Post event report

SECURING MANUFACTURING

Securing Manufacturing

24th April 2025 | Online

Strategic Sponsors

censys

CLAROTY

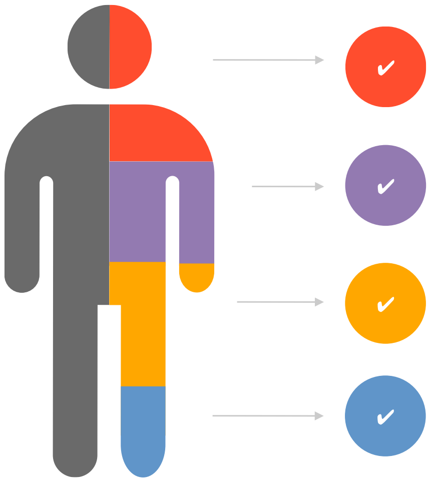
> “As a first-time attendee, I was not sure what to expect but the information was presented in digestible chunks, without being overwhelming. The topics were varied and well-organised and the leads presenting offered a great mix with vast knowledge. Well worth the time attending.”
>
> **IT/CIM Engineer – Production IT Security Co-ordinator, ZF Group**

Inside this report:

Key themes

- Transitioning OT to the Cloud?
- Achieving visibility across ecosystems
- Pen testing for OT / SCADA
- OT and the regulations
- Why zero trust, isolation and segmentation are key
- Defending against the latest ransomware variants

Who attended?



Cyber-security
We have a 20-year track record of producing the events cyber-security professionals take seriously

Risk Management
We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance
We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy
We are a key venue for decision-makers with budget and purchasing authority

Speakers

Simon Brady,
Event Chairman
AKJ Associates

Ian Cowhig,
Operating Technology Lead
Diageo

Rob Flanders,
Head of Threat and Incident Response
BAE Systems

Elliot Gidley,
CTO
Claroty

David McIlwaine,
Head of Cyber Practice
Pinsent Masons

Nick Palmer,
Technical Lead, EMEA
Censys

Matthew Rogers,
Industrial Control Systems
Cybersecurity Expert
CISA

Quentyn Taylor,
Senior Director –
Product, Information Security and
Global Incident Response
Canon Europe, Middle East and Africa

Ian Thompson,
Head of Cyber Threat Intelligence
BP

Agenda

09:30 Chair's welcome

09:35 **Secure by Design: Strengthening cybersecurity in manufacturing**

Matthew Rogers, Industrial Control Systems Cybersecurity Expert, CISA

- The international focus on shifting security to the manufacturer
- Key Secure by Design principles to consider as a manufacturer and as a customer of other manufacturers in the supply chain
- Considerations for navigating out of legacy operational technology patterns when embedding security into the product
- The importance of tying together human centred design research and cybersecurity

09:55 **Securing the supply chain: Cyber-risk management for manufacturers**

Nick Palmer, Technical Lead, EMEA, Censys

- Identify and mitigate cybersecurity risks in the manufacturing supply chain
- Protect infrastructure, sensitive data, and business continuity from third-party threats
- Implement advanced security solutions for threat detection and response
- Strengthen risk communication strategies to improve supply chain resilience

10:15 **FIRESIDE CHAT: Cyber on tap – protecting the systems behind the spirits**

Ian Cowhig, Operating Technology Lead, Diageo

- How do you manage cyber-risk across its vendors?
- How do you stay ahead of tech changes in OT without disrupting operations?
- What's your approach to securing legacy systems?
- How do you build cyber-awareness on the factory floor?
- If you could wave a magic wand and fix one cybersecurity challenge overnight – what would it be?

10:45 **Adapting to new regulations: Strengthening product security**

Quentyn Taylor, Senior Director – Product, Information Security and Global Incident Response, Canon Europe, Middle East and Africa

- Navigating new regulation – balancing risk mitigation with strategic opportunities
- Placing product security – where should security teams sit for maximum impact?
- Building strong teams – key steps and benefits beyond compliance

11:10 Comfort break

11:20 **0-day bingo: Depth in incident response**

Rob Flanders, Head of Threat and Incident Response, BAE Systems

- Insights and experiences from BAE Systems on managing cyber-attacks
- Strategies for safeguarding critical infrastructure and supply chain partners
- The growing complexity of the cyber-threat landscape
- Reducing the impact of incidents through proactive defence

11:40 **State of CPS Security: OT Exposures 2025**

Elliot Gidley, CTO, Claroty

Elliot delves into the new research report 'State of CPS Security: OT Exposures 2025.' The report covers 940,000-plus OT devices analysed across 270 organisations and lays out the greatest risks associated with OT and ICS beyond merely assessing the criticality of a vulnerability. Key takeaways:

- Prioritise highest risk: Redefine vulnerability management and prioritise remediation based on KEVs that are insecurely exposed to the internet and linked to ransomware
- Shift to exposure management: Enrich your risk assessment with known exploits, exploit prediction scores, and business impact assessments to focus on the most consequential impacts to production and narrow the effort to risks that are exploitable today
- Ensure secure access: Secure access is an indispensable control given the need for remote access to OT environments from employees and third parties
- Protect the network: Network segmentation is a critical control within CPS environments

Agenda

12:00	**FIRESIDE CHAT: Beyond threat awareness to action – a necessary revolution** **Simon Brady,** Event Chairman, AKJ Associates; **Ian Thompson,** Head of Cyber Threat Intelligence, BP • Why do organisations need to change their approach to threat management? • How can we evolve our security strategies to incorporate threat intelligence and counter-threat tradecraft as distinct and vital elements of our overall cybersecurity efforts? • How do we separate threat management from traditional governance and policy frameworks in practice, and why is this essential in the evolution of security strategies? • As we can't manage threat the same way we manage risk, how do we develop a deeper understanding of how threat actors operate and succeed? • What specific tailored strategies for threat mitigation and management have you put in place in BP? What, in your opinion, has had the biggest impact and how do you measure this? • What practical advice would you give to those wishing to integrate threat intelligence and counter-threat strategies into their core security mission? Where do they start?
12:30	**Implementing CRA: Legacy products, components, and compliance obligations** **David McIlwaine,** Head of Cyber Practice, Pinsent Masons • Defining scope and applicability for manufacturing operations • Core compliance actions for manufacturers • Embedding CRA requirements from design to deployment
12:50	Chair's closing remarks
13:00	End of conference