


Post event report



Strategic Sponsor



Key themes	Speakers
Defending against the latest ransomware variants	Dr. Hans-Martin von Stockhausen, Principal Key Expert for Cybersecurity Siemens Healthineers
Transitioning OT to the Cloud?	Eltjo Hofstee, Global Director Sales EasyDMARC
Achieving visibility across ecosystems	Manit Sahib, Ethical Hacker The Global Fund
OT and the regulations	Martin Jarvis, Incident Management Lead, Cyber Security Operations Centre NHS England
Why zero trust, isolation and segmentation are key	Nasser Arif, Cyber Security Manager LNWUH NHS Trust & THH NHS Foundation Trust
Pen testing for OT / SCADA	Nick Palmer, Technical Lead, EMEA Censys
Who attended?	Prakhar Chandra, Cyber Security Business Partner, CISO Function NHS England
	Seema Srihari, Information Governance Manager & DPO North East Ambulance Service NHS Foundation Trust (NEAS)
	Ty Greenhalgh, Industry Principal – Healthcare Claroty

Agenda		
09:20	Chair's welcome	
09:30	An insight into securing healthcare CNI	
	Prakhar Chandra , Cyber Security Business Partner, CISO Function, NHS England <ul style="list-style-type: none"> How do we identify our CNI/mission critical systems The 3 line of defence model Major threats and challenges facing our CNI 	
09:50	Post-market cyber-transparency for medical devices	
	Dr. Hans-Martin von Stockhausen , Principal Key Expert for Cybersecurity, Siemens Healthineers <ul style="list-style-type: none"> Demystifying 'shared responsibility' for the cybersecurity of medical devices Why can't we have patches for our device on patch Thursday? About the importance of communication in vulnerability management 	
10:10	The hidden perimeter: Managing third-party risk in connected care	
	Ty Greenhalgh , Industry Principal – Healthcare, Claroty <ul style="list-style-type: none"> Third-party access is one of the most exploited threat vectors in healthcare – find out why it's escalating, especially through IoMT, IoT, and OT ecosystems that blur the boundaries of traditional network security Examine real-world attack data, including volume, breach frequency, and operational consequences linked to unauthorised external access across connected medical and operational devices Learn how NIS2 and the UK's Cyber Assessment Framework are reshaping expectations around third-party risk and secure connectivity in hospitals and critical care environments Contrast global approaches, including lessons from the US healthcare sector's ongoing struggle to manage secure third-party access amid rising digital complexity 	
10:30	People, pressure, and possibility in cyber-response	
	Martin Jarvis , Incident Management Lead, Cyber Security Operations Centre, NHS England <ul style="list-style-type: none"> What trips you up – lessons learned from navigating real-world cybersecurity incidents and how to get ahead of them Managing an incident in unfamiliar environments Why your team is your greatest asset, and how to build it, keep them motivated and mission-ready Embracing opportunities for growth, improvement, and transformation that can emerge from a cybersecurity breach 	
10:50	Comfort break	
11:00	Is there really a cybersecurity skills gap?	
	Nasser Arif , Cyber Security Manager, LNWUH NHS Trust & THH NHS Foundation Trust <ul style="list-style-type: none"> Addressing the so called cybersecurity skills gap within the healthcare sector Highlighting the benefits of focusing on transferable skills Practical tips and tricks to improve the security culture within your organisation 	
11:20	Securing healthcare: How Attack Surface Management protects critical systems & digital frontline	
	Nick Palmer , Technical Lead, EMEA, Censys <ul style="list-style-type: none"> Healthcare organisations face an expanding digital attack surface, making full visibility into internet-exposed assets critical Attack Surface Management (ASM) is essential to identifying security blind spots and mitigating cyber-threats in real time Leading healthcare providers are integrating ASM with existing security stacks to proactively defend against attacks Real-world use cases show how ASM helps reduce risks, enhance security operations, and protect patient data 	
11:40	Information governance & cybersecurity: Guardians of the data	
	Seema Srihari , Information Governance Manager & DPO, North East Ambulance Service NHS Foundation Trust (NEAS) <ul style="list-style-type: none"> How do we ensure compliance, policies, and training protect NHS data? Safeguarding patient data while embracing digital transformation Cybersecurity and IG: two sides of the same coin AI governance 	
12:00	Email security in healthcare: From threat to trust	
	Eltjo Hofstee , Global Director Sales, EasyDMARC <ul style="list-style-type: none"> Covering the latest email security and deliverability challenges in the healthcare sector The latest research from May 2025 on DMARC adoption and phishing, and how public and private sector healthcare organisations need to comply with the latest directives and regulations Showing the best practice example for successfully securing your healthcare domain and email infrastructure 	
12:20	Ransomware in healthcare: The growing threat to patient safety	
	Manit Sahib , Ethical Hacker, The Global Fund <ul style="list-style-type: none"> Why healthcare is the #1 ransomware target – why attacks are increasing and how ransomware gangs break in more easily than expected Real-world hacking insights – firsthand stories from ethical hacking operations and the biggest security gaps in healthcare, including legacy tech, access control, and the lack of real-world testing Why traditional security fails – the limitations of compliance checklists and why conventional security tools don't stop ransomware Building real ransomware resilience – what healthcare CISOs and IT leaders must do NOW to avoid becoming the next headline 	
12:50	Chair's closing remarks	13:00 Conference close