

Post event report

SECURING
FINANCIAL SERVICES

The 5th
Securing Financial Services

5th July 2023 | London, UK

Strategic Sponsors



Education Seminar Sponsors



Networking Sponsors



Branding Sponsors



“ It was a great event. Speakers were very knowledgeable and approachable. Overall arrangement was great and one of the best parts, venue was very close to underground and accessible. I was grateful to be a part of the event. ”

Senior Financial Crime Monitoring and AML Specialist,
Crown Agents Bank

“ It was a pleasure attending the Securing Financial Services summit. The event was well organised and provided the ideal opportunity to network with attendees and hear security specialists speak about topical issues facing the financial sector. ”

Group and UK Data Protection Officer, Stonehage Fleming

“ Well done. I enjoyed the presentations and information provided all day by competent participants. Excellent organised and managed. Thank you for the very positive experience. ”

Director of IT Governance & Risk Manager, Commerzbank

Inside this report:

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



Speakers

Matt Adams, Security Architect
Santander

Sylvain Cortes, VP Strategy
Hackuity

Emmanuel Dahunsi,
Security Architect EMEA
Goldman Sachs

Guillaume Ehny, CISO
Kroo

Chris Fuller, Principal Product and
Solutions Architect
Obsidian Security

Archie Ghinn, Account Executive –
Technology and Cyber Practic
Gallagher

Dave Gill, EMEA Channel Director
Kela Group

Luke Hebbes, Director of Business
Information Security
London Stock Exchange Group (LSEG)

David Hitchen,
Senior Solutions Architect
Semperis

Emily Hodges, Chief of Staff
Risk Ledger

Phillip Hodgins, CISO
Pension Insurance Corporation

Ash Hunt, CISO
Apex Group

Petri Kuivala, Strategic Advisor
Hoxhunt

Andy Lalaguna,
Senior Solutions Architect
eSentire

Dom Lucas, Head of Security
British International Investment

Richard Meeus, Director of Security
Technology and Strategy – EMEA
Akamai

Raghu Nandakumara,
Senior Director – Solution Marketing
Illumio

Drew Perry, Chief Innovation Officer
Ontinue

Jill Robertson,
Head of Information Security Change
Metro Bank

Brandon Romisher, VP International
AppOmni

Peter Smith, CISO, **Allica Bank**

Ryan Virani, Head of UK&I –
Cybersecurity Recruitment
Adeptis Group

Key themes

The rise and rise of effective cybersecurity regulation

Developing the next generation of security leaders

Cloud native next

From Cloud security to Cloud incident response

Reining in BigTech

Securing the technologies of the future

Managing insider threats at a time of crisis

Mapping resources and controls to material business risks

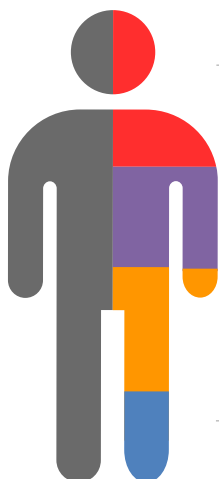
From cybercrime to cyberwar

Securing digital currencies and DLT

Embracing risk management

Solutions for CISO burnout

Who attended?



Cyber-security

We have a 15-year track record of producing the events cybersecurity 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

Agenda		
08:30	Registration and networking break	
09:20	Chairman's welcome	
09:30	Managing security in an ever-evolving supply chain	
	<p>Dom Lucas, Head of Security, British International Investment</p> <ul style="list-style-type: none"> Who are the heroes and who are the villains: the broader third-party ecosystem – regulators, clients and interested parties Evolving the assurance model – it's not always about technology Considerations for the future 	
09:50	Help drive down financial fraud with insightful API security	
	<p>Richard Meeus, Director of Security Technology and Strategy – EMEA, Akamai</p> <ul style="list-style-type: none"> What are best practices for managing, governing, and securing APIs? How can financial institutions gain visibility into their API estate and detect threats or abuse in their APIs? How can API security help financial institutions detect and remediate fraud before it impacts the business? 	
10:10	FIRESIDE CHAT How to measure the value of your technology risk management programme?	
	<p>Ash Hunt, CISO, Apex Group; Luke Hebbes, Director of Business Information Security, London Stock Exchange Group (LSEG)</p> <ul style="list-style-type: none"> What is the right amount of data to model a technology risk? How do I know my controls are reducing loss exposure? How can I articulate the link between risk reduction and business growth to the board? 	
10:30	Education Seminars Session 1	
	<p>AppOmni SaaS is the new business OS. How to harden SaaS apps at scale Brandon Romisher, VP International, AppOmni</p>	<p>eSentire How to improve cyber-resilience in your organisation Andy Lalaguna, Senior Solutions Architect, eSentire</p>
		<p>Hoxhunt From war stories to human threat detection Petri Kuivala, Strategic Advisor, Hoxhunt</p>
11:10	Networking break	
11:40	Cyber-risk – boardroom concern, or compliance burden?	
	<p>Phillip Hodgins, CISO, Pension Insurance Corporation</p> <ul style="list-style-type: none"> The benefits of cyber-risk understanding at board level The benefits of non-competitive cross-sector collaboration The competitive advantages of effective cyber-risk management 	
12:00	Stories from the trenches – identity & incident response	
	<p>David Hitchen, Senior Solutions Architect, Semperis</p> <ul style="list-style-type: none"> In the aftermath of an identity attack that compromises Active Directory, how can you quickly recover and restore trust in AD? Hear real-world examples that illustrate how you can perform attack forensics without alerting the attacker, build a defence, recover Active Directory, and make AD more resilient to compromise in the future Learn the simple steps that your organisation can take to improve your Active Directory security posture and protect AD against today's widespread cyber-threats 	
12:20	An enterprise guide to using large language models (ChatGPT, Github Co-Pilot, etc) securely	
	<p>Emmanuel Dahunsi, Security Architect EMEA, Goldman Sachs</p> <ul style="list-style-type: none"> What are the major risks of ChatGPT & other LLMs to your organisations? What security controls & best practices should you consider? What are large language models (LLMs) and what are the benefits to your organisation? 	

Agenda			
12:40	Education Seminars Session 2		
	KELA Group From initial access to ransomware attack Dave Gill , EMEA Channel Director, KELA Group	Obsidian Security SaaS ransomware – How old threats are migrating to the new SaaS landscape Chris Fuller , Principal Product and Solutions Architect, Obsidian Security	Ontinue Using Microsoft Teams & AI for effective SecOps collaboration Drew Perry , Chief Innovation Officer, Ontinue
13:20	Lunch and networking break		
14:20	The cybersecurity insurance market		
	Archie Ghinn , Account Executive – Technology and Cyber Practice, Gallagher <ul style="list-style-type: none"> • Current market trends • The growing problem: tracking technologies • The interconnectedness of exposures • Getting the right cover 		
14:40	From strength to success: Creating a winning security team for a competitive edge		
	Ryan Virani , Head of UK&I – Cybersecurity Recruitment, Adeptis Group <ul style="list-style-type: none"> • Current market trends • Is there really a skills shortage? • Why do people leave their roles? • Are you being paid and paying enough? • Ironing out the challenges in your search process • Retention and upskilling 		
15:00	Education Seminars Session 3		
	Hackuity The magic of the Vulnerability Operation Centre (VOC) applied to risk management in banking and finance Sylvain Cortes , VP Strategy, Hackuity	Illumio From digital laggard to cybersecurity leader Raghu Nandakumara , Senior Director – Solution Marketing, Illumio	Risk Ledger How concentration risk in your supply chain affects operational resilience and what to do about it Emily Hodges , Chief of Staff, Risk Ledger
15:40	Networking break		
16:10	EXECUTIVE PANEL DISCUSSION Senior leadership discussion		
	Peter Smith , CISO, Allica Bank; Guillaume Ehny , CISO, Kroo; Jill Robertson , Head of Information Security Change, Metro Bank; Matt Adams , Security Architect, Santander <ul style="list-style-type: none"> • Integrating cybersecurity into wider enterprise risk management frameworks • Becoming a more strategic partner to the business? • Building resilience against third-party security threats • Web 3.0 and the next generation of the internet: securing new technologies and services 		
16:50	Chairman's close		
17:00	Drinks reception		
18:00	Conference close		

Education Seminars	
<p>AppOmni</p> <p>SaaS is the new business OS. How to harden SaaS apps at scale</p> <p>Brandon Romisher, VP International, AppOmni</p>	<p>Today's SaaS apps are complex platforms, endlessly configurable and integrated everywhere in order to power internal and externally facing business processes. When it comes to securing SaaS, it's all about your config, but security is flying blind and with limited subject matter expertise. How do you harden access controls, ensure correct RBAC constructs and permissions assignments, identify risky 4th party connected apps, monitor high-risk users and detect security events?</p> <p>In this session, you'll learn</p> <ul style="list-style-type: none"> • How FS companies of all shapes and sizes are using AppOmni to automate SaaS security, at scale
<p>eSentire</p> <p>How to improve cyber-resilience in your organisation</p> <p>Andy Lalaguna, Senior Solutions Architect, eSentire</p>	<p>In today's threat landscape, security leaders must shift their focus to improving their cyber-resilience. The ability to anticipate, withstand, recover from, and adapt to the evolving cyber-threats will dictate how well-equipped your cybersecurity programme is at defending against these threats. However, given the lack of skilled in-house security resources, it can be challenging to balance the number of incoming security alerts with delivering swift response to eliminate known and unknown threats.</p> <p>Join eSentire's Senior Solution Architect, Andy Lalaguna as he shares insights on how you can leverage 24/7 threat detection, investigation, and response capabilities to reduce your cyber-risk, build resilience and prevent business disruption.</p> <p>Key takeaways include:</p> <ul style="list-style-type: none"> • How to assess, understand, and quantify your cyber-risks • Why you should shift your focus to building cyber-resilience in addition to managing your cyber-risks • How proactive threat hunting, combined with 24/7 threat detection and response, are critical in developing a strong cyber-defence strategy
<p>Hackuity</p> <p>The magic of the Vulnerability Operation Centre (VOC) applied to risk management in banking and finance</p> <p>Sylvain Cortes, VP Strategy, Hackuity</p>	<ul style="list-style-type: none"> • Why standard vulnerability management practices are no match for attackers? • The banking and financial sectors have their own special characteristics, which must be taken into account • Understand the different levels of vulnerability management maturity and carry out your own introspective assessment • Take account of the actual threat, so as to define a risk based on facts rather than scores • Draw up a battle plan to maximise the use and exploitation of existing security tools within the organisation
<p>Hoxhunt</p> <p>From war stories to human threat detection</p> <p>Petri Kuivala, Strategic Advisor, Hoxhunt</p>	<p>As a CISO, Petri Kuivala has established board reporting, run OT security programmes, run insider protection programmes and evicted nation-state attackers from the network, which is his story...</p> <p>This session will look at the following;</p> <ul style="list-style-type: none"> • Detailed anatomy of a major breach • How can complex organisations protect themselves as attackers continue to grow more sophisticated • How to turn people into one of your greatest resources to detect true attacks • Crossing the chasm in communicating with the board about cyber-risk

Education Seminars	
<p>Illumio</p> <p>From digital laggard to cybersecurity leader</p> <p>Raghu Nandakumara, Senior Director – Solution Marketing, Illumio</p>	<p>The need for financial organisations to transform was driven by the pandemic with the adoption of new applications and automation. The challenge is delivering cyber-resilience as the criminal gangs have transformed the way they operate, improving their evasion techniques for detection products and targeting critical infrastructure.</p> <p>In this session, you will learn:</p> <ul style="list-style-type: none"> • Why adopting Zero Trust segmentation is a simple way to deliver a structured approach to security • About some of the risks and an effective approach to identifying them through deploying preventive measures to contain an attack • And how to limit the overall spread of ransomware and breaches
<p>Kela</p> <p>From initial access to ransomware attack</p> <p>Dave Gill, EMEA Channel Director, KELA Group</p>	<p>How long does it take for a ransomware attack to occur from the moment of purchasing the access? KELA has been monitoring Initial Access Brokers’ activity and their part in the RaaS economy for over a year now. This presentation will demonstrate a direct connection between these focal threat actors’ network access listings and actual ransomware attacks.</p> <ul style="list-style-type: none"> • Identify network access victims • How to connect access on sale to a successful ransomware operation • Can we prevent the next attack?
<p>Obsidian Security</p> <p>SaaS ransomware – How old threats are migrating to the new SaaS landscape</p> <p>Chris Fuller, Principal Product and Solutions Architect, Obsidian Security</p>	<p>Today, leading SaaS applications like Microsoft 365, Google Workspace, and Salesforce effectively function as centralised platforms accessed by a sprawling number of interconnected integrations and APIs. While the productivity benefits of these connections are clear, the security risks they introduce are often overlooked.</p> <p>Recently, Obsidian observed the first ransomware attack in SaaS, and we expect to see more. Meanwhile, attackers have realised how SaaS-to-SaaS integrations are often the largest conduit for data movement within organisations, so it’s no surprise that threat actors are increasingly exploiting this interconnection. High-profile breaches like Sunburst or more recently involving GitHub and CircleCI, highlight the lack of visibility organisations have into SaaS threats.</p> <p>In this session, you will learn:</p> <ul style="list-style-type: none"> • How attackers deployed an SaaS ransomware attack in a hugely popular SaaS application • The invisible security risk of your SaaS integrations and observations from the Obsidian customer base • How session hijacking and MFA spamming helps attackers compromise key SaaS applications • Guidance on securing SaaS integrations and detecting MFA bypass

Education Seminars	
<p>Ontinue</p> <p>Using Microsoft Teams & AI for effective SecOps collaboration</p> <p>Drew Perry, Chief Innovation Officer, Ontinue</p>	<p>Do you collaborate with your MSSP or SOC provider in real-time? Have you automated Tier 1 SOC analysts? Learn about the ‘collaboration & automation’ security operations mindset and create a force multiplier to prevent cyber-incidents. The SecOps world has changed, AI is here... are you ready for it?</p> <ul style="list-style-type: none"> • Safely integrating AI capabilities: Insights from real-world AI integration using Azure OpenAI service • The impact of Co-Pilot on reshaping workflows and future implications • Practical ways AI can reduce costs for Microsoft Sentinel and alleviate SOC analyst workload • Embracing AI capabilities: The importance of company-wide engagement and support
<p>Risk Ledger</p> <p>How concentration risk in your supply chain affects operational resilience and what to do about it</p> <p>Emily Hodges, Chief of Staff, Risk Ledger</p>	<p>True operational resilience can feel an unfair demand when you are reliant on an interconnected system of suppliers, outside of your direct control. There are so many complexities and dependencies, and it’s incredibly difficult to get visibility beyond your direct supplier relationships.</p> <p>Ideally, we’d be able to view the relationships across the whole financial sector and identify where incidents at a particular supplier would cause significant wide-spread disruption. We could then focus our attention on mitigating these outsized risks.</p> <p>In this session, you will learn:</p> <ul style="list-style-type: none"> • What are the different types of concentration risk and how they can impact resilience of the sector • How you can identify concentration risks in your own supply chain and get in front of them before they cause major disruption • Ways to reduce the manual slog of third-party risk management by leveraging shared relationships • How, by aligning interests with your suppliers, you can reduce the likelihood of an incident and respond more effectively when it happens • How a tier 1 bank identified 7 concentration risks in their first two days using Risk Ledger