INDUSTRIAL CYBERSECURITY

MARKET TRENDS AND DEVELOPMENTS

Ronen Rabinovich - Global Senior Product Manager / OT Firewalls and Cyber Security

Industrial Cyber Security

10 oktober 2023 | Congrescentrum 1931, den Bosch

AGENDA

Belden industrial cyber security October 2023

- Market Drivers & Inhibitors.
- OT Cyber Security Trends And Challenges.
- What's Next?

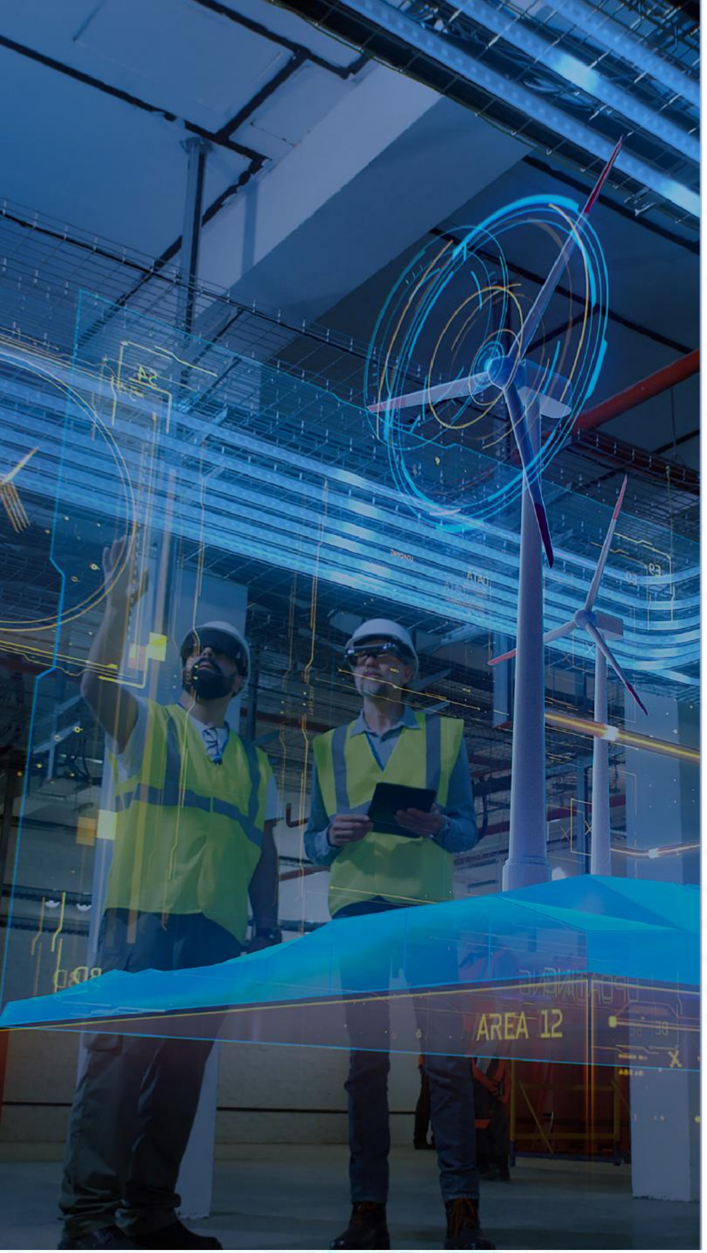
DETAILS

Event: FHI Industrial Cyber Security

Date: 10-10-2023

Speaker: Ronen Rabinovich

Time: 00:25:00



MARKET DRIVERS & INHIBITORS.

Various factors driving and inhibiting growth in the industrial cybersecurity products and services market.

1. Changes in user concerns and needs
2. Regional and industrial sector developments
3. Growth in compliance requirements
4. Evolution of the OT cybersecurity marketplace

MARKET DRIVERS & INHIBITORS.

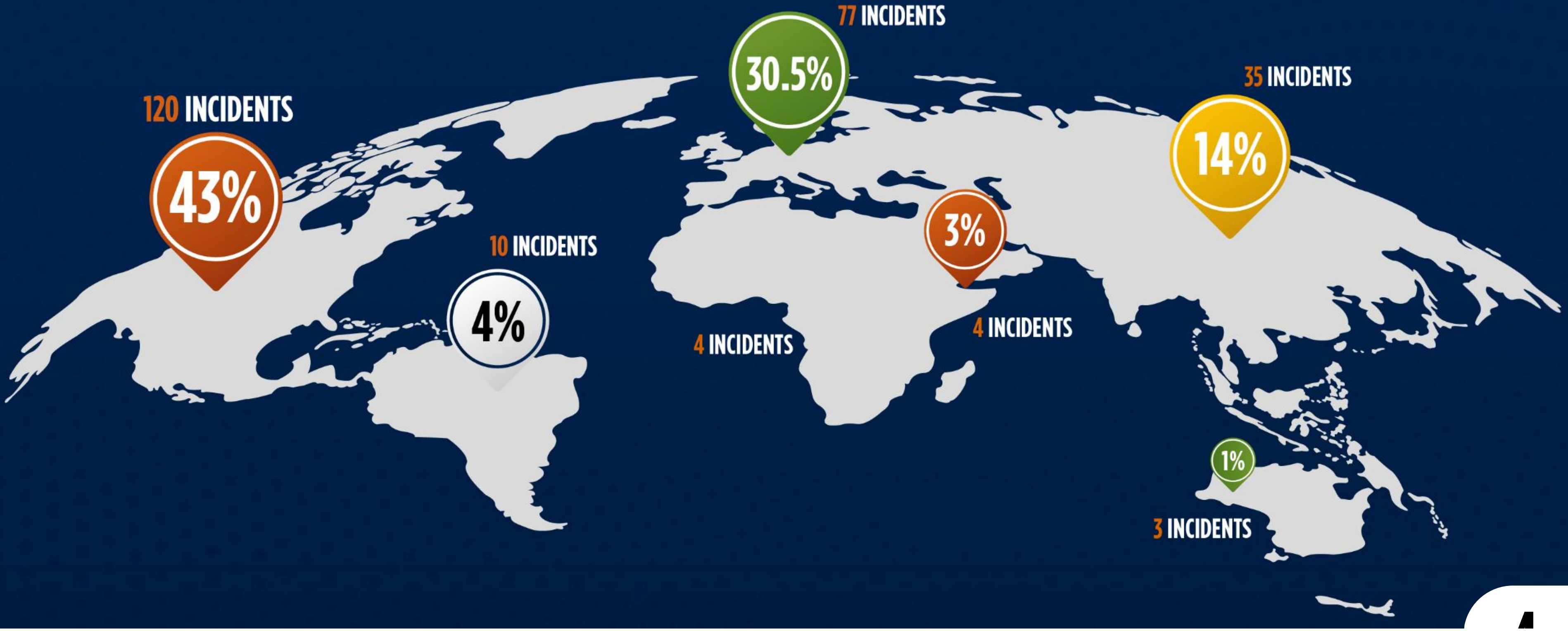
Ransomware incidents by continent Q2 2023.

27% ↑ 120 INCIDENTS NA

47.5% NA 253 RANSOMWARE ATTACKS

41% US Q1 → US Q2 43%

28% EU Q1 59 → EU Q2 30.5% 77



MARKET DRIVERS & INHIBITORS.

Ransomware incidents by sector and subsector Q2 2023.

INCIDENTS 177

MANUFACTURING
70% of all ransomware attacks impacted the manufacturing sector

41

ICS
16% of attacks, 30 incidents on ICS equipment, 11 incidents on ICS engineering

24

TRANSPORTATION
Transportation sector targeted with 5.5% of attacks

10

OIL & NATURAL GAS
Oil and Natural Gas sector had around 4% of attacks

INCIDENTS 05

MINING SECTOR
Mining sector was impacted by 2% of the attacks.

03

RENEWABLE ENERGY
Renewable energy sector had 3 incidents

02

WATER SECTOR
Water sector had 2 incidents

01

PT&D AND ENERGY
Electric sector 1 incident

MARKET DRIVERS & INHIBITORS.

Regional and Industrial Sector Developments

INCREASE BUSINESS-IMPACTING RANSOMWARE ATTACKS

Political tension between NATO countries and Russia motivates Russian-aligned ransomware groups to continue targeting and disrupting critical infrastructure in NATO countries.

Number of victims willing to pay ransoms diminishes, RaaS groups have shifted their focus towards larger organizations, resorting to widespread ransomware distribution attacks to sustain their revenues.

Increase demand pipelines and water & wastewater facilities

This is primarily driven by recent incidents (Colonial Pipeline and Oldsmar water treatment plant) and the release of new TSA directives.

MARKET DRIVERS & INHIBITORS.

Increased OT Cybersecurity Regulatory Requirements

01 Ransomware and political unrest have stimulated regulatory actions, like the EU NIS 2 Directive and the IT-SIG 2.0 legislation in Germany.

02 Increased regulation is also occurring in the USA as is evident in the

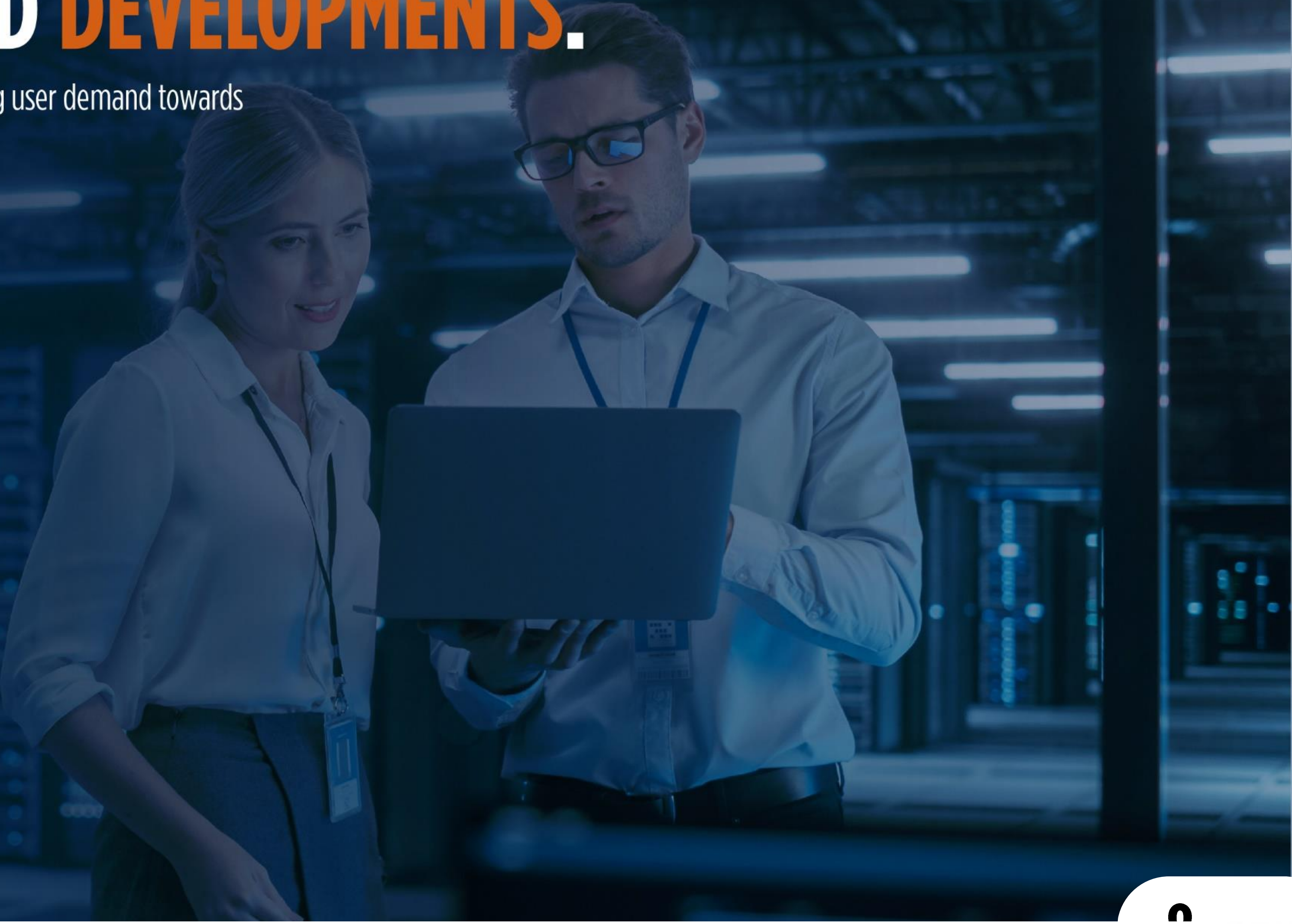
→

03 Increasing demand for products that can help users collect compliance data, prepare periodic reports, and support regulatory queries.

04 Requirements for consistency across industrial cybersecurity programs.

PRODUCT TRENDS AND DEVELOPMENTS.

The increase of cyber threats and regulatory compliance is driving user demand towards more comprehensive asset inventory solutions.



Asset discovery and data collection capabilities including:

Passive scanning, OT-intelligent active scanning, agents that can be embedded within certain devices. Virtual, containerized and cloud-based solutions.

Solutions that support more:

Assets in isolated networks; more detailed information about each device's hardware, firmware, and software including versions, patches, configuration, etc.

PRODUCT TRENDS AND DEVELOPMENTS.

Developments in OT network security solutions.

CYBER SECURITY

Granular security policies, isolate individual devices, enable virtual patching, and implement zero trust strategies.

FIREWALLS

Next generation firewalls that can block messages based on users, devices, and protocols. In some cases, these devices can also support rules that include content within industrial protocols.

REMOTE ACCESS

Some companies are also developing industrial versions of NAC, OT remote access, and network management products with enhanced granularity and Purdue Model system views.

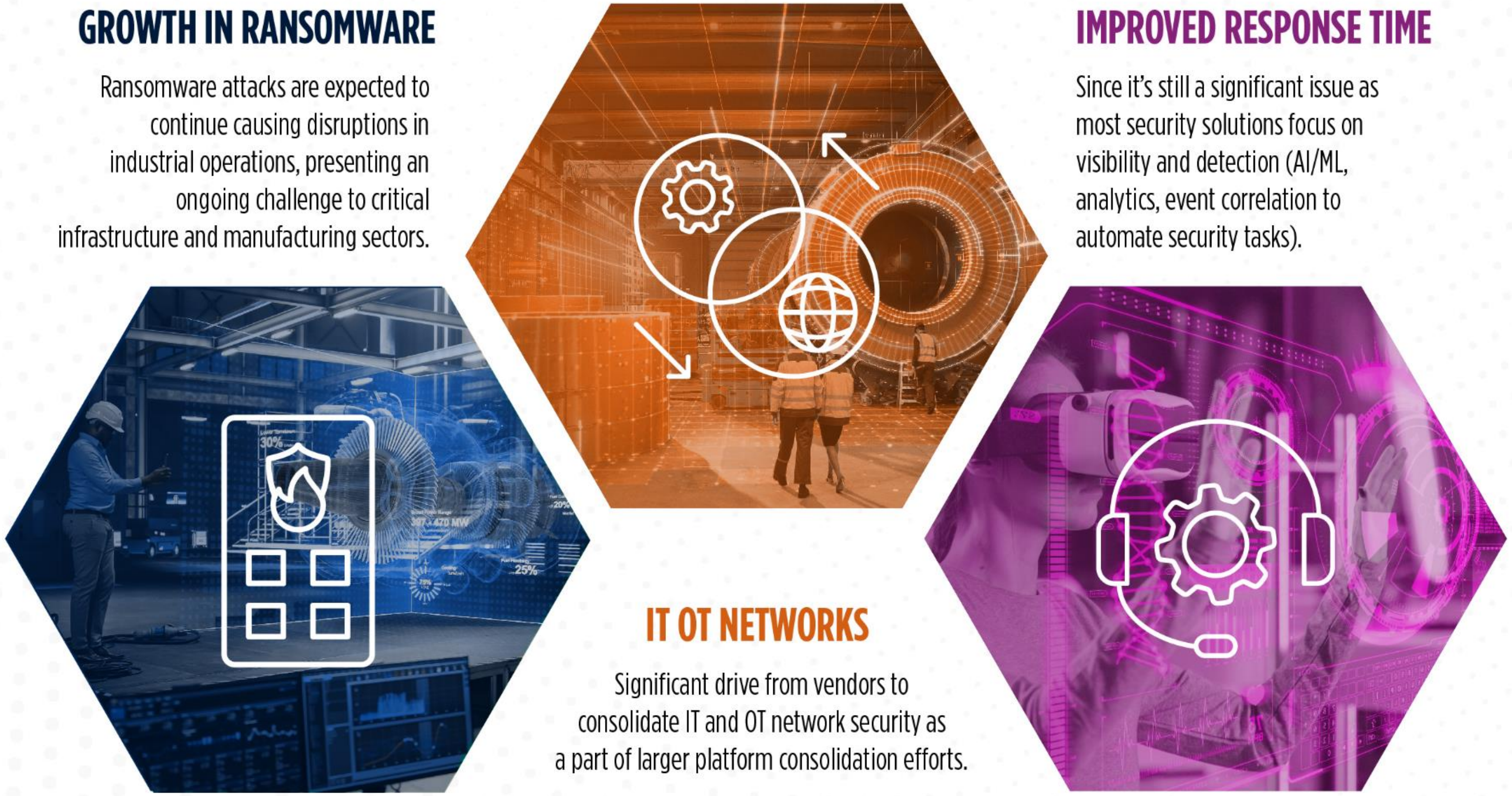
OT CYBER SECURITY MODEL.

Cyber Security Challenges

		No Security	Coincidental Security	Basic Security	Security Awarex	Advanced Security
	Identify				Basic asset management OT asset detection	IT/OT asset management (both network and non network assets) OT visibility
	Protect	No firewall No endpoint security No or poor network segmentation	Basic firewall at selected network intersection Basic endpoint security (for IT system in OT network) Coincidental network segmentation	Basic firewall with proper OT deployment concept Updated endpoint security with ransomware protection (for IT system in OT network) Basic network segmentation	Next-gen firewall Updated endpoint security with ransomware protection (for IT system in OT network) Basic or advanced network segmentation Basic NAC	Next-gen firewall with DPI Updated endpoint security with ransomware protection (for IT and OT system in OT network) Fine-grained network segmentation Next-gen NAC & micro segmentation
	Monitor & Detect	No vulnerability awareness	No vulnerability awareness	Limited vulnerability awareness – from retrospect, reactive rather than proactive	Basic intrusion detection system Limited vulnerability awareness Centralized log	Active vulnerability detection Industrial intrusion detection system with baselining Advanced threat detection Centralized log SIEM
	Remediation	No incident response plan No onsite or remote backup	No onsite or remote backup No incident response plan	Essential backup of IT system in OT Basic incident response plan for IT systems in OT	Essential backup of IT and important OT systems Basic incident response plan for IT and important OT systems	Backup with tested recovery Offline offsite backup Hot stand by system Incident response plan Log management 24/7 monitoring and response
Process	Process and people	No specialized process and people	No specialized process and people	IT and OT security as part of OT networking team	Security expert in OT networking team Focus on security standards E.g: IEC-62443-4-2	Employee awareness and training Specialized OT security team Focus on security standards E.g: IEC-62443-4-2

WHAT'S NEXT?

How will the market develop into the future and how does this affect user demand.



GROWTH IN RANSOMWARE

Ransomware attacks are expected to continue causing disruptions in industrial operations, presenting an ongoing challenge to critical infrastructure and manufacturing sectors.

IMPROVED RESPONSE TIME

Since it's still a significant issue as most security solutions focus on visibility and detection (AI/ML, analytics, event correlation to automate security tasks).

IT OT NETWORKS

Significant drive from vendors to consolidate IT and OT network security as a part of larger platform consolidation efforts.

THANK YOU!

BEDANKT

QUESTIONS?