Post event report

Securing Financial Services

3rd July 2024 | London, UK

Strategic Sponsors

ANOMALI®

Balbix®

TANIUM™

Education Seminar Sponsors

exponential-e
APPLIED INNOVATION

GATEWATCHER

MENLO SECURITY

ONE IDENTITY
by Quest

Quest®

VERACODE

Networking Sponsor

iZOOlogic

Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

AI in threat intelligence and detection

AI in network anomaly detection

AI vs ransomware

AI in the SOC: transforming a failing legacy model

AI and third-party security

AI boosts XDR?

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

Matt Adams,
Head of Security Enablement
Citi

Jonathan Armstrong, Partner
Punter Southall Law

Steve Benton,
VP Anomali Threat Research
Anomali

Simon Brady,
Managing Editor & Event Chairman
AKJ Associates

Natalija Buldakova,
Solution Architect
Quest Software

Robin Bylenga,
VP Digital Strategy, AI Security
DWS

Rob Byrne, Field Strategist
One Identity

Ian Dutton,
Senior Sales Engineer UK
Gatewatcher

Jay Gray,
Interim Head of Cyber Solutions,
Cloud Renewals & Standard Soln
Exponential-e

Ash Hunt, CISO
Apex Group

Dan Jones, Senior Security Advisor
Tanium

Yair Kler,
Head of Security Architecture
Standard Chartered Bank

Dom Lucas, Head of Security
British International Investment

Tom McVey,
Sr. Solution Architect
Menlo Security

Peter Olivier, Head of Security Delivery
Admiral Insurance

Charlee Ryman, Co-founder
Trident Search

Kerry Sheehan, AI Policy Lead,
UK AI Taskforce, AI Regulation
UK Civil Service

Garry Sidaway,
Principal Solutions Engineer
Balbix

Andy Sutcliffe,
Principal Solution Architect
Veracode

Ben Trethowan, CISO
Brit Insurance

Agenda

08:00	Breakfast & networking
08:50	Chair's welcome

09:00 — Head in the Clouds: Securing the cloud-native enterprise

Ben Trethowan, CISO, Brit Insurance
- The importance of effective Cloud-platform control, management and visibility
- The role of machine identity in Cloud-native architectures
- Leveraging identity governance to prevent the accumulation of privilege
- 'Designing in' secure configuration and hardening prior to deployment
- The relationship between Cloud, application security and software development

09:20 — Beyond visibility: Leveraging AI to burn down cyber-risk

Garry Sidaway, Principal Solutions Engineer, Balbix
- AI has enabled organisations to make significant progress in reducing cyber-risk quickly
- Balbix customers have used AI to analyse and infer vulnerabilities without periodic scans, correlate and deduplicate vulnerabilities to reduce the number of vulnerability instances, understand the business impact in monetary terms of mitigating specific vulnerabilities, and prioritise vulnerabilities based on threats, controls, exposure, and business impact
- The key to effective risk management lies in the ability to process vast amounts of data and identify specific vulnerabilities that need to be mitigated now
- Using measurable data, organisations can reduce risk while improving collaboration and communication between security and IT teams. Discover how leading organisations are leveraging AI to manage their risk effectively

09:40 — Elite soc performance through intelligence led security operations – the 'Wartime' perspective

Steve Benton, VP Anomali Threat Research, Anomali
- With over a decade of experience protecting BT across the globe, Steve will share his real-world experience and how the security mission can be achieved at an elite level of performance. He will share a different approach that recognises the two states organisations operate in versus the dynamic cyber-threat – 'Peacetime' and 'Wartime'. In this tal,k he will focus on 'Wartime' (where a threat is coming at, or has hit, the organisation).
- Smart use of intelligence in Wartime drives the core decision-making cycle critical for incident response to disrupt the attack and minimise harm. NIS2 now expects this from organisations – but how? – surely there isn't enough time for anything other than reaction?
- Post the Covid-fuelled rapid digitisation of enterprises, cyber-threat now constitutes a full-on business interruption risk for which the consequences can be significant and potentially existential. C-level execs and boards are worried and the CISO and security team have never been under more pressure to achieve the security mission.
- It is time to do things differently. Steve will tell you how. Be different, be the Anomali.

10:00 — Securing the future: Harnessing AI to safeguard the financial sector

Kerry Sheehan, AI Policy Lead, UK AI Taskforce, AI Regulation, UK Civil Service
- Unlocking value to secure financial services
- The benefits of aligning with the UK's AI Principles
- The UK's AI Principles in the context of financial services
- Potential challenges and strategies for overcoming obstacles and driving successful AI development and implementation

10:20 — Education Seminars | Session 1

Gatewatcher	**Quest Software**
Turning the DORA regulation into a proactive defensive strategy	**Managing security incidents: Prevention strategies and worst-case planning**
Ian Dutton, Senior Sales Engineer UK, Gatewatcher	**Natalija Buldakova,** Solution Architect, Quest Software

11:00	Networking Break

11:30 — The AI genie is out of the bottle – what's next?

Robin Bylenga, VP Digital Strategy, AI Security, DWS

We will discuss the journey of embracing AI within your organisation to include:
- Why it is important to define what AI means to your organisation
- Critical steps in the journey
- Differentiate between Ethical AI and Responsible AI
- Resources for guidance to include how to stay up-to-date on the constantly updated regulations

Agenda	
11:50	**Fire with fire: Leveraging advanced technologies to protect against sophisticated cyber-threats**
	Dan Jones, Senior Security Advisor, Tanium • Examine a brief history and the transformative role of AI in financial sector security • Assess the adoption and the risks of weaponisation of AI • See how fundamental hygiene is essential to safeguard against potential threats in this rapidly evolving landscape, providing practical guidance
12:10	**Building a security programme in the AI age**
	Dom Lucas, Head of Security, British International Investment • Exploring AI threats and necessary frameworks for addressing them • Developing responsible, user-centred principles to balance opportunity and risk • Building a resilient security programme that allows the adoption of AI to flourish
12:30	**Education Seminars	Session 2**

Menlo Security	Veracode
Browser security – the proven prevention layer for enterprise cybersecurity **Tom McVey,** Sr. Solution Architect, Menlo Security	**What can we learn from 1,000,000 applications?** **Andy Sutcliffe,** Principal Solution Architect, Veracode

13:10	Lunch & networking
14:00	**Facing the AI security challenge in the financial sector head on**
	Yair Kler, Head of Security Architecture, Standard Chartered Bank • Adapting risk management frameworks for AI: Exploring how financial institutions can update their risk management frameworks to effectively address the unique security challenges posed by advanced AI technologies • Enhancing operational and development methodologies: Discussing the integration of robust security practices into operational and development processes to safeguard against AI-specific threats • Implementing comprehensive third-party risk assessments: Outlining strategies for evaluating and managing risks associated with third-party AI solutions and partnerships to ensure a secure financial ecosystem
14:20	**Unlocking opportunities and understanding recruitment dynamics**
	Charlee Ryman, Co-founder, Trident Search • The real recruitment market (market trends) • Where clients are failing • How to further your career within security at all levels • What should you be earning? • Certifications VS Real experience
14:40	**Education Seminars	Session 3**

Exponential-e	One Identity
Cyber prevention & remediation: The journey from machine learning to AI **Jay Gray,** Interim Head of Cyber Solutions, Cloud Renewals & Standard Soln, Exponential-e	**AI powered identity: Fact or fantasy?** **Rob Byrne,** Field Strategist, One Identity

15:20	Networking break
15:40	**AttackGen: Leveraging AI for dynamic incident response testing**
	Matt Adams, Head of Security Enablement, Citi • AttackGen makes threat-driven incident response testing more accessible and efficient for organisations of all sizes • It combines data from MITRE ATT&CK with Large Language Models to quickly generate comprehensive incident response scenarios for Red & Blue teams • This talk will feature live demos that explore AttackGen's features
16:00	**EXECUTIVE PANEL DISCUSSION** **Managing personal legal and emotional challenges for CISOs**
	Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator); **Jonathan Armstrong,** Partner, Punter Southall Law; **Peter Olivier,** Head of Security Delivery, Admiral Insurance; **Ash Hunt,** CISO, Apex Group • With increasing personal liability for CISOs under UK regulations and the emotional toll of being held accountable for cyber-incidents – including potential fines and criminal charges – how do you balance legal accountability and personal responsibility? • How can CISOs guard against their own liability? • Are you worried about personal liability? Is insurance a consideration? • Addressing ethical challenges such as balancing business interests with security needs along with the personal consequences of these decisions • With the psychological impact on CISOs, does your organisation offer support for stress management and mental health and what's out there for CISOs?
16:30	Drinks reception & networking **17:30** Conference close

Education Seminars

Exponential-e

Cyber prevention & remediation: The journey from machine learning to AI

Jay Gray, Interim Head of Cyber Solutions, Cloud Renewals & Standard Soln, Exponential-e

AI has been a part of cybersecurity for many years, but maybe not quite as we know it. Machine learning (ML), a subset of AI has been incorporated into dozens of cyber-related technologies over the last decade within solutions such as Next Generation Firewalls, IDS/IPS systems, SASE, the list goes on. However, with new AI advancements, cybersecurity has evolved a great deal – a key component for the financial services sector to be implementing. This session will explore the shift from traditional machine learning to AI-driven approaches, emphasising their impact on financial institutions.

Attendees will learn:

- AI's role in detecting fraudulent activities
- Safeguarding sensitive data
- Automating incident responses
- Our subject matter expert will also delve deeper into how AI can identify complex threats and reduce response times, ensuring robust protection of financial assets and future trends in AI-enhanced cybersecurity for the financial industry

Gatewatcher

Turning the DORA regulation into a proactive defensive strategy

Ian Dutton, Senior Sales Engineer UK, Gatewatcher

Integrating Network Detection and Response (NDR) with DORA raises your defensive strategy to the next level. In 30 minutes, let's cover how NDR's real-time threat detection and automated response capabilities combined with GenAI assistant technology, ensure that organisations can work faster and smarter in detecting and remedying evolving cyber-threats.

Attendees will learn:

- Overview of the DORA regulation
- How to transform a regulation into an opportunity
- Why an NDR is the most appropriate technology to get prepared

Menlo Security

Browser security – the proven prevention layer for enterprise cybersecurity

Tom McVey, Sr. Solution Architect, Menlo Security

According to Google, 98% of attacks originate from internet usage and 80% of those target end user browsers – sadly all too successfully. Combine this stark reality, with users' relentless demand for new SaaS and private applications, often collaborating with external stakeholders, and security pros are always running to stand still.

Attendees will learn:

- *Security* – The proven value of robust browser security across managed and unmanaged devices – automating browser configuration and establishing enhanced browser forensics
- *Connectivity* – Your users and third parties need access to SaaS applications, private web apps and data, including the use of GenAI. We share how organisations are enhancing user protection and productivity while reducing the cost and complexity of solutions such as VDI
- *Compliance* – How browser security supports organisations striving to comply with key NIS 2 requirements for incident management and prevention
- We will provide real-world examples and case studies of how to increase cyber-prevention through improved browser security

One Identity

AI powered identity: Fact or fantasy?

Rob Byrne, Field Strategist, One Identity

AI and machine learning promise to transform our lives and work, including cybersecurity. But is it genuinely 'intelligence',' or is the hype overblown? What risks does it pose? Can AI simplify my life, autonomously protect my organisation, and bring tangible value?

Attendees will learn:

- techniques for integrating identity-centred analytics, insight, and intelligence into your cybersecurity strategy, helping your organisation navigate the AI-powered future effectively

Education Seminars	
Quest Software **Managing security incidents: Prevention strategies and worst-case planning** **Natalija Buldakova,** Solution Architect, Quest Software	With 74% of breaches involving the human element and ransomware attacks skyrocketing, safeguarding business identities has never been more crucial. Join us in this session as we explore the pivotal role of protecting your business from these threats. You'll gain actionable insights into potential consequences and effective mitigation strategies, alongside comprehensive worst-case scenario planning. Empower yourself to fortify your organisation's defences against evolving cyber-threats with practical knowledge and proactive measures. **Attendees will learn:** • Today's cybersecurity challenges • Implementing dynamic preventative measures • Developing robust strategy for worst-case scenarios
Veracode **What can we learn from 1,000,000 applications?** **Andy Sutcliffe,** Principal Solution Architect, Veracode	Generative AI is already having a big impact on the way that software is being developed. AI assistance is allowing code to be produced faster and in greater volume than ever but it is not delivering more secure code. Generative AI models have been trained using existing code with all of the same flaws and weaknesses that plague software. Meanwhile, organisations are already drowning in security debt, so the influx of new vulnerable code could be the straw that breaks the camel's back. **What attendees will learn:** • Review recent research into AI code generation and software security • Gain insight into where we are today and how we can plot a course to more secure software portfolios