Accelerate NextGen

Cibersegurança

António Castro | SIEMENS

Agenda

	Horário	Tópico	Speaker
1	10:00 am	Welcome	Sónia Palma
2	10:05 am	Sobre Accelerate NextGen	Sónia Palma & João Queiroz
3	10:10 am	Industrial Cybersecurity	António Castro
4	10:20 am	Siemens Expertise and Solutions	António Castro
5	10:30 am	SINEC Security Inspector	António Castro
6	10:50 am	Use cases	António Castro
7	11:00 am	Q&A	

SIEMENS

Accelerate NextGen
Overview

Desafio

O Accelerate NextGen envolve estudantes do ensino superior e do ensino técnico-profissional no desenvolvimento de soluções para os desafios reais da transformação digital sustentável, nas áreas das infraestruturas energéticas e da indústria.

Objetivos

Organizados em equipas, os participantes concebem projetos técnicos aplicados a contextos reais, utilizando ferramentas e software Siemens usados no mercado e trabalhando com cenários de consumo, digitalização, eficiência e otimização energética.

Accelerate NextGen
Overview

2
alunos

Por equipa

Finalistas de curso técnico-profissional, licenciatura e mestrado

8
webinares

Com especialistas do setor

Conhecimento nas ferramentas Siemens e apoio ao longo de toda a jornada.

12
semanas

Um percurso acompanhado

Apoio de profissionais da Siemens e mentores durante todo o desafio.

1
pitch

Final

Top 10 teams vão apresentar o projeto final perante um painel de júris.

SIEMENS

Accelerate NextGen
Desafio

	Desafio	Ferramentas
	O desafio consiste no desenvolvimento de soluções inovadoras focadas na modernização e digitalização sustentável de soluções industriais. Este desafio está estruturado em 4 categorias temáticas: Cibersegurança, Automação, Aplicações Low-Code e Simulação Energética e Eficiência Operacional.	**SINEC Security** Node-RED Siemens Solid Edge Simcenter FLOEFD
	O desafio consiste em criar um projeto de uma infraestrutura de energia elétrica, utilizando todos os recursos das ferramentas de dimensionamento da Siemens, que te serão disponibilizadas para esse fim. Este desafio terá três fases distintas e cada fase contará com um webinar que irá permitir aos participantes familiarizarem-se com as ferramentas a utilizar nessa etapa e esclarecer quaisquer dúvidas relativas ao Desafio.	**SIMARIS Project 25** **Blueplanet PV-designer** **SIMARIS Design 25**

SIEMENS

Accelerate NextGen
Vertente Indústria

Categorias	Desafio	Tecnologias	Critérios
	Os jovens engenheiros irão conceber e demonstrar uma solução integrada de cibersegurança, incluindo monitorização, gestão de ativos, deteção de vulnerabilidades e resposta a riscos.	**SINEC Security** Workshop 9 de Março	Grau de inovação Originalidade e criatividade da solução Sustentabilidade Impacto Ambiental Utilização de Tecnologias Correção e eficácia na integração das tecnologias Siemens Replicabilidade Potencial de implementação em diferentes contextos Grau de Dificuldade Complexidade técnica Qualidade e Preparação Clareza, organização e documentação do projeto
	Os alunos devem desenvolver soluções inovadoras e sustentáveis, otimizar as operações críticas, aplicando conhecimentos em automação, IIoT e sustentabilidade.	**Node-RED** Workshop 5 de Março	
	Os participantes concebem aplicações low-code para otimizar operação, gestão e eficiência, transformando dados complexos em soluções simples e acionáveis.	**Mendix** Workshop 24 de Fevereiro	
	Os concorrentes concebem e otimizam quadros elétricos para datacenters, criando gémeos digitais para simular comportamento térmico, fluxos de ar e propor soluções inovadoras e sustentáveis.	**Solid Edge & FloED** Workshop 26 de Fevereiro	

More information here *https://siemens.invitario.com/pt/accelerate-nextgen/registration*

SIEMENS

Accelerate NextGen

Webinar Indústria

Speaker

António Castro

- Specialist Engineer
- Industrial Connectivity and Cybersecurity

SIEMENS

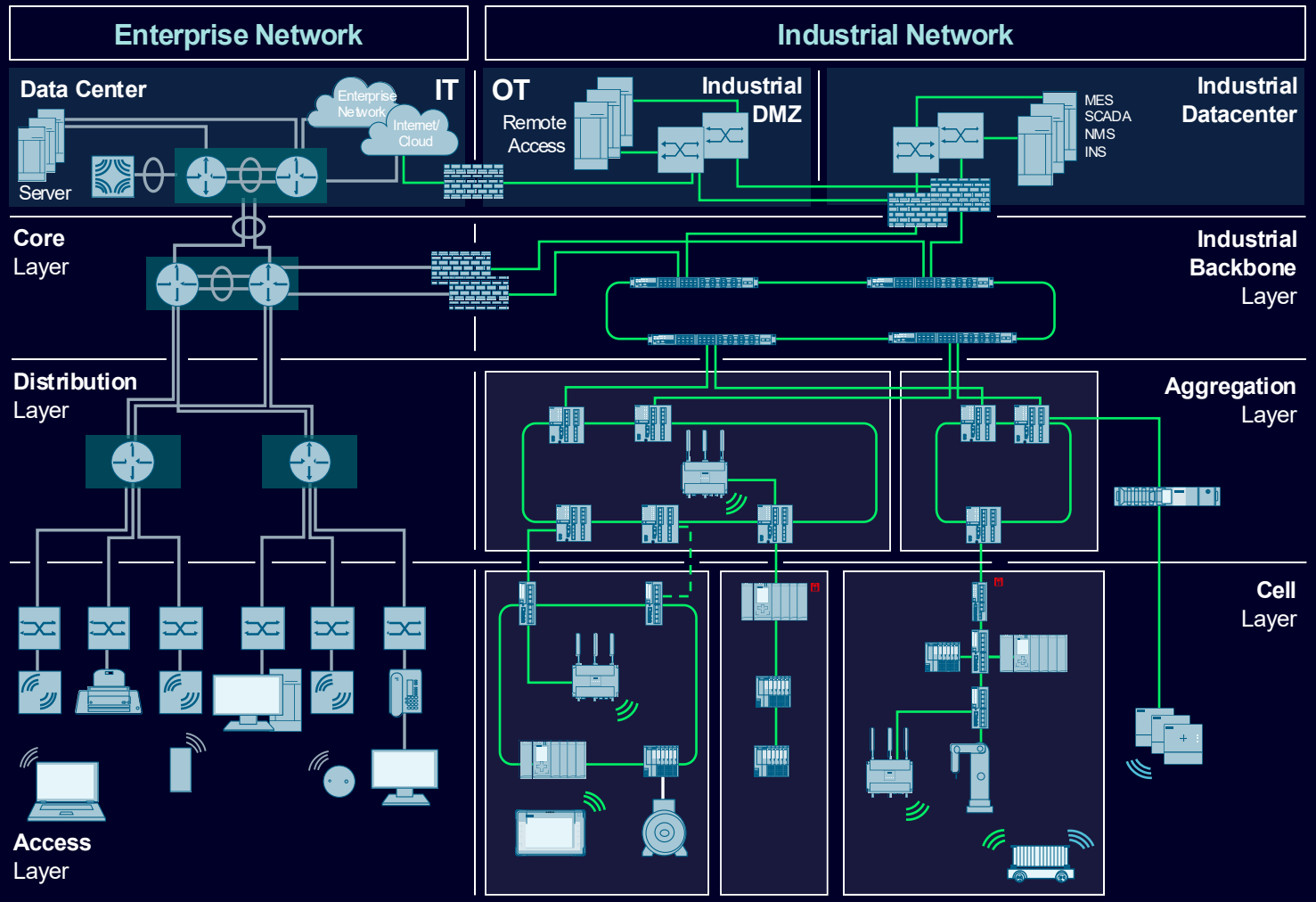
Today everything is connected and therefore at Cyber-risk. Companies mostly secure the IT.

But how secure is your OT?

Can you evaluate the threats and protect your assets accordingly?

SIEMENS

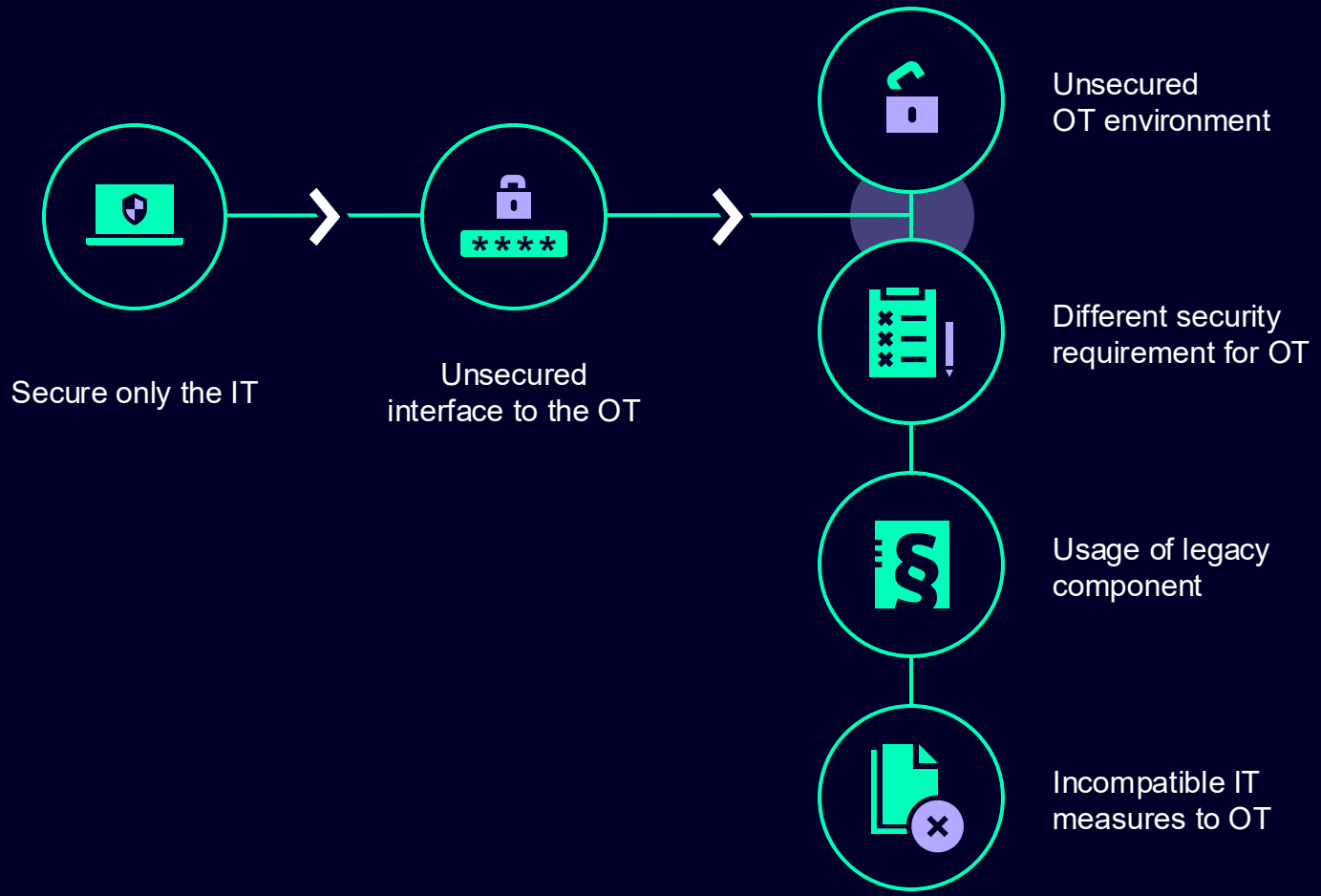
Industrial Networks have critical requirements



- High Availability
- Robustness
- Flexibility
- Determinism
- Industrial Security
- Functional Safety
- Mobile Applications

SIEMENS

OT is often not properly secured making the cybersecurity concept insufficient



IT/OT connection

SIEMENS

What you need is…

… a **multi layered cybersecurity concept** based on the defense in depth principle, which provides an effective protection

SIEMENS

Keeping products secure through whole product life cycle is essential
From ex works till vulnerability patching with Siemens' solutions

Vulnerability Management

Components Update

Product CERT

Customers

System Test

Signed Firmware

R&D

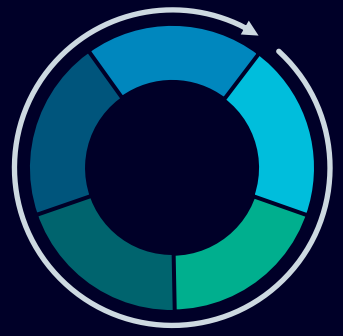
Cybersecurity Policies

Security researcher

SIEMENS

Frameworks, Standards and Maturity models can help you to implement Cybersecurity in your operations

Frameworks



- Gauge current technical state and maturity level
- Plan for future needs
- Identify gaps in workforce skills
- Tools needed

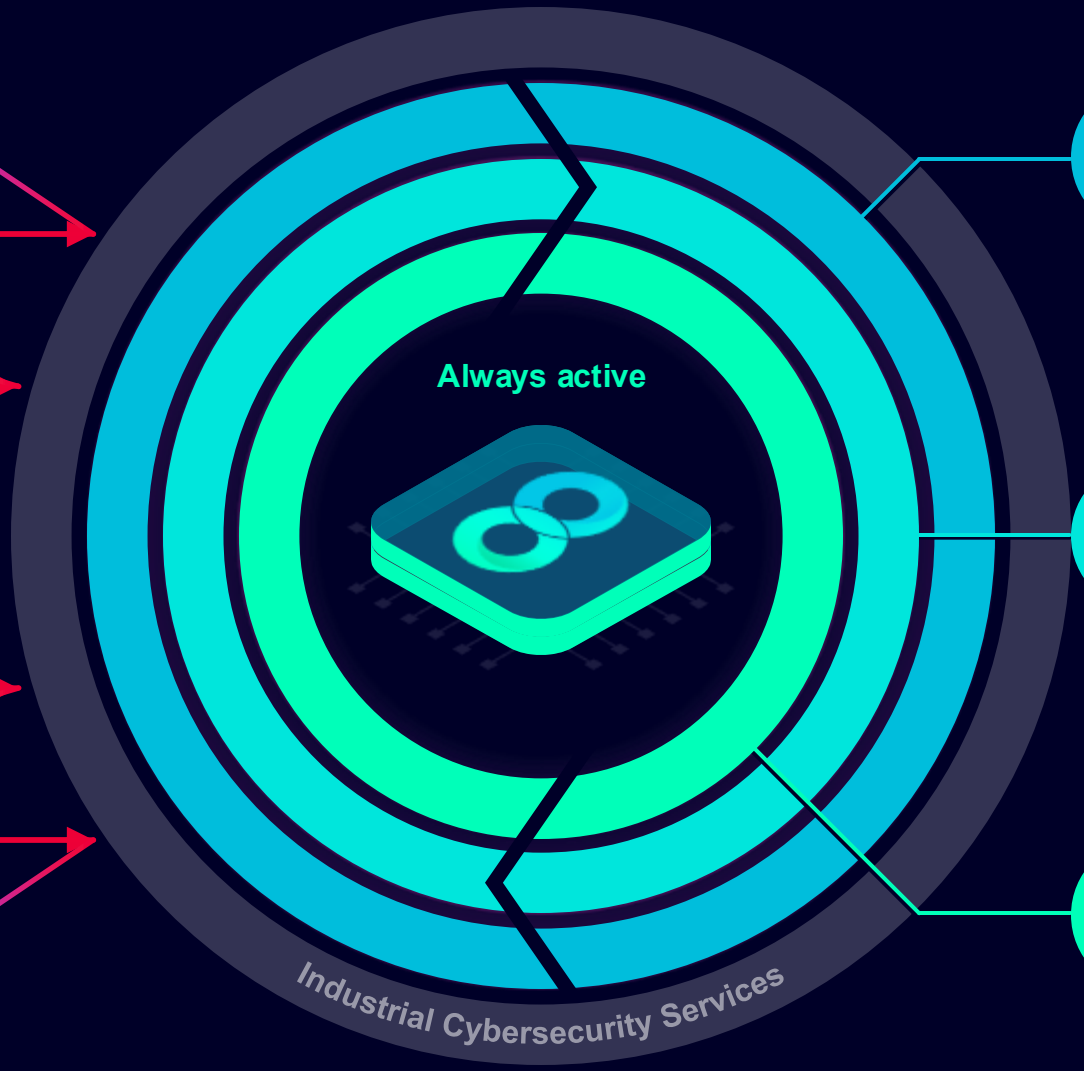
Standards

What to do and how to do it?

IEC NIST ISA ISO

SIEMENS

Only a multi-layered Defense in Depth concept protects in every aspect



Security threats demand action

Plant security

- Physical access protection
- Security Policies
- Security monitoring

Network security

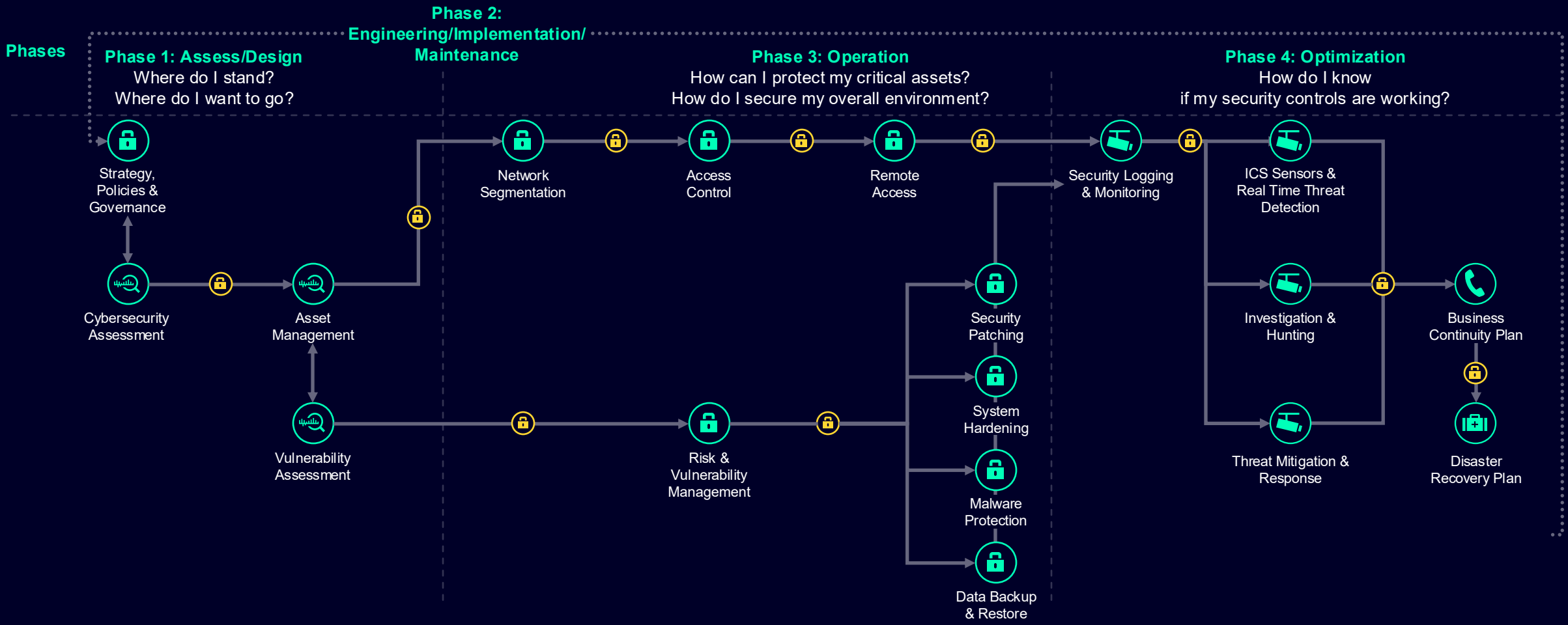
- Cell protection, perimeter network, and trusted zones
- Firewalls and VPN
- Zero trust

System integrity

- System hardening
- Patch management
- Authentication and access protection

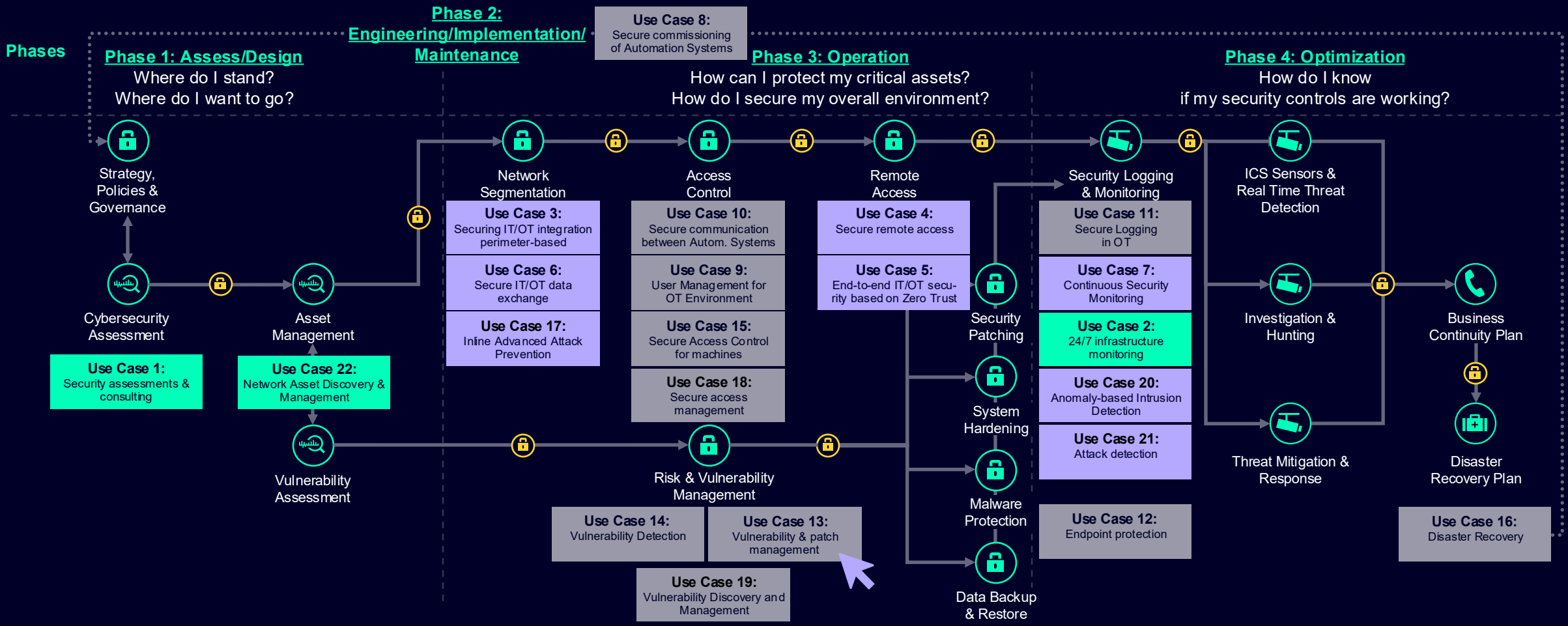
SIEMENS

Cybersecurity step by step



SIEMENS

Siemens supports you throughout the whole customer process with Defense in Depth concept



SIEMENS

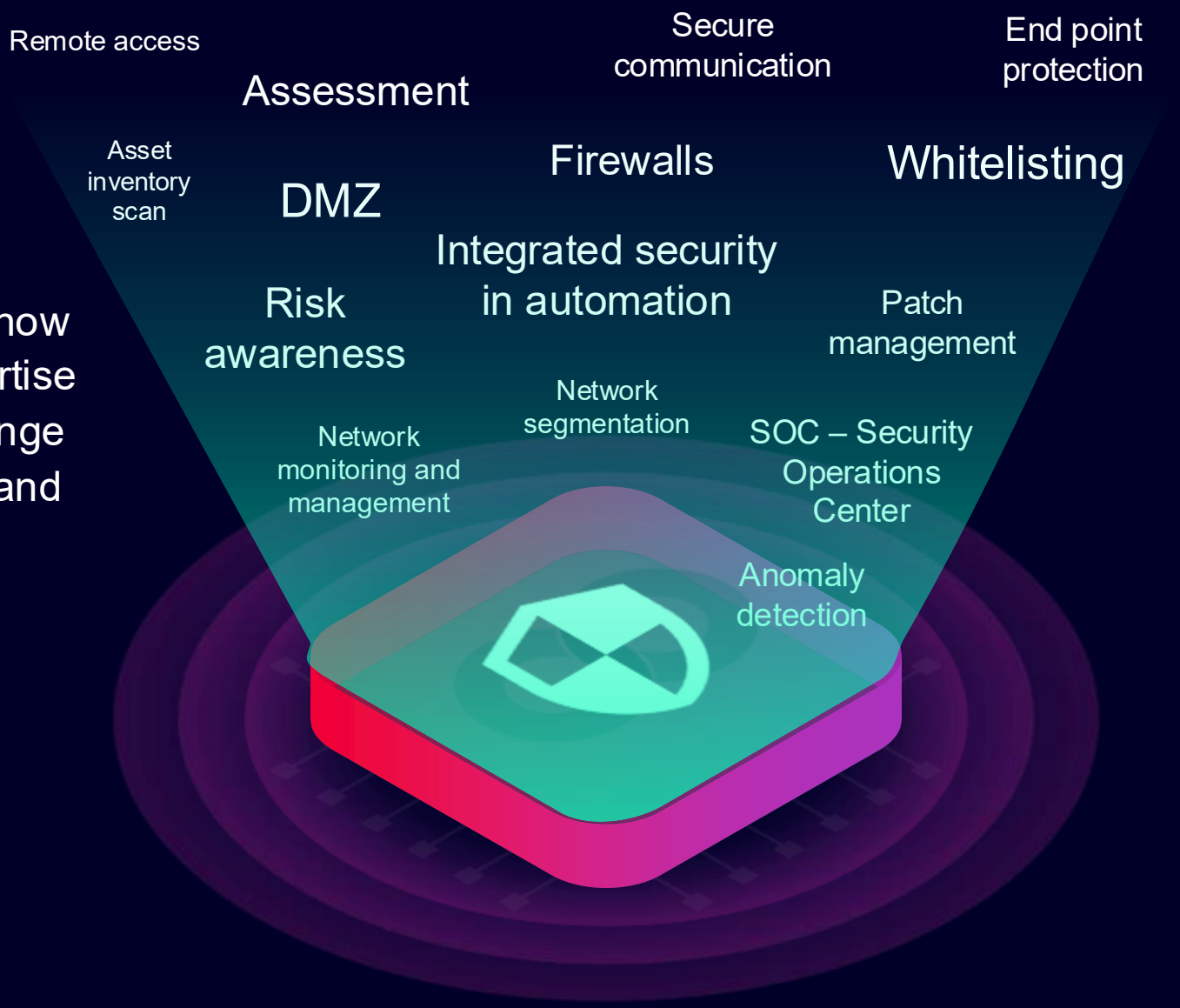
The convergence of IT and OT

Including **secure handling of data** vertically for the successful fusion of IT and OT.

SIEMENS

Complete Cybersecurity for Industry offering

In-depth domain know-how and cybersecurity expertise combined in a broad range of hardware, software, and services for industrial security.

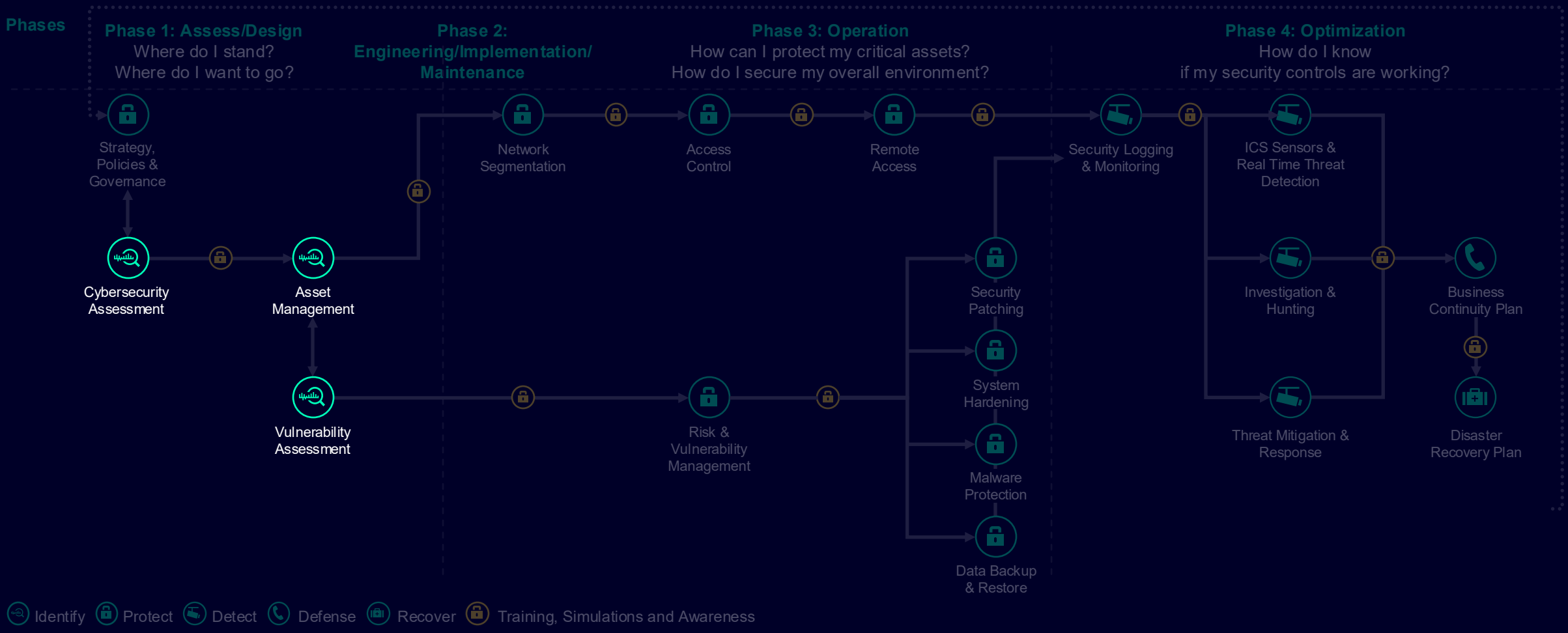


SIEMENS

Siemens multi-layered Defense in Depth concept
– SINEC Security Inspector positioning

SIEMENS

Siemens Cybersecurity step by step approach – SINEC Security Inspector positioning



SIEMENS

SINEC Security Inspector „in a nutshell“

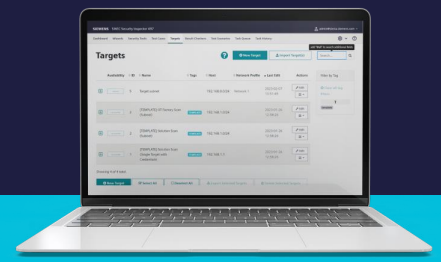
Asset Identification

Vulnerability Scanner

SINEC Security Inspector

Malware Scans

Compliance check

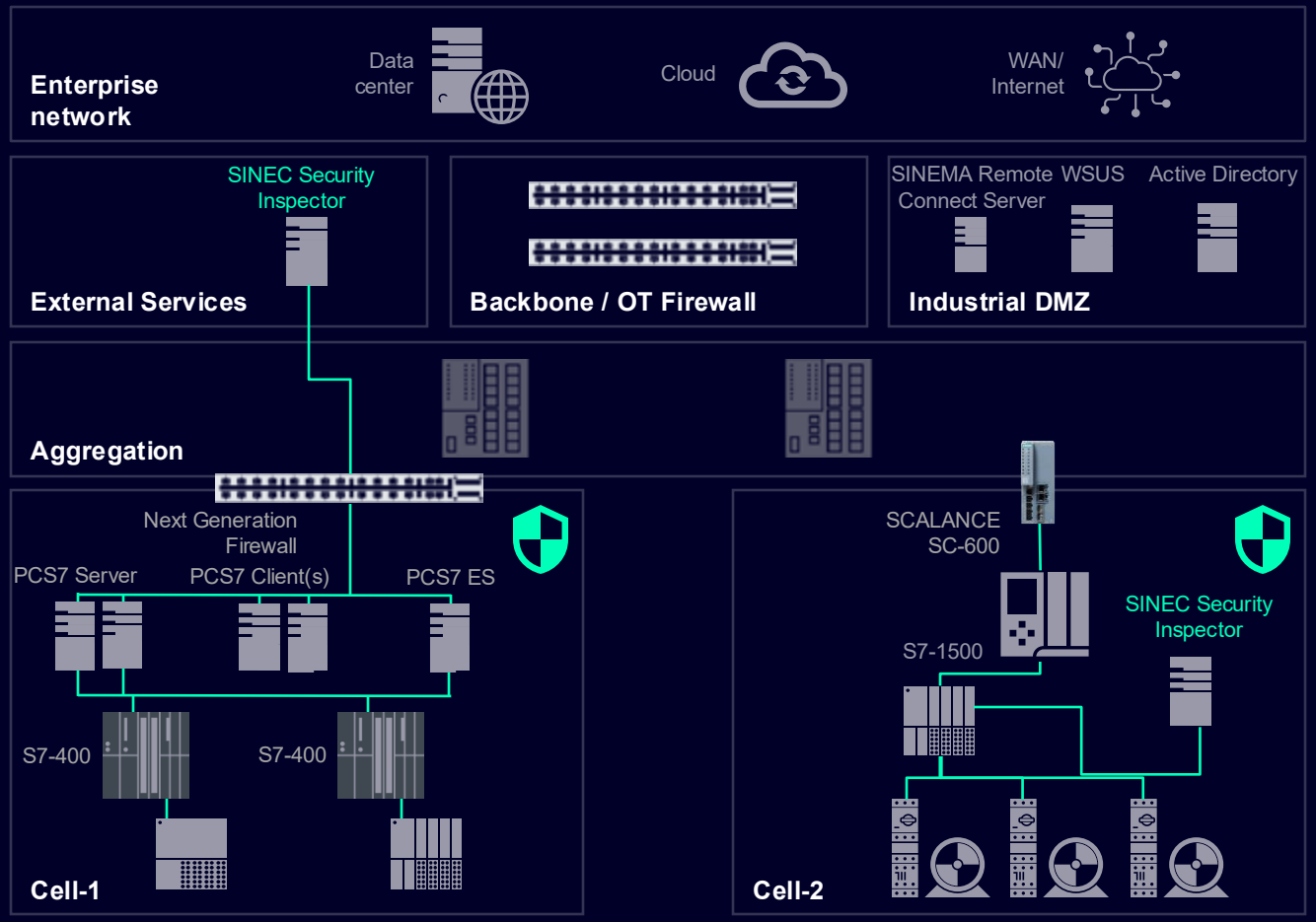


SINEC
Security Inspector

Active, on-prem security scanning of components or networks

SIEMENS

SINEC Security Inspector
Active, on-prem security scanning of components or networks



Technical Solution

- Rapid asset transparency and in-depth data for Siemens OT products, like lifecycle/patch information and advisories.
- Detection of OT & IT vulnerabilities based on up-to-date vulnerability information e.g., Siemens PSIRT advisories as well as cryptography assessment for transparent view on encryption levels.
- Framework with well selected and proven security tools integrated within a single web interface: Asset and Vulnerability Discovery (OT Scanner), Vulnerability Scan (Nessus), Port Scan (Nmap), Asset Discovery (Hosts, Ping Scan)
- Network scanning for missing security patches and verification of hardening measures.
- Predefined test templates to prepare for compliance with international security standards like IEC 62443.
- Possibility to blacklist specific devices from scans as additional safeguard.
- Two main installation scenarios: As an external service scanning down to cell level or integrated on cell level to scan in depth

SIEMENS

SINEC Security Inspector
Top highlights at a glance

Range of predefined test cases allows to get started easily.

Intuitive web-based user interface that support the complete workflow of security testing. Tailored to OT automation experts.

Scan and test cases are adapted to OT networks matured with the experience of Siemens product CERT community.

Result checker that allows comparable format of the test results independent of the executed test tool.

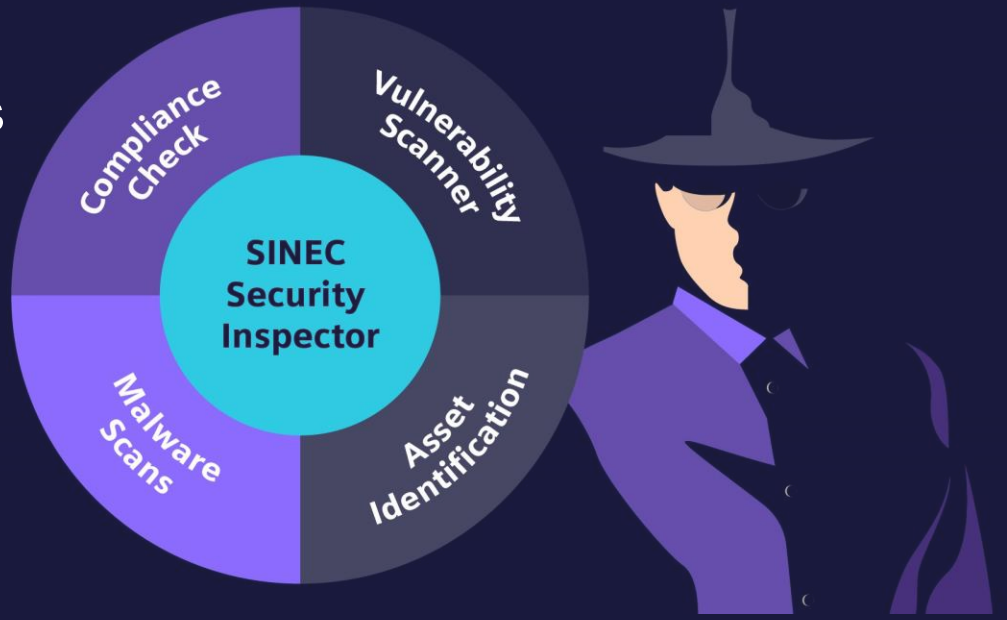
Software offering is accompanied by additional service offering that can be ordered to customized test cases and to interpret results.

SIEMENS

SINEC Security Inspector

Active, on-prem security scanning of components or networks

- Software for active scanning of components or networks (one time) in maintenance windows
- Developed for internal system tests, already in use for internal factories since >7 years
- No additional sensors (hardware) required
- Inspector requires software license (subscription) and optional services

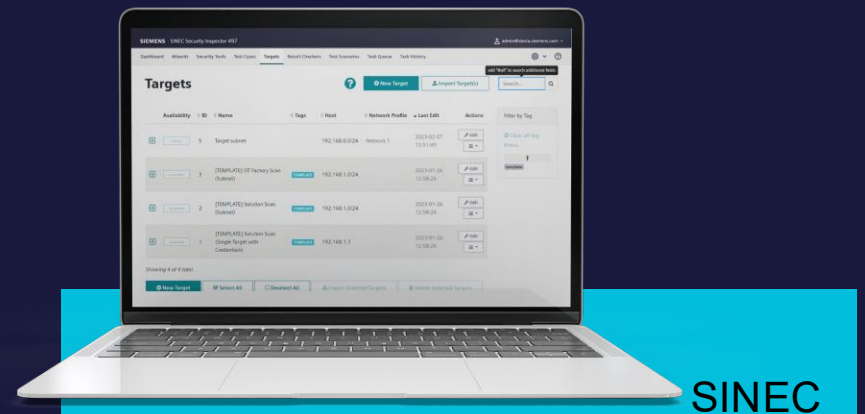


Scheduled Scans Compliance & Vulnerabilities

Outgoing Security Inspection

Incoming Security Inspection

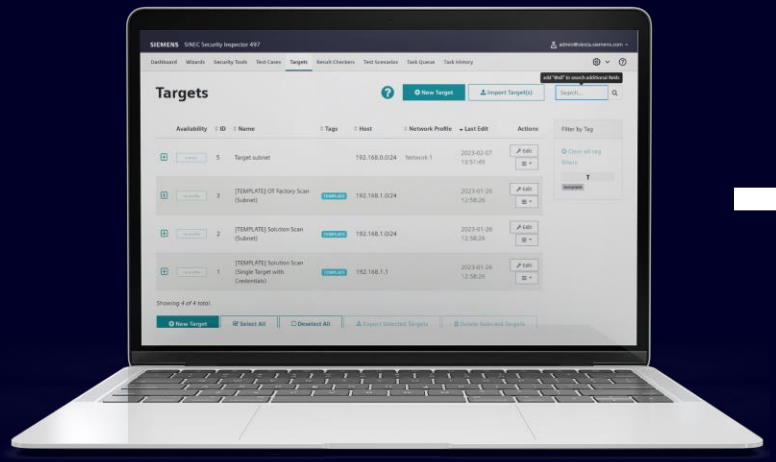
One Time Scan for Security Hardening

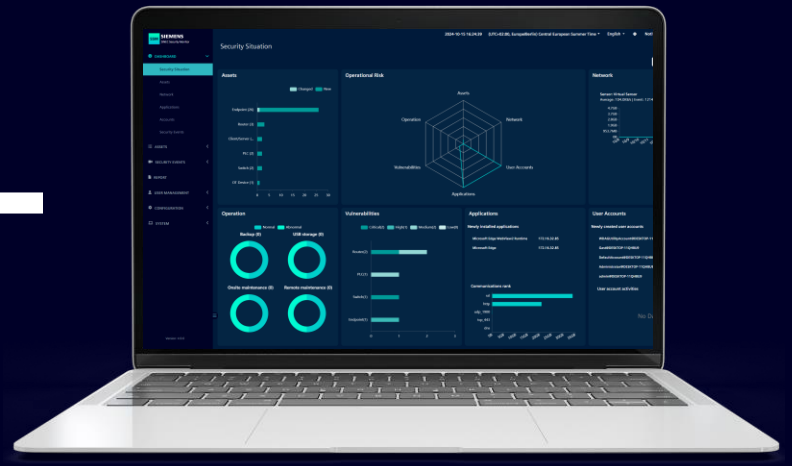


SINEC
Security Inspector

SIEMENS

SINEC Security Software Suite – comprehensive suite of security tools to serve security requirements of our customers.





SINEC Security Inspector

On prem toolbox for active asset detection, acceptance tests and compliance checks

SINEC Security Guard

Cloud-based SaaS for automated vulnerability mapping & security management for non-security experts in OT

SINEC Security Monitor

On prem software for continuous security monitoring incl. passive and active asset detection, vulnerability correlation and intrusion detection.

SIEMENS

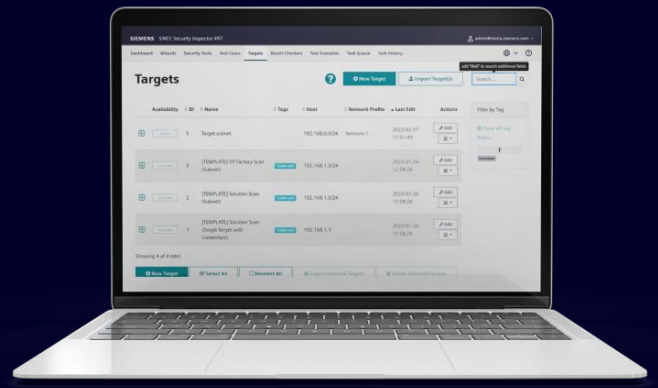
SINEC Security Monitor and Inspector are security software tools for different use cases from passive continuous monitoring to active one time scanning or both.

Monitor in a nutshell

SINEC
Security Monitor

- Software for passive, non-intrusive, continuous on-prem security monitoring during production
- Analysis of network traffic allows anomaly detection and integration into existing Security Information and Event Management (SIEM)
- Developed and used internally by Siemens – from OT experts to OT customers
- Monitor requires hardware (server, sensor, agent), software license (subscription) and services

Asset detection | **Vulnerability detection** | **Anomaly detection** | **SIEM**



- Software for active scanning of components or networks (one time) in maintenance windows
- Developed for internal system tests, already in use for internal factories since >7 years
- No additional sensors (hardware) required
- Inspector requires software license (subscription) and optional services

SINEC
Security Inspector

Inspector in a nutshell

SIEMENS

How does SINEC Security Inspector align within our existing tools?

	SINEC Security Inspector	SINEC Security Monitor	SINEC Security Guard
Deployment Model	On premise solution	On premise solution	Cloud-based solution
Focus application	Asset and vulnerability identification	Security monitoring and intrusion detection	Vulnerability Management/ Risk-based Security Evaluation
Asset detection	Active	Passive/ Active Probing	Import functionality
Range of information	Vendor independent	Vendor independent	Only Siemens Assets (Vendor independent assets later in CY2024)
Configuration weakness detection	● ● ●	-	-
Vulnerability detection	● ● ●	● ● ○	● ● ◐
Vulnerability management (Tasks & Patch)	-	-	● ● ●
Security Evaluation	● ○ ○	● ○ ○	● ● ●
Attack detection (signature based)	-	● ● ●	● ● ●
Attack detection (signature less)	-	● ● ●	-
Compliance testing	● ● ●	● ● ●	-
Interfaces	Standard interfaces to share asset information	OT SIEM functionalities with the possibility to integrate into IT SIEM	REST-API

SIEMENS

Use cases

Automation Applications for Data Center

Integrated Data Center Management

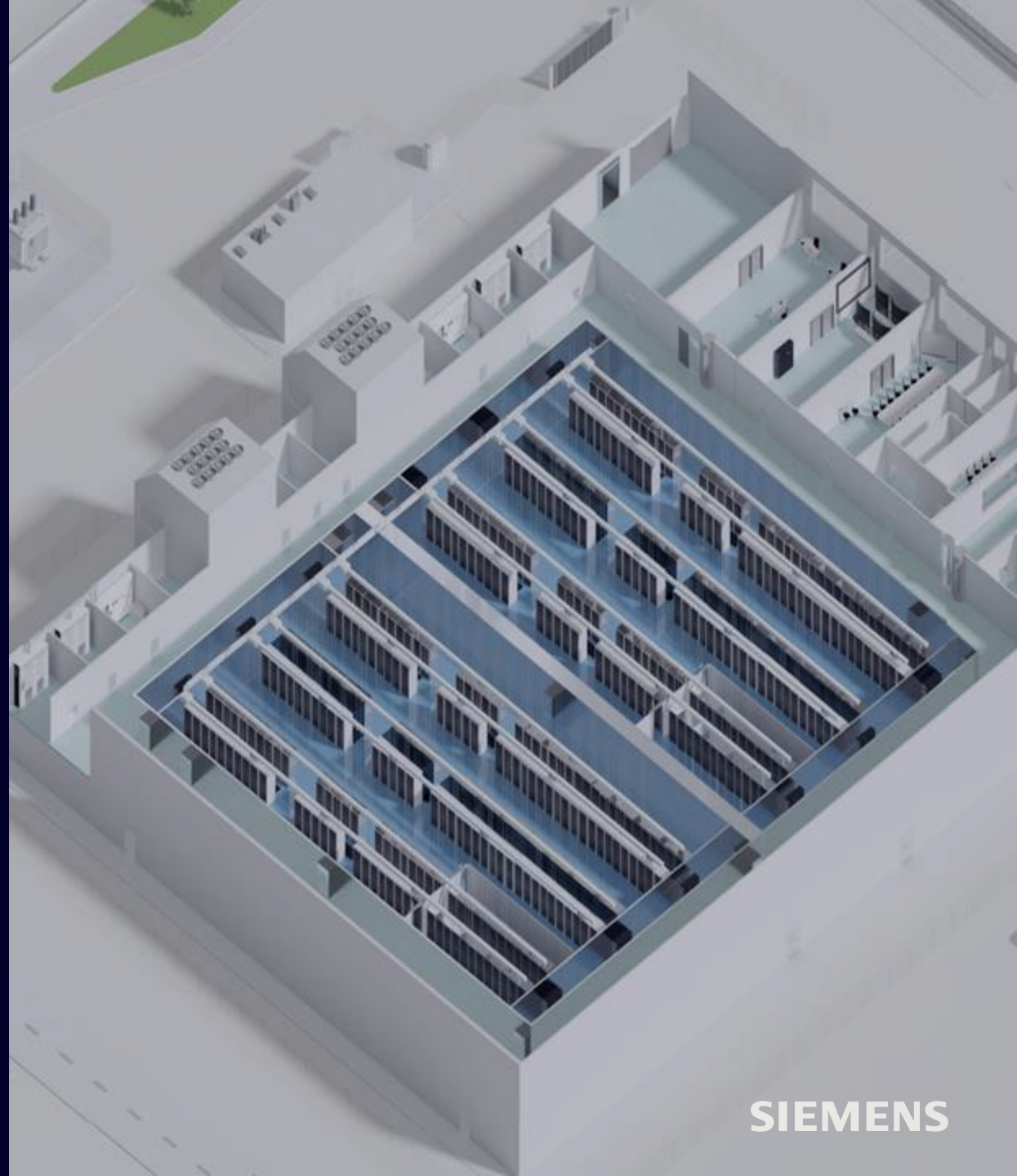
- EPMS
- BMS

Data Center Applications

- Preconfigured data center for industrial plants
- Predictive maintenance
- Digital Twin
- Thermal Design
- Energy monitoring
- Understanding PCF

OEM Applications

- Liquid cooling OEMs
- HVAC OEMs



SIEMENS

Integrated Data Center Management

Cyber Security

Standardization

High Availability

Safety Integrated

Reliability

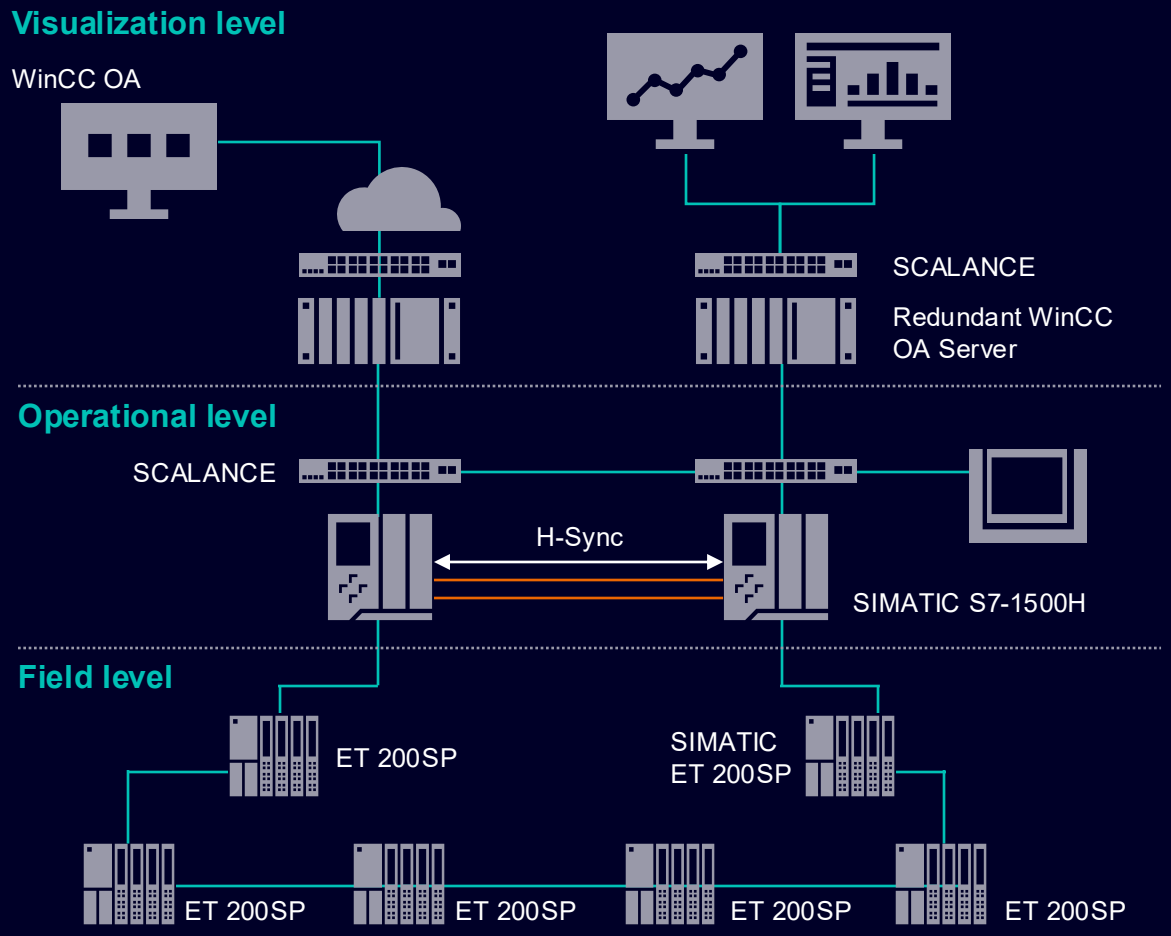
Efficiency

Maintainability

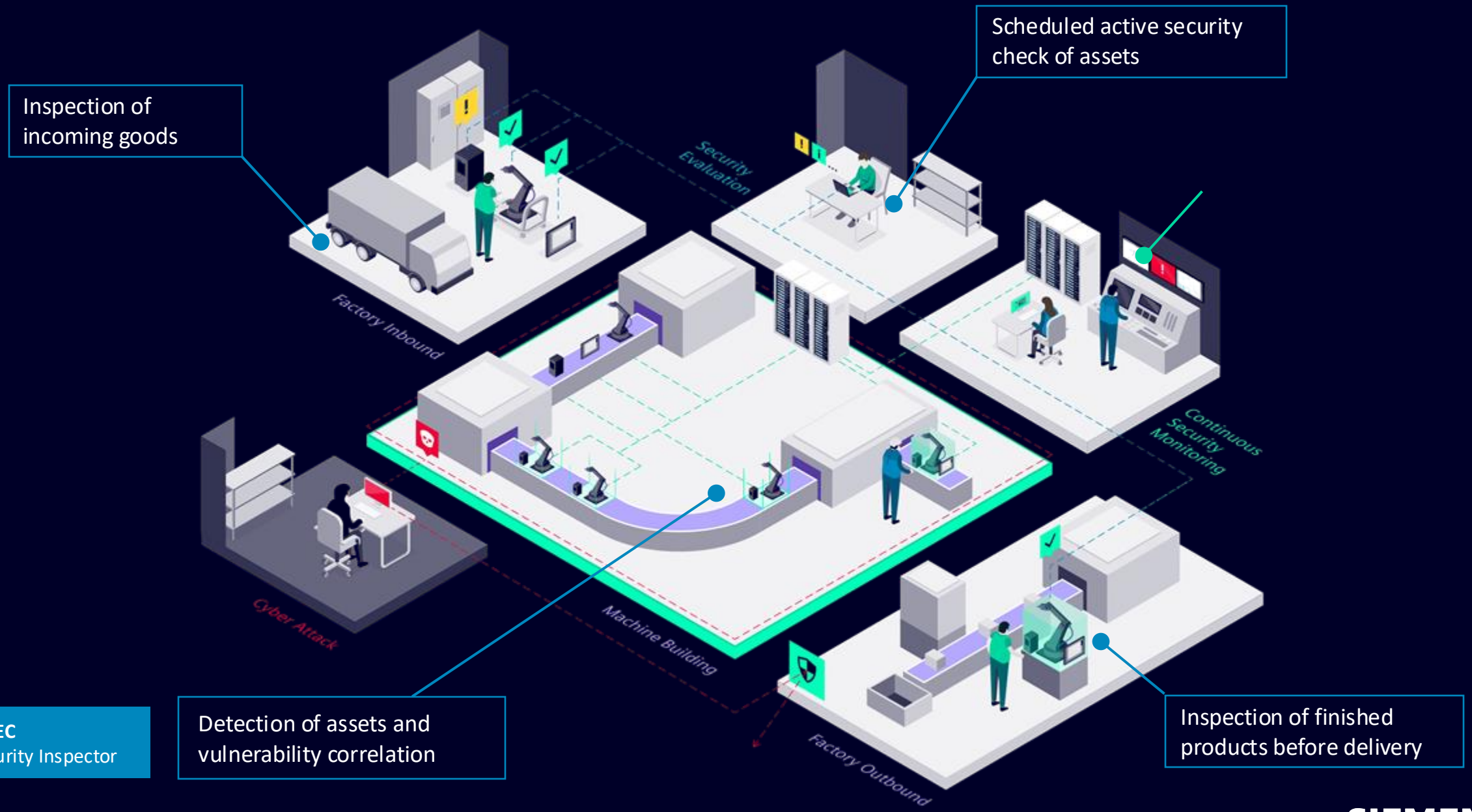
Innovative

Sustainability

Scalable



SIEMENS



SINEC
Security Inspector

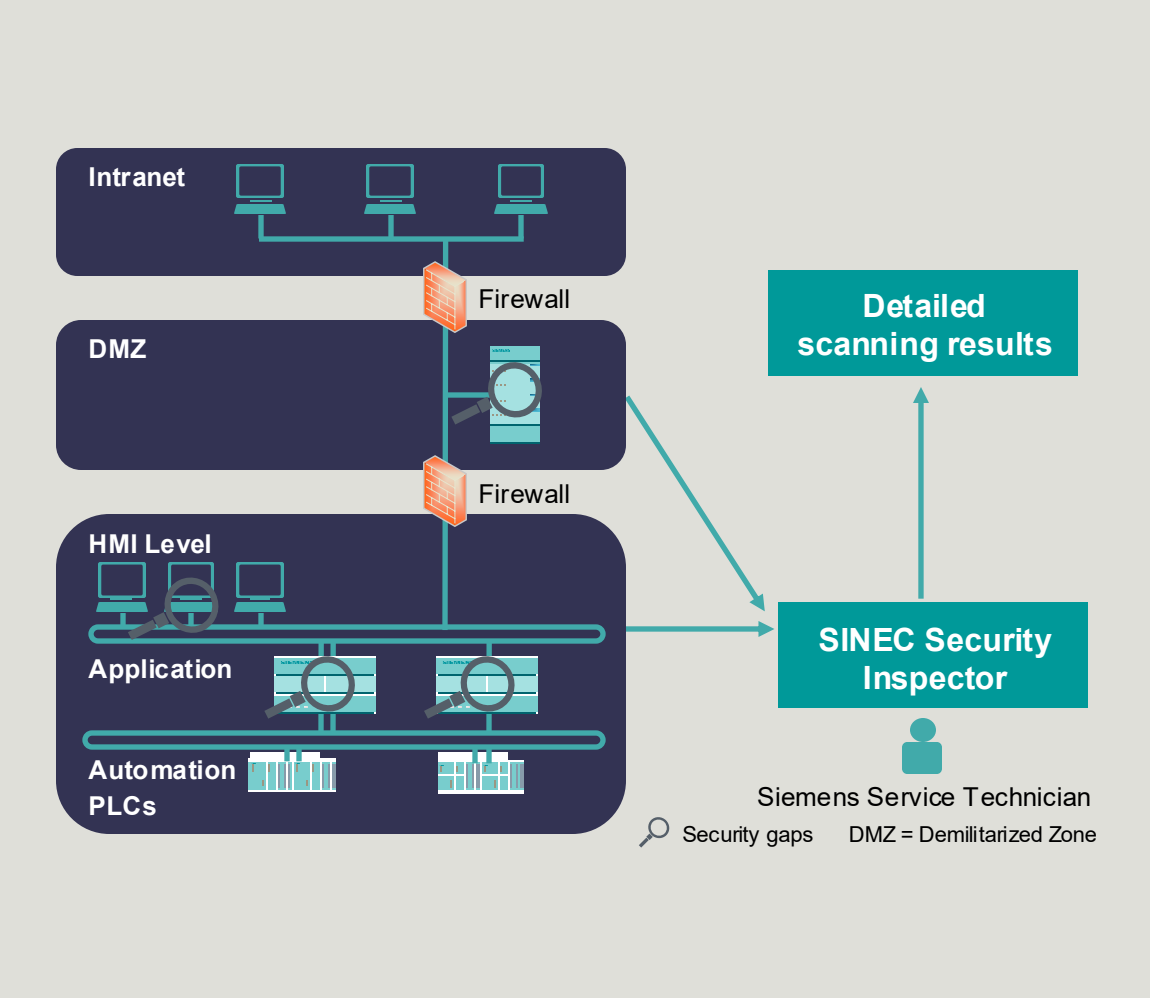
SIEMENS

SINEC Security Inspector
Use case: Asset identification/detection

Task
A factory structure with different machine providers using a vast vendor variety has been grown over years. This generates the demand to gain transparency and system identification within the factory environment to ensure a total cyber security approach.

Solution
SINEC Security Inspector offers a framework performing different possibilities to identify assets. This bandwidth of usable protocols increases the identification rate, especially for OT specific assets.

Benefits
- Discover multi-vendor assets of the entire network.
- Asset information can be shared with external systems using software interfaces (REST API) or the possibility of exports in standardized formats.
- Possibility of soft/non-intrusive OT optimized scans, which are also supporting OT specific communication protocols.

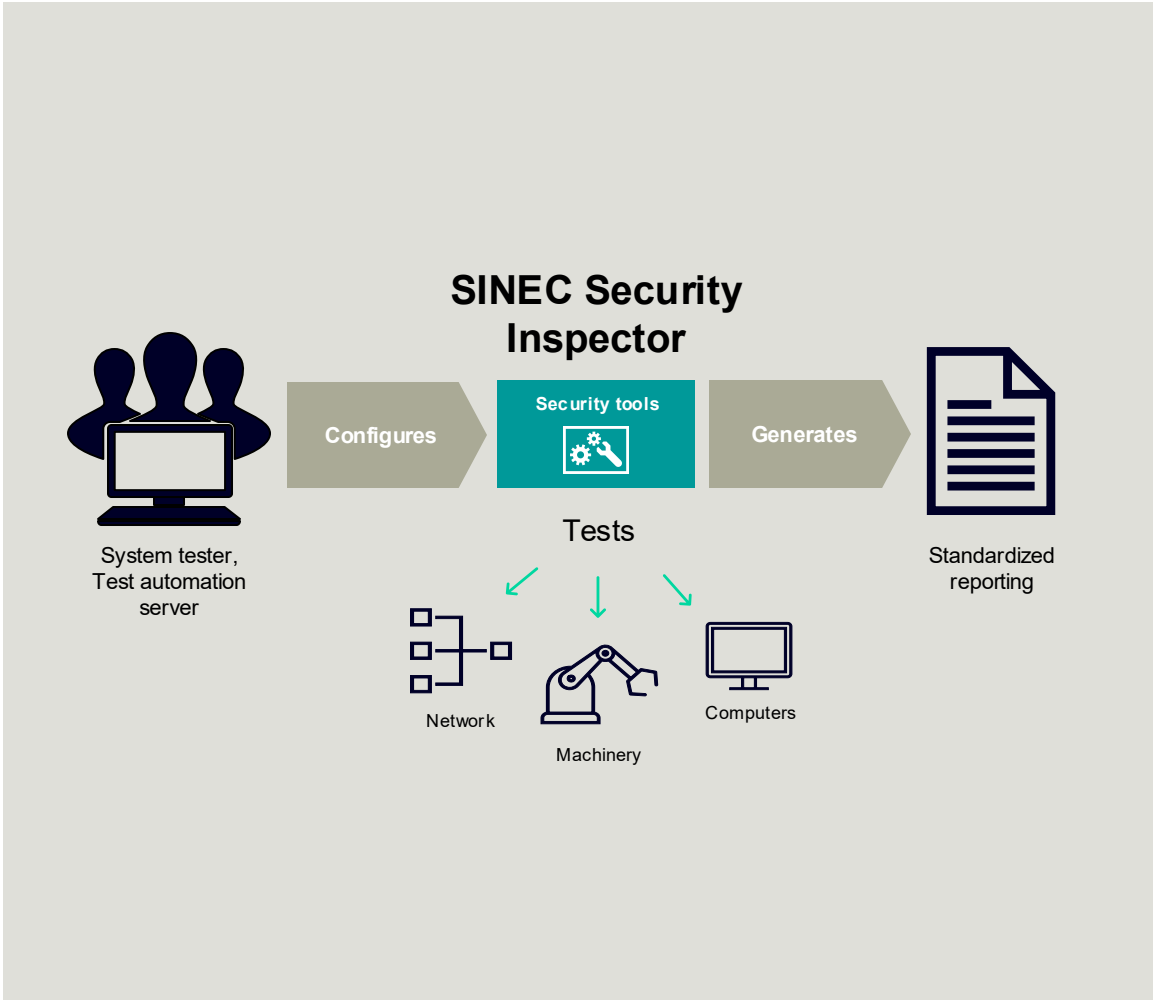


SINEC Security Inspector
Use case: Vulnerability identification

Task
A factory structure with different machine providers using a vast vendor variety is the basis. To ensure a cybersecurity concept asset transparency and a dedicated vulnerability management is needed. On top of this, a centralized patch monitoring is missing as well.

Solution
SINEC Security Inspector offers a framework performing different test cases to identify vulnerabilities. According to these found vulnerabilities mitigation proposals are made to increase the overall cybersecurity.

Benefits
- Discover multi-vendor vulnerabilities of the entire network.
- Vulnerability information can be shared with external systems using software interfaces (REST API), the possibility of exports in standardized formats or summarized vulnerability reports.
- Up to date solution proposals to mitigate discovered vulnerabilities.



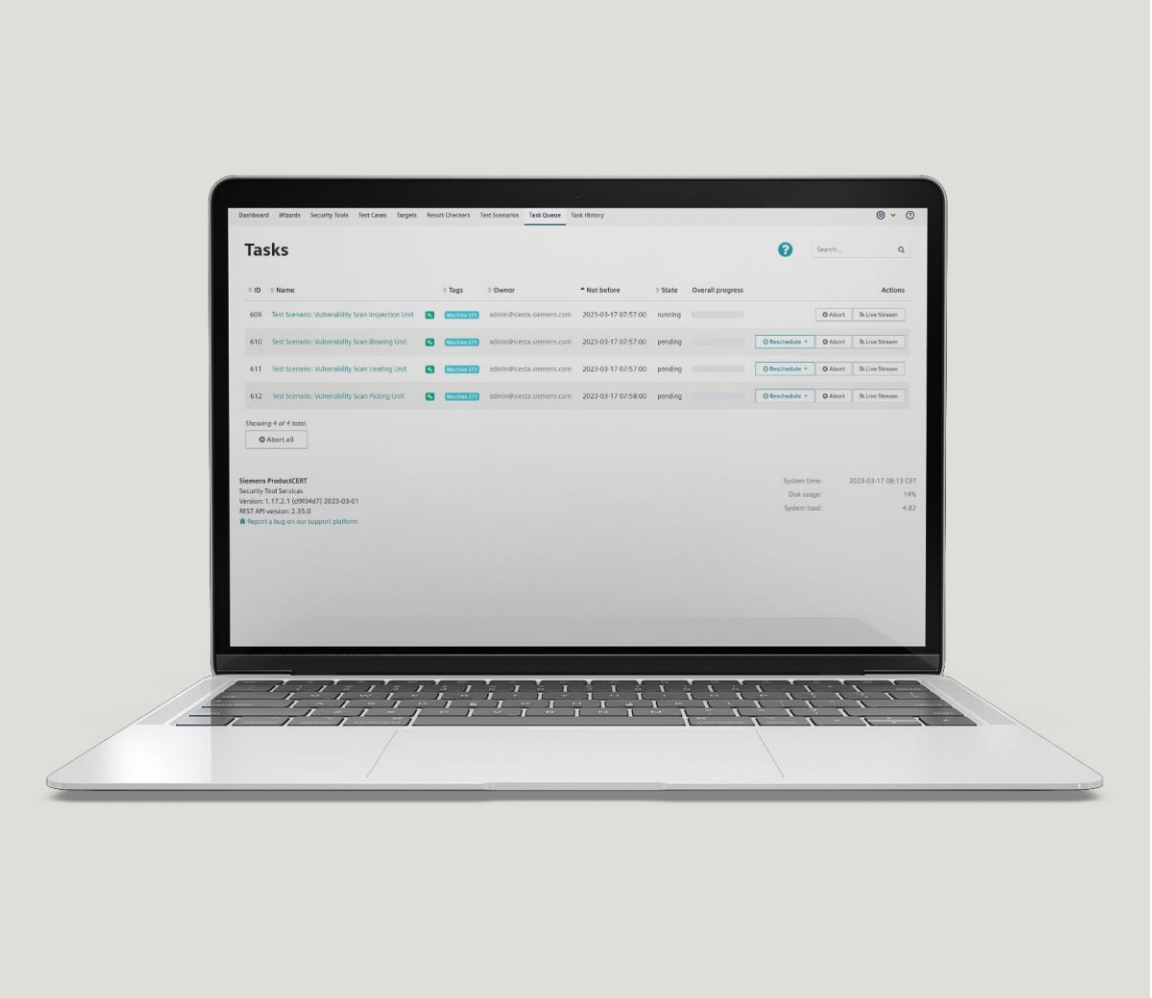
SIEMENS

SINEC Security Inspector
Use case: Compliance Check/Testing

Task
The factory shop floor contains machines from different suppliers. This whole diverse machine infrastructure needs to be compliant with the cybersecurity requirements coming from company IT, customers or public regulations.

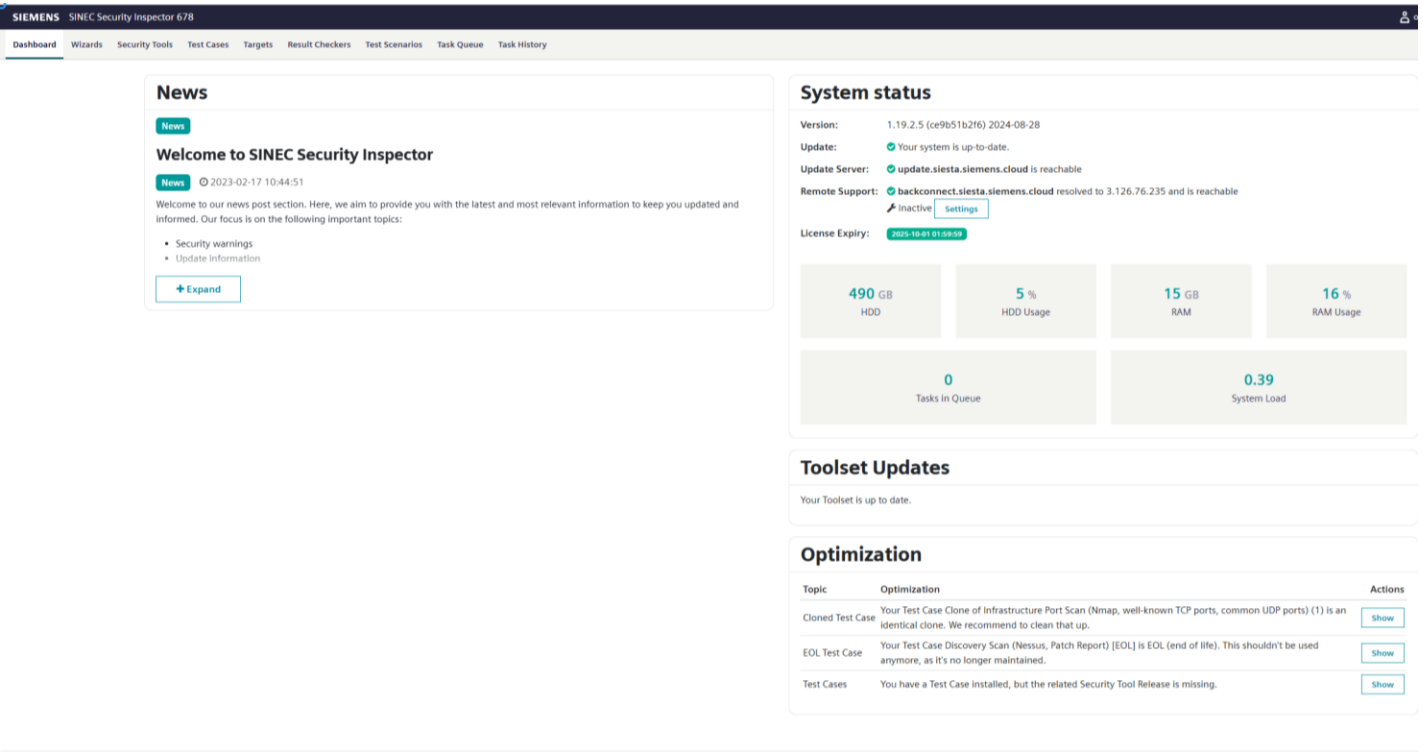
Solution
SINEC Security Inspector offers different tools and supports a range of protocols for a variety of cybersecurity tests to be performed on single products, complex machines or even a larger network environment. Thereby SINEC Security Inspector will support the customer with the implementation of FAT/SAT, compliance measures according to CERT plans or their own defined cybersecurity needs as well as public and governmental regulations.

Benefits
- Cybersecurity test scenarios adjustable to company standards.
- Implement or improve cybersecurity audits for OT with a testing tool designed for the needs of OT.
- Proof of compliance with end customer network and device security requirements with standardized results from the cybersecurity testing.



Product Demo
UI screenshots

SINEC Security Inspector Main Page

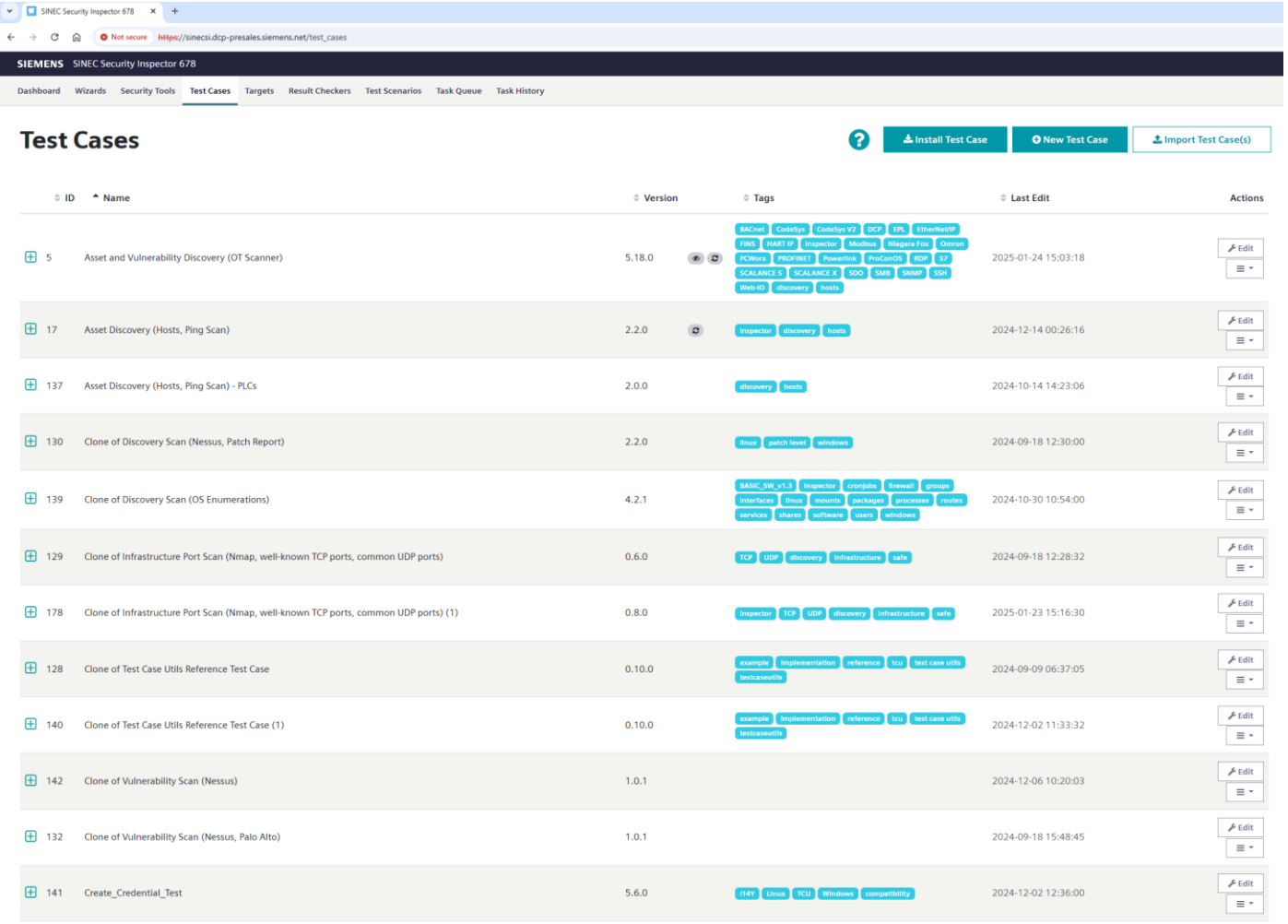


SINEC Security Inspector provides an easy to use entry page to navigate to the required Functions

- Wizards
- Security Tools
- Test Cases
- Result Checker
- Test Scenarios
- Task Queue and
- Task History

SIEMENS

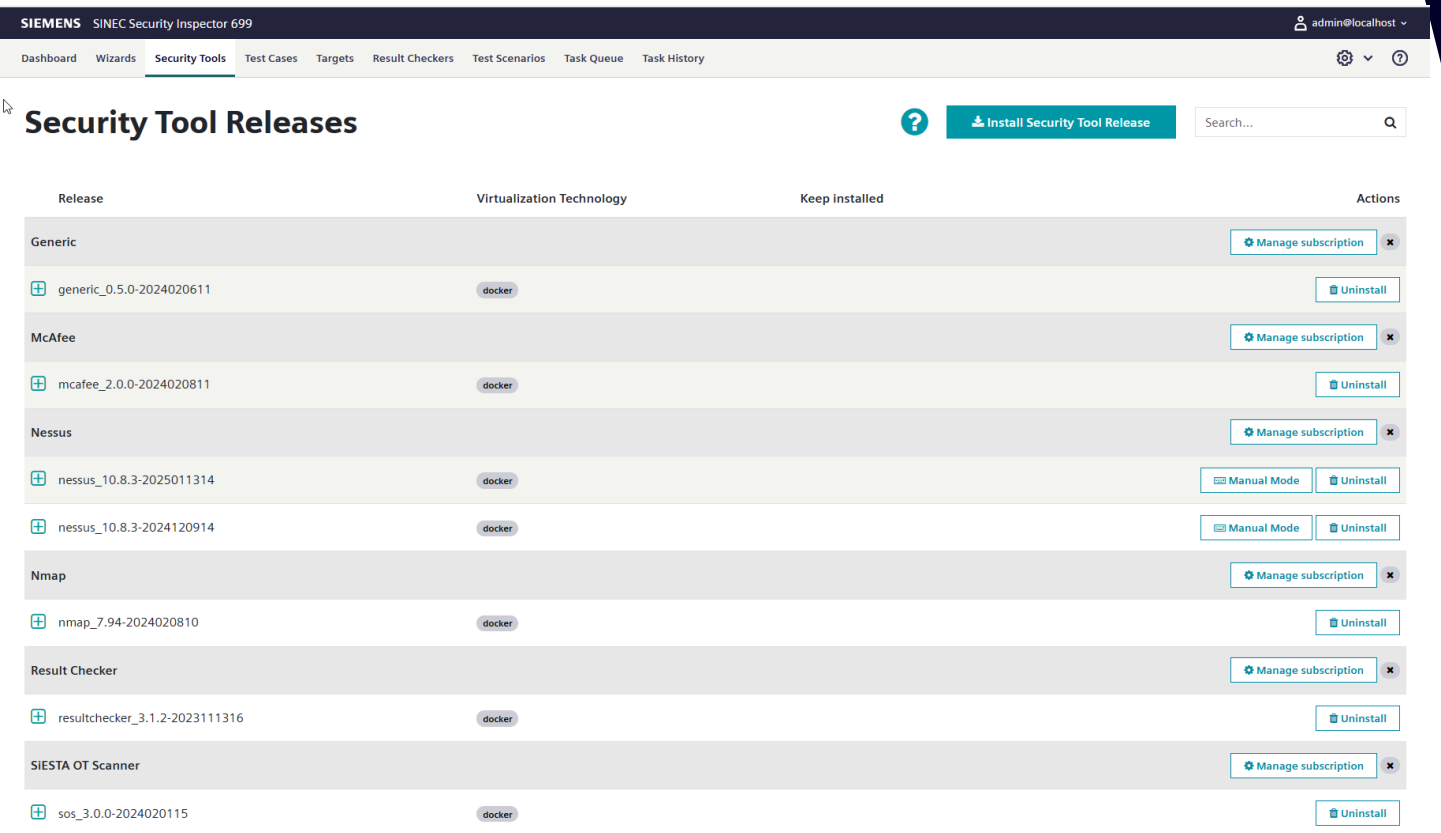
Test Cases



All available Test Cases are listed within this tab with additional information based on your personal tagging.

SIEMENS

Security Tool Releases



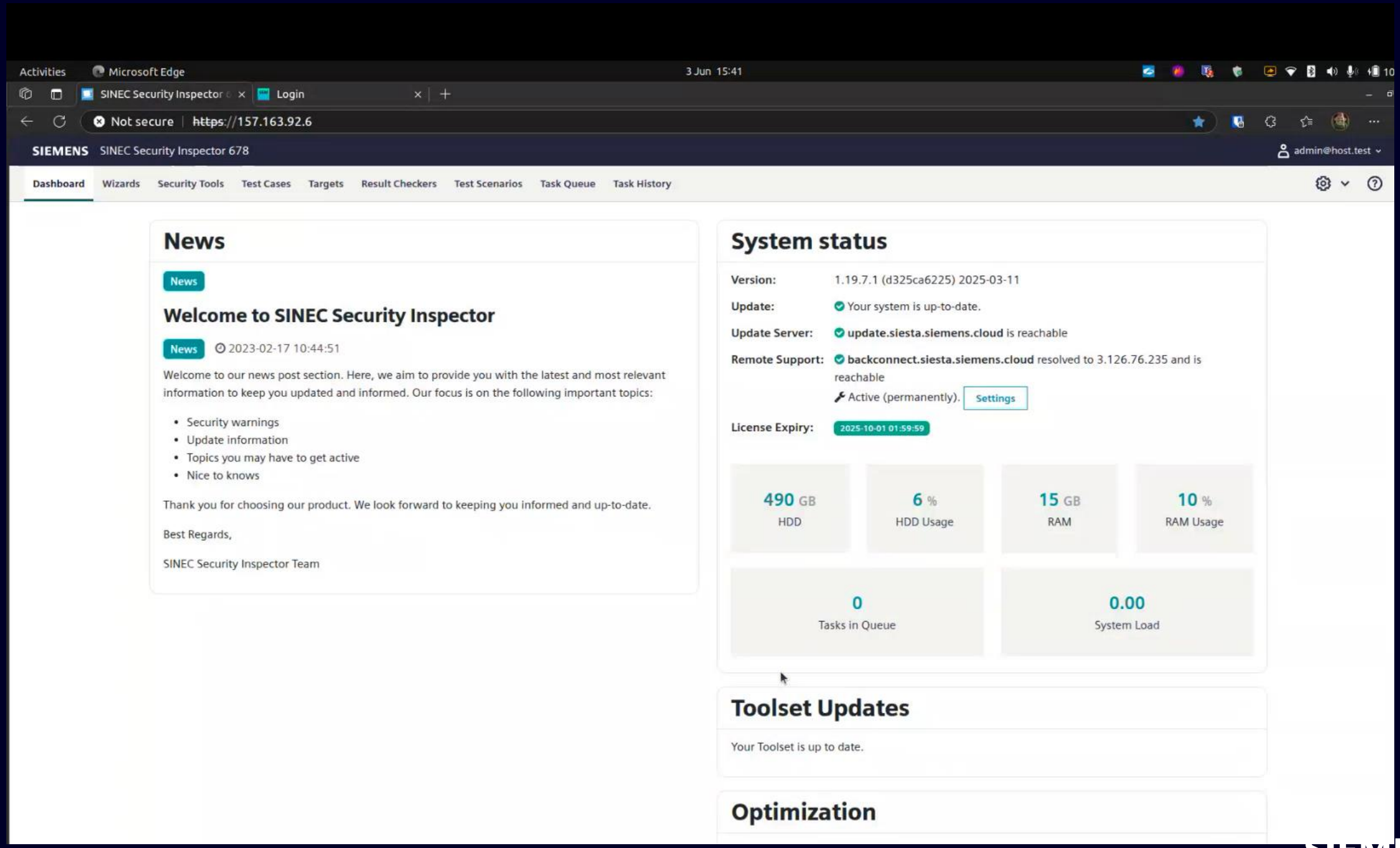
In this overview there are all installed security tools listed.

SIEMENS

PDF Report

PDF Report to summarize the Inspector findings

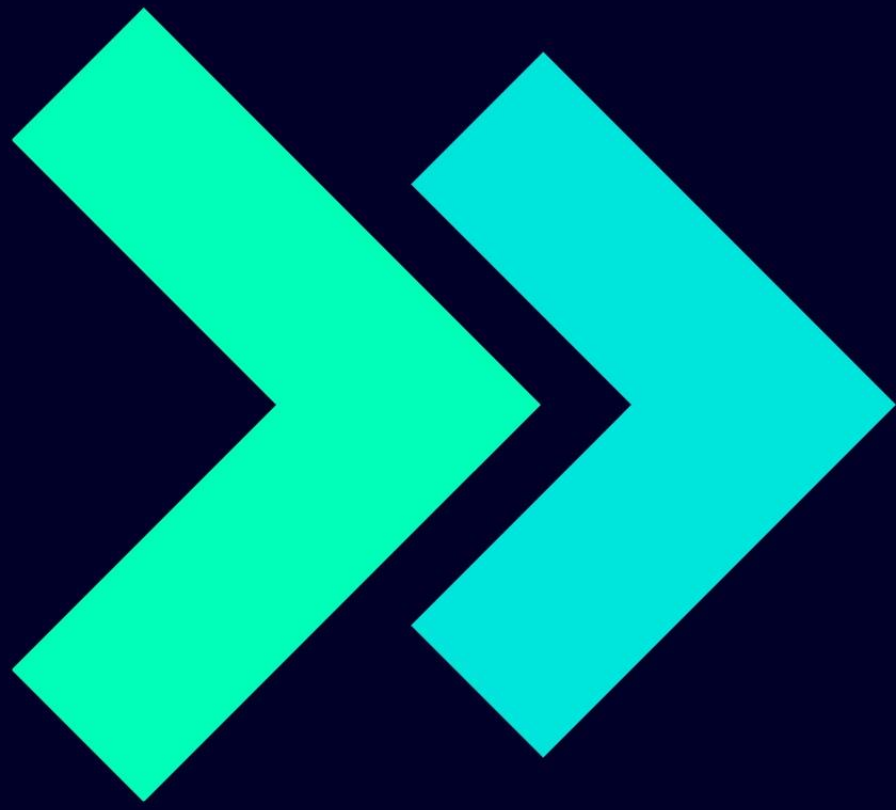
SIEMENS


Activities
Microsoft Edge
3 Jun 15:41
SINEC Security Inspector
Login
Not secure | https://157.163.92.6
SIEMENS SINEC Security Inspector 678
admin@host.test
Dashboard
Wizards
Security Tools
Test Cases
Targets
Result Checkers
Test Scenarios
Task Queue
Task History
News
News
Welcome to SINEC Security Inspector
News
2023-02-17 10:44:51
Welcome to our news post section. Here, we aim to provide you with the latest and most relevant information to keep you updated and informed. Our focus is on the following important topics:
Security warnings
Update information
Topics you may have to get active
Nice to knows
Thank you for choosing our product. We look forward to keeping you informed and up-to-date.
Best Regards,
SINEC Security Inspector Team
System status
Version: 1.19.7.1 (d325ca6225) 2025-03-11
Update: Your system is up-to-date.
Update Server: update.siesta.siemens.cloud is reachable
Remote Support: backconnect.siesta.siemens.cloud resolved to 3.126.76.235 and is reachable
Active (permanently).
Settings
License Expiry: 2025-10-01 01:59:59
490 GB
HDD
6 %
HDD Usage
15 GB
RAM
10 %
RAM Usage
0
Tasks in Queue
0.00
System Load
Toolset Updates
Your Toolset is up to date.
Optimization

SIEMENS

Accelerate NextGen

OBRIGADO



Contactos:

Sónia Palma

sonia.palma@siemens.com
91 010 72 99

António Castro

antonio.ascencao_castro@siemens.com
91 038 95 89

SIEMENS