Post event report

Strategic Sponsors

BeyondTrust

guardsix

RAPID7

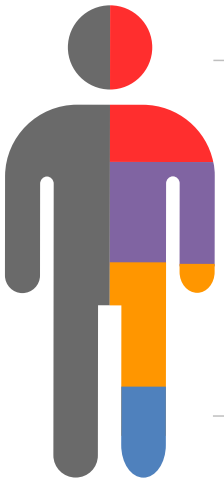
THREATLOCKER®
ZERO TRUST PLATFORM

Inside this report:

Key themes

- Achieving visibility across ecosystems
- Data integrity a critical priority
- Defending against the latest ransomware variants
- Securing Agentic AI
- Why zero trust, isolation and segmentation are key
- From Analysts to AI Supervisors
- 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

Nasser Arif,
Cyber Security Manager
LNWUH NHS Trust

Simon Brady,
Event Chairman
AKJ Associates

Lee Elliott,
Director of Solutions Engineering
BeyondTrust

Holly-Jane Grayling,
Security Culture & Awareness Lead
Tunstall Healthcare

Dulcie Herreros,
Deputy Chief Information Security Officer
NHS England

Thom Langford,
CTO
Rapid7

Eoin McGrath,
Solutions Engineer
ThreatLocker

Mike Owen,
Deputy Director Cyber Operations
NHS England

Alan Simpson,
UK and Ireland Field CISO
Rapid7

James Witt,
Head of Information Security
Barchester Healthcare Ltd

Agenda	
09:30	Chairman's welcome
09:35	**FIRESIDE CHAT: Preparing for the future of Healthcare**
	Dulcie Herreros, Deputy Chief Information Security Officer, NHS England; **Simon Brady,** Event Chairman (Moderator) • How is the security environment changing in the current climate? • What do you think of the current trends towards AI? • What needs to change to enable us to face threats in the modern world? • What are you most worried about & where should investment go?
10:05	**Shifting from urgent to routine care: Unifying visibility & threat intelligence**
	Thom Langford, CTO, and **Alan Simpson,** UK and Ireland Field CISO, Rapid7 • Join Rapid7 to discover how healthcare organisations are shifting from reactive 'urgent care' security to proactive, routine operations. Learn how to eliminate hospital network blind spots, operationalise real-time threat intelligence to stop ransomware before it strikes, and navigate complex compliance minefields – all while maximising and scaling your existing Microsoft security investments
10:25	**Don't fear the auditor!**
	Nasser Arif, Cyber Security Manager, LNWUH NHS Trust • A simple shift in mindset can transform those dreaded NHS security audits into powerful opportunities for learning, improvement, and growth • This is a human centred take on audits that focuses on continuous improvement and not fear • Learn how to prepare and present clear evidence to auditors, how to use audit results to motivate teams and encourage positive change, and why it is not a weakness to ask for help and support when you need it
10:45	Comfort break
10:50	**Preparing organisations for emerging AI threats: Deepfakes, cognitive resilience & trust**
	Holly-Jane Grayling, Security Culture & Awareness Lead, Tunstall Healthcare • How AI-enabled threats such as deepfakes, voice cloning, and synthetic identity attacks are being used to bypass traditional security controls in healthcare • Why attackers increasingly target cognition, trust, and decision-making under pressure rather than technical vulnerabilities • Introducing 'cognitive resilience' as a practical capability for recognising and responding to AI-driven manipulation in real time • Practical approaches to strengthening verification behaviours and organisational readiness for synthetic media incidents
11:10	**The cost of a stolen password: NHS breaches and why privileged access is critical to cyber-resilience**
	Lee Elliott, Director of Solutions Engineering, BeyondTrust • Discover how the Advanced Computer Software and Synnovis breaches exploited compromised credentials to halt critical NHS services • Understand why unprotected privileged accounts remain the number one attack vector in healthcare cyber-incidents • Explore practical privileged access management (PAM) controls that materially reduce risk and strengthen cyber-resilience • Leave with actionable strategies to safeguard NHS and healthcare organisations from the growing threat of credential-based attacks
11:30	Comfort break
11:35	**Building resilience through experience: Lessons from recent cyber-attacks**
	Mike Owen, Deputy Director Cyber Operations, NHS England • How real-world cyber-attacks unfolded in the NHS, including what worked, what failed, and the practical lessons learned from responding under pressure • Key strategies for building organisational cyber-resilience, drawn from first-hand experience of managing incidents in a complex, high-impact environment • Actionable insights leaders can apply immediately to improve preparedness, decision-making, and recovery before, during, and after a cyber-attack

Agenda	
11:55	**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
12:15	**FIRESIDE CHAT: Cyber-resilience, regulation, and risk in modern healthcare**
	Simon Brady, Event Chairman (Moderator); **James Witt,** Head of Information Security, Barchester Healthcare Ltd • With healthcare organisations are under increasing scrutiny from regulators how do you engage (or not) with them proactively on cybersecurity, and what does 'good' look like from their perspective today? • In a care setting where availability can directly impact resident wellbeing, how do you balance strong security controls with the need to keep systems accessible for frontline staff? • Ransomware continues to target healthcare – beyond backups, what does genuine organisational readiness look like in practice? • As care providers increasingly rely on digital suppliers (from EHR systems to connected medical devices) how are you managing cyber-risk across that supply chain, and where do you see the biggest blind spots? • With a largely non-technical workforce in care homes, how do you design security awareness and controls that actually work in day-to-day care delivery?
12:45	Chair's closing remarks
12:50	End of conference