

Post event report

SECURING FINANCIAL SERVICES

Securing Financial Services

2nd July 2025 | London, UK

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsor



“ The summit offered an excellent blend of First and Second Lines of Defence, with everyone sharing their experiences from the front line of cyber-defence. The most valuable sessions for many are the ‘fireside chats’, where specific topics are discussed among peers – it’s always fascinating to hear their perspectives on real-world issues.

I always leave these events more informed than when I arrived. ”

Cyber Security Risk Manager,
Thomas Miller

“ The Securing Financial Services Summit was a very timely and valuable experience as a security manager. The presentations were detailed, relevant and practical in improving our security posture in several areas, allowing us to network with peers and vendors on shared problems and start to remediate these challenges collectively. These topics spanning from internal business process improvement all the way to the cutting-edge AI developments and preparing for the challenges that the Quantum revolution may bring. It was a truly worthwhile day away from the office and I look forward to attending future sessions. ”

Information Security Operations
Manager, Cumberland Building Society

“ It was a really good summit and I learnt [sic] a great deal. ”

Senior Information Security Analyst,
Canada Life

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



Speakers

- Damian Acklam, Founder & CEO,
Gradian
- Adam Avars, Principal for Cyber and
Third-Party Risk Policy, UK Finance
- Matt Baird, Global Head of Customer
Engineering, CyberProof
- Rich Beckett, Product & Solution
Strategy, EMEA, Netskope
- Dhruv Bisani, Head of Adversarial Attack
Simulations, Starling Bank
- James Burchell, Sales Engineering
Manager, CrowdStrike
- Richard Cassidy, EMEA CISO, Rubrik
- Raymond de Jong, EMEA Field CTO,
Isovalent
- William Dixon, Associate Fellow,
Royal United Services Institute Senior
Technology Cyber Fellow,
The Ukraine Foundation
- James Fenton, Senior Regional Sales
Manager UK, Contrast Security
- Simon Fisher CISSP, Senior Cyber
Security Consultant,
Orange Cyberdefense
- Rob Flanders, Head of Threat and
Incident Response, BAE Systems
- Khetan Gajjar, Field CTO, EMEA,
Mimecast
- Lino Gambella, CTO, Defenx
- Henry Glynn, Cyber Security Solutions
Specialist, Bytes
- Federico Iaschi, Information Security
Director, Starling Bank
- James Kwaan, CIO – GS&S,
Lloyds Banking Group
- Peter Lane, Consultancy Director,
Cyro Cyber
- Aaron Mulgrew, Senior Solutions
Architect, Western Europe & UK,
Everfox
- Ian Perry, Head of Sales Engineering,
Searchlight Cyber
- Manit Sahib, Ethical Hacker & Former
Head of Penetration Testing & Red
Teaming, Bank of England
- Rory Shannon, Global VP Engineering,
Cyderes
- Ali Shepherd, Director of Cyber &
Operational Resilience (CISO), FCA
- Daniel Velez, GCITP, ITPM, CISSP, Senior
Advisor, Insider Risk, Everfox
- John Wood, Leader, Next-Gen
Application Security, Contrast Security

Key themes

- Securing AI-driven hyper-personalization
- Securing DeFi and digital coins
- Securing the Quantum world
- Securing Cloud-first and BaaS banking models
- Securing tokenisation
- Securing Open Banking and ecosystem models

Who attended?



Agenda			
08:00	Breakfast networking & registration		
08:50	Chair's welcome		
09:00	Securing GenAI: Our journey & lessons learned		
	Ali Shepherd , Director of Cyber & Operational Resilience (CISO), FCA <ul style="list-style-type: none"> Balancing innovation and risk Embedding responsible AI Addressing novel risks and threats 		
09:20	The attacker's POV: How to build the right continuous threat exposure management (CTEM) program to reduce risk		
	Matt Baird , Global Head of Customer Engineering, CyberProof <ul style="list-style-type: none"> Generating an effective organisational threat profile Identifying the threat actors, campaigns and adversarial TTPs that pose the greatest risk to your organisation Understanding the business and security risks of threat exposure Gathering meaningful metrics to develop the business case for enhanced cybersecurity Developing a threat management solution that clearly helps manage and optimise your organisation's attack and defence surface 		
09:40	New strategies for exposure management of modern infrastructure		
	Ian Perry , Head of Sales Engineering, Searchlight Cyber <ul style="list-style-type: none"> How the traditional perimeter has been dissolved by the realities of cloud adoption The theory of Continuous Threat Exposure Management (CTEM) as a new approach to your cybersecurity How CTEM evolves and realises the lost promise of 'Attack Surface Management' Case study examples of exposure management being deployed to prevent exploitation and cyber-attacks 		
10:00	From threat landscape to defence – how to supercharge your cyber-threat intelligence approach		
	James Kwaan , CIO – GS&S, Lloyds Banking Group <ul style="list-style-type: none"> What the current threat landscape is based on, breaches, data, and the associated risk Diving deeper – How to practically exploit MITRE tools to help in your defence to meet the threat How to process threat intelligence into MITRE ATT&CK How to deal with insider threat How to predict adversary tactics How to measure your CTI maturity 		
10:20	Education Seminars Session 1		
	Netskope Securing the flow of data in the age of AI Rich Beckett , Product & Solution Strategy, EMEA, Netskope	Rubrik Banking on the future: Balancing tech innovation with changing cybersecurity regulations Richard Cassidy , EMEA CISO, Rubrik	Orange Cyberdefense Not just any breach – Dissecting the cyber-attacks shaking the UK market Simon Fisher CISSP, Senior Cyber Security Consultant, Orange Cyberdefense
11:00	Networking break		
11:30	Cyber-leadership in an era of dis-cooperation		
	William Dixon , Associate Fellow, Royal United Services Institute & Senior Technology Cyber Fellow, The Ukraine Foundation <ul style="list-style-type: none"> How global trade fragmentation impacts the community How Western Government Foreign Policy changes could lead to cyber-instability Actions the cyber C-Suite can take 		
11:50	Aggressive defence: Moving from Detect & Respond to Prevent & Investigate with identity-centric security operations		
	Rory Shannon , Global VP Engineering, Cyderes <ul style="list-style-type: none"> As adversary behaviour changes, we must re-orient detection & response into a more pre-emptive function Bringing identity & access management technologies into the threat detection & response process introduces additional friction to the attacker Considering the SecOps technology stack holistically allows us to shift SecOps into a prevent first mindset 		
12:10	Inside the mind of the adversary: Offensive innovation and the future of cyber-threats		
	Manit Sahib , Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England; Dhruv Bisani , Head of Adversarial Attack Simulations, Starling Bank; Rob Flanders , Head of Threat and Incident Response, BAE Systems; Lino Gambella , CTO, Defenx <ul style="list-style-type: none"> How modern threat actors are using AI, supply chain compromises, and 'living-off-the-land' tactics to evade detection and extend their presence What simulated attacks uncover that real-world breaches often miss – and where enterprise defences most frequently break down From social engineering to credential stuffing and zero-click exploits: the methods adversaries use to slip past perimeter defences and establish control What hackers see as tomorrow's easiest targets – quantum-era risks, edge/IoT vulnerabilities, and deepfake-powered social engineering 		

Agenda

12:40	Education Seminars Session 2		
	Contrast Security AI is eating your SDLC: Why it's time to break up with SAST (just a little) James Fenton , Senior Regional Sales Manager UK, Contrast Security & John Wood , Leader, Next-Gen Application Security, Contrast Security	Cyro Cyber This is not a drill – live cyber-incident response exercise Peter Lane , Consultancy Director, Cyro Cyber	Isovalent Building secure and scalable financial services: The Isovalent approach to cloud native transformation Raymond de Jong , EMEA Field CTO, Isovalent
13:20	Lunch networking break		
14:30	Guarding the gates you don't control: Third-party threats and the expanding perimeter		
	Federico Iaschi , Information Security Director, Starling Bank <ul style="list-style-type: none">How do you assess and prioritise cyber-risk across your third-party ecosystem?What contractual, technical, or governance mechanisms have proven most effective in enforcing cybersecurity standards among your vendors?With regulators placing increasing focus on third-party risk (e.g., DORA, SEC, OCC guidance), how are you aligning compliance efforts with operational risk management?How do you ensure your organisation is prepared to respond to a cyber-incident originating from a key third-party or cloud provider?		
14:50	Safeguarding your enterprise: Addressing human and insider risks in data loss prevention		
	Henry Glynn , Cyber Security Solutions Specialist, Bytes; James Burchell , Sales Engineering Manager, CrowdStrike; Khetan Gajjar , Field CTO, EMEA, Mimecast <ul style="list-style-type: none">Addressing both accidental and malicious data lossThe importance of managing human risk and insider threatsHow to enhance user awareness to prevent accidental data lossSecuring collaborative platforms to prevent data breachesEnsuring compliance with regulatory requirements to mitigate risksDetecting anomalous user behaviour to identify potential insider threats and prevent malicious data loss		
15:10	Education Seminars Session 3		
	Everfox Complying with PRA Insider Risk Requirements: Focusing on what's achievable and effective Daniel Velez , GCITP, ITPM, CISSP, Senior Advisor, Insider Risk, Everfox & Aaron Mulgrew , Senior Solutions Architect, Western Europe & UK, Everfox	Gradian Two sides of the same coin: How DLP and Zero Trust create unified data protection Damian Acklam , Founder & CEO, Gradian	
15:50	Networking break		
16:10	Ransomware in financial services: How AI-driven ransomware will trigger the next major breach		
	Manit Sahib , Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England <ul style="list-style-type: none">LIVE DEMO – Inside the first AI-powered ransomware attackWhy financial services is the perfect target – and how attackers are breaking in more easily than most thinkFirst-hand insights from real-world red team opsWhy traditional security fails – compliance checklists and conventional tools don't stop modern ransomwareWhat CISOs and security leaders must do now		
16:30	PANEL DISCUSSION	The quantum threat timeline: Migration challenges and strategic planning	
	Adam Avards , Principal for Cyber and Third-Party Risk Policy, UK Finance (Moderator); William Dixon , Associate Fellow, Royal United Services Institute Senior Technology Cyber Fellow, The Ukraine Foundation; Federico Iaschi , Information Security Director, Starling Bank <ul style="list-style-type: none">What is the current state of quantum computing and how soon must financial institutions act to mitigate quantum threats?What are the real-world implications of transitioning to quantum-resistant algorithms?How can organisations build roadmaps that align with regulatory and operational realities?		
17:00	Chair's closing remarks	17:00	Drinks reception
		18:00	Conference close

Education Seminars

Contrast Security

AI is eating your SDLC: Why it's time to break up with SAST (just a little)

James Fenton, Senior Regional Sales Manager UK, Contrast Security & **John Wood**, Leader, Next-Gen Application Security, Contrast Security

In a world where AI accelerates software development and attackers exploit production logic in real time, financial institutions face a widening gap between risk and reality. The traditional AppSec playbook – scan early, scan often, drown in results – no longer scales. In this interactive session, John Wood and James Fenton unpack how Application Detection and Response (ADR) gives financial services a new way to think about application security – one that's real-time, risk-aligned, and finally developer-friendly. We'll share stories from the field, bust a few myths about shift-left security, and offer a practical framework for CISOs and architects to rethink where and how they apply controls in an AI-native SDLC.

Attendees will learn:

- A clearer understanding of what ADR is (and isn't)
- Practical guidance for reducing noise, closing legacy gaps, and defending Tier 2/3 apps
- A security narrative that developers, risk officers, and regulators can finally agree on

Cyro Cyber

This is not a drill – Live cyber-incident response exercise

Peter Lane, Consultancy Director, Cyro Cyber

Have you ever wondered whether your incident response plans will hold up when really tested? Let's find out.

You've got the playbooks and the policies... but when a major cyber-incident hits, the reality rarely follows the script. In this live scenario exercise, you'll step into the middle of a cyber-incident hitting a financial services organisation, led by award-winning Consultancy Director, Peter Lane. Live and unscripted, Peter will speak with experience as to why each step and activity are so vital, and what the consequences are when there's a missing piece of the puzzle. Get involved, learn best practice from an industry leader and hear how your peers handle those tough calls. Leave with insight. Leave with confidence. Leave better prepared.

Attendees will learn:

- Test your approach and see how others in your shoes would respond in a safe setting
- Test your instincts under pressure with other cyber-leaders facing the same challenges and concerns
- Explore the blind spots that catch even the most prepared teams off guard

Everfox

Complying with PRA Insider Risk Requirements: Focusing on what's achievable and effective

Daniel Velez, GCITP, ITPM, CISSP, Senior Advisor, Insider Risk, Everfox & **Aaron Mulgrew**, Senior Solutions Architect, Western Europe & UK, Everfox

Insider risks, whether caused by negligence, compromise, or malicious intent, are receiving long-overdue attention. Financial firms in the United Kingdom (UK) supervised by the Prudential Regulation Authority (PRA) are now required to implement robust risk strategies and insider risk management systems to strengthen the operational resilience of their most critical business services.

In this session, Insider Risk Advisors will lead a practical discussion designed to help financial organisations align their insider risk strategy with PRA expectations, enabling the ability to defend against, detect, and respond to insider threats effectively. Compliance is more than deploying cybersecurity tools. It requires building a strategic, cross-functional framework that enables continuous improvement in risk posture and resilience.

Attendees will learn:

- First steps your firm can take toward PRA compliance around the requirements for operational resilience
- How to build a 90-day strategy that balances short-term and long-term objectives
- Why effective data collection and incident reporting can deliver unexpected business value

Education Seminars

Gradian

**Two sides of the same coin:
How DLP and Zero Trust
create unified data
protection,**

Damian Acklam, Founder &
CEO, Gradian

Data loss prevention programmes and Zero Trust frameworks are essential initiatives of your organisation's modern cybersecurity strategy. Each embraces the fundamental need to successfully protect organisational data in an increasingly complex threat landscape. It is estimated that 35% of DLP Gen 1 implementations have failed due to them creating 'too much noise', meanwhile Zero Trust is (in some respects) considered 'revolutionary' to help drive user productivity in the face of changing mobility patterns. The modern enterprise now faces two challenges – how to protect your data whilst simultaneously enabling access to it!

Attendees will learn:

- How DLP and Zero Trust are two sides of the same coin
- How 'tooling first' conversations are a hindrance rather than a help
- How 'time' is your friend when it comes to being successful – the programmatic approach wins!
- Why strong policy creation and ongoing policy management are so important
- The only 3 outcomes that you should care about to define success

Isovalent

**Building secure and scalable
Financial Services: The
Isovalent approach to cloud
native transformation**

Raymond de Jong, EMEA
Field CTO, Isovalent

As financial services accelerate their cloud native adoption, security, compliance, and operational excellence become critical at every stage of the journey. The Isovalent Platform, powered by Cilium and eBPF, delivers a unified approach to networking, security, and observability for Kubernetes environments – enabling financial institutions to reduce risk, increase agility, and meet regulatory demands. This session will outline how the Isovalent Platform supports financial organisations from initial deployment to advanced enterprise microservices, ensuring secure, compliant, and scalable cloud native operations.

Attendees will learn:

- Establish reliable connectivity and hardened security for Kubernetes clusters, simplifying troubleshooting and operational management from day one
- Achieve enterprise-grade security and compliance with Zero Trust network segmentation, transparent encryption, forensic insights, and seamless SIEM integration
- Scale across multi-cloud and hybrid environments, bridging modern Kubernetes workloads with legacy infrastructure while maintaining security, observability and control

Netskope

**Securing the flow of data in
the age of AI**

Rich Beckett, Product &
Solution Strategy, EMEA,
Netskope

Sensitive data movement is often seen as a risk, but restricting it outright can create operational and security challenges. In the era of AI, financial institutions need security frameworks that protect data while ensuring agility. This session explores how modern security strategies enable secure data flows that defend against AI risk, adapt to real-time risk signals, and turn security into an enabler for innovation with AI.

Attendees will learn:

- The importance of anchoring AI adoption in your approach to data governance and risk oversight
- How to enable data flows without introducing escalating security risks
- Why security must be adaptive to risk, user behaviour, and AI-driven interactions

Education Seminars	
<div>Orange Cyberdefense</div> <div>Not just any breach – Dissecting the cyber-attacks shaking the UK market</div> <div>Simon Fisher CISSP, Senior Cyber Security Consultant, Orange Cyberdefense</div>	<div>Attendees will learn:</div> <div><ul style="list-style-type: none">• Diving into the recent UK breaches – and dispelling the myths along the way• How was it done? Cyber-attack breakdown• How effective were the responses from those affected and what can we all learn from these?</div>
<div>Rubrik</div> <div>Banking on the future: Balancing tech innovation with changing cybersecurity regulations</div> <div>Richard Cassidy, EMEA CISO, Rubrik</div>	<div>Financial institutions are caught between adopting tech innovation and complying with strict regulations in the dynamic world of cybersecurity. Governments are pushing banks to enhance resilience, emphasising the non-negotiable need for uninterrupted transactions. With the added challenge of managing vast amounts of data and technology, the crucial question is: how can banks kickstart a resilience framework that smoothly aligns with regulatory demands? This presentation will explore the delicate balance between technology-driven innovation and compliance with ever-changing regulations.</div> <div>Attendees will learn:</div> <div><ul style="list-style-type: none">• Compliance nuances in EU regulations, emphasising cross-border operations and organisational adjustment• Best practices for leveraging AI while maintaining ethical standards and regulatory compliance• Balancing the three-pronged approach: tech adoption, compliance alignment, and fostering resilience in the financial sector</div>