SIEMENS

Complying with the Cyber Resilience Act

Support and solutions to master
the cybersecurity regulations together!

Cyber Resilience Act (CRA) – Obligations*

Security Capabilities
Secure by default | Protect from unauthorized access | Data integrity and confidentiality | Resilience against DoS | Limit attack surface | Mechanisms to securely update ...

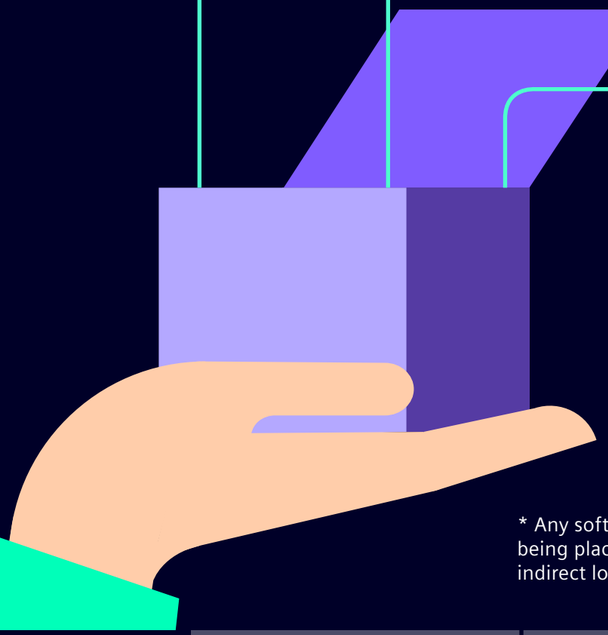
Documentation
Internal technical documentation (compliance, test results,...) | Info and instructions to users (intended purpose, environment, secure configuration)

Lifecycle Process
Cybersecurity risk assessment | Provisioning of updates | Defined support periods ...

Reporting
...of actively exploited vulnerabilities | ...of severe incidents having impact on the security of the product

Vulnerability Handling
Regular testing | Publicly disclose vulnerability info | Provide contact address ...

Conformity Assessment
Depending on product classification: self-declaration alone or inclusion of notified body



* Any software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately, whose intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network

Source:
Regulation - 2024/2847 - EN - EUR-Lex
See, Essential cybersecurity requirements Annex I

Reporting obligations

Type of reporting	Actively exploited vulnerabilities	Severe incidents
Early warning	< 24 h	< 24 h
Vulnerability/incident notification	< 72 h	< 72 h
Final report	< 14 days after availability of a corrective / mitigating measure	< 14 days after submission of the incident notification

Source:
Regulation - 2024/2847 - EN - EUR-Lex
(see Reporting obligations of manufacturers Article 14)

Overview of specific CRA requirements and obligations

The CRA establishes essential obligations for manufacturers to bring secure products to market and maintain their security throughout their lifecycle. These obligations fall into three main categories: secure lifecycle processes, vulnerability management, and security capabilities, each of which has specific technical and procedural requirements.

Lifecycle Process

The Cyber Resilience Act requires manufacturers to implement secure development processes throughout the entire product lifecycle. These processes include conducting cybersecurity risk assessments, maintaining documentation and reports, defining support periods, and performing conformity assessments. These measures ensure security is embedded from design to end of life, and compliance is demonstrated through detailed technical documentation.

Security Capabilities

To meet CRA requirements, products must have essential cybersecurity features. These features include secure authentication, data integrity and confidentiality, minimization of the attack surface, logging of security events, and resilience against denial-of-service attacks. Manufacturers must also ensure secure default configurations, enable updates, and limit the risk of one product compromising others to support a strong security baseline across the digital ecosystem.

Vulnerability Handling

According to the CRA, manufacturers are responsible for identifying and managing product vulnerabilities. This includes performing regular security tests to ensure products are shipped without known vulnerabilities and disclosing relevant vulnerability information. To maintain product integrity over time, companies must also provide a contact point, offer timely updates, and establish mechanisms for secure update distribution.

Solutions based on the cybersecurity guide for machine manufacturers

Lifecycle Process

- CRA Consulting
- Risk Assessment

Security Capabilities

- Perimeter Protection
- Authentication and Access Control
- Event Logging
- Integrity and Confidentiality
- Hardening

Vulnerability Handling

- Security Testing and Scanning
- Vulnerability Discovery and Management
- Vulnerability Management Services

CRA Consulting
From regulatory compliance to DevSecOps

Example

1 **Self-assessment**
Conduct Applicability Assessment to understand if your products are covered by the CRA

2 **Categorization**
Choose the category of the product depending on its functions and check applicability of the CRA

3 **Bringing into compliance**
Conduct risk assessment and bring the product in according with essential cybersecurity requirements

4 **Preparing documentation**
Prepare necessary technical documentation including instructions for users

5 **Formal procedures**
Carry out the chosen conformity assessment procedures, get EU declaration of conformity and CE marking

6 **Continuous monitoring**
Follow notification, monitoring and reporting obligations

CRA compliance for machines
Siemens can help you understand how to achieve CRA compliance with a tailored, risk-based roadmap.

We can help you establish compliance with:

- Product risk assessment and product compliance ✓
- Maintaining product security over the entire lifecycle ✓
- Achieving compliance and fulfilling reporting obligations ✓
- Establishing DevSecOps ✓
- Setting up a solution security organization ✓

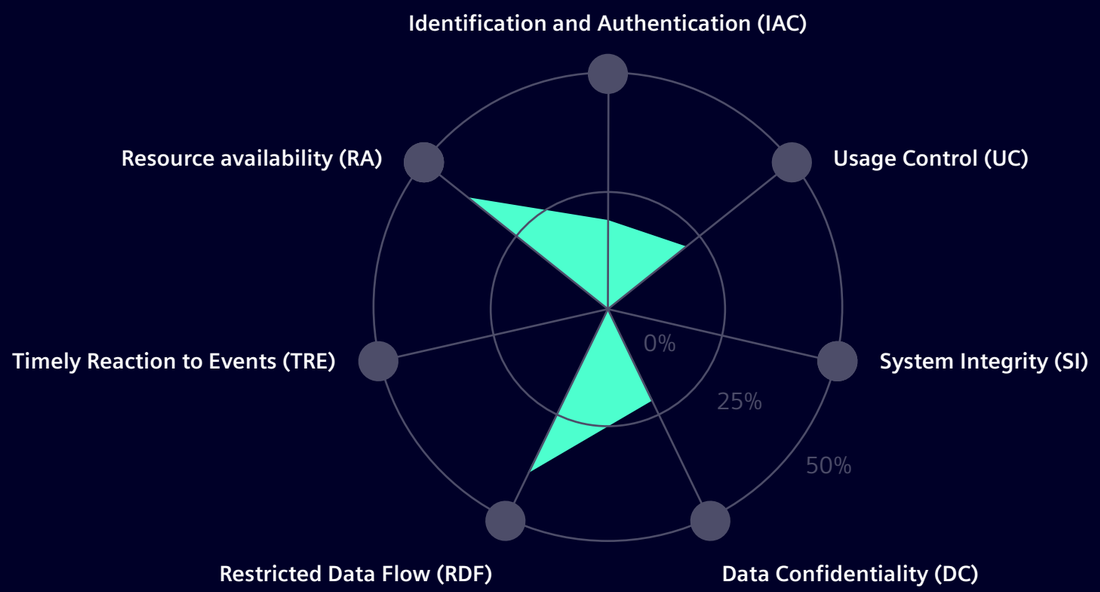
Risk Assessment

CRA-Readiness assessment based on IEC 62443 gap assessment

Report example

Percentage achievement of the Security Level Target (SL-T)

7 foundational requirements



Holistic analysis of threats and vulnerabilities

Security Assessments cover a holistic analysis of threats and vulnerabilities, the identification of risks and recommendations to close the identified gaps. They maximize transparency and provide a complete overview of the current state of security of your machine(s).

We offer a deep assessment of compliance to IEC 62443 and CRA (IEC 62443 / CRA Assessment) to help machine builders to comply with the Cyber Resilience Act.

Security Compliance Coverage Report

Machine and zone criticality

Risk awareness

Gaps to IEC 62443

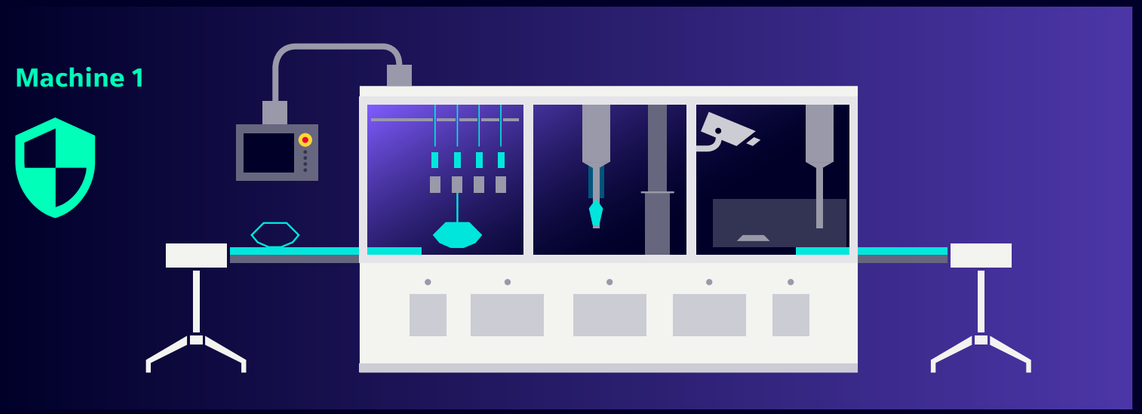
CRA specific answers

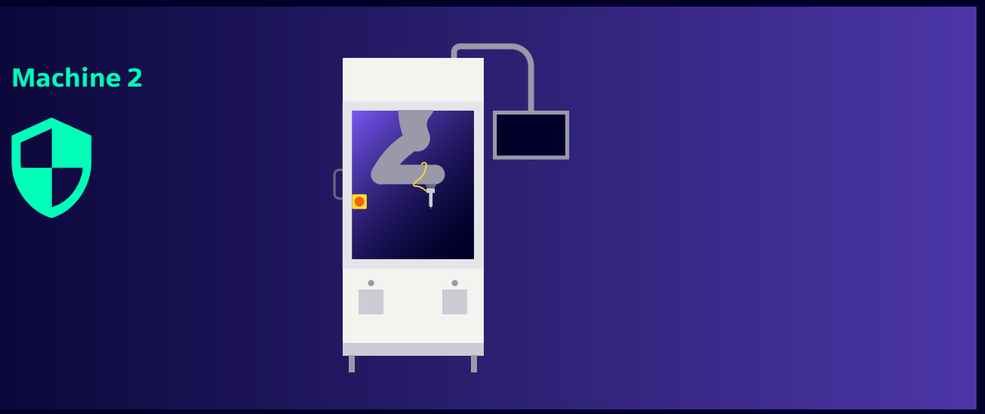
- Reporting obligations
- Vulnerability management

Way forward to improved security

- Specific measures to improve security
- Prioritized according to effort and effect

Perimeter Protection
Firewall-based encapsulation





Encapsulation - restricting the dataflow

Protect the machine subnet by restricting the data flow to and from it by introducing a SCALANCE S firewall.

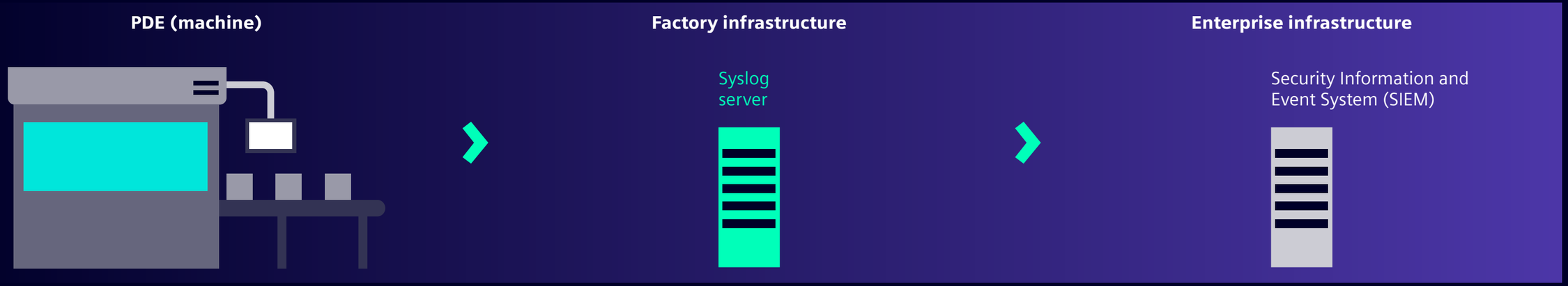
CRA requires to protect the availability of essential functions by implementing or integrating resilience against and mitigation of denial of service (DOS) attacks, limiting the attack surface including external interfaces and reducing the impact of products to other products or networks.

The key points of this approach are:

- SCALANCE S firewall interposed between the machine and other network segments
- Protect the machine network and limiting attack surface
- Restrict the flow of data in and out of the network

Event Logging

How to securely transmit events to detect security incidents



Forwarding security events with secure syslog protocol integrated in various products

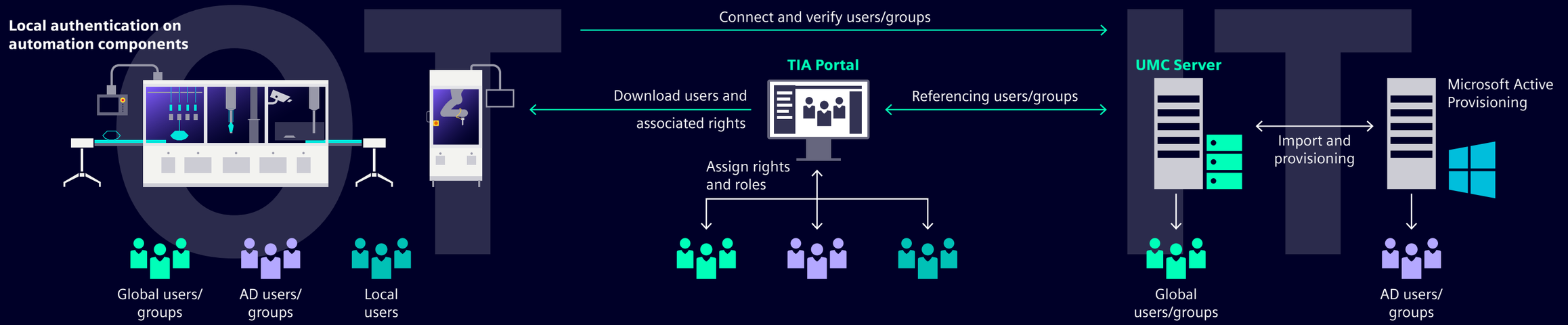
The CRA requires the reporting of various security events. Because the machine network consists of various components, a central event collection system is beneficial for monitoring all events.
The syslog protocol enables to forward events. SINUMERIK CNC and SIMATIC controllers, SCALANCE network components and SINAMICS variable frequency drives have an integrated syslog client feature enabling an easy-to-use solution to centrally collect events.

The software tool SINEC INS (Infrastructure Network Services) for central network services with its integrated syslog server can centrally collect the security events. It also enables to forward the events to an overlying SIEM system.

The key points of this approach are:

- Security event logging
- Securely send events to a central syslog server
- Forward events to a SIEM system

Authentication and Access Control
With centralized user management



Challenge

- Configuring access control for all systems requires a lot of effort
- Manually configuring multiple systems is a repetitive task that is prone to errors

Solution

- Efficient user management with users and groups at the OT level with UMC Server and TIA Portal. Optional mapping of users and groups from Active Directory is possible.

Customer value

- Efficient administration of users for the entire plant
- Users/groups can be imported from an already available Microsoft AD server, saving time and effort
- Improved protection through personalized access instead of generic passwords

Access Control for Machines
Authentication with RFID

Explicit identification of operating staff at machines and plants, including:

- Access control
- Audit trail

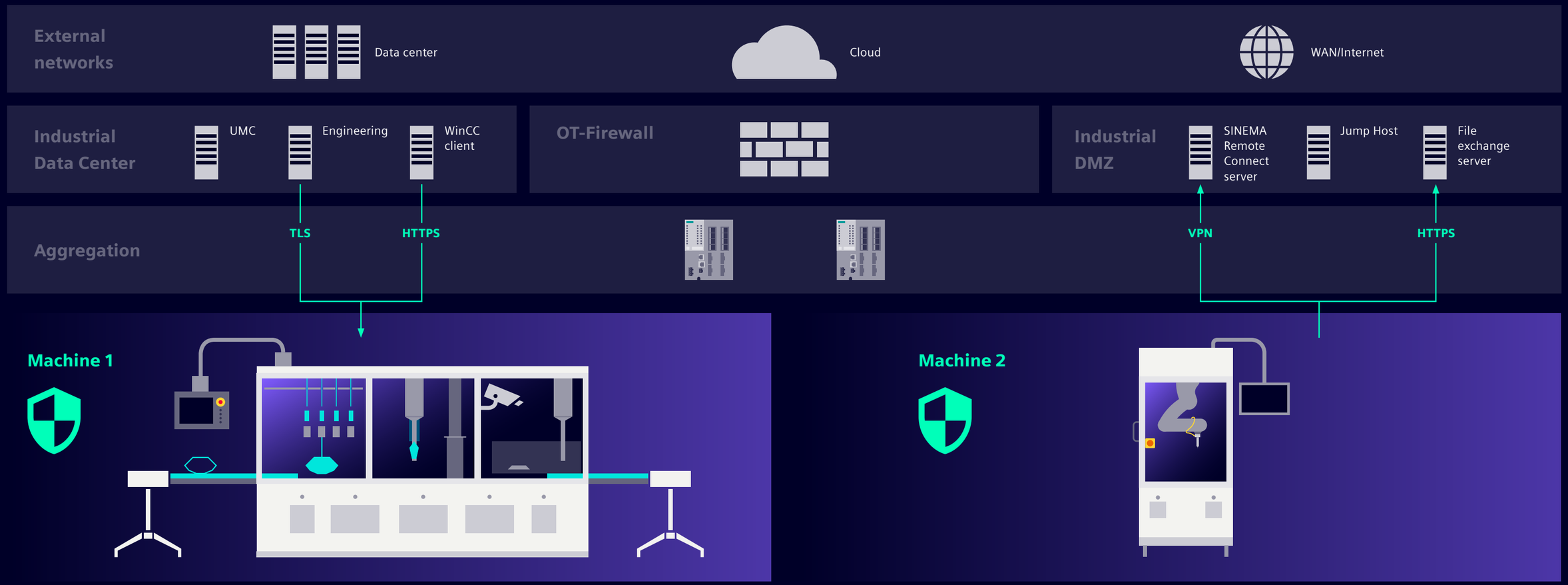
Secure access control and two-factor authentication

The access control reader SIMATIC RF1000 supports one-time and permanent logins with RFID card as well as logins with RFID card including 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

Integrity and Confidentiality

Certificate-based communication with secure protocols



Integrity and Confidentiality
Certificate-based communication with secure protocols

Protect confidentiality of data by using secure protocols

The protection of data integrity and confidentiality are two obligations of CRA. As the machine is typically integrated into a larger automation network, communication to overlying systems must be protected.

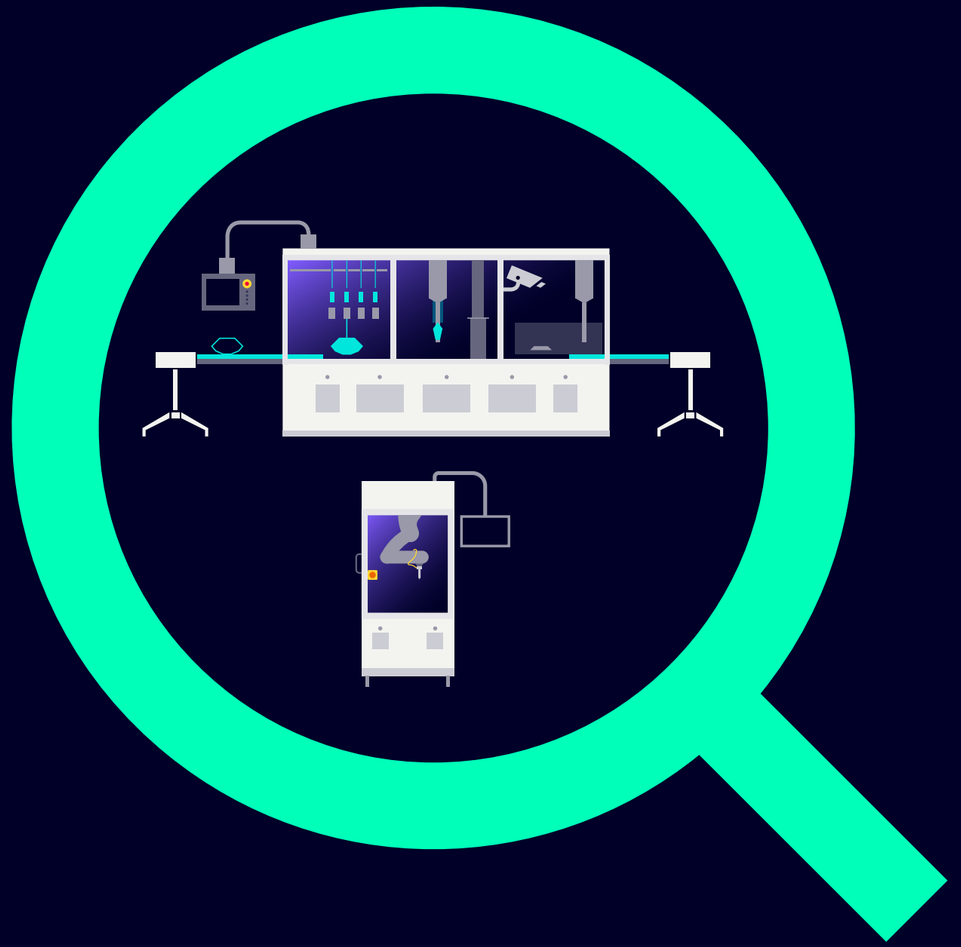
Encrypted protocols can be used in various products:

- SIMATIC and SINUMERIK PLCs can use Open User Communication based on TLS, HTTPS and encrypted OPC UA protocols
- SCALANCE X switches and SCALANCE S firewalls support HTTPS for webserver access
- Industrial Edge supports various secure protocols like HTTPS, OPC UA, MQTT
- Access to WinCC Unified is based on HTTPS
- Furthermore, a VPN can be established with a SCALANCE S firewall to protect any other protocol

The key points of this approach are:

- Encryption with standardized protocols
- Supports PKI certificates

Hardening
of each component to increase protection and resilience



Reduce attack surfaces

The CRA requires reducing attack surfaces, applying secure configurations, and using mitigation measures. Each component offers various security features that need to be configured accordingly.

- Disable of unused services and ports
- Secure the application with know-how protection
- Internal checks for the validity of data, programs, and commands.
- Additional endpoint protection solution, if needed
- Monitor network topology and issue alarms in case of changes
- Additional hardwired monitoring, such as that of the cabinet door, is used to physical tampering

The key points of this approach are:

- Active use of built-in security features of each product
- Use diagnostic data, such as topology and port status, for basic self-monitoring

Security Testing and Scanning

Scan the machine for vulnerabilities and create documentation

Regular tests for documentation

CRA requires to apply effective and regular tests and reviews of the security of the product with digital elements. Furthermore, vulnerabilities need to be identified and documented.

SINEC Security Inspector allows for the application of automated security tests that are easy to execute.

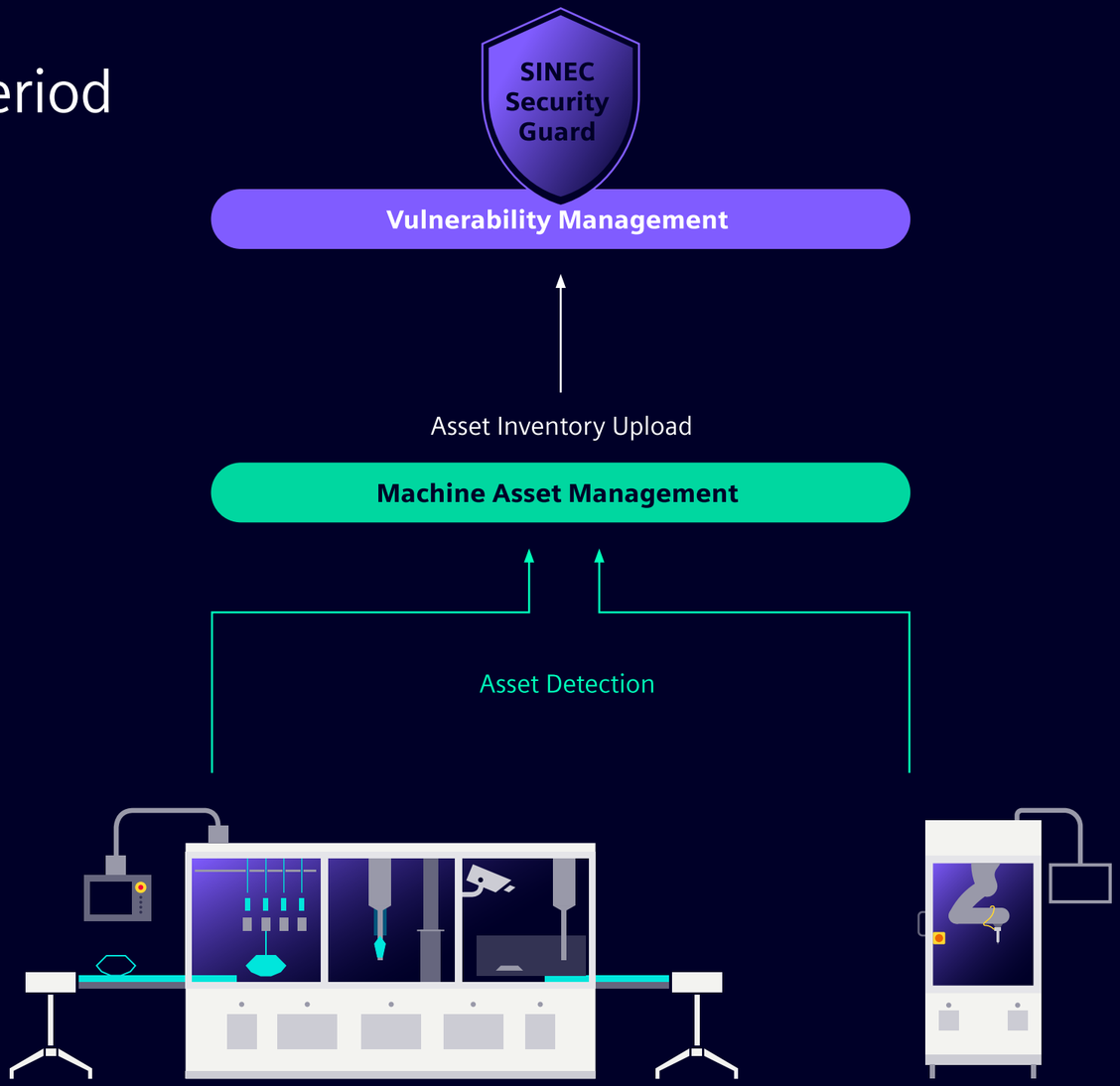
The key points of this approach are:

- An intuitive, web-based user interface with a wizard-supported workflow.
- A broad tool set for increasing insights, compliance, and quality is provided by predefined test cases and supported testing tools
- Scan and test cases have been adapted to fit OT network requirements
- Selection of different security tests with wide-ranging capabilities for detecting vulnerabilities

Alternatively, Siemens offers one-time Scanning Services to conduct such security tests and provide a report.

Vulnerability Discovery and Management

Keep the machine secure during the support period



Identify and document vulnerabilities

Stay informed about vulnerabilities of heterogenous digital asset inventories with a cloud-based, automated solution.

The CRA requires identifying and documenting vulnerabilities, as well as providing updates for those vulnerabilities. Instead of manually matching each published vulnerability with the asset list, SINEC Security Guard automatically notifies users of relevant vulnerabilities affecting their assets. This significantly reduces the effort for the machine builder and enables quick, structured notification of the machine owners.

- Matching the machines' inventory to the component vendor security advisories. (BOM or SBOM)
- Prioritize vulnerability risks based on the unique internal architecture of each machine
- Mitigation measures can be defined and scheduled by an integrated task management or forwarded to workflow solutions (e.g., ServiceNow®)

Vulnerability Management Services

Keep on track with vulnerabilities and react promptly

1. Easy vulnerability management

The Vilocify Vulnerability Service platform offers a secure and efficient solution for vulnerability analysis. Through an HTTPS-encrypted connection, users can access our comprehensive assessment tool. The platform features an intuitive interface that simplifies the vulnerability management process.

2. One service for all components

It supports all types of third-party components, from open source to COTS, from software to hardware, providing an overview of the vulnerability in one single service.

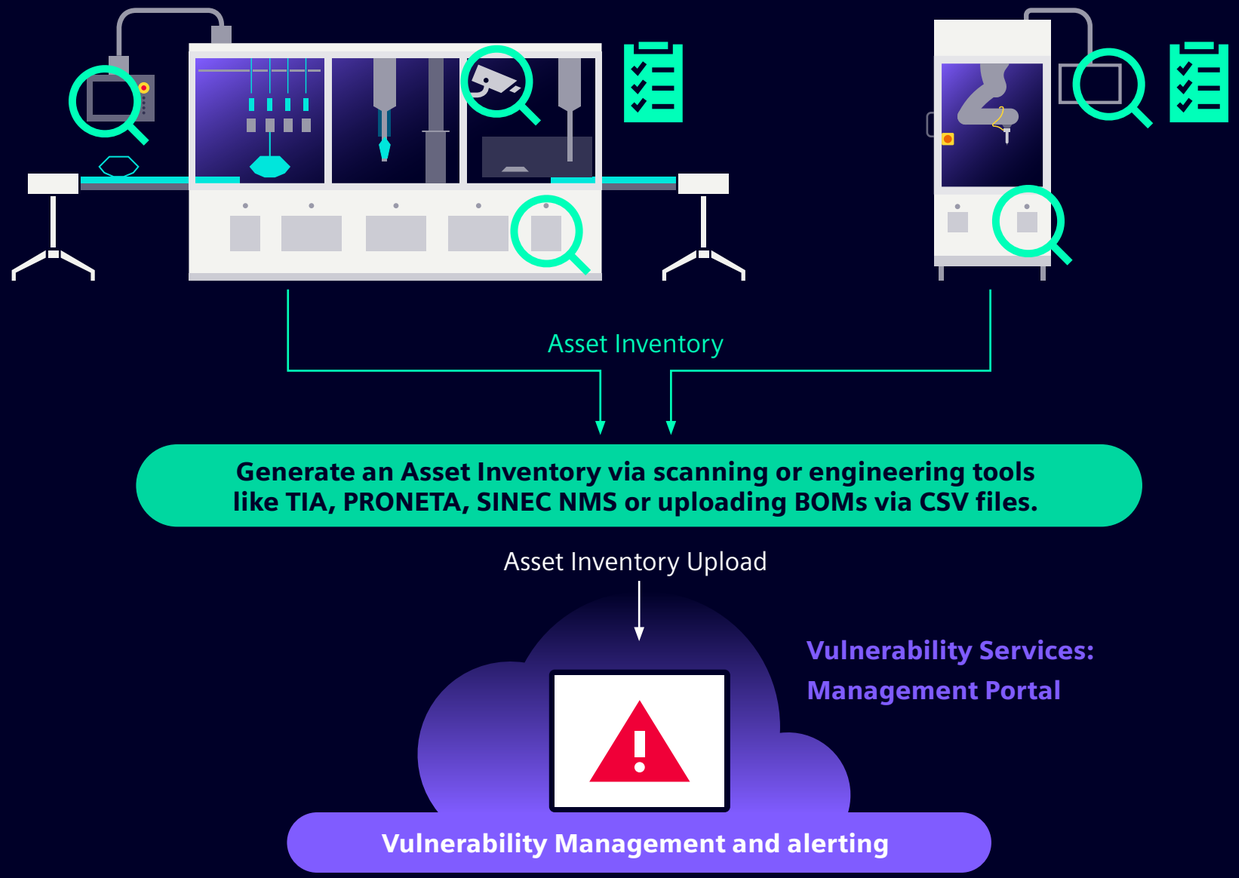
3. Transparent lifecycle information

Vulnerability Services keep you proactively updated on the official support status including end-of-life of components, allowing you to inform your end-customer.

1500
vulnerability information sources

76%
faster than search engines

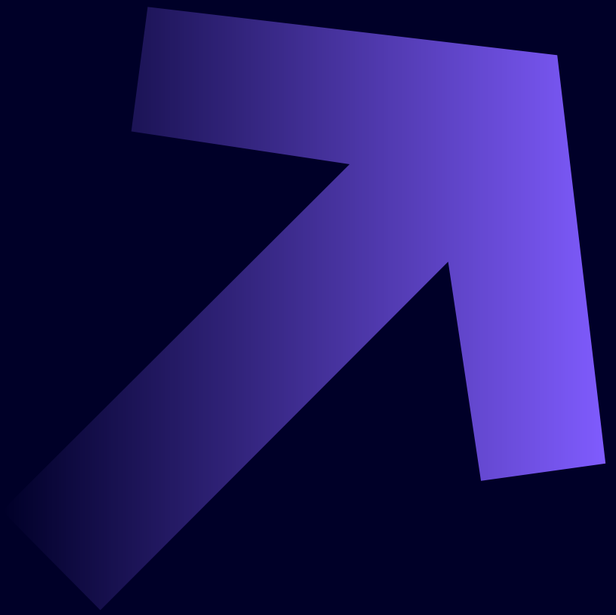
260k
third-party components



Further Security Guidelines
Hardening of Siemens products

Discover more:

- ↗ Additional information on industrial security measures
- ↗ Security guidelines for SIMATIC HMI devices
- ↗ Recommended Security Settings for IPCs in the Industrial Environment
- ↗ Security with SIMATIC S7-Controller
- ↗ SIMATIC Process Control System PCS 7 Security concept (Basic)
- ↗ SIMATIC Process Control System PCS 7 Compendium Part F – Industrial Security
- ↗ SINUMERIK ONE documentation
- ↗ Additional information on Vulnerability Services



Let’s talk about
OT security.
Let’s connect the
experts.

Let’s act together.
Now!

Contact

Published by

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

For the U.S. published by

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