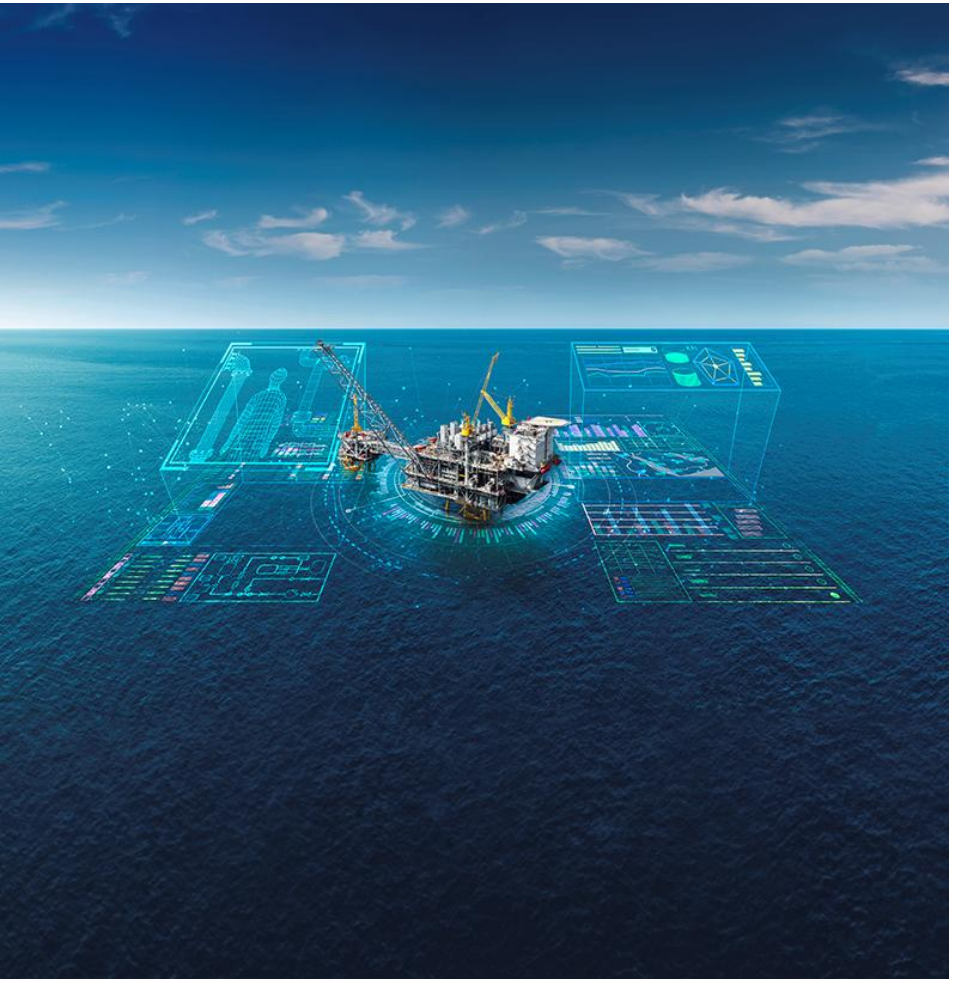
Electricity 2017

Eilat, Israel | November 9, 2017

Securing the Energy Sector
Table of contents

SIEMENS
Ingenuity for life

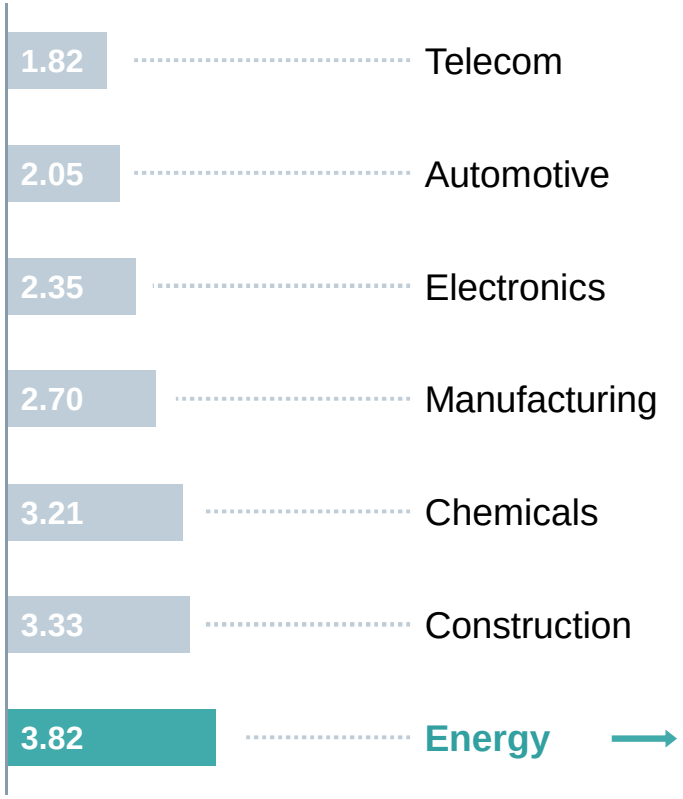


- Digitalization offers operational efficiencies
- Cyber threats are the new Energy risk frontier
- How to secure a complex digital production ecosystem
- Operational technology security methodology
- Helping organizations reduce risk and vulnerability

Focus on digitalization efforts result in game-changing operational improvements

SIEMENS
Ingenuity for life

Digitalization by Industry



Digitalization Opportunities and Benefits

- **Asset management and business analytics**
- **Remote Operation**
- **Industrial Internet of Things (Web of Systems)**
- **Cloud applications**
- **Big data analytics**

$80B Will be spent in the next 24 months on **operational efficiency**…

-25% … that could lead to reduction in OPEX **if smartly spent on digital**…

↑8% … and **produce game-changing** field recovery rates …

+11% … resulting **in sustained profit increase**

Source: McKinsey and Co; Accenture; **1** = high, **2** = medium, **3** = low, **4** = rudimentary

In a digital environment industrial cyber is the new risk frontier

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

2011: Virus Duqu collected industrial control system information

2012: Malware attempting to access SCADA infiltrated Telvent systems

2014: Black Energy malware infiltrating 37% of US energy firms

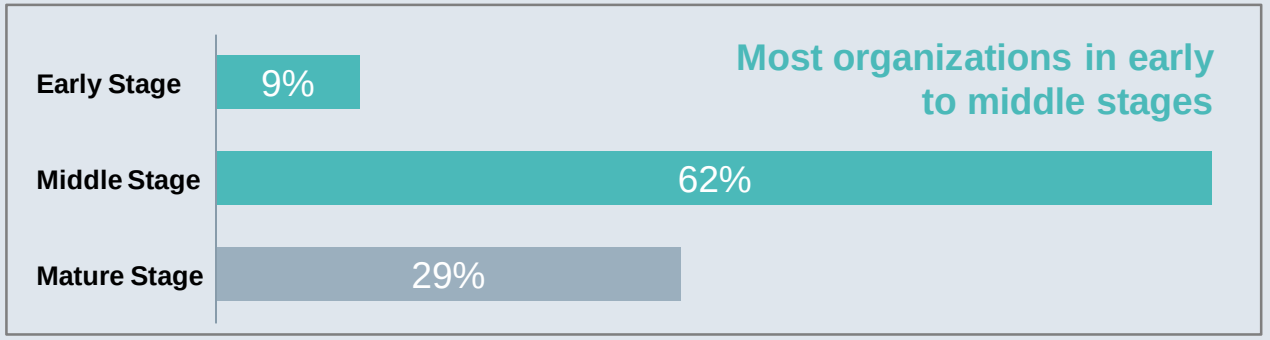
2014: Energetic Bear virus (Havex) infected ICS software updates

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

Energy companies are not prepared …

SIEMENS
Ingenuity for life

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



O&G organizations face recurring pain points in maturing OT cyber programs

- Limited visibility across OT asset base
- Shortage of internal OT security expertise
- Lack of an OT-specific security strategy
- 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

… with current Operational Technology (OT) programs leaving significant security gaps exposed

SIEMENS
Ingenuity for life

People

60%

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

Organizational

1 in 3

respondents believe there is full alignment between IT and OT on security operations

Processes

40%

of respondents have cyber training and aware-ness initiatives in place

Solutions

63% of respondents **view analytics** as **effective/very effective**

20% Yet only **use this technology today**

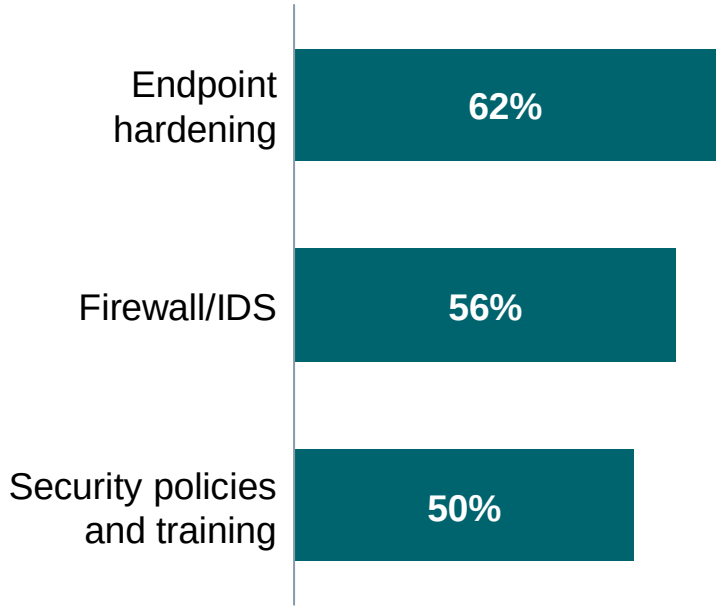
Source: State of OT Cybersecurity in the Oil and Gas Industry, 2017

Customers are looking to address fundamentals before building advanced monitoring capabilities

SIEMENS
Ingenuity for life

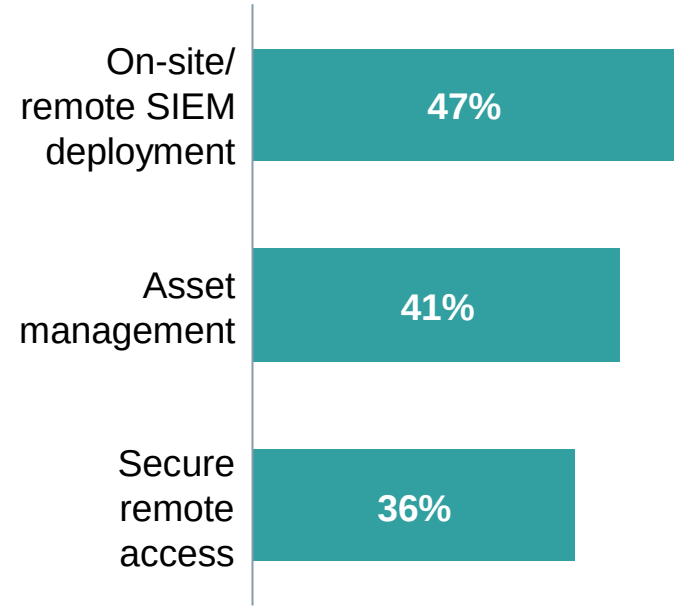
Low Cyber Maturity Organizations

The solutions viewed by respondents as most effective …



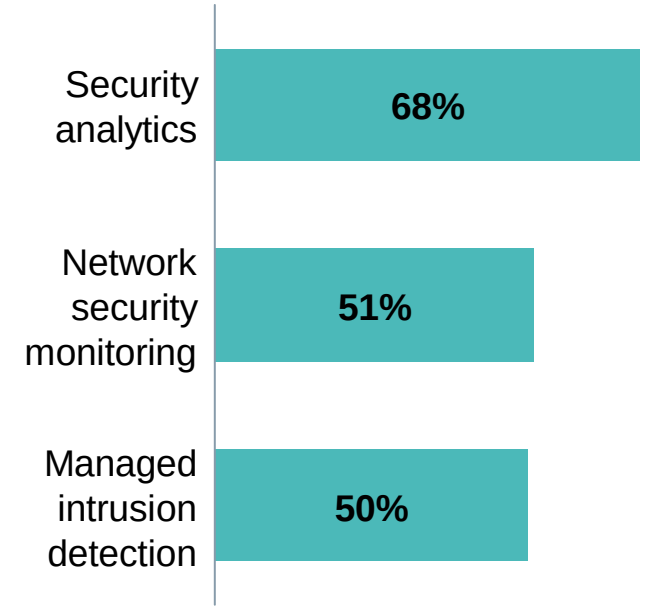
Medium Cyber Maturity Organizations

The solutions viewed by respondents as most effective …



High Cyber Maturity Organizations

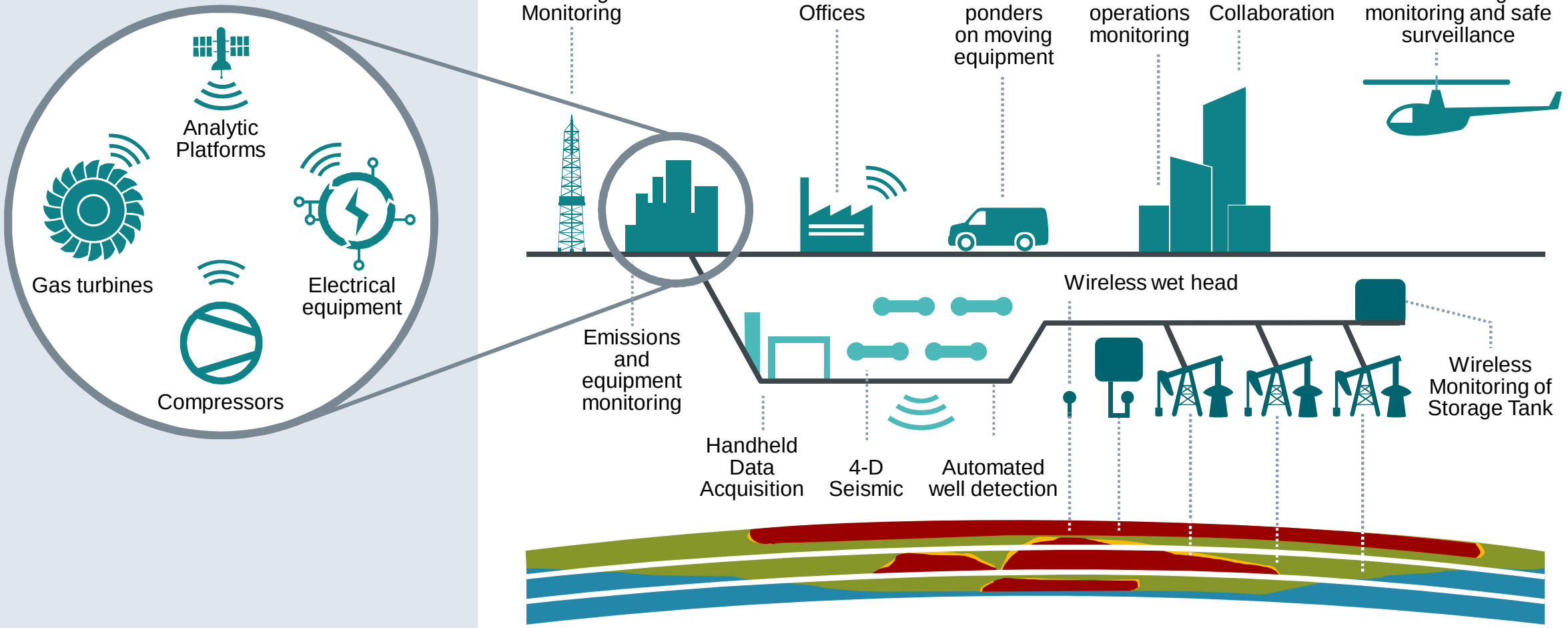
The solutions viewed by respondents as most effective …



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

How do you secure complex digital production environments without sacrificing production efficiency?

SIEMENS
Ingenuity for life



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

Assign ownership for OT

… to drive the change against this complex and quickly growing problem

Overcome the Fear of Connectivity

… as benefits of digitalization are too great. Connectivity equals insight

Secure the edge

… which in the world of digitalization has become the new center

Get cyber transparency

… to baseline OT risk, harden the infrastructure and begin to address fundamentals

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

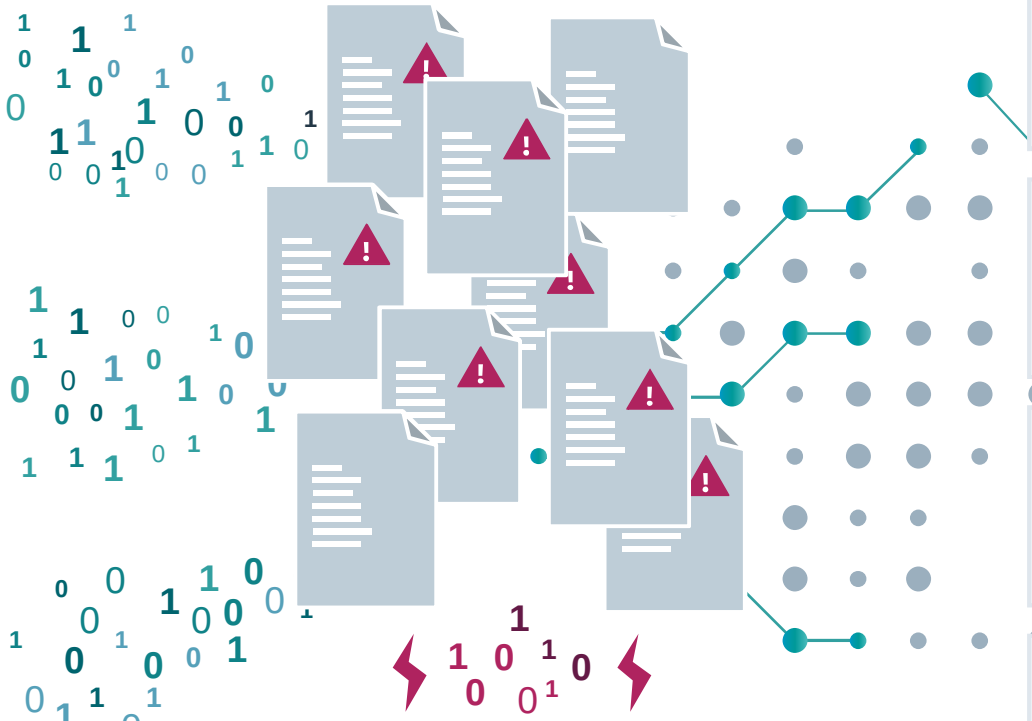
SIEMENS
Ingenuity for life

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 perfor-mance 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

Data Enrichment Sources for Contextualization

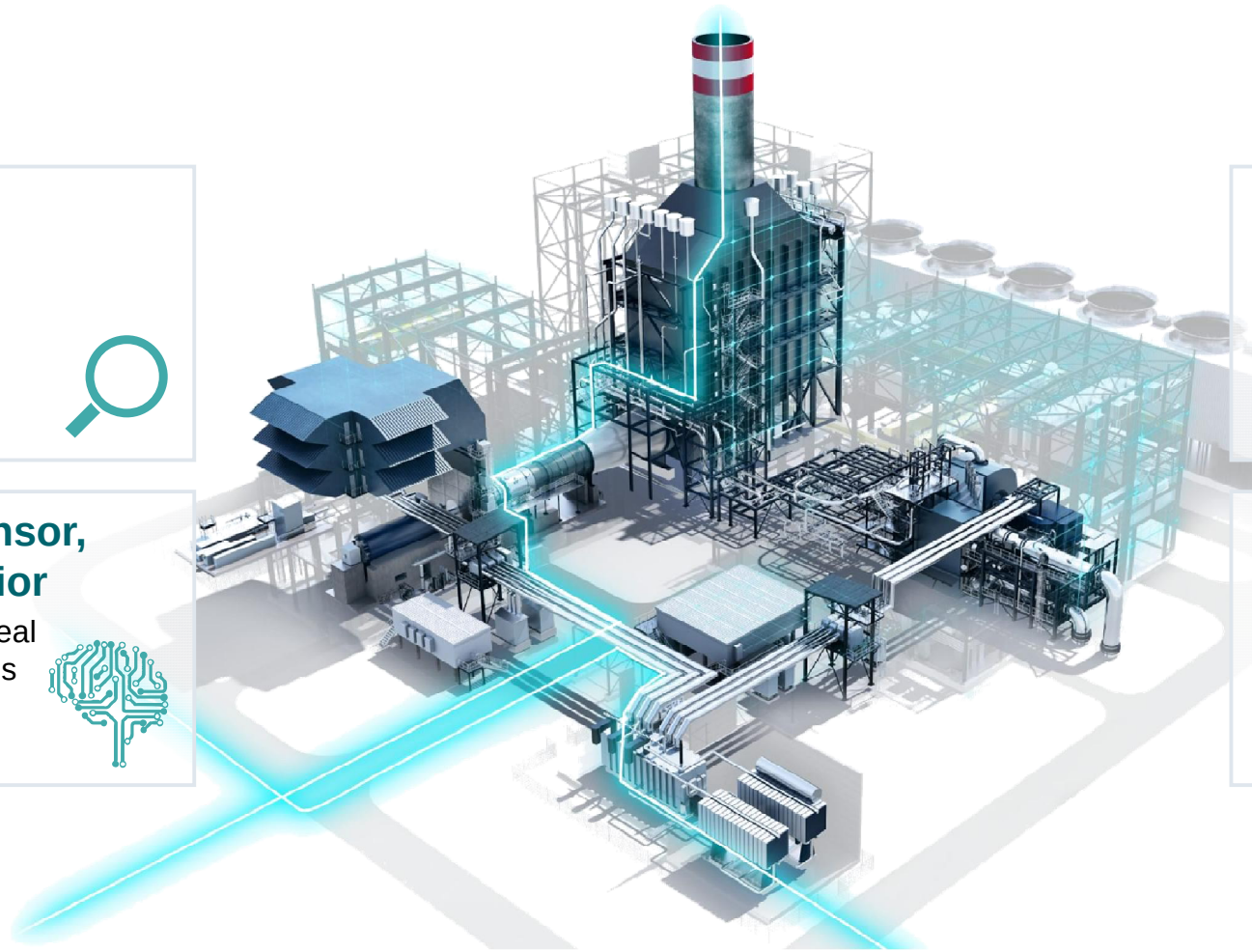
SIEMENS
Ingenuity for life

Asset Dependency Hierarchy

And criticality, that reveals expected attack path in the ICS cyber kill chain

Control System, Sensor, and Machine Behavior

Profiled in-depth profiled in real time leveraging asset owner's knowledge with automated methods at the fleet level



Production and Plant Status

Critical process variables that indicates what is expected next

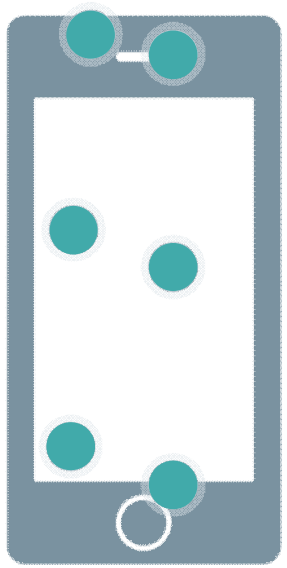
Ongoing External Attack Campaigns (TTP)

And vulnerabilities relevant to actually owned SCADA/ICS systems and IIoT

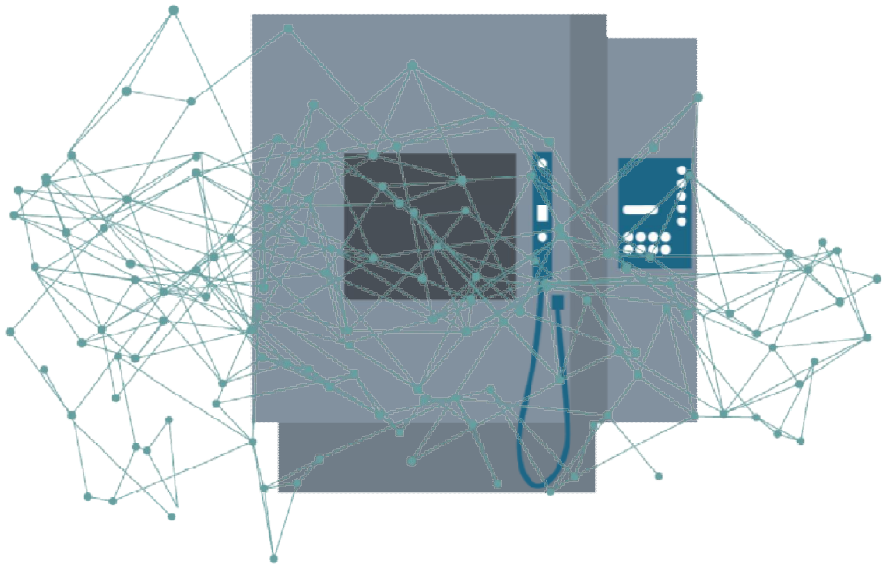
Asset Profiling Challenge and Handling Security Big Data in the IIoT Age

SIEMENS
Ingenuity for life

6 sensors



2,000 data points



Industry expertise

is key to success

How to Address this Challenge?

SIEMENS
Ingenuity for life

These challenges can only
be met when precise

realtime security and performance data

are available for all critical assets

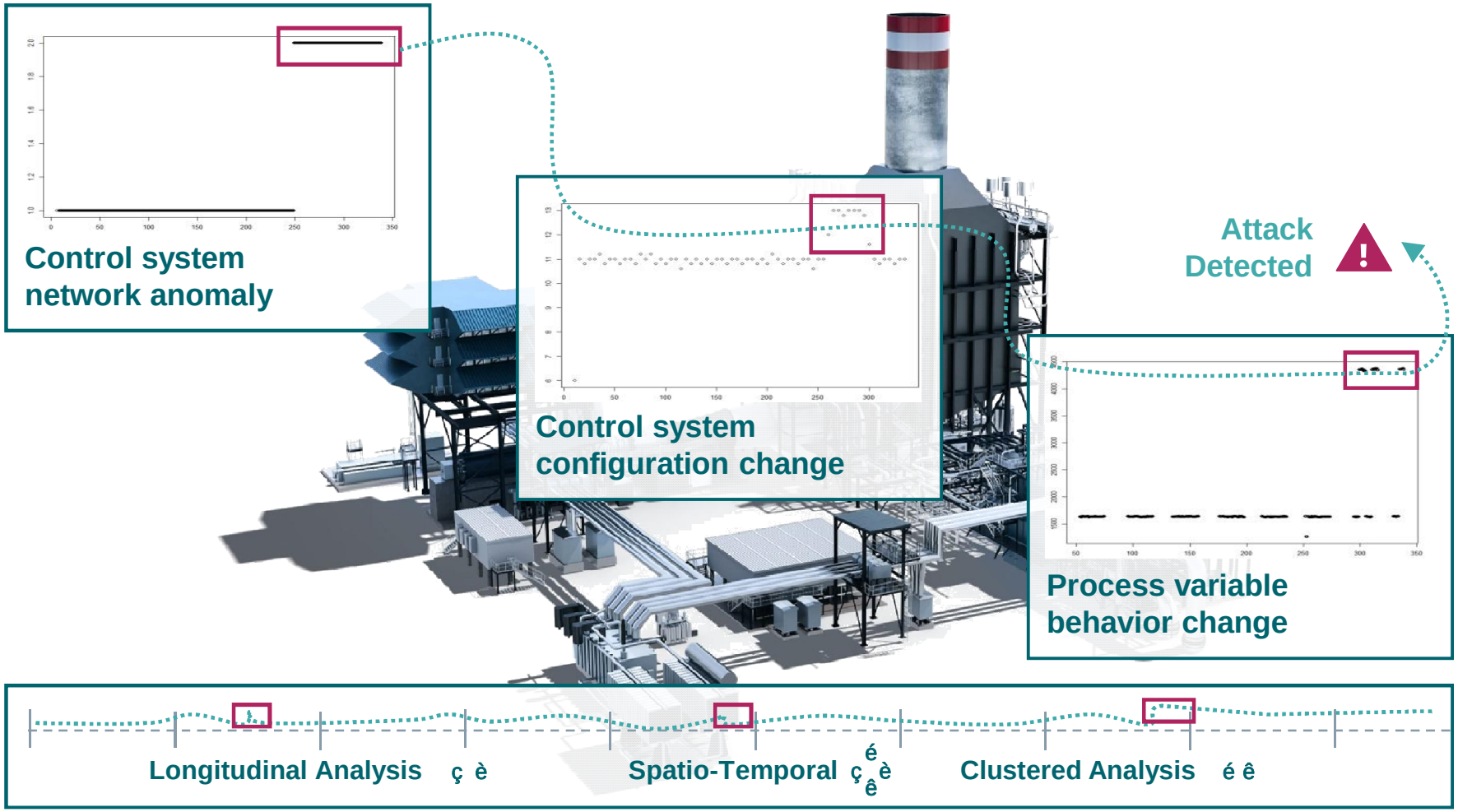
Managing this complexity demands

better situation awareness

and integrated contextualization
approaches to leverage knowledge

How does Detection Work when we approach this as an OT Challenge

SIEMENS
Ingenuity for life



Alert and Respond

Real-time contextual information

Specific recommended actions to decrease risk

Single result from multiple sources

Improved business operation continuity

Specific actions

Continuous Monitoring of the Production Process comes along and delivers additional value

SIEMENS
Ingenuity for life

Continuous monitoring of your entire global machine fleet

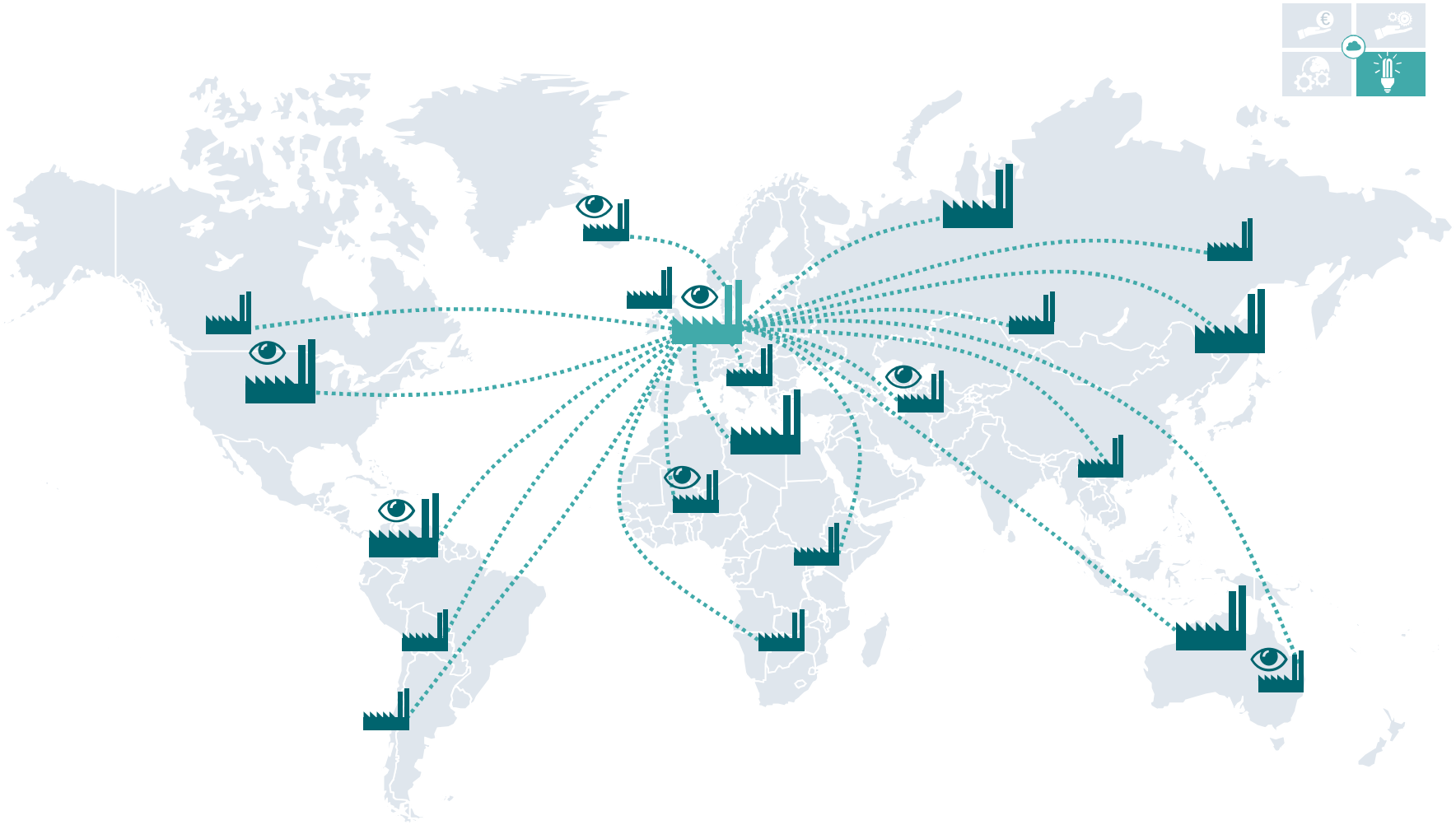
Large data volumes processed

Different deployment options: Public-/Private-Cloud, On-Premise

Today only

3.5% of all

factories!



Thank you for your attention

SIEMENS
Ingenuity for life

Eitan Goldstein

Director, Industrial Cyber and Digital Security
Siemens Energy

E-mail: eitan.goldstein@siemens.com

siemens.com