Post event report

Strategic Sponsors

Akamai

BeyondTrust

CLAROTY

DRAGOS

HUNTRESS

Inside this report:

Key themes

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

Adam Abdat,
SOC Lead
easyJet

Chris Butchart,
Senior Solutions Engineer
BeyondTrust

Robert FitzSimons,
Sales Engineering Manager
Huntress

Julio Gonzalez-Saenz,
Quantum Engagement Lead
Vodafone

Natalie Gristwood,
Associate Principal Consultant
Dragos

Richard Meeus,
Senior Director Security Technology and Strategy, EMEA
Akamai

Julian Smith,
Principal Solutions Engineer
Claroty

Manit Sahib,
Ethical Hacker &
Former Head of Penetration Testing & Red Teaming
Bank of England

Andrea Szeiler,
Group CISO
MVM Ltd

Simon Turner,
Head of Security Governance and Compliance
BT Group

Nathan Wyatt,
Information Security Engineer
The Telegraph Group

Agenda

09:00	Chairman's welcome
09:10	**Compliance as a consequence: Driving security, enabling assurance**
	Simon Turner, Head of Security Governance and Compliance, BT Group • Reframing compliance as the natural result of strengthening governance, managing risk, and designing effective controls, rather than treating it as a standalone or periodic activity • Unifying GRC efforts by embedding clear ownership, aligned controls, and security practices into daily operations while meeting overlapping regulatory and certification requirements • Strengthening resilience and reducing waste by moving from chasing audit evidence to building systems where compliance is the outcome of doing security the right way
09:30	**Building a modern OT security program: From asset visibility to uptime**
	Julian Smith, Principal Solutions Engineer, Claroty • How to overcome IT/OT integration challenges, bridge organisational silos, and prioritise the visibility blind spots that matter most across complex CNI environments • Why behaviour-based monitoring outperforms vulnerability-driven risk scoring when protecting legacy devices and safeguarding system uptime • Best practices for prioritising high-impact risks aligned with regulatory frameworks like NIS2 and NCSC CAF, maximising operational resilience without overloading team capacity
09:50	**Run like a business: What 196,000 leaked ransomware chats teach CNI defenders**
	Chris Butchart, Senior Solutions Engineer, BeyondTrust • Inside the leaked internal chats of a major ransomware operation: roughly 196,000 messages revealing a group run like a business, with salaries, management structure and office hours • Why the front door is remote access, not malware: what the group's own communications show about buying, brute-forcing and reusing VPN and remote access credentials instead of burning zero days • The weakest link in converged IT/OT environments: unmanaged third-party and vendor privileged access, and why the traditional VPN and jump host model cannot answer 'who did what, where, and with which credential' • What good looks like: closing the remote access gap with identity-first controls, including just-in-time access, credential injection and full session recording
10:10	**Defending tomorrow: The future of SOC and cybersecurity**
	Adam Abdat, SOC Lead, easyJet • Enhancing Tier-1 SOC workflows by improving signal quality, reducing alert fatigue, and supporting faster, more accurate triage • Bringing together security, cloud, and IT insights to improve collaboration and cross-team decision-making • Strengthening incident response by improving visibility, reducing tool sprawl, and streamlining operational processes • Tackling emerging threat patterns — including human, machine, and AI-driven behaviours — through improved detection and analysis
10:30	Comfort break
10:35	**Third-party risk? Managed!**
	Andrea Szeiler, Group CISO, MVM Ltd • Understanding your third-party ecosystem: Mapping vendors, services, and business dependencies to identify what truly matters • From compliance to control: Turning regulatory requirements into a practical approach for assessing and managing third-party risks • Trust, verify, collaborate; Strengthening resilience through effective partnerships, clear responsibilities, and shared preparedness
10:55	**Decrease your attack surface whilst decreasing costs – The perfect win-win**
	Richard Meeus, Senior Director Security Technology and Strategy, EMEA, Akamai • As cyber-threats become more sophisticated, traditional network security approaches are no longer enough • In this webinar, we will explore how microsegmentation capabilities help organisations reduce attack surfaces, limit lateral movement, and strengthen security across hybrid and distributed environments • We'll look at how microsegmentation works, the key benefits for modern IT and security teams, and how Akamai can help implement effective segmentation without adding unnecessary complexity • Participants will also gain practical insights into securing applications and workloads against today's evolving threats

Agenda

11:15	**From Telco to Quantum Telco: Reskilling for the quantum era** **Julio Gonzalez-Saenz,** Quantum Engagement Lead, Vodafone • Quantum and the Telco's role • Quantum Telco pillars • Current initiatives & skills transition • Reskilling framework • Engagement & culture		
11:35	Comfort break		
11:40	**Securing the autonomous frontier: Guardrails, governance, and agentic AI** **Nathan Wyatt,** Information Security Engineer, The Telegraph Group • Securing autonomous agents • Hardening the MCP integration layer • Bringing shadow AI to light • Defending the CNI boundary • Actionable security playbook		
12:00	**Protecting critical national infrastructure in a changing threat landscape** **Robert FitzSimons,** Sales Engineering Manager, Huntress • Critical national infrastructure is increasingly targeted by attackers who do not need to break in, they simply log in using stolen credentials, compromised identities, or trusted tools • This session explores how organisations can move beyond alert fatigue and respond to the threats that matter most. We will discuss the modern attack chain, the importance of detecting initial access and lateral movement early, and how human-led threat hunting and security posture management can help protect essential services and strengthen resilience before an incident becomes a national-impact event		
12:20	**From visibility to velocity: Turning OT intelligence into decisive action** **Natalie Gristwood,** Associate Principal Consultant, Dragos • The visibility paradox: more data, slower decisions. Most organisations have deployed visibility tools. So why are response times still measured in days? How are leading organisations using intelligence to cut through noise and move from detection to action in hours, not weeks? • Intelligence-driven prioritisation: Now, Next, Never. Not all threats are equal. How are CISOs and OT leaders using threat context and adversary behaviour to separate what needs immediate action from what can wait – and what never needs to be touched? The difference is measured in operational risk and team capacity • From board questions to board confidence. Executive teams and regulators demand defensible answers: Where is the real risk? What are we doing about it? How do we know it's working? Intelligence-grounded decisions give you the narrative that sticks • Speed as a competitive advantage in incident response. When an incident strikes, velocity matters. How are organisations leveraging pre-incident intelligence and investigation frameworks to shrink mean time to respond (MTTR) and limit operational impact? • Building a decision-support function, not just an alerting function. The gap between security tool alerts and board-level decisions is where most programs stall. What does a true intelligence-informed decision framework look like in practice?		
12:40	**Invisible leaks: The hidden risks of chatting with AI** **Manit Sahib,** Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England • AI privacy risks: How tools like ChatGPT, Claude, and Co-Pilot can end up knowing more about you than your best friend (and never forget a thing). The hidden dangers of casually sharing information with AI • When Small details add up: Why a few 'harmless' details can combine to paint a full picture & How scattered information can reveal sensitive data without you realising • The myth of security: Why AI models aren't as secure as we might think & How attackers can trick them into spilling information • Simple, practical steps: For employees: how to keep personal and company data safe & For organisations: reducing AI-related risks before they grow		
13:00	Chair's closing remarks	**13:05**	Conference end