Post event report

Strategic Sponsors

BEYOND IDENTITY

BeyondTrust

BlackBerry

DARKTRACE

MENLO SECURITY

OneTrust
PRIVACY, SECURITY & GOVERNANCE

SEARCHLIGHT Security

Education Seminar Sponsors

b!nalyze

CEQUENCE SECURITY

COFENSE

CounterCraft

digital element
Location is Elemental™

e2e assure

egress

FIREMON

Kocho

OBSIDIAN

SWIMLANE

Networking Sponsor

Reveal security

Branding Sponsors

Balbix

TESSIAN

"The Securing Financial Services forum was a great event, with some thought provoking presentations across the day and some good risk insights, I found the presentation covering differing approaches to risk appetite to be excellent."

Chief Risk Officer, Monmouthshire Building Society

"The online conference format was intuitive and an excellent user experience – I liked the ability to deal with a few matters arising between sessions and still get the whole session."

Identity and Access Management Specialist, Sanlam

"Very interesting speakers / catch up with contacts etc. Also fantastic virtual experience – well thought out and added lots of value – actually preferred it on one level to the normal (always good) previous events."

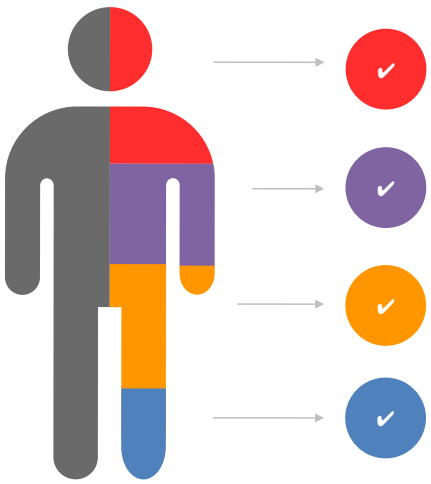
Senior Technology Risk Manager, Credit Suisse

Inside this report:

Key themes

- Building better Cloud security
- How end-user intelligence can improve cybersecurity
- Is zero trust really the answer?
- Behavioural analytics
- Building-in security: from DevOps to SecDevOps?
- Creating friction-free security tools

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

Rohyt Belani, Chief Executive Officer and Co-founder, **Cofense**

Amir Ben-Efraim, CEO, **Menlo Security**

Daniel Brett, Co-founder and CSO, **CounterCraft**

Ian Burgess, Director, Cyber & Third Party Risk, **UK Finance**

Jack Chapman, Vice President of Threat Intelligence, **Egress**

Brian Chappell, Chief Security Strategist, **BeyondTrust**

Marco Cinnirella, Professor of Applied Social Psychology, **Royal Holloway**

Emmanuel Dahunsi, Solutions Architect EMEA, **Goldman Sachs**

Hanah-Marie Darley, Head of Threat Research, **Darktrace**

Rob Demain, Founder and CEO, **e2e-assure**

Jules Ferdinand Pagna Disso, Group Head of Cyber Risk Intelligence & Insider Technology Risk, **BNP Paribas**

Jorge Ferrer Raventos, Solutions Engineering Specialist, **OneTrust**

Paul Fryer, Sr. Manager Sales Engineering, **BlackBerry**

Chris Fuller, Principal Product and Solutions Architect, **Obsidian Security**

Luke Hebbes, Director of Business Information Security, **LSEG**

Joe Hebenstreit, Director of Product Management, **Digital Element**

Owain Howard, Regional Sales Manager, EMEA, **FireMon**

Vinod Kashyap, Head of Product, **Digital Element**

Chris Meidinger, Technical Director, **Beyond Identity**

Tim Neill, Chief Risk Officer, New Payments Platform, **Mastercard**

Dr Gareth Owenson, Chief Technology Officer, **Searchlight**

Santosh Pandit, Head of Cyber and Operational Resilience-Insurance, **Bank of England**

Lina Sabestinaite, Information Security Officer, **Handelsbanken**

James Sherlow, Senior Field Solutions Engineer EMEA, **Cequence Security**

John Skipper, CISO, **Metro Bank**

Emre Tinaztepe, Founder & CEO, **Binalyze**

Toby Van De Grift, VP of EMEA, **Swimlane**

Anna Webb, Head of Security Operations, **Kocho**

Agenda

08:00 Registration & networking

08:50 Chairman's welcome

09:00 **Why do they do that? Harnessing psychology to inform information security in organisations**

Marco Cinnirella, Professor of Applied Social Psychology, Royal Holloway

- How to best leverage insights offered by psychology when investigating risky information security behaviours
- Understanding how risk perception is impacted by cognitive biases, culture, and the 'psychological work contract'
- Why a mixed methods approach to collecting data is vital
- How psychology can inform communication and education
- Why you can never completely 'design out' behavioural issues

09:20 **Threats to financial services from the dark web**

Dr Gareth Owenson, Chief Technology Officer, Searchlight

- An overview of the dark web cybercriminal underground
- An examination of dark web financial crimes
- Threats to financial organisations by hackers on the dark web
- Practical approaches to reducing your risk exposure

09:40 **Why Zero Trust, why now?**

Brian Chappell, Chief Security Strategist, BeyondTrust

Join Brian Chappell, Chief Security Strategist, who will share:

- What is Zero Trust?
- Zero Trust vs. Zero Trust Architecture – are they different?
- The recommended path to Zero Trust

10:00 **Operational resilience & cybersecurity**

Santosh Pandit, Head of Cyber and Operational Resilience-Insurance, Bank of England

- SS1/ 21 testing
- Severe and plausible scenarios
- Cybersecurity role on OpRes

10:20 **Education Seminars | Session 1**

Cofense	e2e-assure	Obsidian Security	Swimlane
Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for financial service **Rohyt Belani,** Chief Executive Officer and Co-founder, Cofense	**Elevating cybersecurity from a cost centre to a source of competitive advantage** **Rob Demain,** Founder and CEO, e2e-assure	**Obsidian Security: Extending Zero Trust to SaaS** **Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security	**The future of security automation** **Toby Van De Grift,** VP of EMEA, Swimlane

11:00 Networking break

11:30 **Vulnerability management and moving from following scores from tools to risk-based prioritisation**

Luke Hebbes, Director of Business Information Security, LSEG

- Vulnerability score ≠ Risk score
- In large organisations raw numbers of vulnerabilities can look scary out of context, so provide the context not the raw numbers
- Prioritisation must be based on your environment, but this doesn't have to be a complex manual process
- Accept that you can't close all vulnerabilities and work to your risk appetite/resource constraints
- Why I don't believe in blanket SLAs for remediation

11:50 **How successful security teams manage risk to build trust and drive growth**

Jorge Ferrer Raventos, Solutions Engineering Specialist, OneTrust

- Explore the definition of trust and what it means to be a trusted organisation
- Discuss the evolution of your audience and why the language you use is critical for adoption
- Understand 2 practical exercises that can help you understand attitudes towards security risk from the top-down and bottom-up
- Have a look at some questions you can put to the business to get you started

12:10 **Why attack surfaces heat up with remote work**

Amir Ben-Efraim, CEO, Menlo Security

- Why has the pivot to new working models increased cyber-risk?
- How are attackers leverage Highly Evasive Adaptive Threats (HEAT) to launch ransomware attacks?
- What can organisations do to avoid the next class of browser-based attacks?

Agenda

12:30 — Banking on AI: Neutralising threats before cyber-attackers strike gold

Hanah-Marie Darley, Head of Threat Research, Darktrace

- Learn how Autonomous Response knows exactly the right action to take, at the right time, to contain an in-person attack
- How AI takes precise action to neutralise threats on the behalf of security teams
- Use of real-world threat finds to illustrate the workings of Autonomous Response technology

12:50 — Education Seminars | Session 2

Binalyze	CounterCraft	Digital Element	Kocho
Forensics 2.0 – The growing role of enterprise forensics in resilient incident response strategies	**How deception technology can be used to detect threat actors in SWIFT networks (real use cases)**	**From prevention to forensics: IP address data's role in cybersecurity**	**Why outsourcing security operations is a smart investment**
Emre Tinaztepe, Founder & CEO, Binalyze	**Daniel Brett,** Co-founder and CSO, CounterCraft	**Vinod Kashyap,** Head of Product, and **Joe Hebenstreit,** Director of Product Management, Digital Element	**Anna Webb,** Head of Security Operations, Kocho

13:30 — Lunch break

14:30 — SENIOR LEADERSHIP PRIORITIES PANEL

Santosh Pandit, Head of Cyber and Operational Resilience-Insurance, Bank of England; **Jules Ferdinand Pagna Disso,** Group Head of Cyber Risk Intelligence & Insider Technology Risk, BNP Paribas; **Emmanuel Dahunsi,** Solutions Architect EMEA, Goldman Sachs; **Lina Sabestinaite,** Information Security Officer, Handelsbanken; **John Skipper,** CISO, Metro Bank

- Data privacy or security? How will companies view 'security' in the post-pandemic world?
- Hybrid working: problem solved or problem postponed?
- The issue of 'basic' cyber-hygiene (or 'why can't we stop ransomware?')
- Is 2022 the year of Cloud? And have the security implications of Cloud been exaggerated?
- The future of the security stack: insource/outsource/reduce number of solutions/rely on large application and infrastructure providers more
- Reining in the costs of cybersecurity

14:50 — Why legacy MFA is not good enough for modern authentication requirements

Chris Meidinger, Technical Director, Beyond Identity

- A brief history of MFA
- We look into why traditional MFA was appropriate at the time but has kept up with the progress of attackers
- We detail the dangers posed by passwords and traditional MFA that requires a second device and/or push notifications
- Finally we cover off the alternative which is unphisable passwordless MFA

15:10 — In an ever-changing landscape of cybersecurity, preventing cyber-attacks doesn't have to be a rat race

Paul Fryer, Sr. Manager Sales Engineering, BlackBerry

- The evolution of BlackBerry – where are we now?
- Security challenges and opportunities of hybrid working and what solutions BlackBerry has to offer
- What BlackBerry is doing differently to get Zero Trust

15:30 — Education Seminars | Session 3

Cequence Security	Egress	FireMon
Protecting the entire API lifecycle	**The changing email threat landscape**	**Simple does scale: Automating security fundamentals**
James Sherlow, Senior Field Solutions Engineer EMEA, Cequence Security	**Jack Chapman,** Vice President of Threat Intelligence, Egress	**Owain Howard,** Regional Sales Manager, EMEA, FireMon

16:10 — Networking break

16:30 — Challenging the CISO

Tim Neill, Chief Risk Officer, New Payments Platform, Mastercard

- Assuring the security programme
- Check and challenge transparency
- Corporate governance and the CISO

16:50 — Collaboration in financial services

Ian Burgess, Director, Cyber & Third Party Risk, UK Finance

- Why collaboration is important and how this benefits firms
- Development and operationalisation of the FSCCC, and how it is helping to make the financial sector more cyber-resilient
- What else is the sector doing

17:10 — Drinks reception & conference close

Education Seminars	
Binalyze **Forensics 2.0 – The growing role of enterprise forensics in resilient incident response strategies** **Emre Tinaztepe,** Founder & CEO, Binalyze	There is a new breed of digital forensics solutions that are lightning fast, remote, scalable, automated and integrated. They are dramatically changing when, where and how forensic visibility can be leveraged, in traditional investigations, but also for proactive threat hunting and incident response. During the session, you will learn: • How enterprise forensics is disrupting the traditional digital forensics landscape and delivering forensic capability to the centre of the security stack • How speed, automation and integration can dramatically reduced incident response dwell times and improve SOC productivity by 50% • Why assisted compromise assessment will help to reduce your skills shortage by allowing analysts to focus on high-value actions • Why proactive forensic diffing is a game-changer for cyber-resilience and vulnerability management
Cequence Security **Protecting the entire API lifecycle** **James Sherlow,** Senior Field Solutions Engineer EMEA, Cequence Security	APIs bring benefits of ease of use, efficiency, and flexibility to the development community and agility to the business; therefore, most companies employ an API-first development strategy. This is creating an explosive use of APIs, which shows no signs of abating. However, they can also carry risks, making them ideal targets for attackers. To address this, many security teams are trying to extend the capabilities of existing technologies, leaving them with a lack of visibility and defence capabilities against sophisticated attacks. What's needed is a way to protect organisations from security threats, losses and compliance exposures across the entire API risk surface. To do this, businesses need a unified and fully integrated approach that covers the entire API lifecycle. This session will delve into the different approaches to protecting APIs from a range of security risks and how security teams can make strategic decisions on the depth of protection deployed during the lifecycle. • *Discovery:* Identify all public-facing APIs • *Inventory:* Provide a unified inventory of all APIs • *Compliance:* Ensure adherence to security and governance best practices • *Detection:* Detect attacks as they happen • *Prevention:* Block attacks natively in real-time • *Testing:* Secure new APIs before going live
Cofense **Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for financial services** **Rohyt Belani,** Chief Executive Officer and Co-founder, Cofense	• *What is an adaptive layered security architecture and what are the objectives* – With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation. We'll walk you through the benefits and objectives of implementing an adaptive layered security architecture and risk framework. • *The current situation in email and phishing security* – We'll share some of the latest insights from the financial services industry and what we're seeing through our unique combination of artificial, human, and high-fidelity intelligence. • *Implementing adaptive layered security architecture and risk frameworks with Cofense* – We'll talk through how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity.
CounterCraft **How deception technology can be used to detect threat actors in SWIFT networks (real use cases)** **Daniel Brett,** Co-founder and CSO, CounterCraft	• Traditional threat intel VS deception-powered threat intel • All about Threat Intelligence 2.0 and its lifecycle • The deception triangle: data exfiltration, |credibility, telemetry • Real use case of how to detect threat actors in SWIFT networks with cyber deception

Education Seminars

Digital Element

From prevention to forensics: IP address data's role in cybersecurity

Vinod Kashyap, Head of Product, and **Joe Hebenstreit,** Director of Product Management, Digital Element

Behind every IP address is a set of data characteristics that is proven to provide crucial context for fighting cybercrime. These include VPN classification, provider's name/URL, IP addresses related to a provider, anonymity level, and more. With this data, security professionals have the ability to identify proxied traffic, as well as glean rich insights and behavioural data that they can leverage to detect and prevent potential criminal activity, understand where attacks originate and what nefarious traffic looks like. They can also use that insight to set rules and alerts for traffic that meets specific criteria. Because IP address data offers a level of rich context that will enhance virtually every security strategy in place today, it is a fundamental building block in a cybersecurity professional's toolkit.

In this session, attendees will learn:

- What role IP intelligence data plays into cybersecurity best practices
- How to prevent intrusions by identifying anonymised connections
- How distinguishing between a residential or commercial connection helps security professionals distinguish between legitimate and nefarious traffic
- Market trends that are impacting security practices, including rising VPN usage among residential users
- How IP address data can help with forensics

e2e-assure

Elevating cybersecurity from a cost centre to a source of competitive advantage

Rob Demain, Founder and CEO, e2e-assure

In this session, Rob Demain will be discussing a paradigm shift in how financial services organisations think of cybersecurity, to bring further business benefits above and beyond just being more secure. He'll be bringing together insights from recent conversations with customers, partners and industry experts as well as practical examples from industry on how to make this shift and give your organisation an additional element of competitive advantage over the competition.

- Foundations for effective cybersecurity, including building the right culture
- Effective communication with board members
- Building trust through transparent communications
- Benefits to organisations of viewing cybersecurity as more than just a cost centre
- How organisations can make cybersecurity a new source of competitive advantage

Egress

The changing email threat landscape

Jack Chapman, Vice President of Threat Intelligence, Egress

Cybercriminals continue to launch increasingly sophisticated social engineering attacks. This is driven by crime as a service ecosystem, change in human behaviour and hardening of traditional routes into organisations. Because of these factors and more, it's no surprise that 85% of today's security breaches involve a human element.

Join this presentation to learn more about:

- Today's email security landscape and how the threats are evolving
- The behaviours behind email data breaches
- Why legacy approaches are no longer fit for purpose
- How to use behavioural science and zero trust to take back control over data loss
- How real-time teachable moments are more effective at changing human behaviour than traditional security awareness training

FireMon

Simple does scale: Automating security fundamentals

Owain Howard, Regional Sales Manager, EMEA, FireMon

It is an axiom of security that the defenders need to be right every time, and the attackers only need to be right once. The biggest breaches rarely use advanced techniques; the attackers merely rely on the fact that consistency is hard and even the simple problems aren't simple at scale. Simple doesn't scale. Repeating a manual process hundreds or thousands of times a week means creating hundreds or thousands of opportunities for a misstep. Fundamentals are easy; fundamentals at scale are hard, and it's security operations, not the latest IPS or EDR tool, that defines success.

In this session, you'll learn:

- Key strategies, techniques, and tools to scale security fundamentals
- How to keep up with the needs of the business without sacrificing security
- Which manual processes can be automated reliably to free resources to focus on strategic initiatives
- Why asset discovery and identification is crucial to securing your environment

Education Seminars	
Kocho **Why outsourcing security operations is a smart investment** **Anna Webb,** Head of Security Operations, Kocho	Data awareness and scrutiny have never been higher in the financial sector. With The FCA reporting a 50% uplift in reported cyber-incidents in 2021 (a fifth involving ransomware). As cybercriminals become more sophisticated and the attack surface continues to grow, now is the time to implement modern security operations practices. This session will look at the technologies and processes involved in transforming your organisation's security operations and how Microsoft and Kocho can monitor and protect you from threats. **Based on the latest Microsoft Defender and Sentinel technologies, this session will show you how to:** • Establish a single view of your security from across your hybrid estate • Quickly detect and respond to threats across your environment • Leverage AI, threat intelligence, and automation to proactively respond to threats • To get up and running with modern security operations using an outsourced, managed security approach
Obsidian Security **Obsidian Security: Extending Zero Trust to SaaS** **Chris Fuller,** Principal Product and Solutions Architect, Obsidian Security	In a world where the natural evolution towards SaaS was accelerated by remote working during the pandemic, do the principles of Zero Trust still apply? SaaS currently makes up 75% of the cloud, yet SaaS security visibility is notoriously difficult for security teams to manage, given the expertise, visibility and control required to manage each disparate SaaS application. Meanwhile, integrations between SaaS applications create a highly interconnected environment. With more sensitive business data entrusted to SaaS than ever before, it's time to consider how best we secure those applications. In this session, we'll explore how the Zero Trust principles of continuous verification, breach impact limitation and facilitation of rapid incident response can be applied to SaaS applications. • Review the guiding principles of Zero Trust • Learn the inherent risks of SaaS usage and why securing SaaS applications goes beyond the identity provider • Understand how the principles of Zero Trust can be applied to SaaS
Swimlane **The future of security automation** **Toby Van De Grift,** VP of EMEA, Swimlane	Security teams everywhere are asked to do the impossible. Processing the deluge of alerts and tasks required to protect an organisation can overwhelm even the most engaged security talent. That's why top performing companies in every industry are turning to low-code security automation to overcome process fatigue, realise the promise of XDR, and centralise operational data as a system of record. But as security operations and the threat landscape continue to evolve, so too does what's possible with security automation. Join Swimlane's VP of EMEA, Toby Van de Grift, for an overview of the future of this exciting technology. **During this presentation, we will explore:** • A brief overview and short history of security automation • How organisations are leveraging the technology today • Trends affecting the future direction of low-code automation