SOGIC 2018

May 8, 2018 | Hyatt Regency, Calgary, Alberta

Siemens Industrial Cyber for Energy

Perpetual Vigilance for What's Critical

www.siemens.com/industrial-security

Industrial cyber is the new risk frontier in Energy

SIEMENS
Ingenuity for life

Rising number of cyber threats to industrial control systems

67% believe the risk level to industrial control systems over the past years has markedly increased because of cyber threats

Increased complexity of risk management across value chain

61% say their organization has difficulty in mitigating cyber risks across the oil and gas value chain

Risk migrating from IT to OT environment

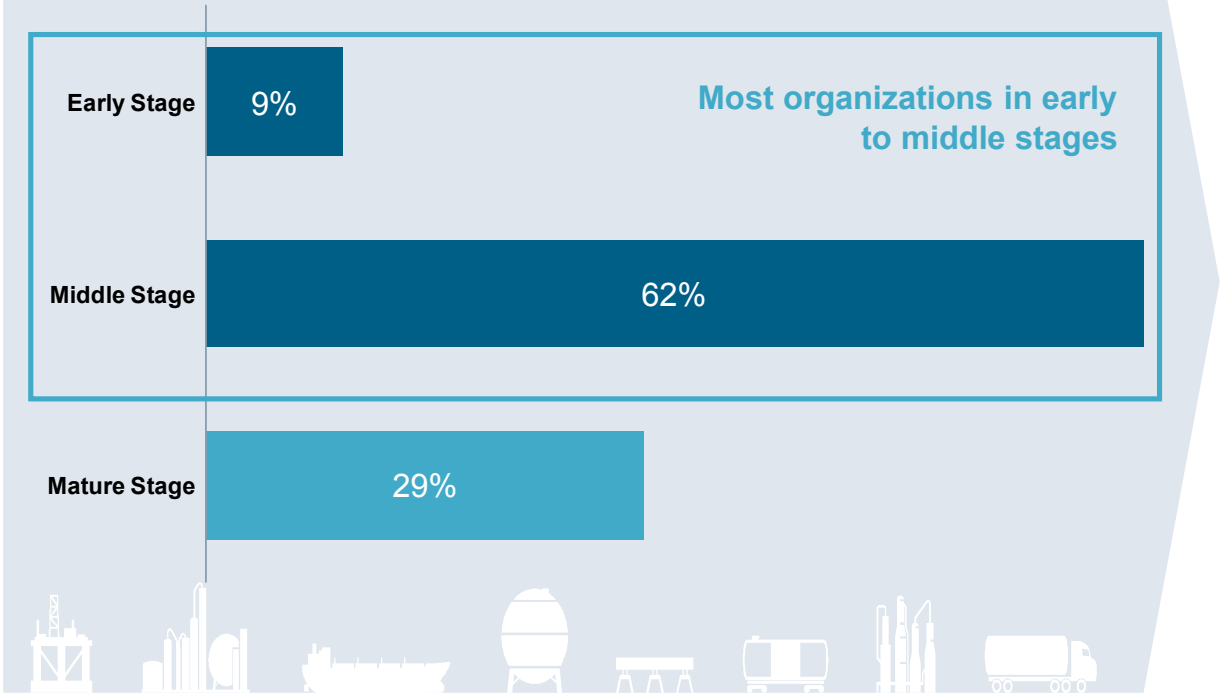
59% believe that there is now a greater level of cyber risk in the OT than in the IT environment

Source: State of OT Cybersecurity in the Oil and Gas Industry, 2017, SGT research

Most energy companies are not prepared to address OT cyber risk …

SIEMENS
Ingenuity for life

What best describes the maturity level of your organization's cyber readiness?



Energy organizations face similar pain points in managing OT cyber programs

- Limited visibility across OT asset base
- Shortage of internal OT security expertise
- Limited understanding of where infrastructure is most vulnerable
- Difficulty of securing multi-vendor, legacy OT assets
- Inability to monitor and respond rapidly to threats
- IT solutions do not translate to OT environment

Source: State of OT Cybersecurity in the Oil and Gas Industry, 2017

…and are struggling to effectively deploy and manage their OT security programs

SIEMENS
Ingenuity for life

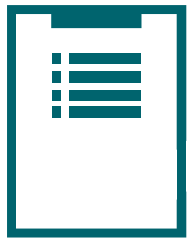
Lack of real-time information

83%

of security professionals are concerned about missing threats between vulnerability scans

Inability to prioritize OT cyber risk

66%



of responded say they lack a clear picture of the risks required to accurately prioritize and take action

Limited visibility

84%

of respondents say they do not have full visibility of potential vulnerabilities to their ICS/SCADA environments

Inadequate manpower

60%

of respondents say they do not have enough staff to effectively meet the challenge

Sources: State of OT Cybersecurity in the Oil and Gas Industry, 2017; Ponemon Institute, 2014 Critical Infrastructure Survey; Forrester purchased study, 2014

The first steps to addressing industrial cyber are to understand the OT risk, get transparency and harden defenses

SIEMENS
Ingenuity for life

Siemens Best Practices

Demand OT Cyber Solutions that meet the unique performance and safety requirements

Overcome the Fear of Connectivity as benefits of digitalization are too great. Connectivity equals insight.

Get cyber transparency to baseline OT risk, harden the infrastructure and begin to address fundamentals

Assign ownership for OT to drive the change against this complex and quickly growing problem

Secure the edge which in the world of digitalization has become the new center

Leverage security analytics to get the advantage as the sophistication and complexity of OT attacks has reached machine speeds

Today's typical dilemma – Understanding security event data

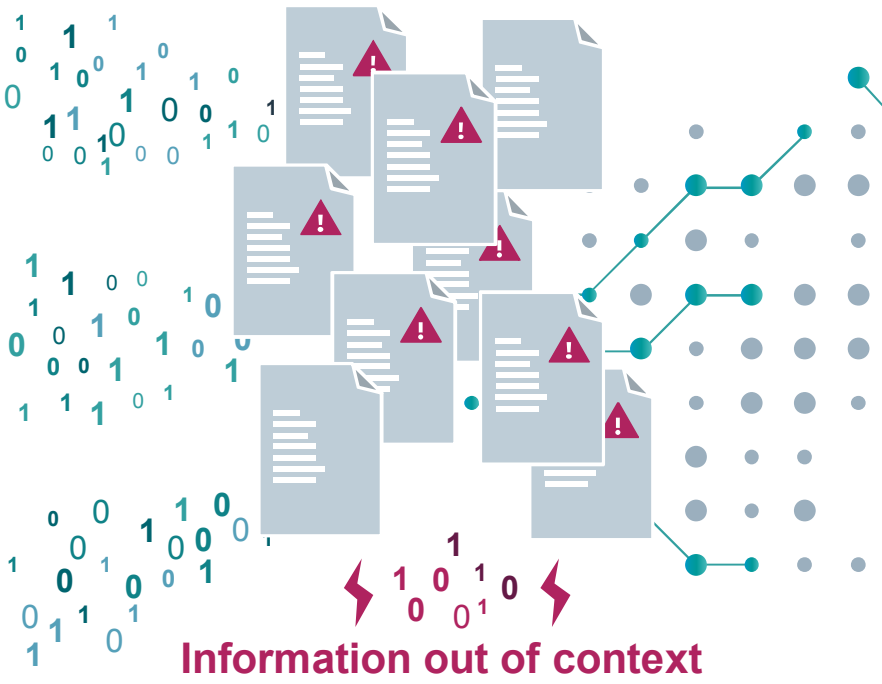
SIEMENS
Ingenuity for life

Disconnected Data Repositories

Security and Asset Monitoring

Scheduled and Unplanned Outages/ Maintenance

Production (historical/ forecast)



Information out of context is often irrelevant

Network Admins — Cumbersome collection of quality security data

Asset Owners — Security performance difficult to benchmark

O&M Staff — No access to full information for security decisions

All user groups — Different reference points and input data for accurate security diagnostic

Siemens has built a dedicated Energy cyber portfolio to address customer needs at every point in the journey

Siemens Cyber Offering for Energy

Step 1
Evaluate

- Cyber Gap Assessment
- Asset Inventory
- Sec. Program Standup
- Sec. Architecture Design

Step 2
Implement & Intervene

- Endpoint Hardening
- Whitelisting Deployment
- Secure Remote Access
- Sec. Awareness Training
- Cyber Security Center

Step 3
Test

- Vulnerability Assessment
- Penetration Testing
- Incident Response Plan Testing

Step 4
Monitor & Maintain

- Device and event monitoring
- Advanced Threat Detection
- Vulnerability Management
- Cyber Asset Management
- 24/7 incident response

Consulting Services

Security Products

Professional Services

Managed Services

Siemens is leveraging its deep OT knowhow and Darktrace AI analytics to offer a first of its kind MSP

SIEMENS
Ingenuity for life

Cyber Defense Center

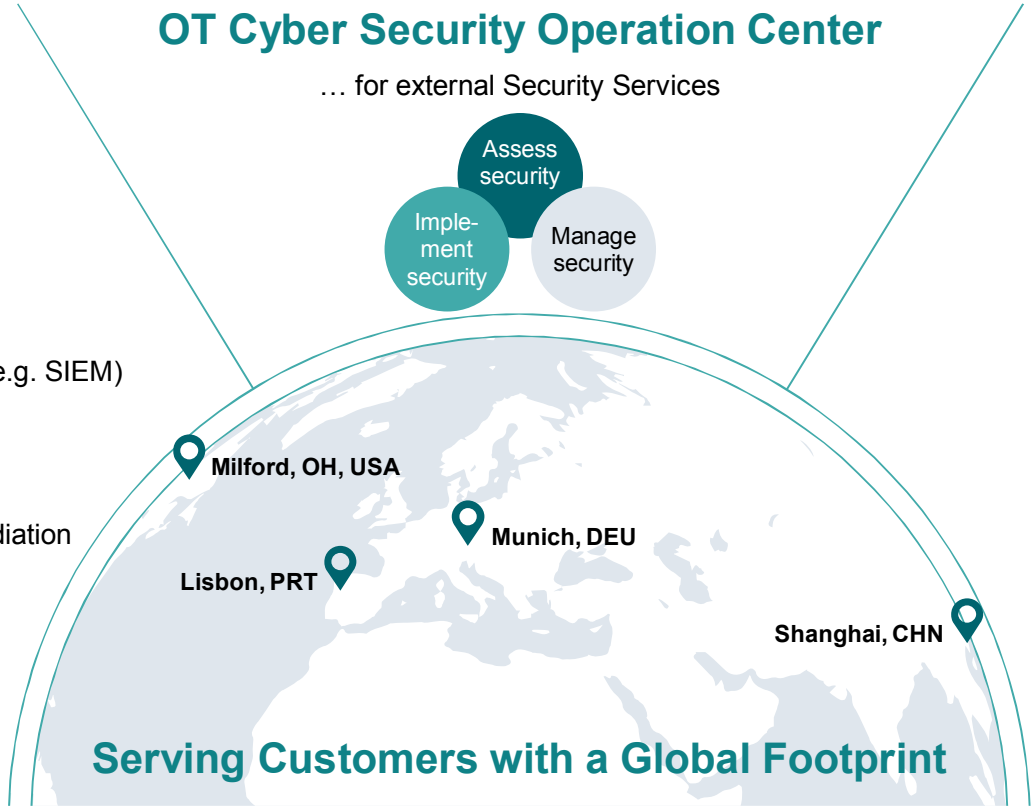
Internal knowledge as foundation …

Detect Investigate Respond

- Global collection of events
- Monitoring and detection platforms (e.g. SIEM)
- Experienced Cyber Analysts
- Threat intelligence and forensics
- Security management platform
- Vulnerability mgmt. and global remediation

OT Cyber Security Operation Center

… for external Security Services



Customers Benefit

- Self-learning; no configuration
- Advanced Threat Detection
- Stop or slow down threats without disrupting operations
- Passive, non-obtrusive
- Prioritizes threats through correlation

1 CDC in Milford, Lisbon and Munich

Siemens MSP is powered by the Darktrace's Industrial Immune System

SIEMENS
Ingenuity for life

Learns "self" in real-time

Analyzes every individual user, device and network, using unsupervised machine learning

Detects threats in network

Detects both insider and sophisticated external threats from within the network

Provides 100% visibility

Visualizes entire network, including traditional and non-traditional OT

Supports every protocol and standard

Includes Modbus, DNP3, OPC, ICCP, IEC-60870-5-104, IEC-61850, etc.

Works across all networks and OT devices

Works across IT, SCADA/ICS systems, and IIoT

Offers unmatched insights into OT

Empowers organizations to make smarter, faster security decisions

Siemens provides automated inventory and configuration management from PAS for multi-vendor asset visibility

SIEMENS
Ingenuity for life

Provides comprehensive asset visibility

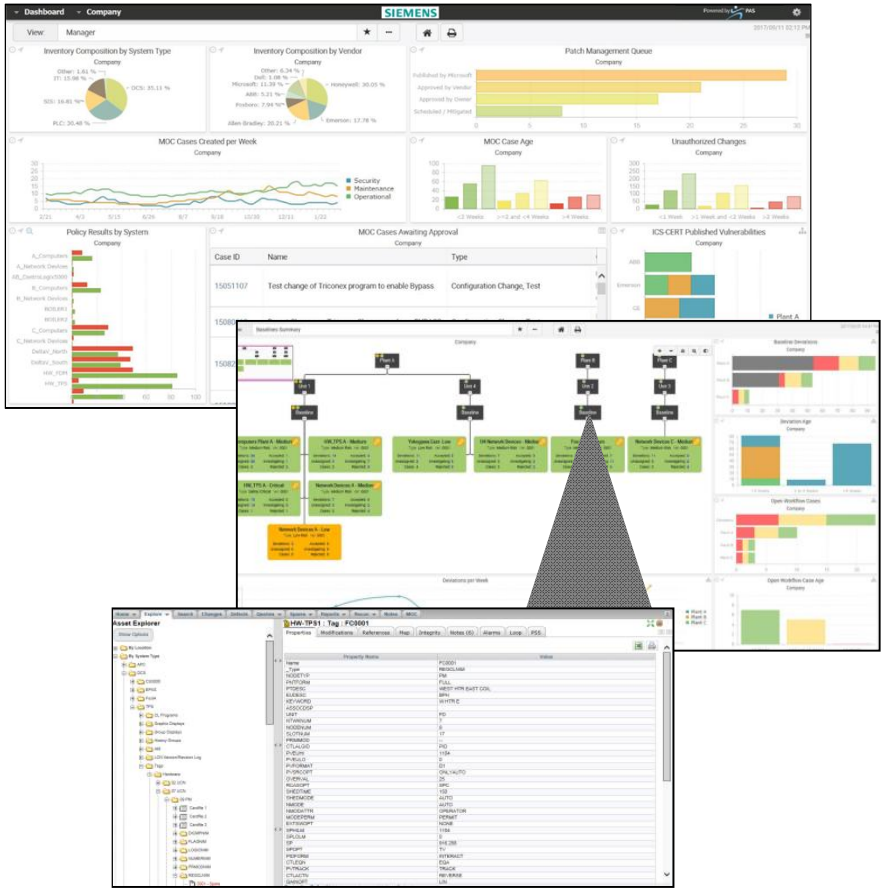
Automates discovery of networked and transient cyber assets in ICS environments

Enables standards compliance

Drives internal and regulatory standards compliance (e.g., ISA/IEC 62443, NERC-CIP, NEI 08-09, NIST & more)

Reduces incident recovery time

Speeds recovery with backups of critical control system data and historical change monitoring



Automates multi-vendor inventory management

Maintains industrial endpoint inventory for all major production-centric ICS and IT-centric assets

Detects unauthorized change

Baselines security configuration data, identifies changes, and drives investigative workflows

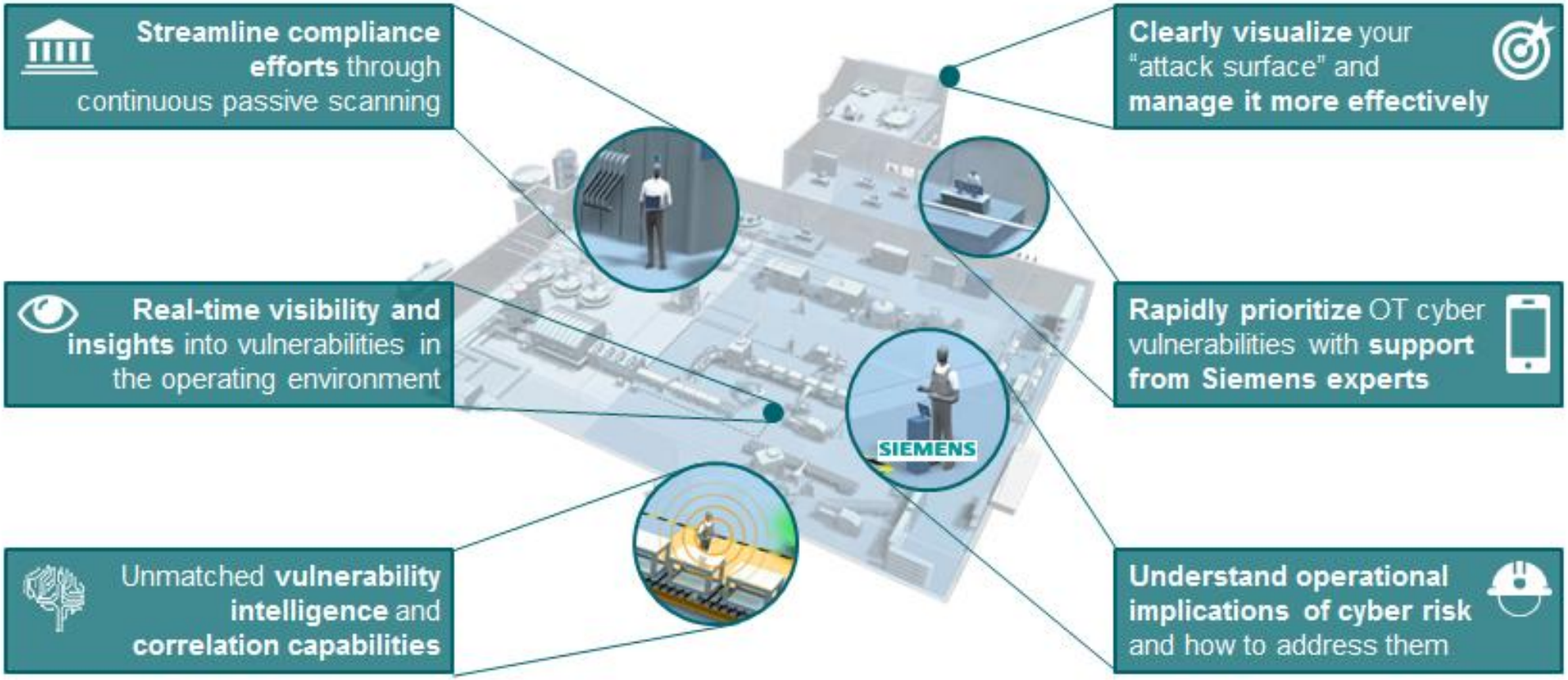
Hardens industrial cyber assets

Works across heterogeneous environment assuring security patch currency via process automation

Powered by PAS

Tenable vulnerability management backed by Siemens expertise helps customers prioritize and manage OT risk

SIEMENS
Ingenuity for life



tenable network security

Thank you

SOGIC 2018