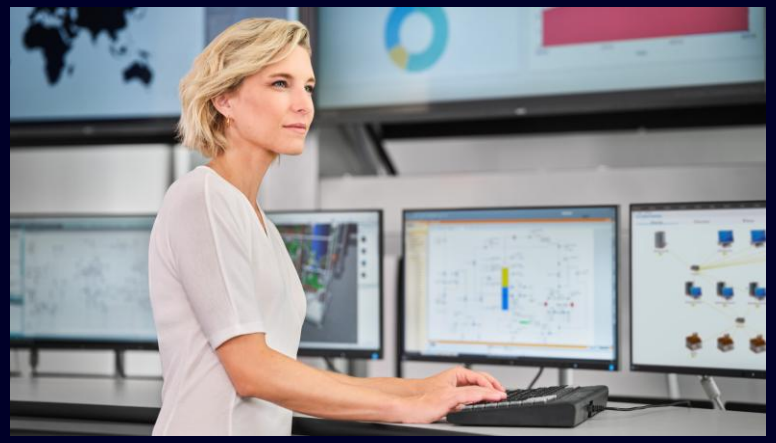
Remote Industrial Operations Services

Presentation

SIEMENS

24/7 managed services for your IT/OT infrastructure
with Remote Industrial Operations Services



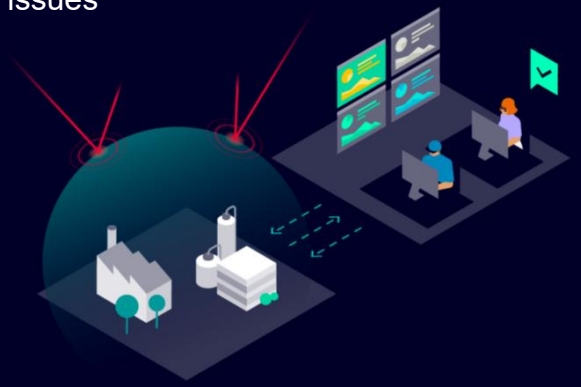
Increasing IT/OT system complexity, lack of resources & cyber threats are major risks for productivity losses in operational technology.

With Remote Industrial Operations Services, you have a team of proven experts who remotely monitor and manage your IT/OT infrastructure 24/7, allowing you to focus on your core business.

Solution and Service

The modular contracting enables you to select only the services you need:

- 24/7 monitoring of IT/OT Infrastructure to prevent downtime
- Managed security services and SOC as a Service for continuous protection against cyber threats
- Proactive identification of maintenance needs in your IT/OT infrastructure and spare parts provision to maximize uptime
- Expert IT and OT technical support from one source to rapidly resolve issues



Your value

Proven IT/OT expertise by our experts

Operational continuity through 24/7 remotely managed IT/OT infrastructure

Compliance with cybersecurity regulations (e.g., NIS 2)

SIEMENS

How do you ensure the operational continuity and security of your IT/OT environment?

SIEMENS

Challenge

IT/OT complexity, resource constraints and cybersecurity threats pose significant risks to operational continuity. Even the failure of the simplest component can lead to a domino effect, causing operational downtime.
Is there a solution?

How to deal with the **increasing gap between IT and OT?**

How to manage the **aging expertise and lack of resources?**

How to avoid **unplanned maintenance and downtime?**

How to face the **lack of compliance with OT security requirements?**

SIEMENS

IT-OT convergence promised a solution.
Why has this been difficult to achieve in practice?

Information Technology

IT Priorities + OT Priorities

Security + Availability

Operational Technology

Confidentiality

Integrity

Availability

Storage

Computing

Infrastructure

Gigabytes

Connected Factory Operations

Machines

Equipment

Industrial Controls

Milliseconds

Safety

Availability

Integrity

Confidentiality

SIEMENS

IT/OT Challenges, Risks and Impacts

Challenges

46% **Resources**

of companies point to limited resources as the biggest challenge in managing OT risk.

ComputerWeekly.com

25% **IT/OT Gap**

of companies say modernizing IT and OT workflows is a collaborative process between both teams

Forrester

2024 **Compliance**

Is the year that all important entities within the member States need to show compliance. In case of non-compliance: a maximum fine of at least € 7,000,000 or at least 1,4% of the total worldwide annual turnover.

European Parliament

Risks

25 **Unplanned Downtime**

hours a month of unplanned downtime for the average plant

Senseye

61% **Cyber Threats**

of smart factories have experienced a cybersecurity incident

Manufacturing Automation

Impacts

Decreased Productivity

- Decreased capacity
- Higher costs
- Production loss

Lack of Compliance

- Cybersecurity hacks & ransomware
- Regulatory penalties and fines

Customer Dissatisfaction

- Negative brand reputation
- Loss of competitive advantage

Stakeholder Concerns

- Investor profitability concerns
- Erosion in stakeholder value

ComputerWeekly.com | A lack of skills and ownership are top challenges to OT security; Forrester | Use IT And OT Integration As A Lever For Digital Transformation; European Parliament | Article 34; Senseye | The True Cost of Downtime 2022; Manufacturing Automation | 61% of manufacturers have had a cybersecurity incident;

SIEMENS

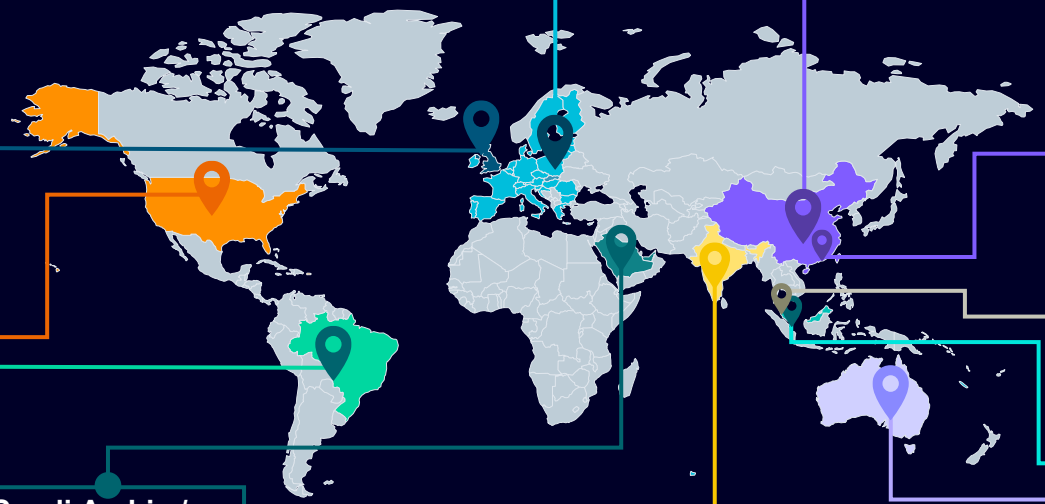
OT Cybersecurity Legislation
Relevant global frameworks

Europe
- Revised Directive on Security of Network and Information Systems (NIS 2)
- Cybersecurity Act (CSA)
- Cyber Resilience Act
- EU Data Act
- Specific vertical requirements, e.g., DORA [1], PSD2 [2], MDR [3]
- Specific technical requirements, e.g., AI Act, Post-quantum cryptography standard

UK with Brexit influence following NIS1 and developing own Cyber Security and Resilience Bill (CS&R)

USA
- Executive orders (e.g., EO 14028)
- IoT Cybersecurity Improvement Act
- Federal and State Laws (e.g., California CCPA [4])
- Specific vertical requirements, e.g., CIRCIA [5], HIPPA [6], GLBA [7]

Brazil Cybersecurity requirements for products with internal connection



Saudi Arabia / UAE ECC [8] issued by NCA [9] for government entities and critical infrastructure

- **India** Increased regulatory activities
- National Critical Information Infrastructure Protection
- Certification and labelling requirements in some key sectors (e.g., power grid)

China
- Cybersecurity Law, Data Security Law, Personal Information, Protection Law (PIPL), Cryptography Law
- Specific technical requirements, e.g., GB/T 40050, GB/T 29246

Hong Kong Critical Infrastructure (CS) Bill for the protection of critical information infrastructure full implementation by 2026

Singapore Cyber Security Act (CSA) protection of critical information infrastructure

Malaysia National Cyber Security Agency ("NACSA") and Cyber Security Act 2024 (Act 854)

Australia mandatory cybersecurity directive for critical infrastructure, SoCI Act 2018

1) DORA: Digital Operational Resilience Act; 2) PSD2: revised Payment Services Directive; 3) MDR: Medical Device Regulation 4) CCPA: California Consumer Privacy Act; 5) CIRCIA: Cyber Incident Reporting for Critical Infrastructure Act; 6) HIPPA: Health Insurance Portability and Accountability Act; 7) GLBA: Gramm-Leach-Bliley Act; 8) EEC: Essential Cybersecurity Controls; 9) NCA: National Cybersecurity Authority

SIEMENS

24/7 Managed Services

Remote Industrial Operations Services

SIEMENS

What are Remote Industrial Operations Services?

Our Operations Center takes care of…..

24

Availability

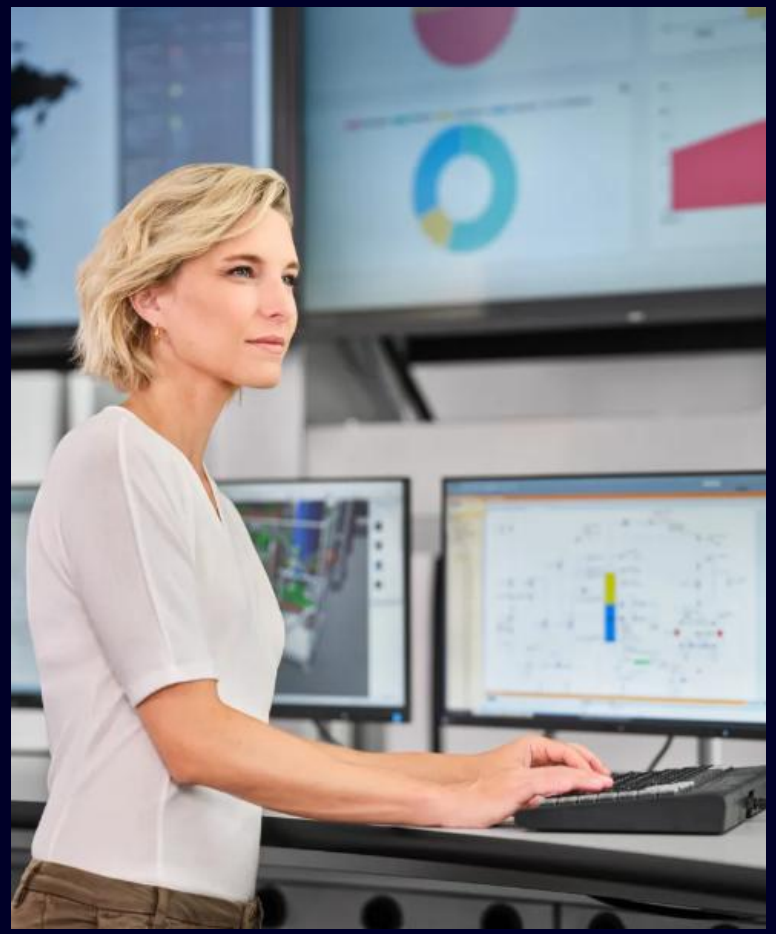
Maintenance

Security

Support

SIEMENS

Secure and reliable plant operations
with Remote Industrial Operations Services

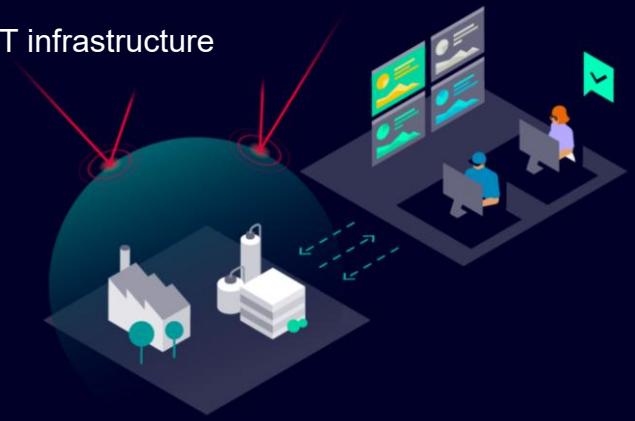


Solution and Service

With Remote Industrial Operations Services, you have a team of proven experts behind you that proactively takes care of your plant's security and operational continuity. You don't need to build up your own resources and specialized know-how to manage your IT/OT infrastructure and cybersecurity. As your partner we provide 24/7 remote monitoring and modular managed services for your IT/OT infrastructure allowing you to focus on your core business.

The modular contracting of Remote Industrial Operations Services enables you to select only the services you need:

- **24/7 monitoring** of IT/OT infrastructure to prevent downtime
- **Managed security services and SOC as a Service** for continuous security monitoring and management to protect you against cyber threats
- **Proactive identification of maintenance needs** in your IT/OT infrastructure and spare parts provision to maximize uptime
- **Expert IT and OT technical support** from one source to rapidly resolve issues



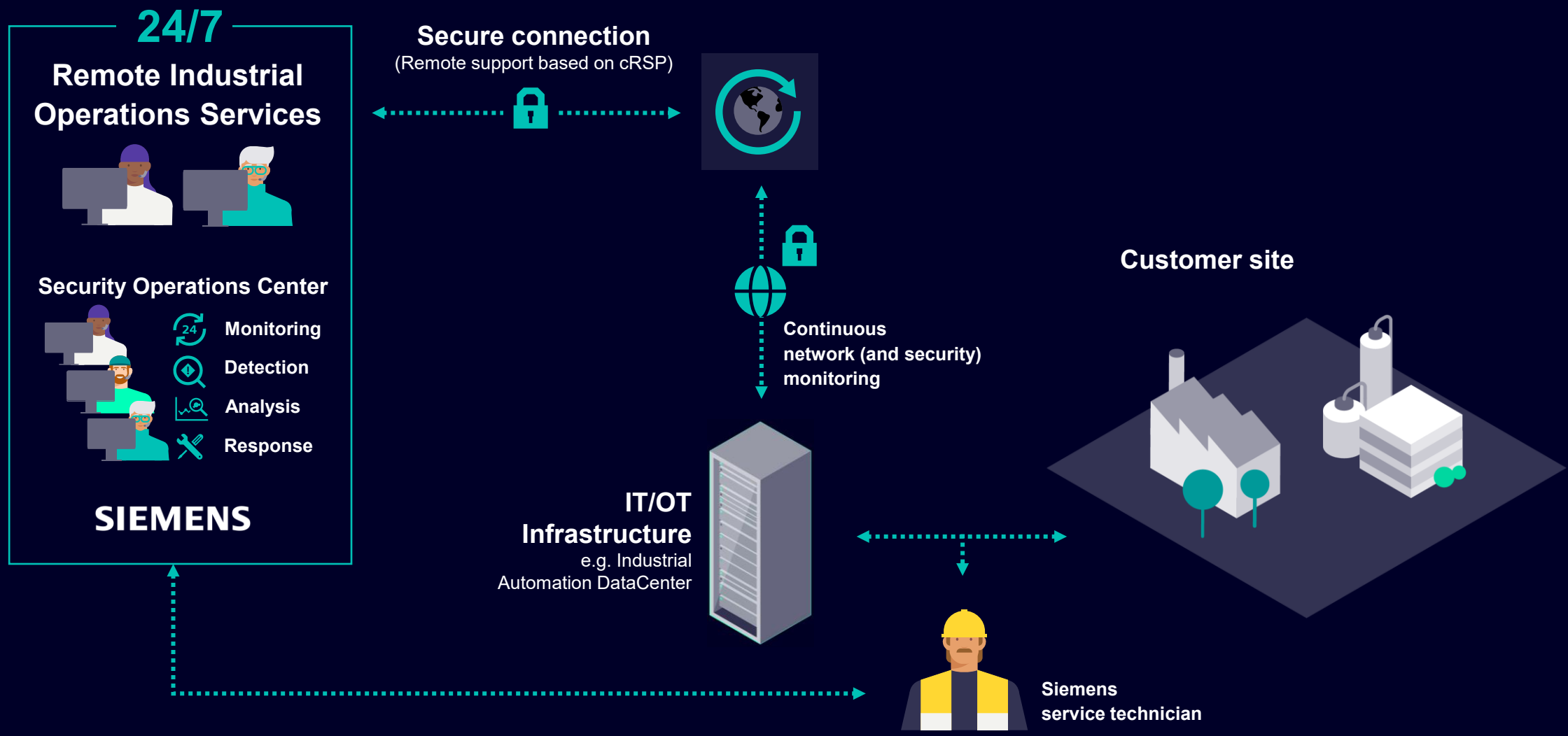
SIEMENS

Remote Industrial Operations Services
Modular services

	Services including reporting	
Available	Continuous Monitoring	
	Incident Management	Optional
	Network Management	Optional
	Domain Management	Optional
Secured	Vulnerability Management	Optional
	Anomaly Detection	Optional
	Security Operations Center	Optional
Maintained	Periodic & Preventive Maintenance	Optional
	Updates & patches	Optional
	Back-up & Restore	Optional
Supported	Remote Support (via secure VPN connection)	
	Service Desk	
	Service Request	
	Technical Product & Hardware Support	

SIEMENS

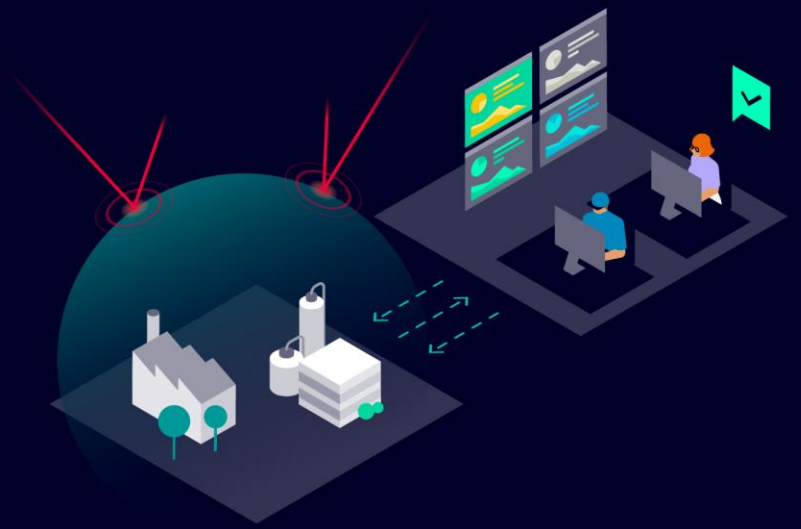
How does the management of the IT/OT infrastructure work?



SIEMENS

Module Security

Security Operations Center as a Service

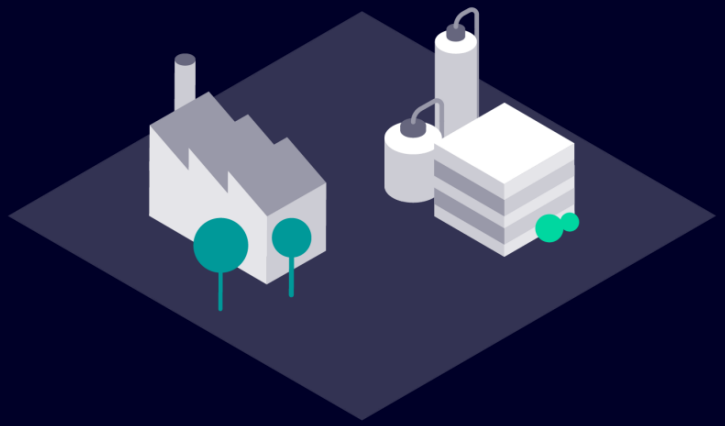


SIEMENS

Security Operations Center as a Service (SOCaaS)

- Continuous Security Monitoring
- Threat Detection
- Data analysis
- Incident Response

… for your IT and OT environment



SIEMENS

Security Operations Center as a Service (SOCaaS)

Key drivers

Regulations

KRITIS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NIS2 Directive

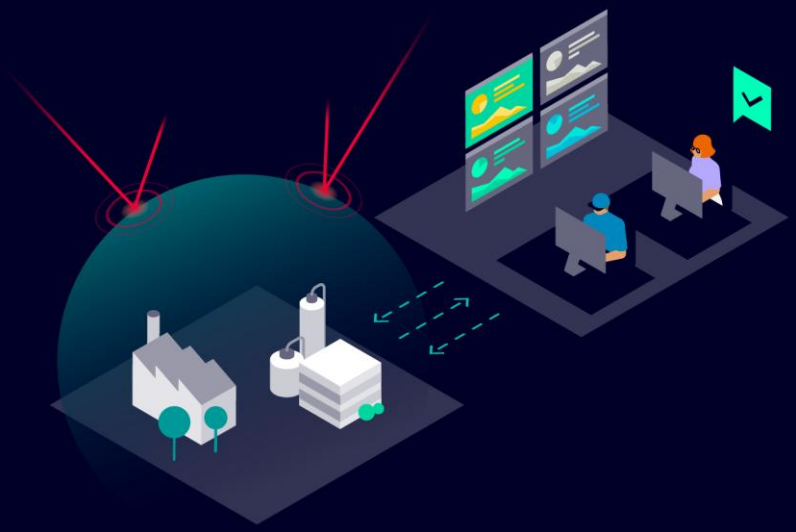
30 billion end points by 2030[1]

6.06 billion malware attacks in 2023[2]

Why Siemens?

- **Our new portfolio supports you in fulfilling governmental regulations.**
- **Expertise in OT and IT support**
- **Proactive approach for up-to-date protection for our customers**
- **Profound experience from industry for industry**
- **Future-proof concept – cloud solution.**

Operational continuity



1 17 billon global IoT devices in 2024 | **2** Includes broad range of cyber threats affecting both IT systems and other digital environments | **Source:** Stakeholder interviews, Statista

SIEMENS

Security Operations Center as a Service (SOCaaS)

Real-time Security Monitoring
A SOC provides 24/7 monitoring and analysis of your environment to uncover any suspicious activity or behavior.

Responds to Incidents
Incident response and recovery. A SOC acts as a first responder for security incidents.
Once an attack has been identified, the SOC responds by performing actions in close alignment with your experts to limit the disruption to the business through actions like isolation endpoints, terminating harmful instances, deleting malicious files, and more.

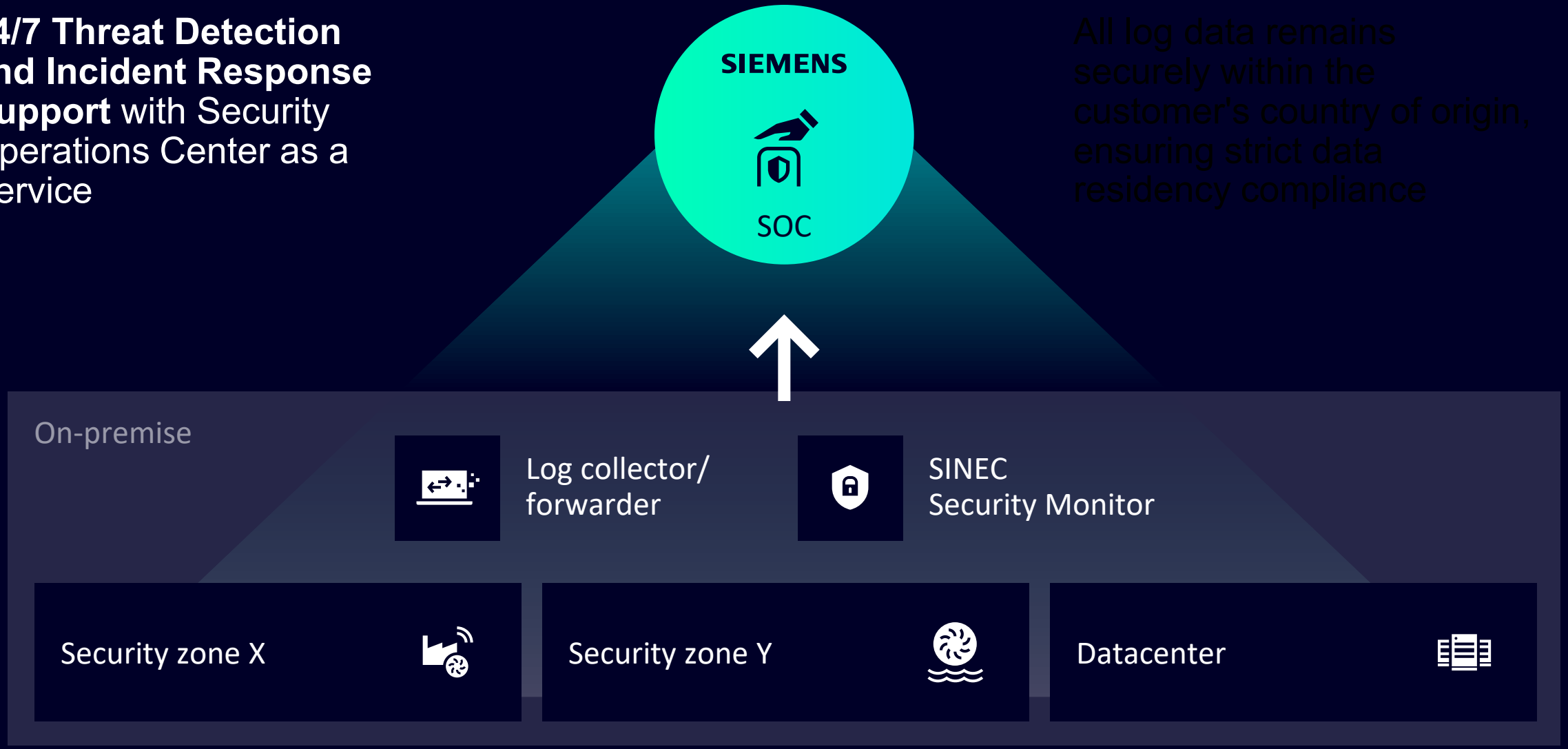
Detects Threats
A SOC detects threats based on triaging and correlating multiple indicators from your environment. In our case the threat detection is based on a) Indicator-of-Compromise, b) Tactics, Techniques and Procedures of malicious actors, c) Anomalies and d) Standard Operating Procedures.

Complies with Regulations
A SOC can help organizations comply with various security regulations, such as NIS2, KRITIS, NERC and more

Decreases Cost of Breaches
A successful breach can be very expensive for organizations, from loss of production, regulatory sanctions to reputational damages. Recovery often leads to significant downtime. By getting ahead of attackers and responding quickly to incidents, a SOC helps organizations save time and money as they get back to normal operations.

SIEMENS

24/7 Threat Detection and Incident Response Support with Security Operations Center as a Service



All log data remains securely within the customer's country of origin, ensuring strict data residency compliance

SIEMENS

OT Security Operations Center as a Service

including log collection, threat detection analysis, triage workflow and incident response

Data collection & Intrusion Detection

Log collection

OT devices
(in control system network, operations network, IT/OT DMZ)

Continuous improvement

SIEM system (processes logs, generates tickets/alerts)

Threat Detection Analysis (triage)

Customer notification
(if critical incident is identified)

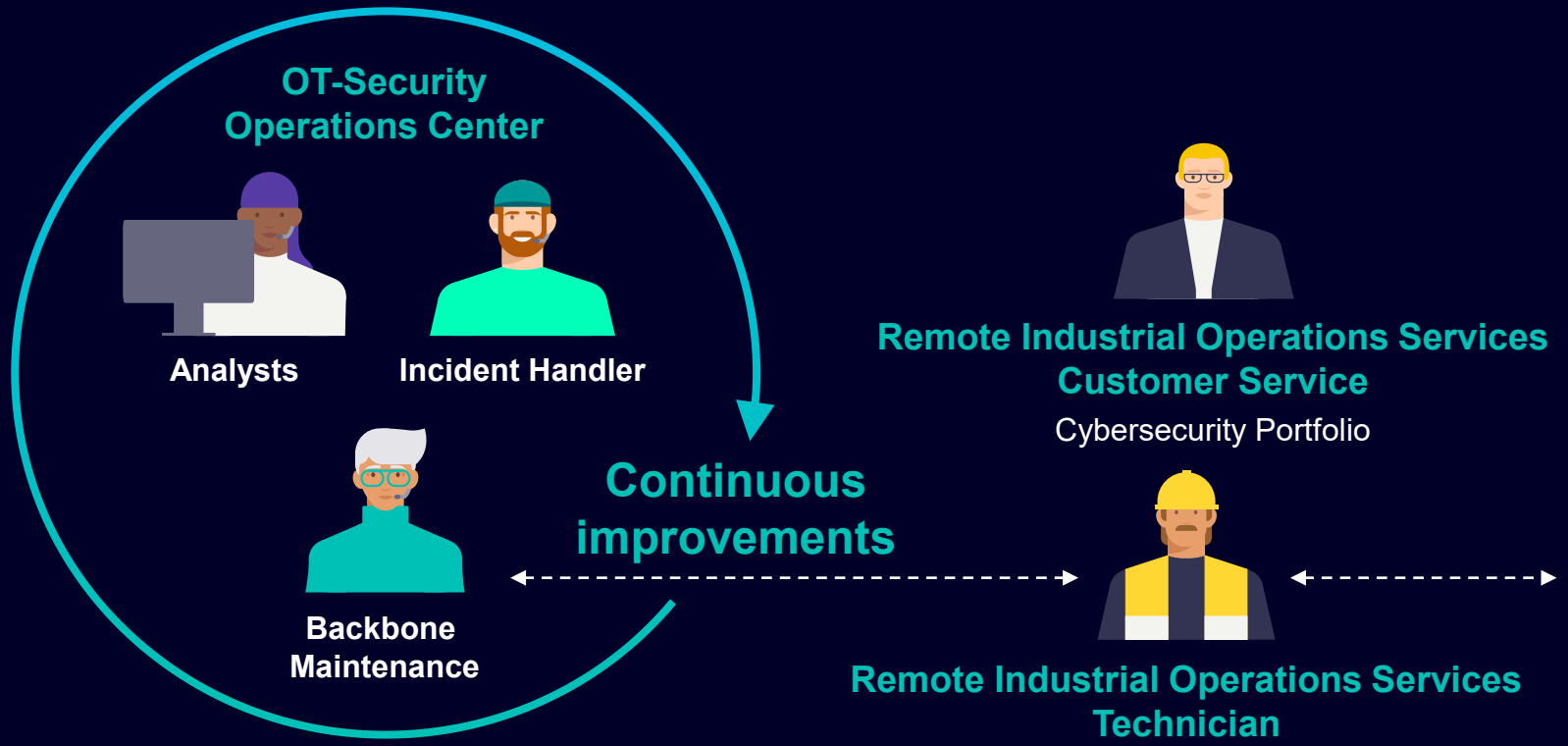
Incident response support
(if needed)

End-customer dashboard for monitoring

SIEMENS

OT Security Operations Center as a Service (SOCaaS) with Remote Industrial Operation Services

Remote Industrial Operations Services including SOCaaS



Remote Industrial Operations Services Customer Service

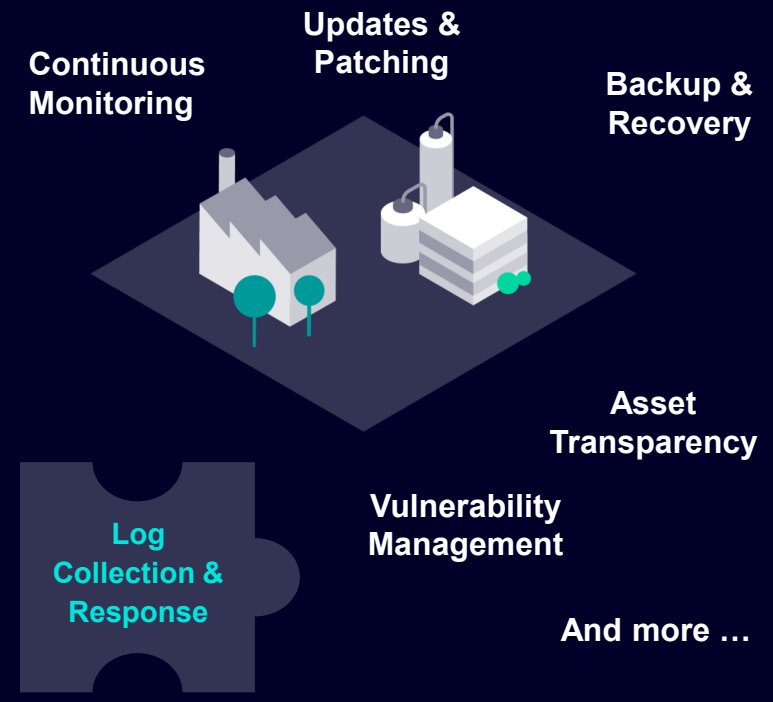
Cybersecurity Portfolio

Remote Industrial Operations Services Technician

Remote support, Service desk & Tech. product & hardware support

Customer

Managed Security Services



SIEMENS

OT SOCaaS with Remote Industrial Operations Services

Log Sources (Customer)


Application


Firewall Logs


OT


SINEC Security Monitor


Windows Logs


EDR[1]

- Custom log source integration according to customer needs
- Integration of Siemens SINEC Security Monitor

Event Processing

Log collection and parsing in Cloud environment

- Log collection and parsing
- Regionalization and scalability according to customer need

Detection Platform

SIEM[2] platform in Cloud environment

- Regionalization and scalability according to customer need
- Analyze and correlate security events

Monitoring, Triage & Response

- Triage events coming from SIEM
- Incident Response support if needed
- Custom dashboards for customers
- Service operations 24x7

1 Endpoint Detection & Response | **2** Security Information & Event Management

SIEMENS

Why should you choose Remote Industrial Operations Services?

Direct access

to proven IT/OT expertise by our experts

Operational continuity

through 24/7 remotely managed IT/OT infrastructure

Compliance

with cybersecurity regulations (e.g. NIS 2)

SIEMENS

Customer Case Studies

SIEMENS

Tata Steel Nederland
Protection of critical IT/OT infrastructure with Remote Industrial Operations Services

Tata Steel is one of the largest steel manufacturers in the world, with an annual crude steel capacity of 35 million tons and more than 77,000 employees worldwide.

Customer objectives

- The Hot Strip Mill and Hot Dip Galvanizing Line use the Industrial Automation DataCenter.
- They required support with maintaining and securing their critical IT/OT infrastructure due to resource constraints and the need for specialized expertise.

Solution and Service

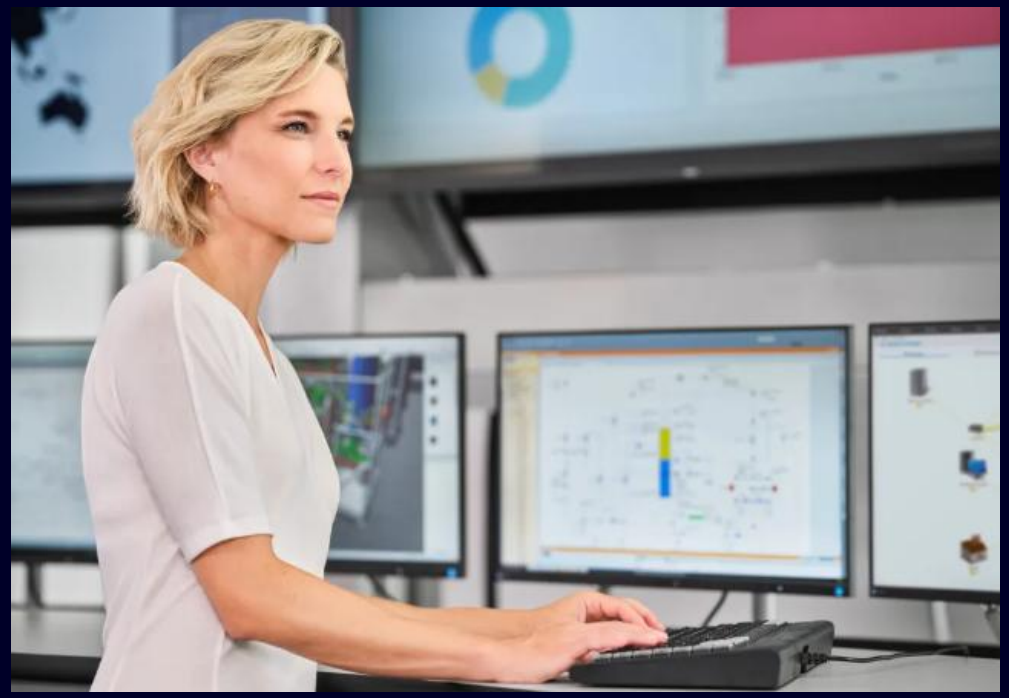
Remote Industrial Operations Services for expert maintenance and security

- System availability is optimized through various services such as continuous monitoring for early detection of issues, incident management for quick restoration to normal operations, disaster recovery support in case of a shutdown, as well as regular reporting for transparency and accountability.
- The system is protected through various security measures such as patching, traffic monitoring and vulnerability management.
- The maintenance of the infrastructure includes update services, preventive and periodic maintenance, backup and restore, configuration and change management as well as asset management.
- Siemens provides remote support and expert assistance as well as technical product and hardware support for the Industrial Automation DataCenter.

Customer benefits

- Through the proactive and continuous monitoring as well as regular maintenance, issues are detected and resolved early on, thereby reducing downtime and costs and maximizing operational continuity.
- By implementing comprehensive cybersecurity measures the plant is protected from cyberattacks.
- They have a central point of contact for resolving any questions and issues.

Siemens References ID: 38896



4-5

Shutdowns prevented

SIEMENS

Waterschap Limburg, water board, Netherlands

24/7 Security Operations Center as a Service and Anomaly Detection with Remote Industrial Operations Services

Waterschap Limburg

Regional water management organization in the province of Limburg in the Netherlands, Water & Wastewater, https://www.waterschaplimburg.nl/

Customer objectives

- Protect critical water and wastewater infrastructure from sophisticated cyber attacks targeting OT (automation) environments, given the high societal impact
- Challenge to comply with cybersecurity regulations such as NIS 2 and CSIR, a Dutch derivative of NIS 2

Solution and Service

Remote Industrial Operations Services with Security Operations Center as a Service (SOCaaS)

- 24/7 Threat Detection and Incident Response support for OT infrastructure provided by OT SOCaaS
- SINEC Security Monitor implemented to identify anomalies in OT networks with Security Operations Center integration
- Asset discovery and vulnerability management with SINEC Security Monitor.

Customer benefits

- End-to-end approach for security monitoring and vulnerability management from a single source
- 24/7 Cybersecurity protection from a service provider with deep OT know-how

Siemens References ID: 43478

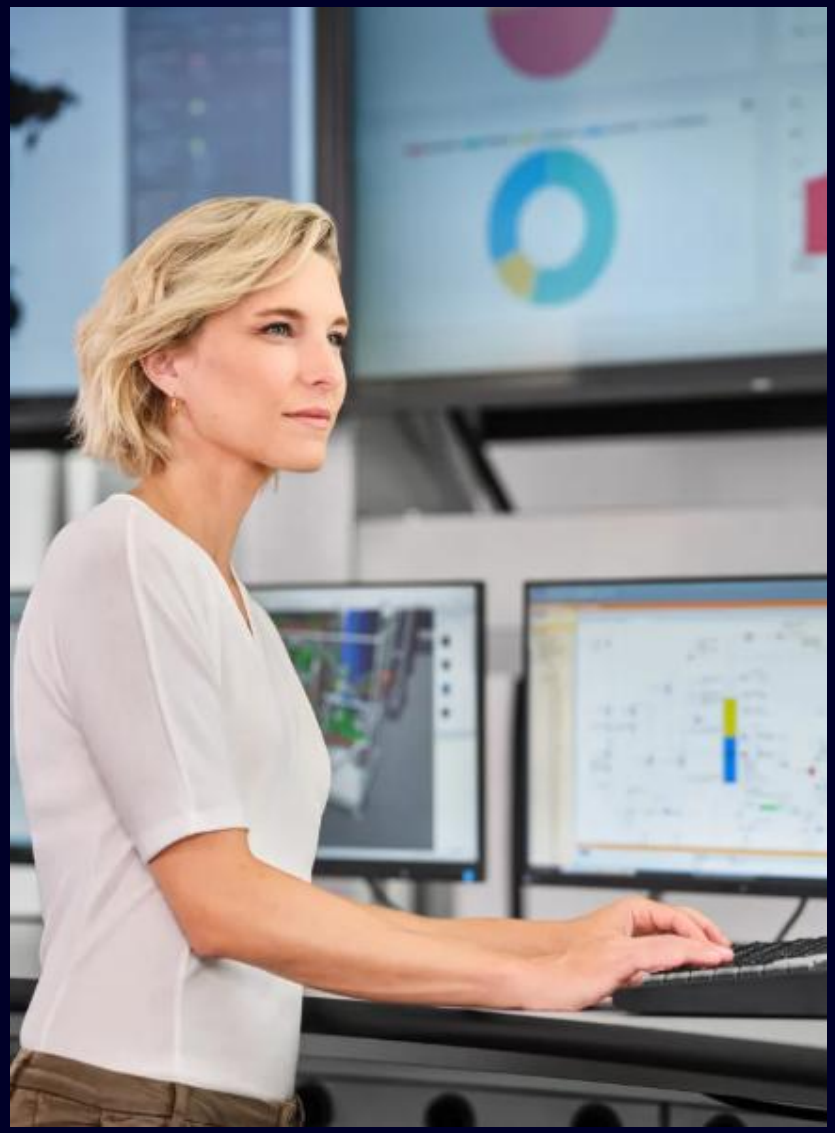
24/7

Security monitoring

"We need an OT company who understands Cybersecurity"

Leon Verhaegen, Manager automation, Waterschap Limburg

SIEMENS



You want to find out **more**?

[Remote Industrial Operations Services]

[Siemens Contact Database]

[Podcast: Navigating IT/OT Convergence]

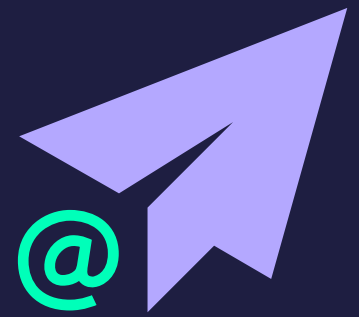
[Blog post: The Urgency of Cybersecurity]

SIEMENS

Contact

E-mail riops.support.industry@siemens.com

Website siemens.com/riops



SIEMENS

Disclaimer

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.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/cybersecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cybersecurity.

SIEMENS