SECURING FINANCIAL SERVICES

5th July 2022
London

@eCrime_Congress
#securingfinancialservices

#securingfinancialservices

Solving the behaviour problem
How can we blend technology with behavioural science to build better security?

Forthcoming events

e-crime & cybersecurity CONGRESS

21st September 2022
Abu Dhabi

e-crime & cybersecurity SWITZERLAND

28th September 2022
Zurich

e-crime & cybersecurity MID-YEAR

19th October 2022
London

e-crime & cybersecurity NORDICS

1st November 2022
Copenhagen

e-crime & cybersecurity SPAIN

16th November 2022
Madrid

e-crime & cybersecurity BENELUX

8th December 2022
Amsterdam

For more information, please visit
akjassociates.com/contact-us

Solving the human problem

Welcome back to a face-to-face version of Securing Financial Services. It's great to be back. Unfortunately, the hackers are enjoying the summer too: the humans who develop cyber-threats continue to outrun the defenders and one reason for that is that the humans operating the increasingly digital tools businesses need to survive, whether employees or clients or third parties, can be easily tricked into undermining those technology-driven security solutions. The simplest attack vectors, such as email phishing, are still the most successful.

One answer to this is the application of behavioural science to both sides of this equation. So, analytics focused on user behaviour can mitigate the impact of attackers' social engineering and cognitive hacking methods; they can identify unusual patterns of user behaviour that indicate an attack at network, asset and user levels.

This is just one of the many topics that we will be discussing today at Securing Financial Services. In addition, we have sessions on operational resilience (a critical subject for CISOs in this sector), vulnerability management, the need for increased collaboration and changing the role of the CISO. All this as well as hearing about the latest technologies from some of the key providers.

But one of the main aims of our events is to facilitate conversation and dialogue. So please, enjoy your event, and take the opportunity to mingle with peers, colleagues and solution providers. If you have any questions, please do not hesitate to ask any member of the team.

Simon Brady
Editor

@eCrime_Congress #securingfinancialservices

5th July 2022
Park Plaza Victoria
London

SECURING
FINANCIAL SERVICES

Editor:
Simon Brady
e: simon.brady@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
t: +44 (0) 20 7242 7820
e: simon.brady@akjassociates.com

Booklet printed by:
Method UK Ltd
Baird House
15–17 St Cross Street
London EC1N 8UN
e: hello@thisismethod.co.uk

Articles published in this magazine are not necessarily the views of AKJ Associates Ltd. The publishers and authors of this magazine do not bear any responsibility for errors contained within this publication, or for any omissions. This magazine does not purport to offer investment, legal or any other type of advice, and should not be read as if it does.

Those organisations sponsoring or supporting the Securing Financial Services bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting the Securing Financial Services, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

SECURING FINANCIAL SERVICES

Protecting financial services from threats on the dark web

There is an opportunity for financial services organisations that are proactive to identify criminal activity that could affect them

Gareth Owenson reports

Cyber-attacks don't happen out of the blue. Like everyone else, threat actors have to organise themselves. They do their due diligence, coordinate their efforts, perform reconnaissance, and purchase the tools, credentials or access they need to orchestrate their attacks. This activity takes place on the dark web, which means there is an opportunity for financial services organisations that are proactive to identify criminal activity that could affect them – whether they are financial crimes that target customers or cyber-attacks directly targeting financial services companies themselves.

Financial crimes on the dark web

One of the most prevalent financial crimes is the sale of personal financial accounts, with some estimates putting the number of credit cards for sale on the dark web into the millions.[1] There are marketplaces known as 'autoshops' that are dedicated exclusively to the sale of credit card, debit card or bank account information – as well as the credentials, cookies and remote access needed to takeover online accounts.

The name 'autoshop' refers to the transaction process being more automated than other dark web markets – the customer receives a digital product instantly after purchase, with little to no input required from the vendor. They differ from other dark web marketplaces because of this focus on digital products but they also tend to have fewer vendors, in some cases with all of the listings originating from just the site operator. Many autoshops are also viewable in the 'clear web', if you know where to find them. The top autoshops (which currently includes the likes of Blackpass, 2easy and Russian Market) regularly post tens of thousands of new listings per week – which gives an indication of the scale of this problem.

> There are marketplaces known as 'autoshops' that are dedicated exclusively to the sale of credit card, debit card or bank account information – as well as the credentials, cookies and remote access needed to takeover online accounts.

Autoshops have a number of different sources for the products they sell:

- ***Historic data breach sets:*** There are large datasets of stolen credit card details from financial institutions for sale on the dark web, however these are sometimes viewed sceptically in criminal forums as they are often old, meaning that they contain few 'live' credit cards for hackers to exploit.
- ***Attacks against e-commerce sites:*** Cybercriminals exploit vulnerabilities in websites to extract customer card data through a technique known as web skimming. If undetected, attackers can extract thousands of customers' payment information through automated software, a technique infamously used in the Magecart attacks against British Airways, Ticketmaster and Newegg.[2]
- ***Phishing sites:*** Where customers are tricked into entering their credit card information into a fraudulent website, often imitating a known and trusted brand.
- ***Banking trojans and stealer malware:*** Malware that is directly installed onto a user's computer to capture card data. Notable examples have included Zeus, Emotet and Trickbot.
- ***Insider threat:*** Customer information sold by employees from within financial institutions, a prime example of 'insider threat'.

As well as giving us visibility into autoshops, monitoring the dark web also allows us to see the activity being undertaken to supply them. For example, stealer malware and banking trojans can be found for sale on markets and forums, as well as user guides for how to use them. Spamming tools and phishing pages are also sold, as well as reverse proxy servers (such as Modlishka and Evilginx) to bypass bank's two-factor authentication (2FA).

Threats against financial institutions

Financial institutions tend to have a large dark web 'footprint', meaning that there is a lot of information on the dark web around them. Firstly, this is because they are a popular target for cybercriminals, which means there is a large volume of chatter on forums about how to target and exploit them. Secondly, this is a result of financial institutions typically being large and complex enterprises – with a lot of staff across

> Visibility into criminal activity on the deep and dark web can allow financial institutions to take proactive action to prevent attacks against themselves and their customers.

different departments, offices, and geographies, a large and intricate IT infrastructure, and many customer facing applications – creating a very big attack surface for cybercriminals to probe and exploit on the dark web.

Common threats against financial institutions that are visible on the dark web include (but are not limited to):

- *Leaked employee credentials:* Databases including employee's names, email addresses, and passwords can leave employees vulnerable to a number of attacks. With just a name and email address, cybercriminals can conduct very effective phishing campaigns against employees, which – according to IBM – was the most common infection vector into financial services organisations last year (responsible for 46% of attacks).[3] With an email address and password a criminal could potentially login to a corporate email account and conduct fraud attempts against employees, which is known as Business Email Compromise.
- *Vulnerability exploitation:* Cybercriminals sell vulnerabilities in an organisation's software, devices, and the supply chain companies they use. According to IBM, vulnerability exploitation is the second most popular route into a financial institution, leading to 31% of attacks in 2021.[4]
- *Dark web traffic:* Incoming traffic from the dark web could indicate that the corporate network is being actively scanned for vulnerabilities. Outgoing traffic is potentially even more serious, as there is virtually no good reason why there should be traffic to the dark web from within a financial institution. It may indicate that an employee is doing something malicious or, worse, that a command and control server has been established so that cybercriminals can remotely execute their attack.

Actioning dark web intelligence

Visibility into criminal activity on the deep and dark web can allow financial institutions to take proactive action to prevent attacks against themselves and their customers.

For example, by searching for Bank Identification Numbers (BIN), a bank could find all of its credit card details leaked on the dark web, block the cards, and inform customers and the authorities – preventing fraud at scale. Similarly, monitoring the dark web for their company name, IP addresses, and credentials, could help to identify when staff are at risk from phishing attacks and business email compromise, or if executives are being actively targeted by criminals on the dark web.

Financial institutions could also identify commodities available on dark web marketplaces that could either be used to target their organisation (e.g. software vulnerabilities and exploits) or their customers (banking trojans or 2FA bypass tools). This intelligence can help them patch vulnerabilities before they are exploited and, with insight into where and by whom such tools are being sold, gain an understanding of the adversarial landscape. Visibility into dark web traffic can also help an organisation take defensive action to protect the specific part of the network that is being targeted, or where data is being potentially leaked from.

Moving left in the cyber kill chain

One of the benefits of dark web monitoring is that the intelligence is specific to the organisation. If a bank CEO's personal details are on a dark web forum, or a vulnerability in their software is for sale on a dark web marketplace, there is no grey area – they are at risk and there are clear preventative actions that need to be taken. This ability to pre-empt the actions of threat actors means that financial services can move to defend much earlier in the 'cyber kill chain' and identify potential attacks against their infrastructure or their customers before they are launched. □

[1] https://www.computerweekly.com/news/252510368/Millions-of-credit-card-details-for-sale-on-dark-web-for-a-few-pounds-each

[2] https://www.itpro.co.uk/cyber-attacks/31992/british-airways-ticketmaster-and-newegg-hacks-part-of-massive-magecart

[3] https://www.ibm.com/security/data-breach/threat-intelligence/

[4] https://www.ibm.com/security/data-breach/threat-intelligence/

Gareth Owenson is CTO of Searchlight Security.

For more information, please visit
www.slcyber.io

SEARCHLIGHT
Security

www.slcyber.io

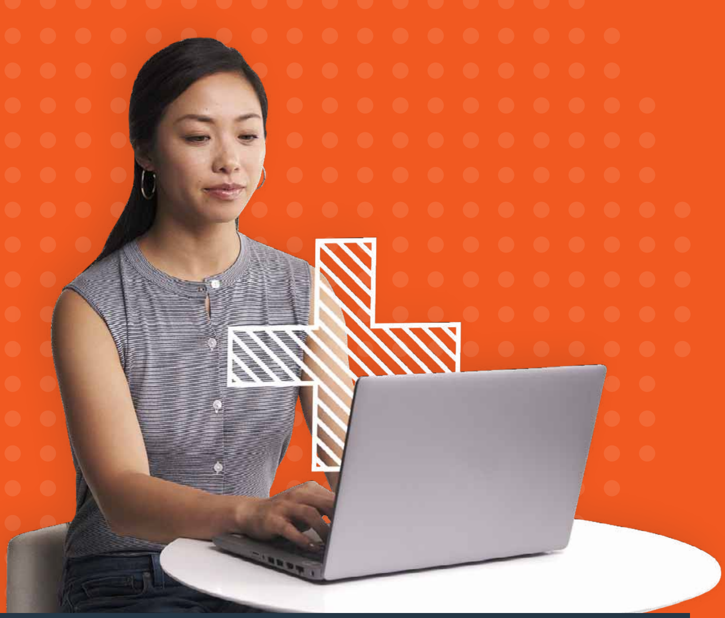
Illuminate Threats, Prevent Attacks

Relevant, actionable
dark web threat intelligence

SEARCHLIGHT
Security

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS



BeyondTrust – a zero-trust approach to secure remote access

Protecting privileged access for all remote sessions.

BeyondTrust reports

By definition, a zero-trust security model advocates for the creation of zones and segmentation to control sensitive IT resources. This also entails the deployment of technology to monitor and manage data between zones, and, more importantly, authentication within a zone(s). This encompasses users, applications, context, attribution, and other resources and parameters.

In addition, the zero-trust model redefines the architecture of a trusted network inside a logical and software-defined perimeter. This can be on-premises or in the cloud. Only trusted resources should interact based on an authentication model within that construct.

Zero trust is increasingly relevant today as technologies and processes like the cloud, virtualisation, DevOps, edge computing, edge security, personification, and IoT have either blurred or dissolved the idea of a traditional firewall and network-zoned perimeter. The seismic shift to remote working has only accelerated the demise of the traditional perimeter.

While zero trust has become a trendy catchword in IT, it's important to call out that, in practice, this model is very specific about how things should be designed and operate. Zero trust may not work for every environment. In practice, it is best suited for new or refreshed deployments, or to strictly control user access to sensitive resources, especially when they are connecting remotely.

When applying the granularity of privileged access management, which includes secure remote access, zero trust can ensure all access is appropriate, managed, and documented – regardless of how the perimeter has been redefined.

Securing today's workforce – at home, in the office, or anywhere in between

As a security best practice, native remote access protocols should be disabled for corporate-issued computing device(s). Unfortunately, in many environments (especially for users working from home), this security control has not been implemented and remote devices may be accessing corporate resources using remote access pathways that aren't adequately secured.

The rationale behind enabling protocols like RDP, SSH, and VNC has been a source of contention between information technology and information security teams. One argument is the need for low-cost remote access technology natively supported by the operating system. This is generally advocated by IT. Security and compliance teams, on the other hand, are wary of the inherent vulnerabilities, wormable exploits, and the lack of auditing and secure network routing of native protocols.

There needs to be a balance between these approaches. Authorised users need to initiate a secure remote access session to any device, any place, regardless of protocol. In addition, session monitoring, credential injection, and least privilege must be applied to overcome the security and compliance concerns governing an organisation. These capabilities must be in place whether the employee is working from the corporate office or from a remote location. Here, zero-trust architecture can play a pivotal role to overcoming native remote access protocol challenges. A zero-trust implementation can accommodate almost any environment and allow for remote sessions using proprietary access technologies.

Zero trust and secure remote access in the 'new normal'

Amidst travel shutdowns, social distancing, and stay-at-home orders, employees find themselves working with new freedoms and new restrictions. Employees working from home are using video conferencing, VPN, and remote access solutions to conduct business. Within this 'new normal', there are plenty of operational tasks now being performed from home that require privileged access. This runs the gamut from managing the organisation's social media accounts to administering servers, databases, applications, and SaaS solutions.

Our home networks are now serving entertainment, school, work, and providing an active conduit into our business. As a result, we are allowing our insecure home networks to be an extension of our information technology 'perimeters' to perform tasks in our business environments.

We have already seen security weakness related to these trends in the form of ransomware and breaches that only succeed due to threat actors

Together, zero trust and secure remote access can solve remote worker and remote session challenges and even strengthen your security posture for on-site and travelling workers.

having compromised remote access. With hardening and re-architecture of remote access, we can minimise this risk.

Remote working introduces new attack vectors and potential regulatory compliance issues that need to be resolved. For most organisations, this represents an unacceptable risk to the business since most of their highly sensitive data and applications reside on mission-critical platforms within their data centres and trusted cloud environments.

As the concept of a perimeter has fundamentally changed, and the way we use privileges and access sensitive information has broken our traditional security best practices, we need to rearchitect a solution that can address these underlying issues.

VPN security challenges

VPN and other traditional endpoint security solutions (especially on-premises) were never designed or architected to manage remote workers and cannot effectively manage risks outside of a defined perimeter. For zero trust to succeed, the network and environment need to be secured before a zero-trust architecture can be implemented.

Remote access technology was designed to manage sessions and, with a few considerations, can be implemented using a zero-trust model. However, a combination of zero trust, endpoint security, and IT managed devices with secure connectivity can accomplish the desired goals.

Secure remote access with zero trust can provide the following advantages over VPN alone:

- Scalable
- Secure
- Network layer access (protocol tunnelling)
- Role-based access
- Encrypted traffic
- Application layer virtualisation
- Remote desktop
- Virtualised web application access (HTTP/HTTPS)
- Proxied RDP access
- Proxied SSH access
- Application session monitoring
- Application session recording
- Just-in-time access
- Privileged access management integration
- ITSM integration for access
- Password management/credential storage
- Agentless access
- Prevent lateral movement

Achieving zero trust, as defined by NIST, with secure remote access

Based on the guidance defined by NIST 800-207, a zero-trust architecture clearly states that the goal is to focus security on a small group of resources (zones) in lieu of wide network perimeters or environments with large quantities of resources interacting 'freely'. It is a strategy where no implicit trust is granted to systems based on their physical or network location (local area network, wide area networks, or the cloud), but rather access is granted by a trusted source for either a user or application.

Zero-trust design considerations for secure remote access

Zero trust has been developed in response to industry trends that include remote users, dissolving network perimeters, and dynamic, cloud-based assets. It focuses on protecting resources, not logical network segments, as network segmentation is no longer seen as the prime component to the security posture of the resource.

Together, zero trust and secure remote access can solve remote worker and remote session challenges and even strengthen your security posture for on-site and travelling workers.

Next steps towards zero trust

Today, we are challenged with securing significantly more remote workers than in years past – many of them working from home. A secure remote access solution using a zero-trust architecture can ensure these resources are managed from potential inappropriate connection abuse and that all applications are executed within a zero-trust model. This means no end users are ever trusted for a remote session unless the confidence for execution can be measured. This is true for any location an asset may reside, irrespective of the perimeter. □

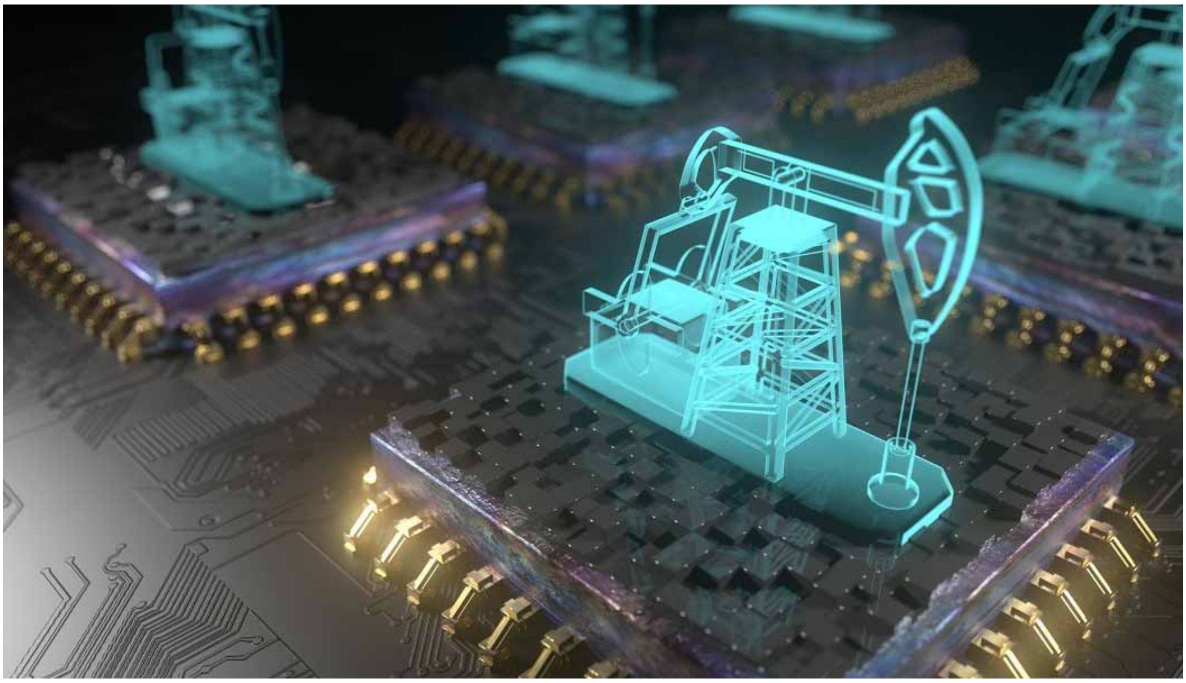
Visit **beyondtrust.com/solutions/zero-trust** to find out more.

BeyondTrust

How cybercriminals are cashing in on crypto

Cryptocurrencies have become increasingly mainstream in recent years, and opportunistic threat actors have not been slow to cash in.

Oakley Cox reports



Long before the peak values recorded in 2021, Darktrace reported on the close relationship between the value of cryptocurrency and the prevalence of malicious crypto-mining activity, commonly referred to as 'crypto-jacking'. Since then, we have reported crypto-jacking from botnets, rogue insiders, compromised IoT devices, and even as a precursor to ransomware.

Now, the Darktrace SOC team reports on how the prolific Sysrv botnet is evolving to evade traditional cyber-defences in order to mine cryptocurrency on vulnerable Internet-facing machines. By pivoting to Pastebin for command and control infrastructure, the malware is better able to remain hidden from tools using signature-based threat detection.

Recently, however, Darktrace AI was able to identify a server compromised by Sysrv despite it being a pre-existing infection. Darktrace autonomously grouped the server into a 'peer group' of similar devices, recognising the behaviour as anomalous in comparison to the wider group. The same technique was used to find a pre-existing Trojan hiding in an energy grid in 2020.

Evolution of the Syrsrv botnet

The Sysrv botnet has a rich history in adapting new techniques in order to remain relevant. When the botnet was first identified in early 2020, it made its name for its use of the GO language ('Golang'). It allowed the malware authors to target multiple operating systems. While financially motivated cybercriminals have traditionally targeted the widely used Windows OS, the proliferation of IoT devices using Linux OS has made them an attractive target, especially for those looking to make a quick buck from crypto-mining.

More recent Sysrv variants have come equipped with a host of exploits, ready to make the most of the diverse set of security holes it may encounter.

More recent Sysrv variants have come equipped with a host of exploits, ready to make the most of the diverse set of security holes it may encounter. Many are added to the malware's tool kit just days after the public release of a new vulnerability, demonstrating the sophistication of the attackers.

The botnet has also proven adaptable in which cryptocurrency it chooses to mine. The bots switched to Nano in 2021 during the currency's boom in value, but more recently reverted to Monero. Monero is a mainstream cryptocurrency and, similar to Bitcoin, is expected to hold its value better than other

Darktrace Attack Surface Management forms just one part of Darktrace Prevent, a product family that also empowers defenders to model likely attack paths, intelligently prioritise vulnerabilities, simulate attacks, and more.

currencies in the notoriously volatile crypto markets. Monero mining also has a technical advantage, in that it runs efficiently on CPUs. Other cryptocurrencies prefer GPUs and ASICs, which are unlikely to be found in the server environments targeted by Sysrv.

The storyline of botnet malware such as Sysrv over the last few years shows the sophistication and creativity of cyber-criminals out to cash in on crypto. These advancements and adaptations will continue to surface, but with the upcoming launch of Darktrace Prevent, defenders can prepare their organisations against the most sophisticated attacks.

With Darktrace Attack Surface Management, organisations discover potential weak points in their exposed environments, and take action before attackers can. In the case of the Sysrv botnet, which preys on vulnerable Internet-facing machines, Attack Surface Management will be able to identify machines and proactively harden defences before an attack like Sysrv could strike.

Darktrace Attack Surface Management forms just one part of Darktrace Prevent, a product family that also empowers defenders to model likely attack paths, intelligently prioritise vulnerabilities, simulate attacks, and more.

Insights gained are then fed into Darktrace's Detect and Respond capabilities, hardening defences and protecting organisations from the full range of cyber-threats – from crypto-jacking and supply chain compromise to phishing and spoofing attacks. □

Oakley Cox is Analyst Technical Director at Darktrace.

For more information, please visit **www.darktrace.com**

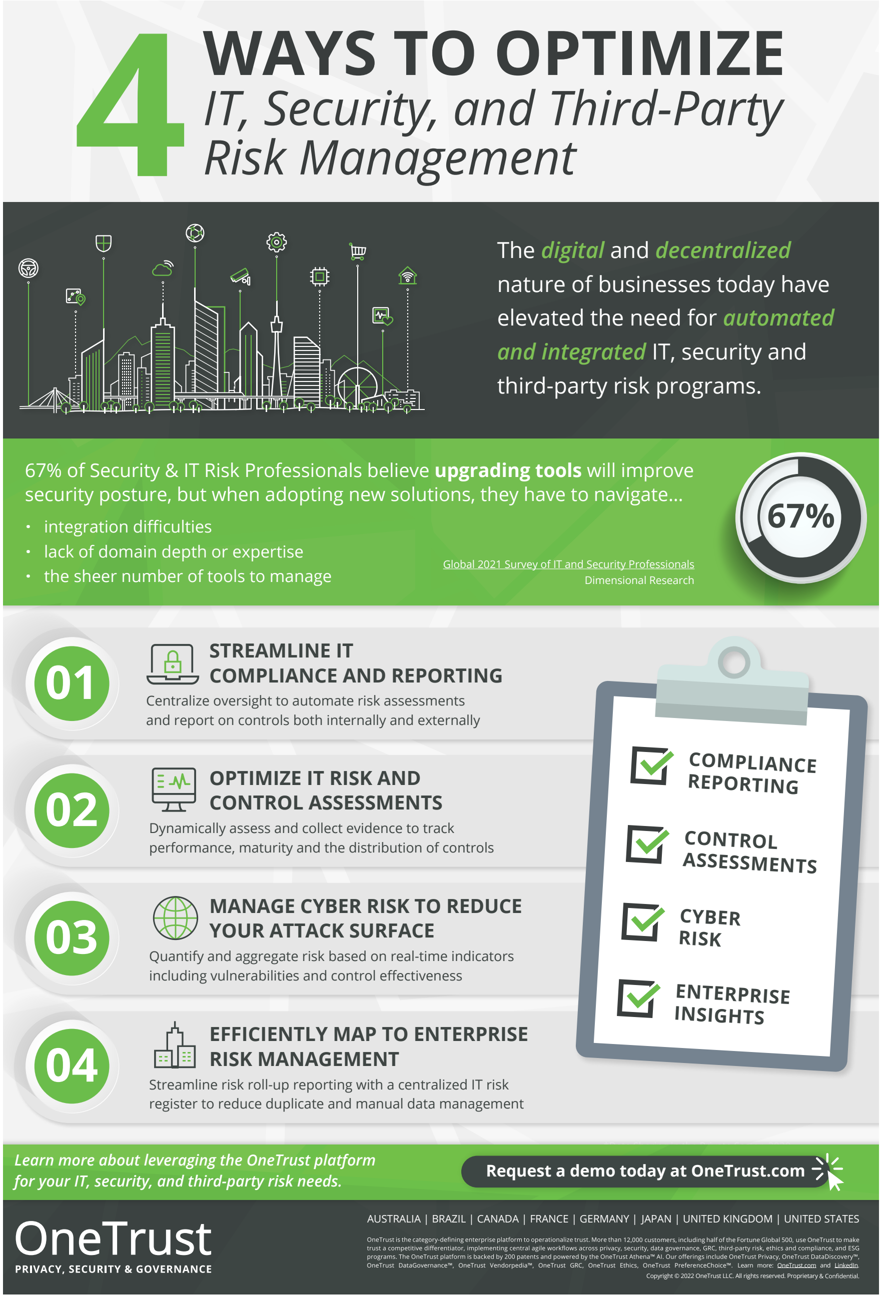
4 ways to optimize IT, security and third-party risk management

The *digital* and *decentralized* nature of businesses today have elevated the need for *automated and integrated* IT, security and third-party risk programs.

OneTrust reports

Risk today is fast, fluid, and interconnected, which means that evaluation and mitigation have an impact across risk domains. Have a look at this infographic to better understand how businesses can enhance automation with an integrated IT and third-party risk platform to improve security compliance and gain more holistic enterprise insights.

- Optimize resource capacity by deduplicating efforts across risk and controls
- Streamline risk assessments both internally and externally
- By-pass integration difficulties and simplify your tech stack by consolidating risk management tools



4 WAYS TO OPTIMIZE *IT, Security, and Third-Party Risk Management*

The *digital* and *decentralized* nature of businesses today have elevated the need for *automated and integrated* IT, security and third-party risk programs.

67% of Security & IT Risk Professionals believe **upgrading tools** will improve security posture, but when adopting new solutions, they have to navigate…

- integration difficulties
- lack of domain depth or expertise
- the sheer number of tools to manage

Global 2021 Survey of IT and Security Professionals
Dimensional Research

01 STREAMLINE IT COMPLIANCE AND REPORTING
Centralize oversight to automate risk assessments and report on controls both internally and externally

02 OPTIMIZE IT RISK AND CONTROL ASSESSMENTS
Dynamically assess and collect evidence to track performance, maturity and the distribution of controls

03 MANAGE CYBER RISK TO REDUCE YOUR ATTACK SURFACE
Quantify and aggregate risk based on real-time indicators including vulnerabilities and control effectiveness

04 EFFICIENTLY MAP TO ENTERPRISE RISK MANAGEMENT
Streamline risk roll-up reporting with a centralized IT risk register to reduce duplicate and manual data management

Learn more about leveraging the OneTrust platform for your IT, security, and third-party risk needs.

Request a demo today at OneTrust.com

OneTrust
PRIVACY, SECURITY & GOVERNANCE

AUSTRALIA | BRAZIL | CANADA | FRANCE | GERMANY | JAPAN | UNITED KINGDOM | UNITED STATES

OneTrust is the category-defining enterprise platform to operationalize trust. More than 12,000 customers, including half of the Fortune Global 500, use OneTrust to make trust a competitive differentiator, implementing central agile workflows across privacy, security, data governance, GRC, third-party risk, ethics and compliance, and ESG programs. The OneTrust platform is backed by 200 patents and powered by the OneTrust Athena™ AI. Our offerings include OneTrust Privacy, OneTrust DataDiscovery™, OneTrust DataGovernance™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust PreferenceChoice™. Learn more: OneTrust.com and LinkedIn.

OneTrust is the #1 fastest growing and most widely used technology platform to help organisations be more trusted, and operationalise privacy, security, and governance programmes.

More than 7,500 customers, including half of the Fortune 500, use OneTrust to comply with the CCPA, GDPR, LGPD, PDPA, ISO27001 and hundreds of the world's privacy and security laws.

For more information, please visit **www.onetrust.com**

OneTrust
PRIVACY, SECURITY & GOVERNANCE

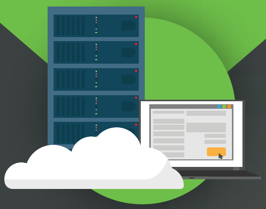
OneTrust

PRIVACY, SECURITY & GOVERNANCE

THE 4 PILLARS OF DATA INTELLIGENCE

1 KNOW YOUR DATA

- Leverage AI-Driven data discovery
- Catalog data from structured and unstructured sources
- Classify your data
  - Types of data
  - Location of data
  - Technical metadata
- Utilize a data dictionary and business glossary



2 GOVERN YOUR DATA

- Ensure data collection, storage, and use meets all applicable privacy rules and regulations, specifically:
  - Access
  - Retention and residency
  - Data minimization
  - Data protection
- Identify policy violations and take remediation action
- Define roles, responsibilities, and processes for reviewing data governance
- Monitor the use and quality of your data assets

3 USE YOUR DATA

- Search your catalog to find the data you need for your purpose
- Understand the obligations and requirements tied to your data
- Utilize easy access to the data set you need
- Be mindful of suggestions, warnings, and feedback to help you make the best decision

4 IMPROVE

- Monitor the maturity of your data governance program
- Generate regular progress reports, feedback, and trust scoring
- Regularly review policies
- Set KPIs including:
  - Levels of usage
  - ROI
- Anecdotal evidence the data intelligence efforts have been successful

VISIT ONETRUST.COM

Visit OneTrust.com to request a demo or to learn more about the range of data intelligence solutions including Automated Data Discovery and Data Catalog that can help your organization build effective data intelligence

Are you prepared for the non-secure 'new reality'?

With every transition there is always an opportunity to take advantage of change and raise the security bar.

BlackBerry reports

There is a two-fold method for successfully solving the problem of securing a remote workforce. Devices and technology can be reliably protected by taking a Zero Trust approach to accessing organisational resources. Likewise, employees can be protected through active measures that continuously assess their security risks, but remain out of their view. This non-intrusive form of personalised employee cybersecurity is possible through recent advancements in artificial intelligence (AI), and is called Zero Trust.

The idea behind Zero Trust is simple – anything wishing to interact with organisational resources must first acquire a certain level of trust. By default, everything starts with a trust score of zero. As interactions occur between the business infrastructure and another actor, trust levels may increase or decrease. The amount of access an actor is granted changes in real-time, along with their trust rating.

While the problem of personal technology connecting to workplace devices is solved with Zero Trust, the vulnerabilities caused by human nature must still be addressed. How does one create a secure environment when workers prioritise productivity over good security practices? How can the 20% of workers apathetic towards additional security measures be protected without their active cooperation? The answer is through implementing a Zero Touch approach to cybersecurity.

Zero Touch, as the name implies, seeks to give users immediate access to their productive assets without taking multiple intermediary steps. Workers who can do their jobs without entering passwords, experiencing timeouts, requesting special permissions, or multiple authentications are less likely to seek shortcuts or workarounds. When no additional security tasks exist for the user to perform, it does not matter if 20% of employees ignore new security measures.

The Zero Touch approach goes hand-in-hand with Zero Trust. Users establish trusted routines and interactions with workplace infrastructure. While performing trusted tasks, they experience no interference from cybersecurity related processes. When unusual activity occurs, trust must be gained or reestablished with the system though minimally intrusive verification. The end result: organisational infrastructure is continuously secured while employee productivity continues without interruption.

While the problem of personal technology connecting to workplace devices is solved with Zero Trust, the vulnerabilities caused by human nature must still be addressed.

Putting it all together

Employees shifting to work-from-home arrangements has increased cybersecurity risks beyond the initial estimates of experts.

Another point to consider is that very few homes have as fast or as reliable an internet connection as a business or campus network. Many employees live in areas with marginal connections or have their entire family accessing their internet connection at the same time, thus saturating it. Some employees have no wired internet connections at home and rely on cellular data services with limited bandwidth.

CISOs and security analysts must look beyond traditional EDR solutions and start thinking in terms of extended detection and response (XDR). While securing endpoints is critical for protecting the environment, today's workplace demands holistic solutions that include network telemetry, behavioural analysis, and continuous authentication.

The threat landscape has changed with the mass adoption of remote work and BYOD policies. However, the fundamentals of cybersecurity remain sound.

For information on how BlackBerry can help your organisation prepare for, prevent, detect, and respond to cyber-threats, visit us at **BlackBerry.com**

BlackBerry

YOUR PREDICTIVE, HOLISTIC AND HUMAN ADVANTAGE

Powered by Cylance AI

Be Proactive, Not Reactive

BlackBerry | Cybersecurity

Why SASE is primed to secure the evolution of finserv

Finserv is an industry leading the charge when it comes to the digitisation of services, yet, despite the consolidation of hybrid and remote working models, a degree of scepticism remains over networking alterations owing to the vital importance of industry security. Here we explore SASE as a means of enhancing productivity while

Tom McVey reports

Few industries have changed as dramatically as financial services (finserv) in the last decade.

Where banking and financial transactions were once exclusively an in-person and largely paper-based process, the vast majority of financial affairs are today managed digitally, with a variety of new innovations and services powering an ever-advancing market.

Be it fintechs, challenger banks, blockchain, mobile banking solutions and more, finserv today looks unrecognisable compared to the industry that existed even a mere half decade ago.

The improvement of service forms just one element of the industry's innovative focus, however. Behind the scenes, banks, credit unions, insurance firms, mortgage companies and others have been working to transform their own infrastructure to streamline processes, optimise productivity, enhance security, and operate in a more effective, agile, and flexible manner.

COVID-19 needs little by way of introduction. Much like many industries, finserv was flipped on its head by the pandemic back in early 2020.

Where industry players had primarily operated out of offices, social distancing restrictions and enforced national lockdowns shifted the hub of productivity to the home, with organisations having to adapt to such dramatic overhauls in a matter of days.

From an IT perspective, it presented a challenge. Where many felt the pandemic may have lasted a matter of weeks and a necessity for home working was therefore a temporary fixture, VPNs were implemented to provide disparate employees access to key resources and applications by tapping into on-prem network infrastructure.

18 months on, however, it's safe to say that flexible, remote and hybrid operating models are – at least in part – here to stay. With this in mind, it is time for organisations to consider how they might uphold such models more effectively moving forward.

Why SASE?

Yes, VPNs initially made sense, acting as an extension of a company's on-premise IT infrastructure. Yet they are equally fraught with challenges, and are simply not a viable, productive long-term solution.

While VPNs are capable of connecting employees in disparate locations to a centralised on-premises network, these very same networks were not designed to support remote operations. As a result, they can lead to bottlenecked traffic, hampered productivity and security vulnerabilities where network managers are forced to make visibility concessions.

With employees now located across varied locations, as are many of the cloud-based tools and applications they use to complete their work effectively, the question is why would their network need to be managed and secured from a centralised, on-premise location that is no longer being physically used?

Finserv should instead shift this activity to where the work is now happening – in the cloud. In doing so, a variety of benefits can be realised.

Visibility can be increased using products like CASB, DLP and Secure Gateway, while bottlenecked traffic and friction with users will be eliminated without the need for them to jump through intricate, laborious, sub-optimal hoops to access vital tools and data.

Here lies the argument for Secure Access Service Edge (SASE) adoption.

Coined by Gartner, SASE entails the simplification of a company's networking and security functions by interlinking both elements as a cloud service that acts as an extension of the user, bypassing the need for an enterprise data centre.

SASE is not a single solution. Rather, it is a concept comprising the amalgamation of pre-existing software-defined wide networking (SD-WAN) capabilities and network security functions (such as

Unlike legacy solutions and the use of 'square-peg-round-hole' VPNs, SASE has been built with a cloud-first mindset. As a result, it is able to provide complete, seamless protection and visibility, while equally prioritising productivity.

CASB, Cloud SWG, ZTNA/VPN, WAAPaaS, FWaaS, DNS, RBI and other relevant components).

The key thing is that SASE is not a case of revolutionising security. Rather, it is a natural evolution that uses the same techniques used by on-prem infrastructure in the cloud.

Unlike legacy solutions and the use of 'square-peg-round-hole' VPNs, SASE has been built with a cloud-first mindset. As a result, it is able to provide complete, seamless protection and visibility, while equally prioritising productivity.

Indeed, SASE is garnering significant attention at present as an IT framework that is much better suited to supporting today's dynamic secure access needs. Yet as a relatively novel concept, there is naturally some hesitancy as to its effectiveness, particularly within highly sensitive circles such as finserv.

While legacy security solutions are arguably outdated in terms of their usability, they are extremely secure. The question, therefore, is whether SASE can match these standards.

Zero Trust is key

In order for it to achieve the required levels of security, SASE should be incorporated in tandem with a Zero Trust philosophy.

Zero Trust is a natural fit for the finserv industry. The sector has historically taken a Zero Trust approach with its vital assets, having previously used bank vaults and other high-tech security investments that keep all persons out – both internally and externally of the organisation.

Isolation is one method in which Zero Trust can be achieved in a highly effective manner within a cloud network.

It is a technique that shifts the point of execution for active content away from a user's browser to a disposable, cloud-based virtual container. This essentially acts as a screen, preventing all active content including exploit code from reaching its intended target. Thus, it prevents cyber-attacks on a user's machine.

Isolation separates the enterprise network from public access while providing users with secure, low-latency connections to the vital resources and SaaS applications that they need. All content is rendered safely in a remote browser so that any potentially malicious code simply does not have an opportunity to execute on the end point.

It is not 'almost safe' like other security solutions. Rather, it can stop malware 100% of the time.

Cloud-first is inevitable

Indeed, while SASE, Zero Trust and isolation may appear to be relatively novel trends, it is important to understand that technologies such as these that have been engineered to support cloud-first models will undoubtedly become the future of networking and security.

In the case of SASE, where Gartner had originally predicted that it would take 10 years for the concept to become mainstream, the pandemic has now cut this projected timeframe in half.

Research shows that 67% of finserv firms will be looking to deploy an SD-WAN in the next year – a key component in SASE. Further, 54% of organisations are prioritising improvements of visibility and security for home infrastructure.

Despite having barely been mentioned two years ago, the technologies and ideals that underpin SASE are rapidly becoming a priority for many businesses looking to optimise their hybrid, flexible and remote business models in the new normal.

The tide is clearly turning in favour of cloud-first models. And while security hasn't always been a primary investment priority for businesses, owing to a lack of tangible return on investment, SASE is changing that narrative, with its productivity, accessibility and futureproofed characteristics capable of embedding sound security alongside a series of wider benefits. □

Tom McVey is Sales Engineer EMEA at Menlo Security.

For more information,
please visit
www.menlosecurity.com

MENLO
SECURITY

Cost of passwords: Resets, breaches, and more

Organisations are spending more than ever to protect themselves from cybercriminals.

Beyond Identity reports

A recent Deloitte study found that companies spend roughly $2,700 on each full-time employee for security each year. For companies with large workforces, that can add up to millions. But all the spending in the world won't matter if you're using passwords and the weak security they provide in your authentication processes.

Passwords are a massive security issue for organisations. Verizon's 2021 DBIR found that hacked and stolen passwords cause 89% of web application breaches, and these attacks can take months and millions of dollars to recover from.

To illustrate the costs of continuing to rely on the password, we've picked out a few statistics that show that passwords aren't only insecure but costing your organisation a lot of money.

The monetary cost of a breach

IBM's Cost of a Data Breach 2021 report found that the average cost of a data breach for an organisation was $4.24 million. Here's the breakdown of the average cost for different types of attacks:

- *Phishing:* $4.65 million
- *Malicious insiders:* $4.61 million
- *Social engineering:* $4.47 million
- *Compromised credentials:* $4.37 million

It's important to note that passwords play a critical role in all of these attacks. Phishing attacks are usually targeted at getting users to unwittingly give away passwords, social engineering uses fake authority figures to trick people into giving away passwords to 'verify' accounts, and insider attacks often rely on passwords not being updated and changed after employee turnover. The password remains the target for all of these attacks.

> Breaches caused by compromised credentials took the longest to identify and contain. On average, the password-related attacks IBM studied took 250 days to identify and another 90 days to contain, totalling 341 days.

Remote work has made data breaches more costly. For organisations that have 81–100% of their workforce remote, the average cost of a breach was $5.54 million. Companies with less than 10% of employees working from home had data breaches that cost an average of $3.56 million, which is still a significant amount of money but a dramatic difference from the costs to more remote work organisations.

The costs are often much higher for companies with remote employees because they are accessing resources on many different devices where the company has no way of assessing the risk or security posture of the device. Users can just enter their username and password and access sensitive data on any malware-infested device and a hacker has their way into the network.

It also often takes longer to discover breaches when the workforce is remote, allowing malicious attackers to wreak havoc and drive up costs for the recovery process. Companies with more than 50% of employees working remotely took 316 days to identify and contain breaches while organisations with more in-office employees only took 258 days.

Breaches caused by compromised credentials took the longest to identify and contain. On average, the password-related attacks IBM studied took 250 days to identify and another 90 days to contain, totalling 341 days. An attack on New Years Day wouldn't be detected until sometime around Labor Day and likely not resolved until early December. That's nearly an entire year, and attackers can do a lot of damage in that time.

It only takes one compromised password from a phishing attack or a hacker to employ a successful credential stuffing attack to cause all these financial and productivity losses.

Password resets = lost productivity

While the previous study looked at passwords and the costs associated with password-related attacks, Forrester looked at the cost of passwords from a productivity aspect.

Passwords suck up our time in one of two ways: either through recalling and entering them or spending time resetting them. Forrester's

Beyond Identity's platform offers an easy way for organisations to ditch passwords for good. Your customers are secured with our product by using immutable credentials backed by private keys that never leave the device.

researchers found that employees spend an average of 11 hours per year performing these two tasks. In a company of 15,000, an organisation would pay $5.2 million in wages just for employees to enter or reset their passwords!

Those employees aren't the only payroll costs associated with lost or forgotten passwords, however. Forrester also estimated that large organisations were spending an average of $1 million a year in help desk costs to assist employees with password-related issues.

Password issues hit e-commerce especially hard

In e-commerce, getting people to add items to their cart and successfully check out is the utmost priority for these websites. If customers encounter friction during shopping or checking out, it can easily lead them to abandon their carts. And often passwords are a big source of friction for customers.

Our research found that a quarter of those surveyed were willing to abandon a high-value cart ($100+) if a password reset was necessary. Password issues during the checkout process are disastrous.

We also found that one out of every eight shoppers will abandon their carts if you ask them to create an account before checking out. This is most likely due to the friction of having to create yet another username and password. In fact, we found that 84% of users are tired of remembering so many passwords.

It's already difficult enough to make a sale. The friction of passwords is making it even harder – and costing companies potential revenue.

Passwordless authentication pays for itself

Eliminating passwords doesn't just make good security sense – it makes equally good fiscal sense. Password-based attacks are often only discovered after the attacker has had months to scour your servers for high-value targets. Who knows what they might be able to find with that amount of time?

Secure Customers brings the convenience and security of passwordless authentication to your customers. Beyond Identity's platform offers an easy way for organisations to ditch passwords for good. Your customers are secured with our product by using immutable credentials backed by private keys that never leave the device.

Every time a customer logs in, you know they are who they say they are, and the device they're using is a known device to your network. Secure Work does the same thing for your workforce with passwordless multi-factor authentication (MFA) where only secure, phishing-resistant factors are used. Our product integrates with popular single-sign-ons and totally removes passwords from the authentication process and all the costs associated with them.

We'd love to show you how passwordless MFA can secure your network, streamline authentication, and save you money. Ask for a demo today.

About Beyond Identity
Invisible multi-factor authentication
Eliminate ransomware and account takeovers.

Invisible strong authentication. Security without friction. No passwords, no one-time codes, no user actions or second devices required. Just three unphishable factors.

The most advanced MFA on the planet – only one device needed.

Beyond Identity verifies users by cryptographically binding identities to devices to provide the most secure and frictionless MFA experience ever.

Implement a state-of-the-art MFA solution or add frictionless security to your existing MFA in 30 minutes or less.

For more information, please visit
www.beyondidentity.com

BEYOND IDENTITY

Deception-powered threat intelligence for financial services

Traditional cybersecurity is not enough to mitigate risk and protect financial institutions.

Financial services is one of the most targeted industries today, bombarded with ransomware and phishing attacks daily. 74% of financial institutions experienced a rise in cybercrime over 2020 and 2021[1], with the average cost of a data breach in the financial sector totalling $5.72 million.[2]

Growing cyber-fraud, a mobile attack surface, the emergence of cryptocurrency, and a move toward third-party payment partners – all create new cybersecurity challenges that demand powerful, flexible defence with deep visibility and minimal management. Traditional cybersecurity is not enough to mitigate risk and protect financial institutions. Deception technology makes it possible to take a proactive cybersecurity stance.

We've created a full data sheet on how deception technology can improve the security posture of financial services that you can download here. Read more about the specific challenges and our solution below.

The specific challenges of financial services

The financial sector is made up of very high-value targets, which is one of the biggest challenges faced when protecting it. The stakes are high, and therefore the attacks tend to be more sophisticated.

- Banks and financial institutions are a major target of both ransomware and phishing attacks because of their monetary value and transactions.
- Identity and financial fraud are rampant.
- Critical payment systems (such as SWIFT) are complex and high stakes.
- Financial organisations have limited cycles because they are always defending against something, making innovation difficult.

As these high-value networks are ever more vulnerable to attack, it is vital to find new security solutions. Deception technologies can be used to provide an extra dimension of security to banking and financial services networks. With deception, it is possible to detect malicious activity, collect valuable threat intel and also create and respond to adversary activity in real time.

> With deception, it is possible to detect malicious activity, collect valuable threat intel and also create and respond to adversary activity in real time.

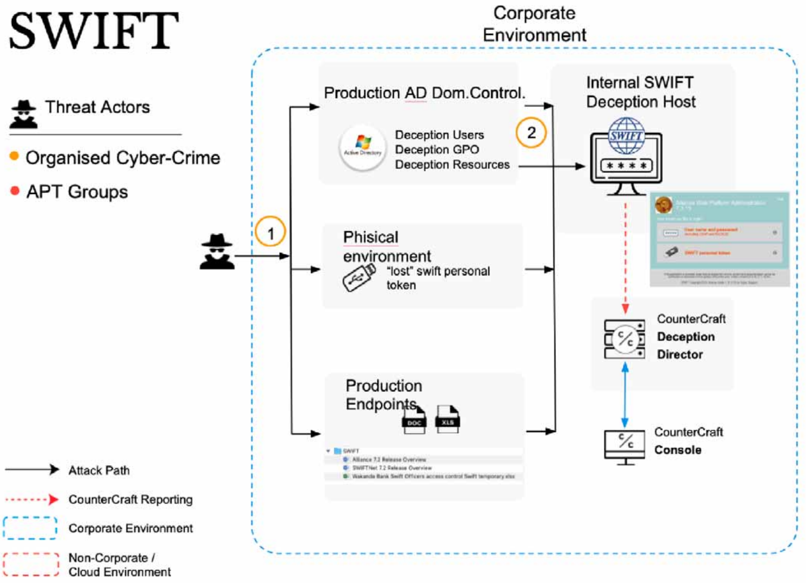
All of this is achieved with zero impact on existing systems, and zero risk to business continuity. This is a major plus for financial services organisations, which often have complex systems that cannot be touched.

Example: Deception campaign for financial services

Here is a real-life example of how deception has worked to protect an important aspect of financial services – SWIFT networks. This campaign allows organisations to track the data that the adversary is interested in as well as how they are trying to get it.

1. In Phase 1 of this campaign, the attacker tries to enter the production environment via an Active Directory domain controller.
2. In this environment, the attacker finds decoy users, decoy GPOs (Group Policy Objects) and other deception decoys.
3. The attacker accesses an internal deception host that simulates a SWIFT network. It reports every move of the attacker to the deception director, who can manage the attacker's movements via the console.

CounterCraft reports


SWIFT
Threat Actors
Organised Cyber-Crime
APT Groups
Corporate Environment
1
Production AD Dom.Control.
Active Directory
Deception Users
Deception GPO
Deception Resources
2
Internal SWIFT Deception Host
SWIFT
Phisical environment
"lost" swift personal token
Production Endpoints
DOC
XLS
SWIFT
Alliance 7.2 Release Overview
SWIFTNet 7.2 Release Overview
Wakanda Bank Swift Officers access control Swift temporary.xlsx
CounterCraft Deception Director
CounterCraft Console
Attack Path
CounterCraft Reporting
Corporate Environment
Non-Corporate / Cloud Environment

Deception can help in the proactive protection of high-value targets without imposing any burden on the normal operation of services.

The result

The compromise of a SWIFT network and the subsequent misuse of funds and transfers was successfully avoided.

Benefits

Deception can help in the proactive protection of high-value targets without imposing any burden on the normal operation of services.

- Actionable threat intelligence with zero false positives tailored to your organisation
- Intuitive platform requiring minimal technical resources to manage
- Flexible deployment model that includes on premise within the network, on premise outside the network, and in any Cloud Service Provider environment
- No emulations and no complicated physical and/or virtual appliances. We install on real unallocated/nonproduction physical or virtual systems
- Truly mimic your production environment by deploying the necessary servers, endpoints, applications, and services required
- Real-time telemetry, Indicators of Comprise (IOCs), and Techniques, Tactics, and Procedures (TTPs)
- Automatically map threat intelligence to the native MITRE ATT&CK Framework integration within the platform
- Protects your current investments by integrating with existing solutions

To learn more about how deception is uniquely positioned to protect financial services, download the full data sheet at **www.countercraftsec.com/resources.html**

For more examples of how deception has prevented cyber-attacks and to learn more about CounterCraft, contact us at craft@countercraftsec.com

CounterCraft

[1] https://www.businesswire.com/news/home/20210428005365/en/COVID-Cyber-Crime-74-of-Financial-Institutions-Experience-Significant-Spike-in-Threats-Linked-To-COVID-19

[2] https://www.upguard.com/blog/cost-of-data-breach

Counter
Craft

VISIT US IN THE EXHIBITION HALL

Deception-Powered Threat Intelligence for Financial Services

Real-time actionable threat intel
specific to your organization.

Security teams across the globe trust CounterCraft

World-renowned financial institutions, government bodies, pharma, retail, industrial, and law-enforcement agencies are defending their organization with CounterCraft. Join them!

Gartner
COOL VENDOR 2021

OVERALL LEADER
LEADERSHIP COMPASS 2021

INFOSEC AWARDS
WINNERS
CYBER DEFENSE MAGAZINE
2019

Follow us: @countercraftsec
@countercraft
@countercraftsec

www.countercraftsec.com
San Sebastián - Madrid - Londres - Nueva York

Sponsors and exhibitors

Beyond Identity | Strategic Sponsor

Organisations rely on Beyond Identity to secure identities on the internet. Beyond Identity secures access to SaaS applications and cloud resources to protect data and privacy. Breaking down the barriers between cybersecurity, identity, and device management, Beyond Identity provides the most secure authentication on the planet, and dramatically improves the way the world logs in.

With the Beyond Identity Passwordless Identity Platform, organisations can eliminate passwords, positively verify user identities, confirm device trust, and enforce risk-based access controls. Beyond Identity enables security teams to implement zero trust so their organisations can safely and securely work in hybrid-work environments with increasingly cloud-centric IT. Organisations turn to Beyond Identity to stop cyber-attacks, protect their most critical data, and meet compliance requirements.

We offer SaaS, subscription-based software.

Founded in 2019, Beyond Identity is headquartered in NYC, and has offices in Boston, Dallas, and London.

For more information, please visit www.beyondidentity.com

BeyondTrust | Strategic Sponsor

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organisations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organisations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organisations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including more than 70% of the Fortune 500, and a global partner network.

Learn more at www.beyondtrust.com

BlackBerry | Strategic Sponsor

BlackBerry provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500m endpoints including 175m cars on the road. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear – to secure a connected future you can trust. BlackBerry. Intelligent Security. Everywhere.

For more information, visit BlackBerry.com and follow @BlackBerry

Darktrace | Strategic Sponsor

Darktrace (DARK:L), a global leader in cybersecurity AI, delivers world-class technology that protects over 5,000 customers worldwide from advanced threats, including ransomware and cloud and SaaS attacks. The company's fundamentally different approach applies self-learning AI to enable machines to understand the business in order to autonomously defend it. Headquartered in Cambridge, UK, the company has 1,500 employees and over 30 offices worldwide. Darktrace was named one of TIME magazine's 'Most Influential Companies' for 2021.

For more information, please visit www.darktrace.com

Menlo Security | Strategic Sponsor

Menlo Security protects organisations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

For more information, please visit www.menlosecurity.com

OneTrust | Strategic Sponsor

OneTrust is the #1 fastest growing and most widely used technology platform to help organisations be more trusted, and operationalise privacy, security, and governance programmes. More than 7,500 customers, including half of the Fortune 500, use OneTrust to comply with the CCPA, GDPR, LGPD, PDPA, ISO27001 and hundreds of the world's privacy and security laws.

The OneTrust platform is powered by the OneTrust Athena™ AI, and our offerings include OneTrust Privacy, OneTrust PreferenceChoice™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust DataGuidance™, OneTrust DataDiscovery™, and OneTrust DataGovernance™.

Learn more at OneTrust.com and LinkedIn

Searchlight Security | Strategic Sponsor

Like all of the greatest innovations, Searchlight Security was born out of the need to solve a problem: criminals being able to act with impunity on the darkweb.

Founders and long-term friends Ben Jones and Dr Gareth Owenson decided to use their combined skills, knowledge and experience to create a solution to this problem, and so Searchlight Security came into being.

A pre-eminent Tor expert, Gareth combined cutting edge cyber-defence experience and ground-breaking academic research with Ben's experience in defence to create a world-leading suite of investigative darkweb products which afford business and law enforcement agencies an unmatched toolset in their fight against criminal activity on the darkweb.

Utilised by the world's most innovative and forward-thinking government agencies, companies and charities, Searchlight Security are shedding a light into the most hidden realms of the darkweb for all to see, and fulfilling their mission of protecting society as a whole.

For more information, please visit www.slcyber.io

SECURING
FINANCIAL SERVICES

Binalyze | Education Seminar Sponsor

Binalyze is the world's fastest and most comprehensive enterprise forensics solution. Our software remotely, securely and automatically collects more than 160 digital forensic artifacts in under 10 minutes.

With evidence collected, our Timeline, Triage, interACT and DRONE product modules help you analyse, collaborate and complete incident response investigations quickly to dramatically reduce dwell time and make reporting compliance simpler.

Binalyze saves you time, reduces cybersecurity operational costs in your SOC and helps you prevent financial and reputational losses associated with cyber-attacks.

For more information, please visit www.binalyze.com

Cequence Security | Education Seminar Sponsor

Organisations trust Cequence Security to protect their web apps and APIs with the most effective and adaptive defence against online fraud, business logic attacks, exploits and unintended data leakage, which enables them to remain resilient in today's ever-changing business and threat landscape.

Millions of ransomware, business email compromise and credential harvesting attacks bypass expensive email security solutions every year. They are in your users' inboxes right now.

For more information, please visit www.cequence.ai

Cofense | Education Seminar Sponsor

Cofense is the only company that combines a global network of 30 million people reporting phish with advanced AI-based automation to stop phishing attacks fast. That's why over half of the Fortune 500 trust us.

We're Cofense. We Stop Phish.

Our Phishing Detection and Response platform catches the phishing emails that your secure email gateway inevitably misses. We deliver the technology and insight needed to detect, analyse, and stop phishing attacks.

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organisations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of nearly 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organisations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defence, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise.

For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn

CounterCraft | Education Seminar Sponsor

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defence powered by high-interaction deception technology. CounterCraft detects threats early, collects personalised, actionable intelligence, and enables organisations to defend their valuable data in real time. The award-winning solution, fully integrated with MITRE ATT&CK®, fits seamlessly into existing security strategies and uses powerful automation features to reduce operator workload.

Founded in 2015, CounterCraft is present in London, New York, and Madrid, with R&D in San Sebastian, Spain. CounterCraft recently raised additional funding from venture capital firms including cybersecurity-specific funds Adara Ventures, eCAPITAL, In-Q-Tel and Evolution Equity, bringing the total investment to date to $10 million.

Learn more at www.countercraftsec.com

Digital Element | Education Seminar Sponsor

Digital Element, is the industry-leading geolocation and IP data services provider. Our solutions offer accurate and time-relevant information about online entities such as location, proxy/VPN, ISP, time zone, and more. Our accurate data allows real-time intelligence about inbound/outbound network traffic, provides location/connection type, identifies potential threats, and is critical to instantly identifying and evaluating suspicious transactions.

Our solutions help to: balance risk management, shore up fraud controls, and strengthen digital profiles; identifying: suspect traffic, real-time global location data and mobile network information.

Customers such as JP Morgan Chase, BBC, AWS, Experian, Criteo, Oracle, Codewise, AppsFlyer, eTrade, DoubleVerify, SourceFire, eBay, LogRhythm, and more utilise our solutions.

For more information, please visit www.digitalelement.com

e2e-assure | Education Seminar Sponsor

e2e-assure provide CISOs, CEOs and other owners of cyber-risk with confidence, through transparent and tailored Security Operations Centre (SOC) and Managed Detection and Response (MDR) services. We leverage existing investments to reduce the total cost of ownership and share our cybersecurity expertise through our Cyber Maturity Programme.

We believe that passionate and diverse people are key to dealing with the complex and dynamic challenges of cybersecurity. We do this through hiring great people and investing in them throughout their careers at e2e.

We don’t buy into technology being the single answer and build our services around having just enough technology, supported by world-class people and processes. We make life easier for ourselves and our customers, providing rich data across all technologies within a network through a single pane of glass using our SOC Platform, Cumulo.

These principles support all our SOC services, from our Microsoft Defender Services to SOC Simulation, from Proof of Concepts to full SOC models.

For more information, please visit e2e-assure.com

SECURING
FINANCIAL SERVICES

Egress | Education Seminar Sponsor

Egress makes digital communication safer for everyone. As advanced and persistent cybersecurity threats continue to evolve, we recognise that people get hacked, make mistakes, and break the rules. Egress's Intelligent Cloud Email Security suite uses patented self-learning technology to detect sophisticated inbound and outbound threats, protect against data loss, resulting in the reduction of human activated risk.

Used by the world's biggest brands, Egress is private equity backed and has offices in London, New York, and Boston.

For more information, please visit www.egress.com

FireMon | Education Seminar Sponsor

FireMon is the only real-time security policy management solution built for today's complex multi-vendor, enterprise environments. Supporting the latest firewall and policy enforcement technologies spanning on-premises networks to the cloud, only FireMon delivers visibility and control across the entire IT landscape to automate policy changes, meet compliance standards, and minimise policy-related risk. Since creating the first-ever policy management solution in 2004, FireMon has helped more than 1,700 enterprises in nearly 70 countries secure their networks. FireMon leads the way with solutions that extend and integrate policy management with today's latest technologies including SD-WAN, SASE, XDR, and SOAR.

For more information, please visit www.firemon.com

Kocho | Education Seminar Sponsor

At Kocho, we believe greatness lies in everyone. That's why we exist, to help companies realise their potential. By combining the power of Microsoft cloud technology with world-class identity, cybersecurity and our team of brilliant people – we take our clients on a journey of secure transformation.

And we're with you every step of the way. Because the path to greatness isn't walked alone. We help you adopt and embrace the right tech solutions at the right time.

The result? Sustainable and secure growth that amplifies your business success.
Kocho. Become greater.

For more information, please visit kocho.co.uk

Obsidian Security | Education Seminar Sponsor

Obsidian Security is the first truly comprehensive threat and posture management solution built for SaaS. Our platform consolidates data across core applications to help your team optimise configurations, reduce over-privilege, and mitigate account compromise and insider threats. The company was founded in 2017 by industry experts from Carbon Black and Cylance including Ben Johnson, Glenn Chisholm and Matt Wolff. Notable Fortune 500 companies trust Obsidian Security to secure SaaS applications, like Salesforce, Workday, Microsoft 365, ServiceNow, Google Workspace and Github. Headquartered in Southern California, Obsidian Security is privately held and backed by Menlo Ventures, IVP, Greylock, GV, Norwest Venture Partners, and Wing.

For more information, please visit www.obsidiansecurity.com

Swimlane | Education Seminar Sponsor

Swimlane is the leader in cloud-scale, low-code security automation. Swimlane unifies security operations in-and-beyond the SOC into a single system of record that helps overcome process and data fatigue, chronic staffing shortages, and quantifying business value. The Swimlane Turbine platform combines human and machine data into actionable intelligence for security leaders.

For more information, please visit swimlane.com

RevealSecurity | Networking Sponsor

We Are RevealSecurity. Rule-based solutions detect only known attack patterns, and they generate a high number of false alerts. TrackerIQ learns user activity flow profiles, which in turn enable accurate detection of anomalous activity flows and the discovery of unpredictable breaches. RevealSecurity's detection solution is application agnostic, analysing user journeys in and between different types of applications – SaaS, cloud and custom-built applications.

For more information, please visit www.reveal.security

Balbix | Branding Sponsor

Balbix enables businesses to reduce cyber-risk by identifying and mitigating their riskiest cybersecurity issues faster. Our SaaS platform, the Balbix Security Cloud™, ingests data from businesses' security and IT tools so they can understand every aspect of their cybersecurity posture, build a unified cyber-risk model and obtain actionable insights for risk reduction. With Balbix, businesses can automate inventory of their cloud and on-premise assets, conduct continuous risk-based vulnerability management and quantify cyber-risk in dollars.

For more information, please visit www.balbix.com

Tessian | Branding Sponsor

Tessian is a machine intelligent email security platform that automatically prevents security threats like misaddressed emails, unauthorised emails and non-compliance. Tessian uses machine learning to understand normal email communication patterns in order to automatically identify email security threats in real time, without the need for end user behaviour change or pre-defined rules and policies. Tessian makes email safe at some of the world's largest enterprises across the financial, legal and technology sectors.

To find out more, visit www.tessian.com

SECURING
FINANCIAL SERVICES

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** **See pages 32 to 35 for more details**

Cofense

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

e2e-assure

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

Rob Demain, Founder and CEO, e2e-assure

Obsidian Security

Obsidian Security: Extending Zero Trust to SaaS

Chris Fuller, Principal Product and Solutions Architect, Obsidian Security

Swimlane

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

SECURING FINANCIAL SERVICES

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** **See pages 32 to 35 for more details**

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** **See pages 32 to 35 for more details**

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

Throughout the day a series of education seminars will take place as part of the main agenda. Delegates will be able to choose to attend any of the seminars, all of which will provide vendor-neutral, hands-on advice. Seminars within each session run concurrently.

Session 1: 10:20–11:00

Cofense

SESSION 1
10:20–11:00

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.

e2e-assure

SESSION 1
10:20–11:00

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

Obsidian Security

SESSION 1
10:20–11:00

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

SECURING
FINANCIAL SERVICES

Swimlane

SESSION 1
10:20–11:00

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

Session 2: 12:50–13:30

Binalyze

SESSION 2
12:50–13:30

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

CounterCraft

SESSION 2
12:50–13:30

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

Digital Element

SESSION 2
12:50–13:30

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

SECURING
FINANCIAL SERVICES

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

Kocho

SESSION 2
12:50–13:30

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

Session 3: 15:30–16:10

Cequence Security

SESSION 3
15:30–16:10

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

SECURING
FINANCIAL SERVICES

Egress

SESSION 3
15:30–16:10

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

SESSION 3
15:30–16:10

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 □

Speakers and panellists

Bev Allen

Head of Information Security Assurance, Quilter

Bev Allen is an information security professional with more than 30 years' experience in delivering operational and strategic privacy, information security and information risk management, including the development and delivery of security and privacy policies, standards, and security training, in a variety of culturally diverse organisations and industries.

Rohyt Belani

Chief Executive Officer and Co-founder, Cofense

Rohyt Belani is an industry veteran with over 18 years of experience in technical and senior management roles at leading cybersecurity companies. Prior to founding Cofense (formerly PhishMe), Rohyt served as the CEO of Intrepidus Group (acquired by NCC Group PLC), Managing Director at Mandiant (acquired by FireEye, Inc.) and Principal Consultant at Foundstone (acquired by McAfee). At Cofense, Rohyt has led the company's growth from concept to over 400 employees globally, serving over 2,000 enterprise customers including half of the Fortune 100. During his tenure, Cofense has established itself as a global leader in phishing defence and was acquired in February 2018 by BlackRock Private Equity Partners. Rohyt has been honoured with the 2017 EY Entrepreneur of the Year and Washington Business Journal's 40 Under 40.

Amir Ben-Efraim

Co-founder and CEO, Menlo Security

Amir Ben-Efraim is Co-founder and CEO of Menlo Security. Previously, Amir was Vice President of cloud security at Juniper Networks where he helped define the company's strategy to secure the virtualised data centre, public and private clouds. He joined Juniper via its acquisition of Altor Networks, which he led as Founder and CEO. Prior to Altor, Amir was an executive at Check Point Software, a pioneer in internet security. He holds an MBA from UCLA, an MSEE from Stanford University and a BSEE from UC Berkeley.

Daniel Brett

Co-founder and CSO, CounterCraft

Daniel Brett is the Chief Strategy Officer and Co-founder at CounterCraft. Daniel is highly accomplished in achieving outstanding B2B growth for visionary companies and contributes over 15 years of marketing expertise to the business. His deep industry knowledge and understanding of consumer behaviour enables him to thrive in new markets and achieve rapid sales success on a global scale.

Formerly responsible for the launch of a dedicated cybercrime division at leading pure-play cybersecurity company, S21sec, he also established a strong track record in international B2B business development at IKUSI, where he capitalised on his talent for innovation and business transformation. Daniel is widely recognised as an authoritative voice on cybersecurity by top industry agendas as well as media outlets such as the BBC. Driven by creativity and known for his energetic optimism, Daniel also brings a healthy dose of British wit to the team and knows from experience that a strong company culture serves as a very powerful commercial asset.

"I think anyone with experience in cybersecurity will tell you it grabs you by the scruff of the neck and is impossible to shake off. This, of course, is the best thing about it, because absolutely everyone has a role to play. The CounterCraft solution is focused on behaviour, and it's with great pride that I can contribute an expertise that's both integral to the growth of the business, but also the design and technical development of our product."

Ian Burgess

Director, Cyber and Third-Party Risk, UK Finance

Ian leads UK Finance's operational and policy work on cybersecurity and third-party risk management. Beside responding to regulatory papers both in the UK and internationally, he regularly engages with key stakeholders to determine the applicability of collective action initiatives on behalf of the financial sector. Most notably he operationalised the Financial

Sector Cyber Collaboration Centre (FSCCC), a unique industry utility designed to promote cyber-intelligence sharing amongst financial institutions. Before joining UK Finance, Ian worked in technology risk at BNY Mellon, where he led the development and deployment of a global framework to map controls to global cyber, technology and data privacy regulations, and before that served an eight-year career as a British Army Officer.

Jack Chapman

Vice President of Threat Intelligence, Egress

Jack Chapman joined Egress as part of their acquisition of Aquilai in June 2021. He co-founded Aquilai in 2018 and oversaw the development of its anti-phishing solution. Based on its technological excellence and vision, Aquilai was hand-selected by the National Cyber Security Centre (NCSC), the UK Government's intelligence and security agency, for its Accelerator program and benefitted from in-depth and strategic insights for product development.

Brian Chappell

Chief Security Strategist (CSS), EMEIA & APAC, BeyondTrust

Brian has more than 30 years of IT and cybersecurity experience in a career that has spanned system integrators, PC and software vendors, and high-tech multi-nationals. He has held senior roles in both the vendor and the enterprise space in companies such as Amstrad plc, BBC Television, GlaxoSmithKline, and BeyondTrust. At BeyondTrust, Brian has led sales engineering across EMEA and APAC, product management globally for privileged password management, and now focuses on security strategy both internally and externally. Brian can also be found speaking at conferences, authoring articles and blog posts, as well as providing expert commentary for the world press.

Marco Cinnirella

Professor of Applied Social Psychology, Royal Holloway

Marco Cinnirella is a Professor of Applied Social Psychology at Royal Holloway, one of the UK's leading psychology departments. He has published widely in peer-reviewed scientific journals on a diverse range of topics such as attitudes, behaviour change, group dynamics and cyber-psychology, and uses a diverse range of qualitative and quantitative techniques in his research. Marco's expertise in behaviour change has led him to advise a range of organisations on behavioural information security challenges, including large multi-nationals in the energy, oil and pharmaceutical sectors. His expertise in behavioural information security challenges has led to invited addresses at the United Nations and he has delivered keynote addresses on information security and psychology at various academic and industry conferences.

Emmanuel Dahunsi

Security Architect EMEA, Goldman Sachs

Emmanuel Dahunsi is a Security Architect at Goldman Sachs in EMEA specialising in cloud security architecture. He previously worked at JP Morgan as an Information Security Manager (public cloud), Network Engineer, Network Security Engineer and as a Consultant to large telecommunication providers in EMEA prior to that. Emmanuel holds several certifications across the major cloud providers like AWS & Google. He also holds a master's degree in Information Security from the Royal Holloway University of London. In his spare time, he enjoys visiting museums, learning about history, and boxing for charity & cancer research.

Hanah-Marie Darley

Head of Threat Research, Darktrace

Hanah-Marie Darley is Head of Threat Research at Darktrace, where she uses her background in psychology and international relations to creatively problem solve and mentor teams. With nearly a decade of experience as a threat intelligence specialist and geopolitical analyst, she is well-equipped to combat the demanding reality of global strategic intelligence, and understands the need for creativity in critical problem solving and resource management.

SECURING
FINANCIAL SERVICES

Rob Demain

Founder and CEO, e2e-assure

Rob Demain is the Founder and CEO of e2e-assure, a company that he started after realising that the traditional delivery model for Security Operations Centres (SOCs), focusing on technology over people and processes, wasn't working. This realisation was backed up with 20+ years' experience in building SOCs for large, complex organisations, such as national telcos, major financial institutions and national public sector and defence organisations.

Paul Fryer

Sr. Manager Sales Engineering, BlackBerry

Paul leads BlackBerry's Sales Engineering Organisation across the UK, Ireland, Middle East and Africa; his team, spread across the region, evangelise BlackBerry's Cyber Security Portfolio and help BlackBerry customers to identify and successfully execute their cybersecurity strategies. At the heart of this is BlackBerry's philosophy that prevention is possible and, through taking a prevention first approach to cybersecurity, customers can eliminate the noise and focus their efforts efficiently and effectively. Paul has been in the cybersecurity industry since 2016, initially specialising in data protection before leading multiple sales engineering teams across Europe.

Chris Fuller

Principal Product and Solutions Architect, Obsidian Security

Chris Fuller is Principal Product and Solutions Architect at Obsidian Security. Chris works with leading enterprises across EMEA to uncover their SaaS security challenges and help them rapidly deploy Obsidian's technology to safeguard the business-critical data held in SaaS apps like Microsoft365, Workday, Salesforce and more. Today, the Obsidian platform secures over 4 million unique SaaS users and thousands of interconnections between SaaS apps. Chris has spent the last decade specialising in web and cybersecurity technologies, focusing on tuning and securing user experiences for major brands across Europe and the Middle East. Prior to Obsidian, Chris built the EMEA Sales Engineering team for Shape Security and managed that team following the $1bn acquisition by F5.

Luke Hebbes

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

Luke Hebbes is a passionate information security leader with 20 years of experience ranging from building high-performing teams to delivering cutting-edge research. He promotes innovative, risk-based solutions rather than the formulaic application of industry standards or vendor solutions. Luke believes that it is essential to view security from the perspective of business critical assets and to adopt a pragmatic approach, not letting technology drive the security requirements. Security is a supporting service to most businesses and, as such, should be a transparent enabler, used to protect the business and its assets, whilst aligning the risk posture with value generation – effective security can only be delivered with an understanding of the business context.

Joe Hebenstreit

Director of Product Management, Digital Element

Joe Hebenstreit leads Digital Element's company-wide IP intelligence technology and strategic database planning, specialising in proxy-detection solutions. An IP intelligence and geolocation data analysis expert, he works closely with a variety of industries around the world to help them leverage IP intelligence and geolocation data. Additionally, he is responsible for Digital Element's strategic partnerships in regard to data sources ultimately leading to product enhancements and new product offerings. In his 20-year career with Digital Element, Hebenstreit has been at the helm of the evolution of IP geolocation data as it grew from an ad targeting and digital marketing tool to one that is utilised for licensing and copyrights enforcement, cybersecurity, network routing and content localisation.

SECURING
FINANCIAL SERVICES

Owain Howard

Regional Sales Manager, EMEA, FireMon

Vinod Kashyap

Head of Product, Digital Element

Vinod Kashyap serves as Digital Element's Head of Product, where he combines his knowledge of product management, lean operations and engineering to guide the long-term product roadmap and go-to-market strategies for the company's location intelligence technology offerings. Kashyap's 20-year career includes expertise in product and strategy leadership, IoT technologies, digital marketing, global e-commerce, and research and development, enabling him to bring broad perspectives when working with customers and partners on innovative and problem-solving solutions.

Chris Meidinger

Technical Director, Beyond Identity

Over the past 20 years, Chris has driven revenue via both pre-sales and post-sales with IT security and communications solutions. His initial career was spent with VARs, architecting and deploying custom solutions to meet specific business requirements. For the last decade, he's been in sales engineering at emerging, venture-backed security companies. He specialises in bringing value to customers by synthesising complex technical concepts into simple business value propositions and presenting tailored, data-driven investment proposals to senior executives to earn their business.

Tim Neill

Chief Risk Officer, NPP, Mastercard

Tim is Mastercard's Chief Risk Officer for its Real Time Payments and Applications business, leading Risk Management across the Product & Engineering divisions, which includes real time payments, applications, digital solutions, commercial products and innovation labs. Responsible for the Product & Engineering 'Business Risk & Control Committee' under the Chief Product Officer, this committee reports to the Audit Committee, Risk Committee, Management Committee and Board of Mastercard.

Tim is also a Board Director and Audit Committee member of Vocalink Ltd UK, a Bank of England approved role. He is Chair of the Mastercard Payment Services Risk Committee in Scandinavia, and reports to the Mastercard Vocalink Asia Pacific Board in the Philippines, which are all directly supervised national payment services. For the past 20 years, Tim has worked in banking, capital markets and technology in risk and operations roles in the UK, Asia and the Middle East. He joined Mastercard from the London Stock Exchange Group where he led Operational Risk and Resilience.

Externally, Tim is a member of the UK Finance Technology & Cyber – Product and Services Board, and a Board Trustee of Voca Pensions Ltd. Tim and his team were recently nominated for 'Risk Management Innovation of the Year' 2021, by CIR Risk Management Awards, in recognition of their development of a risk framework and risk reporting tool within the area of payments. The 'payments rule book' and risk tool is now regularly being discussed with central banks and schemes internationally as a means to accelerate a common criteria approach to payments governance.

Gareth Owenson

Chief Technology Officer and Co-founder, Searchlight

Gareth is an internationally recognised and published darkweb scientist. A former academic with a PhD in Computer Science and a BSc in Internet Technologies, Gareth co-founded Searchlight Security and now oversees the research and development, software engineering and niche cyber-capabilities.

Jules Pagna Disso

Group Head of Cyber Risk Intelligence, BNP Paribas

Dr Jules Pagna Disso is the Group Head of Cyber Risk Intelligence and Insider Technology Risk at BNP

Paribas with nearly 20 years of experience working in IT and cybersecurity. Jules has led the successful completion of large projects on industrial controls systems security, Red Teaming tooling and threat intelligence, SOC incident response tooling development and deployment, deception technologies, security auditing and more. He also enjoys giving guest lectures at various universities around the world including Oxford University, Warwick University. He holds a PhD in Intrusion Detection Systems as well as a number of cybersecurity related qualifications. As part of his role in BNP Paribas, Jules oversees the threat landscape within the second line of defence, ensuring that all threats, across all functions, are identified and appropriately addressed though security controls policies and appropriate governance.

Santosh Pandit

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

Santosh Pandit heads the Operational and Cyber Resilience work in the Insurance Directorate of the Prudential Regulation Authority. He has been actively involved in the joint work of the Bank of England, PRA and the FCA on operational resilience, its implementation in the insurance sector and the cross-directorate and cross-regulatory consistency. Santosh represented the UK on EIOPA's Cyber and IT Project Group and on the cyber-stream of the EU-US Insurance Project. Santosh provides expert guidance to insurance supervisors in the assessment of cyber-resilience of regulated firms and dealing with high-profile cyber-incidents.

Santosh is passionate about quantum computing and applied cryptography. He is very hands-on when it comes to cybersecurity, cloud computing. He regularly speaks on various topics related to operational resilience at seminars and roundtables. Santosh will be happy to share his perspective not only as a regulator but also as a previous Non-Executive Director in the private sector. He strongly believes that cyber and operational resilience is less about regulatory compliance but more about business priorities.

Jorge Ferrer Raventos

Solutions Engineering Specialist, OneTrust

Lina Sabestinaite

ISO, Handelsbanken UK

Lina Sabestinaite is an Information Security Officer at Handelsbanken PLC UK. Her current focus is supporting secure change governance and providing security consultancy for the bank's digital transformation projects. Prior to this role, she worked in finance, healthcare and technology sectors. Lina led many organisations in creating or improving the information security management systems and achieving ISO27001 certifications. Lina holds CISSP, CISM, CRISC and AWS Cloud Practitioner certificates.

James Sherlow

Senior Field Solutions Engineer EMEA, Cequence Security

James Sherlow has extensive application security engineering experience gained in both the private and public sectors. Through many years of practical engineering experience and research, he has become an acknowledged expert in cybersecurity, threat intelligence, secure application delivery of content and the heightened risks & threats associated with them.

Prior to Cequence Security, James was a leading Cybersecurity Specialist at Palo Alto Networks, a role he moved to after leading and building up their Security Systems Engineering team in Western Europe. Before joining Palo Alto Networks, he led the Systems Engineering Team at ConSentry, a market-leading start-up focusing on application visibility, control, and security in wired and wireless local area networks. Previously, he helped pioneer the next generation of cloud-native application delivery at Avi Networks, which VMware acquired. James brings his considerable experience in fast-moving cybersecurity environments to Cequence Security, augmenting its technical presence and adding further capability to deliver API security strategies and services to its customers and channel partners.

John Skipper

CISO,
Metro Bank

John joined Metro Bank as CISO in 2019 after a 20-year career in cyber-consulting. He is accountable to the Board and ExCo for cyber, infosec and data protection, and has kicked off an ambitious programme of improvements across all three areas. As the UK's first new high street bank in 150 years, Metro Bank already has 79 stores (the latest being in Leicester) and a strong presence in mobile and internet banking, with over 2.5 million accounts. John and his team therefore face a unique and interesting set of cyber-challenges. In John's previous career, he has provided cyber-advice ranging from developing national policy through insider risk management to defining technical architecture. He has worked in multiple sectors including national security, defence, financial services, energy, travel and education, and for organisations ranging from start-ups to global banks and critical national infrastructure. He therefore draws on a very broad range of experience, but his heart is in banking.

Emre Tınaztepe

Founder/CEO,
Binalyze

Emre Tınaztepe is the Founder and CEO of Binalyze, an enterprise forensics company headquartered in Estonia with offices in the US and UK. In addition to evangelising the new enterprise forensics category, Emre is actively participating in the development of next-generation digital forensics solutions with Binalyze's world-class team, guiding the company on its mission to disrupt and innovate in the digital forensics space to transform the nature and use of forensics in the enterprise security stack by making it lightning fast, scalable, automated and easy to use. Prior to starting Binalyze, Emre worked in a variety of positions at global cybersecurity companies. His areas of expertise include reverse engineering, malware analysis, driver development, and incident response. He also led the development of an anti-malware suite which is used by millions of users to protect their devices against cyber-attacks.

Toby Van De Grift

VP of EMEA,
Swimlane

Toby has worked in IT security for over 15 years, and started working in the SOAR space in 2016 (before it was even called SOAR!). Toby has helped SOCs evolve and improve from a variety of industries – FS, telco, manufacturing, media, MSSP and more. He also has experience with threat intelligence, EDR, network security, incident response, vulnerability Management and SIEM. He is constantly questioning and looking outside of his immediate area to expand his world view and bring new ideas to his customers. Customers say his key skill is his integrity and authenticity – he will only bring technologies and ideas to customers that he genuinely believes will improve security, add value, reduce risk, or a combination thereof.

Anna Webb

Head of Security Operations,
Kocho

How aligning Security Awareness and Security Operations can reduce dwell time

With Cofense Phishing Detection and Response (PDR), organisations can create a partnership between the Security Awareness and Security Operations teams.

Cofense reports

Email phishing attacks pose a large threat to every organisation around the world and make up 91% of all cyber-attacks. The most effective way for organisations to reduce their risk is to ensure that all aspects of their phishing programme are focused on resiliency and preparing for the attacks that have the highest likelihood of reaching them. Suggested metrics to define and understand include human resiliency, mean time to detect (MTTD), mean time to respond (MTTR), and dwell time.

While MTTR falls under the scope of Security Operations and is a central focus in analysing and remediating attacks, MTTD should also be considered and is often a secondary metric. To fight email phishing attacks, both metrics must be primary objectives of the Information Security programme. The Security Awareness function can make an impact to these metrics by increasing the resiliency of the humans at the organisation to ensure that the threats bypassing traditional email controls are quickly recognised, reported, and placed in the hands of the security operations and response teams.

The first step to reducing dwell time is improving MTTD and can be accomplished by conditioning your employees to be the first line of defence by becoming human sensors to report any email they suspect is malicious. Most security awareness programmes focus on susceptibility, a measure of how many employees click on a simulation. Instead, security awareness programmes should focus on resiliency, which compares the number of employees who reported the simulation to the number of employees who clicked the link. Email phishing attacks can only be removed if Security Operations is aware of them – positioning Security Awareness in the centre of Security Operation's strategy.

The second step to reducing dwell time can be accomplished by enabling Security Operations to analyse the most-likely malicious emails first. While increased reporting rates are a positive change and increase visibility into the threat landscape, it also means threat analysts must spend more time reviewing emails for actual attacks. Various email security vendors provide tools for Security Operation Centres (SOCs) to respond to reported emails, but don't provide the best approach. While most organisations take an approach of 'scoring' threats based on their internal threat intelligence, this does not account for the power of your internal reporters. With highly trained employees as the first line of defence, they become the best 'eyes' of an organisation, and employees with the highest likelihood to spot a phishing email should have their reports analysed first. Combining threat scoring and reporter scoring further emphasises the importance of Security Awareness while making it easier for Security Operations to stop email phishing attacks.

> Security Awareness is more than compliance – it is an integral part in reducing dwell time of the most active and successful threat vector facing every organisation – email phishing attacks.

Security Awareness is more than compliance – it is an integral part in reducing dwell time of the most active and successful threat vector facing every organisation – email phishing attacks. With Cofense Phishing Detection and Response (PDR), organisations can create a partnership between the Security Awareness and Security Operations teams. Cofense enables Security Awareness to build resiliency across their organisation with simulations derived from real phish that are updated every month and is the only vendor that delivers simulations when an employee is active in their inbox, doubling report rates across our customer base. Cofense PDR takes these reported emails and automatically helps analysts in SOCs sift through the noise by scoring reported emails based on indicator of compromise (IOC) scoring and 'reporter reputation', enabling threat analysts to investigate reported emails from employees with the greatest track record of reporting real phish. It is time Security Awareness takes its rightful place next to Security Operations as partners in reducing dwell time and keeping email phishing attacks out of employee inboxes. □

For more information,
please visit
www.cofense.com

COFENSE

The regulators are on the case. Why compliance violations have now become a C-level concern

Make 2022 the year you tackle your compliance challenges.

FireMon reports

The cyber regulation landscape has shifted beyond a mere IT concern, and executive leadership must pay attention. In the summer of 2021, the U.S. Securities and Exchange Commission (SEC) indicated the seriousness of cyber-vulnerabilities by levying fines against two enterprise companies due to the lack of disclosures of cybersecurity issues. In June, First American Financial Corp. settled for $500,000 and in August, Pearson PLC settled for $1m in penalties. In late 2020, the ICO fined British Airways £20m, the largest amount ever handed down due to a significant data incident. In every case, the organisations were critically breached, exposing customer information including financial information and personal records.

With data collection and the management of that data forever under the compliance spotlight, there is nowhere to hide. And as a result, compliance has now become a C-level conversation due to the implications a data breach can have on their organisation.

So why now?

With the shift to hybrid and remote work, cyber-attackers are taking advantage of security vulnerabilities. In the fourth quarter of 2021 alone, cyber-attacks were at an all-time high and businesses suffered 50% more attacks in 2021 compared to 2020. The National Cyber Security Centre (NCSC) has reported that Russian ransomware attacks are happening in record numbers. Breaches on small to medium-sized businesses increased as well, due to a lack of available resources to secure their networks. It's no surprise that as digital citizenship increases, so do the gaps in cybersecurity.

The failure to protect valuable data and lock-down security vulnerabilities is especially harmful to a company's bottom line, with an estimated $1.8 billion lost to cybercrime in 2019. Financial services, technology, pharmaceutical and energy sectors have been hit with the heaviest losses. The implications of a cyber-attack go much further than that with organisations suffering from:

- Disruption to operations
- Reputational damage and loss of customers
- Plummeting stock prices
- Lost revenue, due to not being operational, or for covering ransomware costs
- Increased costs in insurance, public relations and technology

As evidenced with the penalties levied by the SEC and ICO, security vulnerabilities are taken seriously by regulators. Therefore, organisations are seeking to avoid these less than desirable outcomes, and keep customer data safe.

Staying one step ahead

The volume of regulatory change, internal security requirements and cyber-threats has IT and network security teams overwhelmed in attempts to meet regulatory compliance and address violations as they happen in real time. The typical decision is to invest in new technology, which in turn creates a multi-vendor, hybrid environment that becomes even more challenging to manage and secure.

Compliance audits and audit trails can create controls to deter bad behaviour, increase response time and improve intrusion detection. But manual processes can introduce errors, and the time and resources to produce a report can be excessive. That is where automation comes in.

To improve security posture and ensure continuous compliance, these processes need to be automated to simplify reporting, provide real-time violation detection and deliver rule recertification.

Avoid violations. Avoid risk. Avoid fines.

FireMon's compliance management tools create a proactive compliance posture that keeps organisations ahead of violations instead of chasing after them. By taking an automated and proactive approach, organisations can benefit from:

- 90% less time to produce compliance reports
- 100% accurate reporting, eliminating errors
- Eliminate the risk of compliance violations and fines to 0

When network security is improved, C-level executives can be assured that their organisations are not only meeting but exceeding regulatory compliance. The risk of losing customers, revenue or damage to the business' reputation is lessened so that leadership can focus on growing their companies.

Visit firemon.com/continuouscompliance to see how FireMon can efficiently automate network security policies and help achieve continuous compliance. □

For more information, please visit
www.firemon.com

How proxy and VPN data can enhance cybersecurity effectiveness

Today's enterprise professionals are navigating a challenging cybersecurity environment.

Digital Element reports

In many ways, the problem's scope is stunning and alarming. For instance, ransomware attacks increased by 151% year-over-year in 2021, while phishing scams increased by 440% in a single month.

The escalating attacks come with a price. The most recent Cost of a Data Breach Report found that 2021 had the highest average cost of a data breach in the report's 17-year history, surpassing $4 million for the first time. As a result, companies are increasing their cybersecurity investment in 2022, fortifying their defensive postures to avoid the financial expense, reputational damage, and productivity loss that inevitably follows a cybersecurity incident.

In the process, cybersecurity leaders and organisational decision-makers face difficult decisions as they allocate resources, invest in new solutions, and support their personnel. This is especially challenging as threat actors display remarkable agility, exploiting novel vulnerabilities and harnessing the latest technologies to wreak havoc on a company's digital infrastructure. However, by evaluating the latest technology trends, companies can get ahead of the next threats.

New technologies invite threat actors to invoke fresh tactics when launching ransomware attacks, infiltrating company networks, or illegally occupying consumer accounts. In a pandemic-stricken environment, many are leveraging camouflage techniques that allow them to operate anonymously from anywhere in the world.

Most prominently, virtual private networks (VPNs), proxy servers, queue networks, and domain name systems (DNSs) allow threat actors to operate with nearly total anonymity.

At the same time, many organisations have made VPNs, encrypted connections over the internet from a device to a network–through a single IP address, available to the employees, providing expanded access to company IT from anywhere in the world. Collectively, companies deploy VPNs for several reasons, including:

> New technologies invite threat actors to invoke fresh tactics when launching ransomware attacks, infiltrating company networks, or illegally occupying consumer accounts.

- ensuring general security, such as avoiding identity theft
- minimising privacy concerns, such as securing personal data
- mitigating information exposure from public WiFi
- accommodating job-specific requirements

Meanwhile, more than half of VPN users rely on the technology to access region-restricted content from streaming services and digital platforms. Unfortunately, many users are downloading free VPN software to access this region-restricted content, and they've unknowingly had their residential IPs hijacked by these VPN providers.

When consumers download and sign up for a free commercial VPN, many agree to give the VPN provider the right to use their IP address in the entire proxy pool for routing purposes. While this clause is often hidden in the Terms of Service, it can have significant implications for cybersecurity.

Threat actors have found proxies to be an effective way to masquerade their malicious activity. Companies can't prevent VPN users from accessing the internet, but this practice increases the risk of labelling customers or employees as threat actors while failing to detect or discover the root of cybercrime.

Incorporating IP data for protection

Simply put, it's evident that companies need to develop the capacity to separate threat actors from genuine users. The ability to identify threat actors operating through a proxy enables companies to flag potential criminal activities, set protocols for handling this type of 'non-human' traffic, and review post-action analytics.

By incorporating proxy and VPN data on the front-end of online security measures, companies can automatically flag IP addresses as suspicious and reject or block the incoming IP from connecting to their service, website, or network. In addition, proxy data can trigger variable fraud alerts that enable

Developing the capacity to analyse and respond to high-quality proxy and VPN data strips threat actors of their anonymity, making it one cybersecurity strategy that companies can't ignore in the year ahead.

companies to differentiate authentic traffic from fraudulent activity more effectively.

Most importantly, success is predicated on data quality. Information reliability can vary significantly among data sources, but the most accurate proxy data providers ensure that this information is constantly updated and originates from excellent sources. The cybersecurity implications are far-reaching, including:

- government agencies can use IP-based VPN data to filter and identify safe VPNs
- financial services and e-commerce platforms can incorporate proxy and VPN data to implement smart rules to verify consumer IP addresses automatically
- managed security service providers can use proxy and VPN data as a foundational, front-line layer of fraud prevention and security enhancement.

To thrive in a shifting cybersecurity landscape, companies must continually equip themselves with the data and tools to protect their digital assets. Developing the capacity to analyse and respond to high-quality proxy and VPN data strips threat actors of their anonymity, making it one cybersecurity strategy that companies can't ignore in the year ahead. □

Digital Element, is the industry-leading geolocation and IP data services provider. Our accurate data allows real-time intelligence about inbound/outbound network traffic, provides location/connection type, identifies potential threats, and is critical to instantly identifying and evaluating suspicious transactions.

Customers such as JP Morgan Chase, BBC, AWS, Experian, PayPal, Oracle, Codewise, SourceFire, eBay, LogRhythm, and more utilise our solutions.

Please visit **www.digitalelement.com** for more information.

digital**element**®
Location is Elemental ™

The psychology of social engineering and phishing

What specific psychological tricks do cybercriminals use? And how can we use that knowledge against them?

Egress reports

There's a reason phishing attacks are known as *social* engineering. They're human-activated, and simply don't work unless someone takes the figurative bait. That's why even though phishing originates externally, it falls under the umbrella of insider threat – someone internal needs to make a mistake.

Phishing is ultimately an emotional attack. It plays on our emotions and tricks us into doing something we wouldn't normally do when we're concentrating at our best. So what specific psychological tricks do cybercriminals use? And how can we use that knowledge against them?

Why do we still fall for phishing?

Many people think they would never fall for a phishing attack (or scams in general) because they're educated, experienced professionals. They may even have gone through rigorous cybersecurity training. However, this overconfidence can lead to complacency, which is exploited by criminals.

In fairness, most people with even basic cybersecurity training *do* know the warning signs of phishing. They're diligent at work, and they don't act recklessly. The truth though, is there are times when any of us can become stressed, tired, or forced to rush. It's in those mindsets where we're most error-prone, and far better targets for phishing.

For that exact reason, cybercriminals have been quick to pounce on the fallout of the COVID-19 pandemic. Our research shows only 28% of remote workers have access to a solo office, while 46% feel pressured to use email outside of office hours (often from mobile devices). Among others, these factors have made it even easier for hackers to press on the psychological triggers that make phishing so effective.

> There are times when any of us can become stressed, tired, or forced to rush. It's in those mindsets where we're most error-prone, and far better targets for phishing.

Psychological triggers in phishing

The purpose of a phishing attack is to pull us out of our mindset of questioning the validity and security of communications. Consider the hallmarks of the most common form of social engineering – email phishing. These are just some of the psychological triggers scammers use to make us think emotionally, rather than logically.

- ***Urgency:*** a phishing email usually wants something done *right now,* as the longer you have to think, the more you may question whether it's legit
- ***Plausibility:*** the days of foreign princes offering a share of their fortune have gone… modern phishing attempts will be based on real-life, often mundane scenarios
- ***Familiarity:*** there's been a marked rise in spear phishing, where the attack is at least partially tailored to an individual – often claiming to be from an authority figure such as their CEO or head of security
- ***Confidentiality:*** the action required is specific to you and needs to be done by you alone, as getting someone else involved increases the chances of the scam being spotted

It's also common for criminals to target people who have just moved to new companies (info that often can be easily found on social media), as fear and anxiety are powerful motivators. These people are more likely to be anxious to impress a new boss and unaware of the subtle signs that something is amiss with their communication style. If you've worked under a CEO for many years, you'll most likely see the signs of a scam email. On your first day of work? Perhaps not.

Can we use psychology to protect ourselves?

According to Dr Jessica Barker in a recent Egress webinar, the key to stopping phishing could lie in behavioural economics. We process information in two ways: the calm, collected way where we analyse problems in a measured, thoughtful manner. Like doing a difficult maths sum. And then the second, more impulsive way, where we act almost on autopilot – such as driving a car on an empty road.

Phishing attacks use psychological triggers to push us away from the first frame of mind and into the

Egress Defend uses machine learning to analyse the content and context of emails in the background, offering people gentle traffic-light warning prompts when the signs of phishing emerge.

second. They wants us to act quickly, clicking and responding in autopilot rather than in a slow, analytical manner. That's why urgency is so key in phishing – if we came back to the email later in the day, we might not fall for it on closer inspection.

It's for this exact reason that so many people have an 'oh no…' reaction almost immediately after they've fallen for a phishing scam. We see the same thing with misdirected email. As soon as our brain slows down again, we begin to question what we just did. The training is remembered and the warning signs of a mistake start to creep in.

The problem businesses have is that it's all very well understanding these psychological nuances – but how can they help people in practice? How can we get employees to think that split-second earlier? The good news is we can, with a little help from technology.

Evening the odds with human layer security

Cybercriminals aren't looking for technological gaps to exploit when it comes to phishing – they're trying to find cracks in the human layer. That's also why the answer to phishing isn't ever going to be technology alone. It's about empowering people to become an integral part of an organisation's defence, rather than seeing them simply as a security problem to be mitigated.

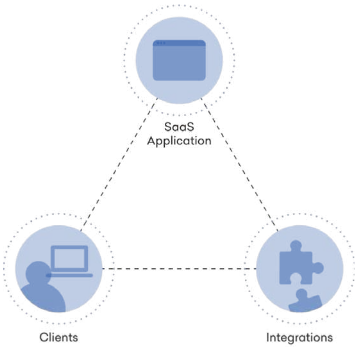
Human layer security tools such as Egress Defend are able to give people a nudge back towards their calmer, more collected way of thinking. Because as we noted before, most of the time people can be trusted to do the right thing. Egress Defend uses machine learning to analyse the content and context of emails in the background, offering people gentle traffic-light warning prompts when the signs of phishing emerge.

Some phishing emails will always slip through the defences, so we need to tap into psychology to beat them. Criminals use psychological triggers to turn people into security risks – so we provide the tools to even up the odds and turn people into security assets. Most employees know the right thing to do, and it's about offering a technological guardrail that can nudge them back towards the place where they make smart security decisions.

For more information, please visit
www.egress.com

The components of a holistic SaaS security strategy

SaaS security: A changing model of cybersecurity.



Obsidian reports

Businesses today commonly employ hundreds of SaaS applications for a variety of functions, but the majority of sensitive data is typically entrusted to a small set of foundational enterprise applications. Security leaders are well aware that the transition to SaaS has prompted increased targeting by bad actors and recognise that SaaS cybersecurity is more important than ever – but the way teams are thinking about and equipped to protect SaaS needs a new approach.

For years, security teams focused on securing *things*: endpoints, servers, and networks. Accordingly, endpoint detection and response (EDR) solutions were used to monitor and mitigate threats residing on user devices and servers, while network detection and response (NDR) tools protected the network.

Although the transition to cloud-based applications has fundamentally changed the coverage model for application security, many teams are still intently focused on securing the clients and their connections while overlooking other critical components of SaaS. Better SaaS security requires a new approach and a different way of thinking uniquely designed around the architecture of cloud-based applications – a holistic solution that extends the principles of zero trust to SaaS.

The core components of SaaS

To better understand how to approach SaaS security, you should first consider three core components of SaaS application:

- The client connection to the application
- The SaaS application itself
- Other applications integrating with it

A holistic approach to SaaS cybersecurity recognises that each of these components can be a source of risk to the entire application, while the interconnected nature of these applications also means that a breach originating at any one of these points can threaten your wider SaaS environment.

Securing the client connection

Monitoring the client connections to your SaaS environment is essential. Your security team needs to understand the authentication, privileges, and actions of your users within and across business-critical applications to define the scope of each user's risk. This data needs to be aggregated and normalised from every application into a single, easily understood format in order to be readily accessible to your security team, extending the zero trust model of 'never trust, always verify' beyond identity providers and into the SaaS applications themselves.

Securing the application

The SaaS applications that are core to your business are inherently unique and complex, with the intricacies and functionality that one might expect from an operating system. Securing these applications requires a deep understanding of each platform, structural vulnerabilities, and issues specific to your own environment. Continuous monitoring of the application security posture is critical here – this includes both application configurations and the privileges granted to your users. Fully securing applications also means going beyond merely knowing the state of controls and privileges, but monitoring associated activities to detect lapses in security and utilising inter-application insight.

Securing the integrations

SaaS users and administrators integrate third-party applications into core applications in order to expand functionality, automate workflows, or even play their favourite games. Once authorised, these connections persist their permissions and access to the core application – a vulnerability which can present serious security risk if left unchecked. Even vetted third-party applications can be compromised by an attacker, providing a backdoor into core applications. Without continuous monitoring and threat detection to verify the integrations, they fall outside of the zero trust framework.

Obsidian's comprehensive approach

Obsidian Security offers the first truly comprehensive SaaS cybersecurity solution built with a deeper understanding of your business-critical applications. This understanding of the three core components of SaaS applications enables Obsidian to take zero trust beyond the identity provider and secure the business-critical data held in SaaS applications. □

For more information, please visit
www.obsidiansecurity.com

OBSIDIAN

Four reasons to outsource your managed security service

An outsourced MSSP can provide a higher-quality and more cost-effective option than building an in-house security function.

Anna Webb reports

Too often, organisations get hung up on cost when considering outsourced security. While getting value for money is important, it's worth prioritising some other important advantages of using a managed security service.

If you're considering how to improve the security posture of your financial services company, an outsourced managed security services provider (MSSP) can provide a higher-quality and more cost-effective option than building an in-house security function.

Using an MSSP can help you:

1. Overcome the skills gap

There's no shortage of headlines about the cybersecurity skills gap, but there is a shortage of people to fill it. Many smaller businesses have only one employee responsible for cybersecurity and they're often a general 'IT person' rather than a cyber-specialist. Large organisations tend to be better resourced with four to five people in cyber-roles, but still struggle to attract and retain talent.

This means they often don't have enough resources to implement essential cybersecurity practices such as firewalls, anti-malware, and data encryption.

Working with an MSSP means savings on recruitment, salaries, bonuses, benefits, and training – plus, your security partner will help establish the optimal security system configurations.

2. Ensure security at all times

Security incidents aren't known for their convenience – they'll happen when you least expect. Even a minor breach can lead to system downtime and delays in service delivery. These can vary from the mildly frustrating to business-critical – particularly in a heavily regulated industry such as the financial services sector.

An outsourced MSSP provides you with consistent and undisrupted monitoring, through both technology and human expertise. By establishing better threat monitoring and security reporting, you also get actionable insight to further improve your security posture.

> More tools isn't always the answer, it's about getting the *right* tools and having the *right* people set-them up correctly and manage them on an ongoing basis.

3. Access the latest technology

The sheer amount of security solutions on the market is intimidating, with updates and new technology appearing all the time. But more tools isn't always the answer, it's about getting the *right* tools and having the *right* people set-them up correctly and manage them on an ongoing basis.

By working with an MSSP, they can guide you to security solutions with the optimal price-to-value ratio – and then implement, integrate, and scale selected technologies within your existing infrastructure.

4. ...and, of course, save money

Cybersecurity can be an expensive function to establish in-house. Setting up an in-house SOC for an organisation with up to 1,000 users can cost up to £1,033,500 over three years in CAPEX and OPEX costs. That's often unrealistic for small- and medium-sized companies.

Partnering with an MSSP, however, could save you over £893,500 in the same time frame. These savings come from not having security staff on the payroll and not having to invest in constant upskilling and training.

Any MSSP worth their salt will ensure the right tool selection and optimise your costs. This ensures that you're spending what you need to secure your operations, vs. going for the vendor-recommended (but not the most cost-effective) technology. □

Anna Webb is Head of Security Operations at Kocho, a leading provider of cybersecurity, identity, and Cloud IT services.

For more information, please visit **kocho.co.uk**

Is automation removing the need for people?

How security automation technology affects SOCs and enables security teams.

Cody Cornell reports

Do you believe that automation will remove the need for people? Most people do.

From a distance, it's easy to understand how someone could come to this conclusion. There's certainly a good deal of hype surrounding security automation and how much automation can improve your security environment. Automation has removed many of the mundane and repetitive tasks that take up time and resources, enabling security operations professionals to focus on higher quality work. But we have a serious conundrum – is automation removing the need for humans, or empowering them?

Security automation at a glance

Security automation is the application of technology to automate security procedures and policies. This could include cyber-threat detection, vulnerability management, and incident response. While the term 'security automation' was once only a buzzword, it has now become mainstream and widely adopted, with three main variations:

- Traditional full-code Security Orchestration, Automation and Response (SOAR)
- Low-Code Security Automation
- No-Code Security Automation

There are many different variations of what it means to automate something in information security, each with its own benefits and limitations.

How automation affects security operations

The security operations centre (SOC) is a challenging environment, filled with growing threats, people who are overworked and understaffed, and repetitive tasks that waste time and resources. These challenges are magnified for financial services organisations:

- 10% of all breaches target the financial services industry.
- The current average time to contain a breach is 233 days.
- Nearly two-thirds have over 1,000 sensitive files open to every employee.

Automation has the power to help alleviate some of these pains by making security operations more efficient. Some effects of automation include:

- Reduce MTTD and MTTR
- Improve incident response processes
- Gain visibility into the value of your security team

Is automation replacing people?

The truth is, automation must be used as a tool to support the SOC, not replace it. It takes the mundane manual tasks off your plate and enables you and your team to become builders of a better security environment. Security teams can focus on analysing risk, prioritising what matters most, and getting ahead of threats before they become incidents. This can mean doing more with fewer people or using your existing staff to get more done in less time.

It's no secret that the security industry is facing major staffing shortages, and the demand for cybersecurity skills has grown by 22% year-over-year in Europe. If automation could completely replace people, now would be a good time to start. But the reality is that security automation still needs humans in order to succeed.

Keeping humans in the loop

So why do we still need humans in the security automation loop? The answer is simple: people are flexible, computers aren't. When facing a security incident, a human can make decisions based on common sense, business context, and real-time facts. Computers can't.

The idea of working with machines and not against them will be increasingly important as we move towards the age of machine learning and deeper automation. Machines are great at doing repetitive tasks over and over again, but they are not good at making human decisions outside their programming.

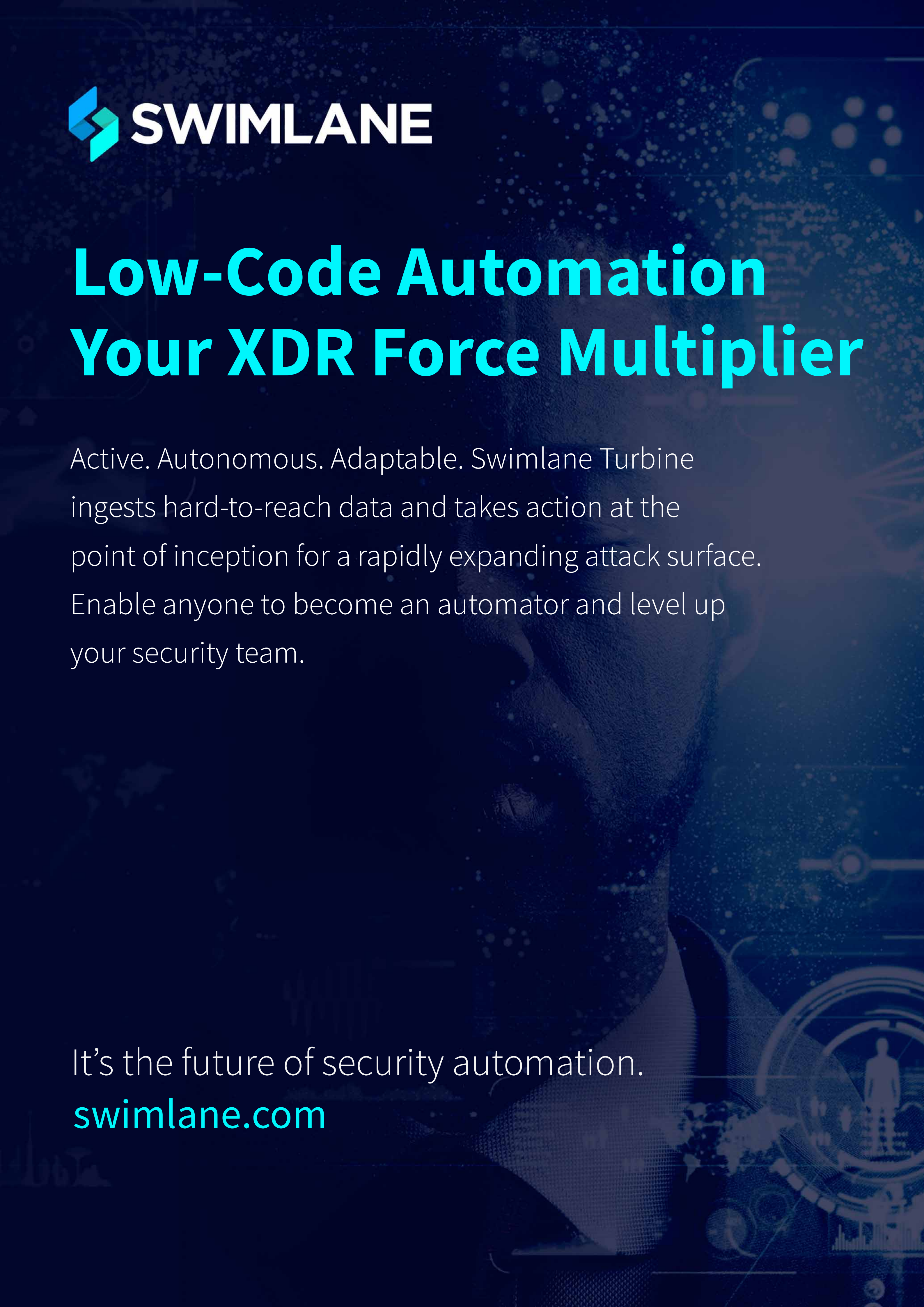
Automation adds value by keeping humans in the loop to make flexible, better business decisions – that's the true power of automation.

It's an exciting time for technology as we start to take advantage of automation across many different industries. However, remember that automation won't remove the need for people; automation enables people to build something even greater. □

Cody Cornell is Co-founder and CSO of Swimlane.

For more information, please visit **swimlane.com**

SWIMLANE



The cybersecurity paradigm shift: from cost centre to competitive differentiator

Why and how organisations should be seeing cybersecurity as more than just a cost centre, to unlock true return on investment.

Rob Demain reports

Historically, cybersecurity has been seen as a cost centre; something that can be reduced when times are tough and gets a budget proportionate to the (sometimes seemingly arbitrary) revenue and margin objectives at the start of the year.

It's understandable, given the nature of cybersecurity spend, often being seen as an insurance against **if** something were to happen, but recently, the best organisations have been able to elevate cybersecurity into a business enabler and source of competitive advantage.

This is a summary of a recent discussion with industry experts on this topic, a full write-up of which can be found at the bottom of this article.

Building a culture of cybersecurity within an organisation

Critical to any attempts to change internal perceptions of cybersecurity is the right culture. Building the foundations for a positive cybersecurity culture starts at the top of the organisation. Culture needs to start with the board building traits such as honesty and transparency into the organisation's core values. The board needs to champion and role-model those behaviours.

Creating a no-blame culture is also very important. If employees know that it is acceptable to make mistakes, as long as they report them quickly and effectively, organisations can solve problems as they arise. Cybersecurity is infinitely easier when people admit mistakes.

Conversations with the board

As cybersecurity has traditionally been seen as an IT issue, boards often lack the awareness and understanding required to make informed decisions. CISOs must talk to board members and give them the knowledge to make better decisions and protect themselves.

Most boards understand that cybersecurity plays a key part in the smooth operation of their business, but many CISOs struggle with what to measure and how to convey information to the board. The traditional risk matrix of likelihood versus impact can create additional noise and cause errors in the judgement process.

Rather than talking about the likelihood and impact of a cybersecurity breach on a company's reputation, engage the board by getting them to understand the risk of damage to what matters most to their organisation and develop metrics to show this. This may centre around data or even the risk of losing business strategy documents, reducing competitive advantage.

Once there is an acceptance of risk and action to mitigate it, the foundations are in place for organisations to make cybersecurity a business enabler.

Elevating cybersecurity into a source of competitive advantage

Being prepared for a cyber-attack is crucial. Reporting a breach promptly with accurate information will stand organisations in good stead to weather the storm. Consider the Maersk breach in 2017 – whilst operational damage and cost of response was huge ($300m), share price bounced back quickly due to their excellent communication and planning.

Customers, prospects and other stakeholders are all interested in how companies handle their cybersecurity. Openly talking about or even publishing your cyber-strategy demonstrates that an organisation takes security seriously and embeds it into everything they do.

In the best organisations, CISOs are now actively included in the bidding process, to help win new business. The beauty of this, is that it can even allow small organisations to 'punch above their weight' and compete with larger companies, simply by getting cybersecurity right.

Finally, boards need to recognise the opportunity that good cybersecurity presents to the business. The board needs to consider how the business can be the best at cybersecurity compared with competitors to innovate, provide products and services more quickly, enter new markets, and deliver value to customers more effectively. Seizing this opportunity is what will really make an organisation stand out against competitors. □

Rob Demain is the CEO and Founder of e2e-assure, a Security Operations Centre (SOC) and Managed Detection & Response (MDR) provider

For more information and to read the full white paper, please visit **e2e-assure.com/resources-cyber-as-competitive-advantage-whitepaper** e2e assure

Your trusted global SOC provider

ELEVATING CYBER SECURITY BEYOND A COST CENTRE.

API Spyder – providing the customer with complete visibility of their attack surface

A customer case study.

Cequence Security reports

One of the nation's largest mobile phone carriers with over 100 million wireless subscribers has been trying to get a complete understanding of its entire API footprint. API applications play a critical role in helping to support and manage their large nationwide network. The security team wanted to ensure that they had complete visibility into all APIs regardless of where they were deployed, to ensure that they had complete oversight and control.

The carrier's security team had been using Cequence's products API Sentinel and Bot Defense, part of our Unified API Protection solution, to protect their mission-critical API applications; however, the team was concerned if their existing count of APIs was accurate. The Cequence account team introduced them to our new offering, API Spyder, also part of our Unified API Protection solution to help them obtain a complete discovery of their entire API attack surface, including all APIs regardless of where the APIs were hosted.

The results

API Spyder provides the customer with complete visibility of their attack surface

After running API Spyder, the security team confirmed their assumption about the number of APIs. There were thousands of unmanaged APIs that existed that the team had no visibility into and therefore no control over. API Spyder crawled through their entire public-facing APIs regardless of where they were hosted, building out their entire API footprint.

With API Spyder the security team was able to discover the following:

- *Complete API footprint:* Obtain a complete API footprint of all API servers regardless of where they were hosted.
- *Automated discovery:* Through API Spyder, they avoided the manual process of discovering and maintaining a list of external-facing API servers. The process of maintaining a complete list of APIs was laborious, never-ending, incomplete, and error prone.
- *Continuous discovery:* API Spyder provided a dashboard that ensured that if a new API application were developed, they would be immediately notified, ensuring that it would be secured.

Goals

- Obtain a complete attack surface report of all API servers regardless of where they were hosted
- Discover if their understanding of the existing API server inventory was accurate
- Remediate any security issues on any API that could serve as a backdoor into their environment

What they achieved

- *Full API server discovery:* Discovered over 1,000 API servers that were not actively protected by any API security solution.
- *Non-production servers:* Discovered that over 18% of their overall servers were exposed to non-production servers with no API security enabled.
- *Log4J vulnerable servers:* Despite a rigorous patching programme, they had discovered that over five API applications with the Log4J vulnerability were not patched.
- *SSL issues:* Over 30% of their API servers had SSL security issues such as invalid or expired certificates, potentially enabling a MITM (man-in-the-middle) attack.
- *Exposed files:* They discovered over 107 files that could expose private keys that could be used to gain access to mission-critical business information. □

Get started with API Spyder by requesting a free 10-day trial at **apispyder.cequence.ai**

CEQUENCE SECURITY

CEQUENCE® SECURITY

Unified API Protection to Safeguard Your Organization

DISCOVER
your entire API attack surface area

DETECT
risks and threats hiding in plain sight

DEFEND
natively, in real time

Eliminate Shadow API Risk and Protect All APIs Against Attacks

Today's security teams simply lack the visibility and defense capabilities they need to protect the ever-growing risk from APIs and other application connections. Cequence Security, the leading provider of Unified API Protection, delivers the only solution that unifies API discovery, inventory, compliance and testing with proven, real-time native detection and prevention against ever-evolving API attacks. Cequence secures more than 6 billion API calls a day and protects more than 2 billion user accounts across our Fortune 500 customers. Our customers eliminate shadow API risk, and protect their entire API inventory from online fraud, business logic attacks, exploits and unintended data leakage while scaling quickly and cost effectively.

100+
Global Brands Protected

6B
Daily API Calls Secured

2B
User Accounts Protected

Request a FREE API Security Assessment Today!

www.cequence.ai/assessment

Why it is time to rethink how you are using digital forensics

Digital Forensics is a vital part of a mature cybersecurity stack but the field of digital forensics is more than 40 years old, and so are the methods.

Binalyze reports

As a consequence of this, chances are you are using digital forensics in a purely reactive, investigative manner to report on a breach after the event and create learnings for the next time. Forensics is capable of providing so much more value to the overall cybersecurity and incident response processes in large enterprises. Fortunately, there is a new breed of digital forensics solution emerging, which is changing the nature of forensics and unleashing a whole new set of valuable use cases and outcomes. This new category is called Enterprise Forensics.

Here are some of the ways Enterprise Forensics is disrupting and innovating to deliver faster containment and remediation of breaches and enhanced levels of resiliency.

Lightning fast

Is there a more critical component in the cybersecurity response than time? When a breach occurs every second counts and costs! Legacy forensic tools take many hours to acquire, and many more to parse, the necessary evidence needed to effectively investigate an attack.

Enterprise Forensic solutions are different, completing evidence acquisition and preparation in just a few minutes. This makes it possible to utilise full forensic-level visibility during a live incident response process for the first time.

Speed is also becoming an essential requirement for regulatory compliance in all major markets. Legislation that mandates a maximum reporting time of breaches is creating additional pressure on the incident response timelines and Enterprise Forensics is helping to alleviate this and ensure compliance is maintained.

Remote & scalable

Enterprise Forensic solutions solve the problem of using legacy desktop and hardware forensics tools, that often require a 1:1 analyst to asset usage model, by centralising the investigation process on a browser-based console in a secure on premise or private cloud environment.

Additionally, thanks to their web-native architecture, modern forensic solutions are completely scalable without adding additional time to the investigation. Investigating 1, 100 or 10000 assets concurrently from a central console with no degradation in performance delivers significant efficiency gains to the SOC team.

Integrated & automated

In a modern cybersecurity environment the ability to integrate different components of the security stack together and automate much of the process is becoming a core requirement. This helps to streamline and speed up processes while also reducing the pressure on the human resources, allowing them to focus on the high-value actions.

Enterprise Forensic solutions meet this requirement by integrating with systems such as SIEM, SOAR, EDR, Syslog etc. and allowing the automatic triggering of secondary forensic actions in response to their alerts. These solutions also incorporate scheduling, playbooks and auto actions to further automate digital forensics tasks.

Collaborative

Incident response and investigation is a team sport! With legacy forensic solutions it has been very challenging to share information at the case level and collaborate with colleagues.

Managing this process in a browser-based modern solution, which is consolidating a broad set of tools into a single platform, is allowing for real-time collaboration and delivering all of the time and efficiency gains that come with that.

AI-assisted

Digital forensics is powerful. Having access to full forensic visibility on an asset offers an unparalleled opportunity to understand the what, when, where, how and who of an attack. However, this level of visibility creates a lot of data that must be analysed and requires very specialist skills and experience to be done at speed.

Modern enterprise forensic tools address this issue by using AI to deliver assisted compromise assessment on forensic evidence acquisitions. This type of technology helps to guide the analyst to important IoC's buried in the forensic data quickly and with confidence. This is also helping to reduce the reliance on high-level analysts in a time of skills shortage in the cybersecurity industry.

Proactive

Finally, by changing the nature of digital forensics, Enterprise Forensics is opening up new proactive use cases that enable enterprises to leverage forensics at scale before an attack is initiated. It is widely accepted that blocking and monitoring security solutions can never be 100% effective and breaches will occur. Proactive forensics is leading the way in assisting security teams to find and identify the 'unknown unknowns' residing on their network through techniques such as baseline comparison and diffing. □

For more information,
please visit
www.binalyze.com

b!nalyze

e-Crime & Cybersecurity Mid-Year Summit 2022

19th October 2022 London

“ Insightful, relevant and thought provoking; no hard sells, sensible practical approaches to current day cybersecurity challenges. ”

Head of Information and Cyber Security, McArthurGlen Group

“ Thanks, very enjoyable. Look forward to my invitation to the March event. Thanks to everyone making this possible in these difficult times. I actually spent the whole day on it! ”

Director of Global Security, American Express

“ Thank you for the update and the invitation to join yesterday’s session. I found the conference to be very informative (as always) and covered the threat landscape in a timely manner. The presenters were excellent and the introduction/continuity was executed to perfection. The content was superb [...]Thank you for the invitation again and I hope to catch up with you in person at the March 2022 event. ”

Information Security, AIB Group Technology Services

“ It’s been a wonderful experience to attend this virtual conference. Many thanks for organising the event. ”

Information Security Officer/ Data Protection Manager, Jein Solicitors

2021 sponsors included:

Principal Sponsor

F-Secure.

Strategic Sponsors

BeyondTrust

DARKTRACE

MENLO SECURITY

okta

proofpoint.

Recorded Future®

SentinelOne™

Education Seminar Sponsors

appgate

axis security

bitglass

corelight

CybelAngel

CyGlass by NOMINET

DEVO

CISCO. KENNA Security

onelogin

PICUS

RANGEFORCE

RED SIFT

For more information, please visit
akjassociates.com/contact-us

Thank you to all our sponsors

Strategic Sponsors

BEYOND IDENTITY

BeyondTrust

BlackBerry

DARKTRACE

MENLO SECURITY

OneTrust
PRIVACY, SECURITY & GOVERNANCE

SEARCHLIGHT Security

Education Seminar Sponsors

b!nalyze

CEQUENCE SECURITY

COFENSE

Counter Craft

digital element
Location is Elemental ™

e2e assure

egress

FIREMON

Kocho

OBSIDIAN

SWIMLANE

Networking Sponsor

Reveal security

Branding Sponsors

Balbix

TESSIAN