EVENT OVERVIEW:

#ManuSec Europe is an intimate and exclusive platform for IT and OT security leaders from Europe’s manufacturing industry to exchange in-depth cybersecurity knowledge. Senior cybersecurity professionals share first-hand insights through real-life case studies, panel debates, and keynote presentations, while bringing forth questions and challenges to be discussed over roundtables and dynamic networking breaks.

This is your annual opportunity to build cross-departmental cybersecurity partnerships, benchmark your company’s digital maturity against peers, and participate in the discussions shaping European manufacturers’ cybersecurity landscape in 2020 and beyond.

SPONSORS:
With the convergence of industrial control systems and enterprise infrastructure, and legacy equipment being connected through the Industrial Internet of Things, cyber security is a top-of-the-list priority.

To properly face cyber risk in the digital age, organisations must fully engage at all levels, to collaborate and establish best practice policies to ensure safety is maintained on the factory floor, prevent production halts from occurring and protect intellectual property from being stolen.

**LEARNING OBJECTIVES**

- Create synergies with IT and OT leaders
- Gain industry-wide perspective on how cyber risk is changing due to the spread of automation on the shop floor
- Find tools and resources for mapping your attack surface
- Learn how to address supply chain vulnerabilities
- Share best practices on incident response and recovery plans

**STEERING COMMITTEE**

**Dr. Bernd Bieker**  
Program Lead OT Cyber Security  
Novartis

**Eric Ten Bos**  
Global Lead OT/IoT/IoT Cyber Security  
Thales

**Jesus Molina**  
Director of Business Development  
Waterfall Security

**Ofer Shaked**  
Co-Founder & CTO  
SCADAfence

**Carlos Olave Rojo**  
Automation Engineer - Industrial OT Cyber Security  
Food Packaging Company

**Adam Wedgbury**  
Cyber Security OT Innovation Lead  
Airbus

**Christian Koch**  
Senior Manager GRC & IoT/OT  
NTT Ltd.

**INDUSTRIES:**
- Automotive
- Food & Beverage
- Energy
- Pharmaceutical
- Chemical
- Electronics
- Machinery
- Agriculture
- FMCG

**Claroty's mission is to protect industrial control networks from cyber-attacks; ensuring the safe and reliable operation of the world most critical infrastructures. Claroty enables customers to enjoy the substantial benefits of increasingly networked control systems without compromising operational resiliency, personnel safety or the security of core assets. The Claroty Platform is an integrated suite of cybersecurity products, providing unmatched threat protection, detection and response.**

**VISIT:** [www.claroty.com](http://www.claroty.com)

**Irdeto** is the world leader in digital platform security, protecting platforms and applications for video entertainment, video games, connected transport and IoT connected industries. Irdeto's solutions and services enable customers to protect their revenue, create new offerings and fight cybercrime. With 50 years of expertise in security, Irdeto's software security technology and cyberservices protect over 5 billion devices and applications for some of the world's best-known brands.

**VISIT:** [irdeto.com](http://irdeto.com)
CyberX provides the most widely-deployed industrial cybersecurity platform for edging ICS risk. Supporting all OT vendors and seamlessly integrating with existing IT security tools, CyberX’s platform combines a deep understanding of industrial protocols, devices and applications with ICS-specific asset discovery, continuous real-time monitoring and incident forensics, risk and vulnerability management and threat intelligence. CyberX recently published the first-ever “Global ICS & IIoT Risk Report,” a DBIR-like analysis of real-world vulnerabilities found in 375 production ICS networks worldwide.

Radiflow is a leading provider of cyber security for critical infrastructure networks. The Radiflow solution provides operators with visibility and control of their OT network; including both non-intrusive Industrial IDS to monitor real-time networks and security gateways to secure access to devices in critical zones.

Rhebo is the only company providing cybersecurity as well as stability for industrial control systems (ICS) in industrial and critical infrastructure companies. The solution monitor all communication within the ICS, and reliably report attacks, vulnerabilities as well as technical error states. Thus, Rhebo increases resilience and reliability to safeguard the digital transformation.

SCADAfence helps companies with large-scale operational technology (OT) networks embrace the benefits of industrial IoT by reducing cyber risks and mitigating operational threats. Our non-intrusive platform provides full coverage of large-scale networks, offering best-in-class detection accuracy, asset discovery and user experience.

Nozomi Networks is revolutionizing Industrial Control System (ICS) cybersecurity with the most comprehensive platform for real-time cybersecurity and operational visibility. Since 2013 the company has innovated the use of machine learning and artificial intelligence to meet the unique challenges of critical infrastructure operations. Deployed in the world’s largest industrial installations, Nozomi Networks delivers network visualization and monitoring, cybersecurity incident and process anomaly detection, asset management and vulnerability assessment.

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, 100-percent real-time discovery and classification, as well as continuous posture assessment.
A CONFERENCE BY QATALYST GLOBAL
T: +44 203 740 9106 | E: event@qatalystglobal.com  |  www.qatalystglobal.com

MANUSEC EUROPE
4-5 February 2020 | Munich, Germany | europe.manusecevent.com | #ManuSec

SPEAKERS

Dr. Bernd Bieker
Programme Lead OT Cyber Security Novartis Business Services

Ali Baccouche
Information Security & Data Protection Officer EMEA Texas Instruments

Petri Ala Annala
CISO Nobia

Elad Ben-Meir
CEO SCADAfence

Leonardo Casubolo
Director Global IT Infrastructure & Security Burckhardt Compression AG

David van Crout
Senior Director Europe Clarity

Peter Dornheim
Head of IT Security Festo

Jakub Duch
Executive Officer, Vice-President International Sales Allied Telesis

Alexander Giehl
Security Expert Fraunhofer AISEC

John Hales
Security Consultant Unisys

Ricardo Hormann
Industrial Security Manager Volkswagen

Michael von der Horst
Managing Director Cyber Security Germany Cisco

Christian Koch
Senior Manager GRC & IoT NTT Ltd.

Thomas Kuhn
CISO s.Oliver

Roberto Lopez
Automation Lead Global Supply – ICS Cybersecurity Programme – Madrid Site Representative Pfizer

SPEAKERS

Trish McGill
Sr. SME Cyber Security Confidential

Prof. Dr.-Ing. Dominik Merli
Head of Institute HSA, inos Augsburg University of Applied Sciences

Andrew Tsonchev
Director of Technology Darktrace Industrial

Klaus Mochalski
CEO & Co-Founder Rhebo

Stefan Wenigmann
CSO Bucher Industries

Ilan Bara
CEO Radiflow

Ilan Bara
CEO Radiflow

Jesper Nilsson
Business Development Director - DACH Region CyberX

Brandon Witte
CEO Sightline

Thomas Nowey
CISO Krones

Speaker TBC
Senior Expert Forescout

Eric ten Bos
Global Lead OT/IIoT Cyber Security Thales

Ilan Bara
CEO Radiflow

Dr. Bernd Bieker
Programme Lead OT Cyber Security Novartis Business Services

Marco Tagliaferro
Senior IT Security Manager Avon

For more information on our Speakers, please visit:
europe.manusecevent.com
CONFERENCE DAY ONE
TUESDAY 4th FEBRUARY 2020

REGISTRATION
08:00

OPENING ADDRESS FROM THE CHAIR:
Stefan Wenigmann, CISO, Bucher Industries
08:45

OPENING PANEL
Managing Cyber Risks in the Age of Smart Production
09:00

Moderator: Jakub Duch, Executive Officer, Vice-President International Sales, Allied Telesis

- Leonardo Casabolo, Director Global IT Infrastructure and Security, Burckhardt Compression
- Dr. Bernd Bieker, Program Lead OT Cyber Security, Novartis
- Martin Schleker, Production IT Security Manager, ZF
- Josef Kriegmaier, IT Security Centre Manager, MTU Aero Engines (TBC)

• How have the proliferation of automation on the shop floor and the convergence of IT and OT changed your cyber risk profile?
• How are you ensuring key security and risk considerations are prioritised over the productivity potential of new digital technologies?
• What measures are you putting in place to prevent new technologies from becoming conduits for security threats?
• Are you assessing and then mitigating the risks they bring?

11:00

PRESENTATION
Top 3 Use Cases for Automated OT Asset Discovery & Management

This session discusses 3 real-life use cases where automated OT asset management was employed and the results. Specifically:
• How these organisations understood and controlled the cyber security resilience of ICS assets
• How they improved incident response, shortened resolution time, ensured operations continuity
• How these profile organisations found a new level of compliance with industry regulations

- Senior Expert, Darktrace Industrial

11:30

PRESENTATION
Bringing IT and OT Together by Using Intrusion Detection Systems and Asset Management

Key points we will discuss during this live interview:
• Setting up an awareness campaign and promoting interdepartmental synergies
• TCOT emergency exercises
• Different approaches for different stakeholders

- Ricardo Homann, Industrial Security Manager, Volkswagen

12:00

SEATED LUNCH

09:40

OFFICIAL KEYNOTE
Protecting Productivity: Walk Throught Our Company’s Journey as They Embraced Digital Modernisation & The Risks Involved

- David van Crout, Senior Director Europe, Claroty

12:30

PRESENTATION
IT and OT Security Aligned - A Story from the ‘Manufacturing’ Trenches

• The Convergence of IT and OT
• Industrial Cyber Attack Components
• Case Study - Largest Manufacturing Company in Europe

- Elad Ben-Moï, CEO, SCADAfence

13:30

PRESENTATION
Protecting Manufacturing Sites from Cyber Attacks - Insights from Procter & Gamble

Operational Technology and manufacturing sites present a unique challenge for security teams. Failing to take proactive security measures can cripple operations and cause major financial losses – as recently shown by the Norrköping attack. In this session, Mark Ruble, the Senior Manager Information Security Cyber Defense at P&G will discuss these challenges as well as innovative ways to detect and mitigate today’s complex cyber attacks.

- Mark Ruble, Senior Manager Information Security Cyber Defense, P&G

14:00

NEWSWORTHY SESSION
Rounding Tables - Delegates will split into 5 working groups, each making up a roundtable, to discuss a specific issue and exchange ideas and experiences related to it. A moderator will be facilitating the discussion at every table.

T1: Leonardo Casabolo, Director Global IT Infrastructure and Security, Burckhardt Compression
T2: Ali Barcuchiche, Regional Information Security & Data Privacy Officer EMEA, Texas Instruments
T3: Michael van der Horst, Managing Director Cyber Security Germany, Cisco
T4: Senior Expert, Forescout
T5: Senior Expert, KPMG

14:30

PRESENTATION
Cyber Securing One of Our Spanish Sites

• How we have restructured the plant’s architecture
• Industrial network segmentation
• Next steps ahead: how we are developing an OT security plan and implementing hardening processes

- Roberto López Martínez-Santos, Automation Lead Pfizer Global Supply - ICS Cyber Security Programme - Madrid Site Representative, Pfizer

15:00

PRESENTATION
A Data-Driven Analysis of Hidden Vulnerabilities in IoT & ICS Networks

• The results of our “2019 Global ICS & IoRT Risk Report,” a data-driven analysis of real-world network traffic captured from more than 850 production ICS networks worldwide
• Four steps towards protecting your “crown jewel” assets, based on INL’s risk-based CCE methodology

- Jesper Nilsson, Business Development Director – DACH Region, CyberX

15:30

NETWORKING BREAK

16:00

PRESENTATION

Where should manufacturers start to implement industrial security according to IEC 62443 and ISO 27000? How can you quickly and comprehensively identify threats to the ICS and determine sound mitigation strategies? And how do you implement a meaningful PoC for your industrial security strategy within a few weeks to identify the relevant actions?

- Klaus Mochalski, CEO & Co-Founder, Rhebo

16:30

NETWORKING DRINKS

17:20

EVALUATION FORMS

17:30

DINNER HOSTED BY:

19:00

HOSTED BY:

T: +44 203 740 9106 | E: event@qatalystglobal.com  |  www.qatalystglobal.com
1. A Guide to a Systematic and Viable Patching

- Petri Ala Annala, CISO, Nokia

2. Insights on Privacy-Preserving Architecture in the Field of Industrial Optimisation

- Dana Samaroo, IT Supervisor, Caribbean Gas Chemical Ltd.

3. Insights into a Cyber Security Culture Which Grows through Collaboration between IT and OT Cyber Security Projects

- Peter Dornheim, Head of IT Security, Festo

4. Manufacturing in R&D: Learning from the Rest of R&D OT

- Yin Tateno, R&D Pharma OT Security, GSK
Upcoming Events:

**Cyber Security for Critical Manufacturing**
- **USA - CHICAGO**
  - October 2020
- **EUROPE - MUNICH**
  - February 2021

**Industrial Internet of Things**
- **USA - CHICAGO**
  - October 2020
- **EUROPE - MUNICH**
  - February 2021

co-hosted with:

Media Partners:

[Logos of the media partners are depicted here.]