly. Capacity for industrial cybersecurity and industrial cybersecurity expertise is scarce, and IT staff need support from security experts with automation expertise. Time pressures are increasing due to new compliance requirements and legislation. In addition, conducting comprehensive assessments and developing customized security plans is not easy and often requires deep knowledge of both OT and IT.

Leverage the expertise of cybersecurity and industry experts

[Security Assessments](#) include a holistic analysis of threats and vulnerabilities, identification of risks, and recommendations for closing identified gaps. They maximize transparency and provide a complete overview of the current security status of your automation systems. You can choose between a compact one-day on-site assessment (Industrial Security Check) or an in-depth assessment of compliance with IEC 62443 (IEC 62443-3-3 / NIS 2 and IEC 62443-2-1 Assessment).

[Industrial Security Consulting](#) provides on-site support from experienced consultants on security policy and plant-specific network design, as well as customized implementation support for the Industrial Security portfolio.



Contact

Published by

Siemens AG
Digital Industries
Factory Automation
P.O. Box 4848
90026 Nuremberg
Germany

© Siemens AG 2024

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

For the U.S. published by

Siemens Industries Inc.
800 North Industry Parkway
Suite 450
Alpharetta, GA 30005
United States



POLICIES ON
RISK ANALYSIS

INCIDENT
HANDLING

BUSINESS
CONTINUITY

SUPPLY CHAIN
SECURITY

NETWORK AND INFORMATION SYSTEMS /
VULNERABILITY HANDLING

CYBERSECURITY
TRAINING

CRYPTOGRAPHY
AND ENCRYPTION

ACCESS CONTROL POLICIES /
ASSET MANAGEMENT

MULTI-FACTOR
AUTHENTICATION

POLICIES AND
PROCEDURES

