Post event report

Strategic Sponsors

BeyondTrust

censys

CLAROTY

CROWDSTRIKE

LMNTRIX
BE THE HUNTER | NOT THE PREY

THREATLOCKER®
ZERO TRUST PLATFORM

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
- Making the best use of threat intelligence
- Security Posture Management
- Improving continuous attack surface discovery
- The power of automation
- Adversary simulation and behavioural analysis
- Dealing with regulations

Who attended?

Cyber-security
We have a 15-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

Marius Ebel,
Senior Security Specialist
Bilfinger

Santtu Erkkilä,
Cyber Governance, Risk & Compliance Lead
Neste

Elliot Gidley, EMEA Field CTO,
Claroty

Kinga Kertesz-Takacs,
Sr. Operational Technology Governance & Compliance Manager
Haleon

Gustavo Mania,
Information Security and Risk Manager (Regional CISO)
HEINEKEN (AME)

Eoin McGrath,
Solutions Engineer
ThreatLocker

Carlo Minassian,
Founder & CEO
LMNTRIX

Nick Palmer,
Senior Solutions Engineer
Censys

Matthew Rogers,
Industrial Control Systems Cybersecurity Expert
CISA

Tom Scase,
Principal Solutions Engineer
BeyondTrust

Kate Silverman,
Deputy CISO
Ardagh Group

Sam Thompson,
Senior Corporate Sales Engineer
CrowdStrike

Agenda	
08:50	Chair's opening remarks
09:05	**The risks and opportunities that AI brings to cybersecurity** **Gustavo Mania,** Information Security and Risk Manager (Regional CISO), HEINEKEN (AME) • Real-world AI-driven cyber-risks – from phishing automation to deepfakes and agentic AI threats • Learn how HEINEKEN manages emerging AI risks while harnessing AI to strengthen defence • Gain practical insights to help your organisation embrace AI securely and strategically
09:25	**From blind spots to control: Achieving complete ICS/OT exposure visibility in manufacturing** **Nick Palmer,** Senior Solutions Engineer, Censys • Gain full ICS/OT visibility: Discover exposed HMIs, PLCs, and controllers with continuous global scanning and asset intelligence • Validate exposures quickly: Use real HMI screenshots and metadata to confirm risks with confidence • Speed up incident response: Triage alerts faster with contextual evidence and historical exposure data • Simplify compliance reporting: Generate audit-ready insights for industry regulators
09:45	**Inside the manufacturing threat landscape – and how beyondtrust closes the gaps** **Tom Scase,** Principal Solutions Engineer, BeyondTrust • UK manufacturers face rising cyber-risk across operational technology, driven by ransomware, insecure remote access, and IT/OT convergence • This session examines why legacy approaches no longer protect modern plants and shows how a framework-driven model aligned to Purdue and ISA-95 enables secure access without disrupting production • Learn how BeyondTrust helps manufacturers secure vendor access, control credentials, and reduce OT attack surface pragmatically • Understand how OT cyber-risk is rising and directly threatens uptime and safety • How legacy remote access and VPNs are no longer fit for manufacturing • Secure OT access can align to Purdue without disrupting production • How to reduce risk fast with credential management and controlled vendor access
10:05	**Cyber crisis in manufacturing: Prioritising recovery when everything is critical** **Kinga Kertesz-Takacs,** Sr. Operational Technology Governance & Compliance Manager, Haleon • Risk-based restoration sequencing: How to determine what truly needs to come back online first during multi-site disruptions • Executive decision-making under pressure: Strategies for making fast, defensible recovery choices when every system feels mission-critical • Building resilience before the crisis: Using governance frameworks to strengthen operational recovery and long-term stability
10:25	Comfort break
10:30	**How Neste built a business-driven cyber-risk program** **Santtu Erkkilä,** Cyber Governance, Risk & Compliance Lead, Neste • Understand the key challenges Neste faced in managing cyber-risk across a global, complex industrial and R&D environment • See the step-by-step journey of transforming their cyber-program into one that is business-driven and risk-informed • Learn the lessons from Neste's experience that you can apply to mature your own organisation's risk management program
10:50	**CrowdStrike 2026 Global Threat Report: A review of key findings** **Sam Thompson,** Senior Corporate Sales Engineer, CrowdStrike • Adversaries are becoming more evasive, faster, and harder to stop – they're leveraging AI and abusing unmanaged edge devices to move rapidly across endpoint, identity, cloud, and SaaS environments while operating in plain sight • Join us for an in-depth review of the findings from the CrowdStrike 2026 Global Threat Report to gain actionable insights, strengthen your defences, and learn the critical steps needed to protect your organisation in the year ahead
11:10	**Insights for OT resilience, reduce exposure & supply chain attack in 2026** **Elliot Gidley,** EMEA Field CTO, Claroty • Manufacturing is being targeted by cybercriminal gangs • Exposed HMIs and Open VNC is the weapon of choice • Supply chain using non-central Secure Remote Access solutions are a risk • Centralising Secure Remote Access

Agenda			
11:30	**Maintaining operations through conflict: Emergency planning in a connected OT environment** **Matthew Rogers,** Industrial Control Systems Cybersecurity Expert, CISA • Security connectivity principles for OT, designing OT systems to be interconnected while maintaining operator control • Threats impacting reliable telecommunications and internet, as well as disrupting and destroying OT • CI Fortify, isolation and recovery goals for preventing some impact to OT in a crisis or conflict • How to address connectivity requirements impact on isolation and recovery		
11:50	Comfort break		
11:55	**How conversations about risk shape everyday security decisions** **Marius Ebel,** Senior Security Specialist, Bilfinger • How everyday interactions and language shape shared reasoning about security risk • Why the way security discussions start often matters more than the controls or policies being discussed • How risk-based thinking plays out in day-to-day decisions beyond rules, tools, or processes		
12:15	**Beyond logs: Why manufacturers need active defence to detect earlier and respond faster** **Carlo Minassian,** Founder & CEO, LMNTRIX • Manufacturing has been the #1-targeted industry by cybercriminals four years running – yet most security budgets still pour 80% into prevention, leaving detection and response chronically underfunded and understaffed • Logs-only approaches are failing: 99% of successful attacks go undiscovered by log analysis alone, and 83% of incidents take weeks or more to uncover. The industry needs a structural shift toward active defence – real-time monitoring, behavioural analysis, and human threat hunters who can spot what automated tools miss • Building a tiered Cyber Defence Centre (CDC), combining automation for high-volume triage with expert analysts for adversary hunting, gives manufacturers a practical framework for slashing mean time to remediate and limiting attacker dwell time • As ransomware actors evolve from encryption to pure extortion and IP theft, how do manufacturing security teams secure executive buy-in, the right organisational structure, and the authority to act – before the next incident forces the issue?		
12:35	**Make your business a hard target for cybercriminals** **Eoin McGrath,** Solutions Engineer, ThreatLocker • When it comes to potential targets for cyber-attacks, easier to breach means more likely to fall victim • While you might not be able to influence your perceived value, there are changes that can eliminate your organisation from being seen as an easy target • We'll explore practical tactics to reduce your surface area of attack and controls to prevent lateral movement should a breach occur		
12:55	**IT/OT data convergence and data value** **Kate Silverman,** Deputy CISO, Ardagh Group • Understand how IT and OT data integration creates unified, real-time operational and business insights • Identify practical IT and OT data insights that drive performance, reliability, and efficiency improvements • Learn how to evaluate and define measurable data value aligned to business outcomes • Explore key data sharing considerations, including governance, ownership, interoperability, and cybersecurity • Recognise regulatory and compliance considerations impacting IT/OT data environments		
13:05	Chair's closing remarks	**13:15**	End of conference