e-crime & cybersecurity CONGRESS

2nd and 3rd March 2022
London

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Safeguarding the digital citizen, securing the metaverse

Forthcoming events

e-crime & cybersecurity CONGRESS

7th March 2022
Dubai

e-crime & cybersecurity FRANCE

5th April 2022
Paris

e-crime & cybersecurity NORDICS

24th May 2022
Stockholm

e-crime & cybersecurity GERMANY

2nd June 2022
Munich

e-crime & cybersecurity CONGRESS

7th June 2022
Doha

SECURING THE LAW FIRM

6th July 2022
London

SECURING FINANCIAL SERVICES

6th July 2022
London

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 SCOTLAND

9th November 2022
Edinburgh

e-crime & cybersecurity SPAIN

16th November 2022
Madrid

e-crime & cybersecurity BENELUX

8th December 2022
Amsterdam

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

Dear delegate,

It is great to be welcoming you back to a physical version of the e-Crime Congress, particularly as this is our 20th anniversary.

Twenty years ago, a handful of far-sighted individuals in government, law enforcement and the private sector got together to launch the first e-Crime Congress. That year, Microsoft released Internet Explorer 6.0; Apple introduced macOS X 10.1, the iPod and Apple earbuds; and Bungie released the game Halo for the newly launched Xbox gaming system.

More significantly for those watching the emerging world of digital threats, a new infection technique appeared: users no longer needed to download files – visiting an infected website was enough as bad actors replaced clean pages with infected ones or 'hid' malware on legitimate webpages. Instant messaging services also began to get attacked, and worms designed to propagate via IRC (Internet Chat Relay) channel also arrived.

Twenty years on and how different the world looks: mobile, IoT, VR/AR, the car-as-API-wallet, the DLT-based tokenisation of everything from currencies to funds to real estate – the digitalisation of everything everywhere. And cybercriminals are exploiting this new world ever more cleverly and ruthlessly.

As ever, the e-Crime Congress will be trying to make sense of the latest developments in both offence and defence. A roster of some of the most respected names in the sector will deliver a mix of real-life case studies and in-depth technical sessions to help you drive your cybersecurity efforts forward.

Please take this opportunity to network with your peers in the networking area, mingle with solution providers and swap war stories. We hope you enjoy the event, please do visit our team at the registration desk if you have any questions! And thank you for coming.

Simon Brady | Event Chair

@eCrime_Congress **#ecrimecongress**

2nd and 3rd March 2022

Park Plaza Victoria London, UK

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

Introducing SenseOn

Helping stretched security and IT teams defeat threats with self-driving cyber-defence.

For security professionals and their employers alike, stopping cyber-attacks has never been more important or more challenging. On one side of the security equation, distributed digital estates are getting harder to delineate and defend. On the other, advanced threats like targeted ransomware are now available on subscription models, and the rise of cryptocurrencies has made monetising illicit network access regrettably easy. As a result, business-critical threats are everywhere and, in today's environment, threat actors have an almost infinite number of ways to deploy attacks within victim networks.

Unfortunately, the typical cybersecurity tool stack deployed by most organisations to counter these challenges is dangerously siloed and noisy. While many solutions are highly effective in identifying singular threats in particular areas, this can be cold comfort for defenders tasked with maintaining a holistic picture of their organisation's security posture.

Paradoxically, deploying more layers of disparate point solutions like AV, endpoint protection, and NDR decreases visibility, making it easy to miss fundamental security gaps and straining overstretched analysts even further.

In response, some organisations have invested in implementing SIEM software to try and give teams a single pane of glass insight into their estates. However, the volume of data typically sent into a SIEM only adds to security challenges because analysts and engineers have to spend their time trying to make sense of it.

With lean security teams bombarded with hundreds of meaningless, unconnected alerts, it is unsurprising that over 79% of SOC analysts find themselves overwhelmed by the task of managing their security solutions. At the same time, the tiny percentage of network traffic that is malicious ends up ignored, and real threats easily slip through intricate security nets.

Multiple senses in one solution

SenseOn's mission is to break this status quo and make organisations safer by liberating security teams from the curse of siloed solutions and meaningless data.

To replace the need for a suite of disparate tools, SenseOn has developed a Universal Sensor. A first in cybersecurity, this is a single piece of low-impact software deployed across an organisation's devices, servers, databases, and cloud environments. Making complex security stacks redundant, our Universal Sensor captures a rich picture of users, devices, processes and network telemetry, all the way down to deep packet inspection.

Capturing network telemetry from endpoints and servers, this capability allows SenseOn to give security and IT teams granular visibility into their entire estate – a critical asset in the modern IT environment. Also, in contrast to solutions that take careful calibration and disruptive setups, deploying SenseOn is extremely straightforward. Our solution immediately gets to work, gaining an understanding of how an organisation's digital estate works over time.

Automated investigation and response through AI Triangulation

While SenseOn's Universal Sensor eliminates the need for multiple tools, our groundbreaking AI engine, which we call 'AI Triangulation', removes stress and prevents IT team burnout by dramatically reducing the time needed for analysis.

Designed to augment security staff by acting like another team member, our AI Triangulation mimics the thought process a human analyst would use to automate routine analysis.

This means that SenseOn takes a staged approach to any potential alerts before bringing them to human attention, critically examining each to filter out the noise that typically plagues analysts. This process starts each time SenseOn detects something of interest, like unusual login activity. Noting it as an observation, SenseOn's AI Triangulation will automatically run over analysis using data from multiple sources on that observation in isolation and in conjunction with all other observations and data points.

In instances where SenseOn concludes that an observation is 'otherwise normal', it will not surface as an analyst alert. Instead, it will keep it logged as an observation that a security team can revert back to. By taking this approach, SenseOn filters out false positive alerts and only raises genuine threats in the form of what we call 'Cases'. These Cases are then either automatically remediated or flagged for further investigation.

When SenseOn needs to bring a threat Case to the attention of a human analyst, our solution provides all the necessary information and context on one dashboard. This allows security staff to immediately assess the impact and severity of the Case and its root cause. In doing so, SenseOn gives analysts a rich

SenseOn reports

Figure1: Automated investigations that are easy to understand

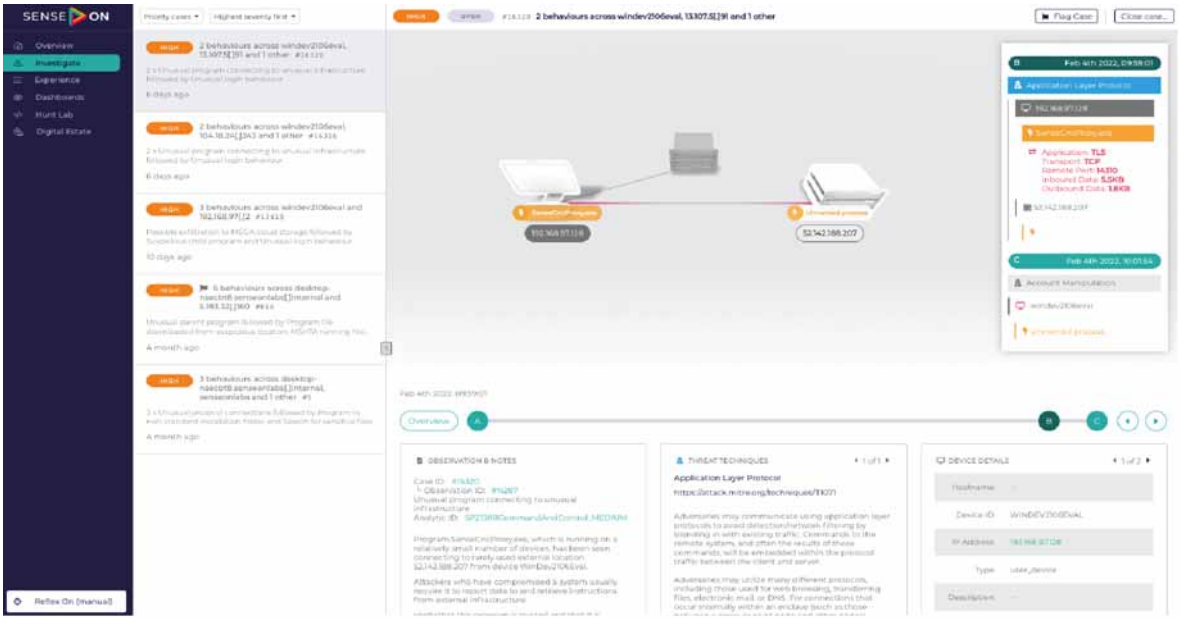
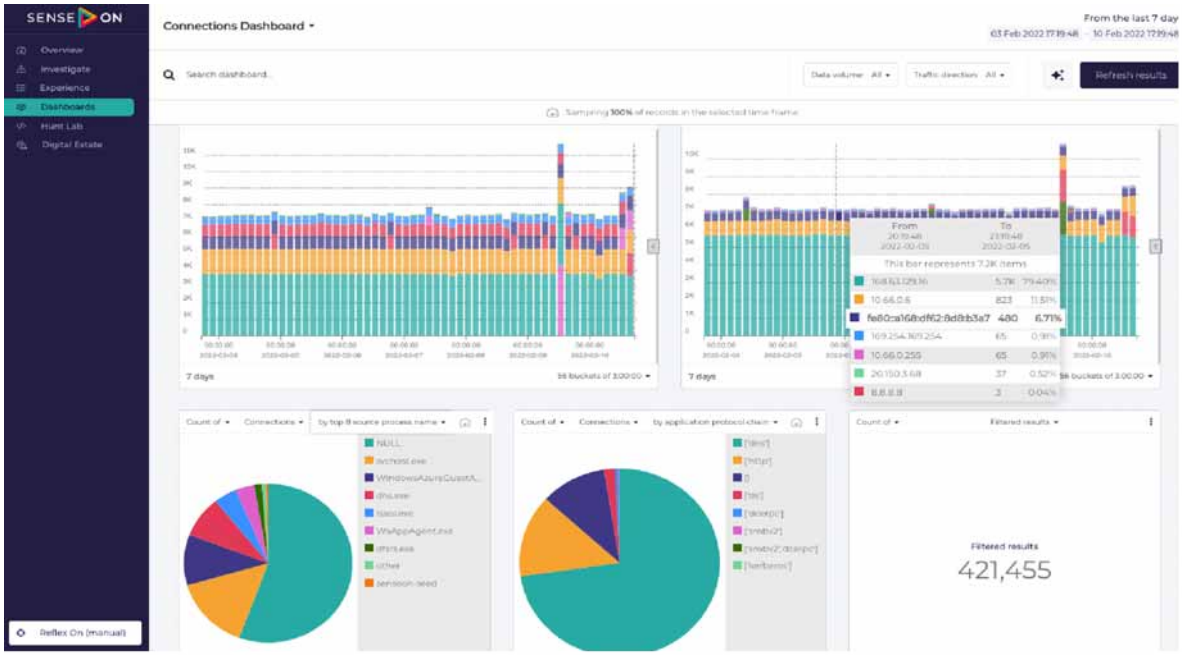


Figure 2: Comprehensive data to enable threat hunting at enterprise scale.



timeline of all of its observations, along with a simple description of the threat techniques detected, each mapped to the MITRE ATT&CK framework with a link for further reading. For an organisation that deploys 20,000 devices, this capability means that each analyst only has to spend 41 minutes per day reviewing all the recommended Cases.

To remove the uncertainty that typically comes from trying to stitch this data together from multiple tools, SenseOn also presents analysts with all of the host level information they need, including users, devices, and processes alongside all network activity. As a result, analysts can immediately see which assets are impacted and the steps required to resolve the threat.

More with less

Customers in areas ranging from manufacturing to financial services already use SenseOn to improve visibility and dramatically reduce security teams' workload without comprising defence. Because SenseOn immediately adds capacity to IT teams, it allows organisations to consolidate their security tooling and completely remove dependencies on outsourced MSSP/SIEM services without increasing their headcount internally. □

For more information, please visit
www.senseon.io

SENSE ON

PROTECTION FOR EVERYONE

SenseOn triangulates data from three different sources then uses AI to prioritise threats – exactly the way a human analyst would. Which means you get fewer false positives, freeing up resource to focus on what really matters.

SENSEON
ON A MISSION

NETACEA

25% of enterprises are losing $250 million to bots every year

We protect your websites, mobile apps and APIs with industry leading sophisticated bot management

Rapid

Quickly detect, respond and mitigate attacks

Accurate

Understand intent and prioritise genuine users

Transparent

Empower your teams with actionable threat intelligence

Find out what bots are costing your business with Netacea's free bot calculator

Netacea @Netacea_AI www.netacea.com hello@netacea.com

Bad bots 101: Dissecting a credential stuffing attack

Malicious bot attacks are becoming ever more frequent, and high profile.

Businesses today are increasingly turning to automation in their efforts to improve efficiency and profitability. The same is also true for cybercriminals. Malicious bot attacks are becoming ever more frequent, and high profile. Since 2020, we have seen a slew of scalper bot attacks hit the headlines, as adversaries target in-demand items such as the PlayStation 5 and even Covid-19 vaccine appointments.

But scalpers are not the only bot threats that should give businesses pause for thought. According to our research, nearly half (46%) of enterprise organisations experienced a credential stuffing attack in 2020.

It's as easy as 1, 2, 3

Credential stuffing is a technique used by adversaries to gain unauthorised access to legitimate user accounts. It doesn't require an abundance of skill or knowledge to carry out a credential stuffing attack, and everything you need is readily accessible. As long as you know where to look.

Unlike credential cracking, the other notable technique used for account takeover attacks, credential stuffing does not involve guessing usernames or passwords. Instead, adversaries inject previously leaked username and password combinations, or combos, into the login page of their target website. These combos do not need to have been leaked from the website being targeted.

Step 1: Source your data

The first step for the adversary is to obtain a combo-list, a set of combos from a previous, often unrelated, data breach. This is trivial. Dumps from previous data breaches are readily available, on both the clear and the dark web, for free or a nominal fee. Some of these contain millions of unique combos. All too often, a new data breach makes the headlines, and the repositories grow.

Step 2: Find the perfect match

Next adversaries validate these combos by submitting login requests at scale against target webservices using automated tools, or bots. One popular tool used for this is OpenBullet, an open-source automation suite freely available on GitHub. It allows adversaries to import combo-lists and automate authentication attempts, which can be routed through proxies to defeat basic IP based protection. These proxies are not included with OpenBullet but can easily be purchased by adversaries. Proxies that route connections through clean residential IP addresses are less likely to be blocked by organisations and therefore command a higher price than data centre proxies, but neither are prohibitively priced. A configuration file, or config, defining how OpenBullet will interact with the target website's authentication processes, is also needed for each website being targeted. As a result, an underground market has grown for config trading and some configs are even available for free.

Step 3: Start making money

Once an adversary has successfully validated a set of credentials, they have many options to monetise them, depending on the type of account targeted. These include:

- Transferring or withdrawing money from banking and fintech accounts,
- Making purchases from online shopping accounts, or
- Reselling accounts for subscription services, for example streaming sites, at discount rates.

Adversaries can also scrape personal identifiable information from accounts to use as a launchpad for other fraudulent activity.

Why are credential stuffing attacks a threat to businesses?

The success of these attacks comes down to a simple question: What are the chances that a known username and password combination has been reused elsewhere? With millions of unique combos easily accessible, the scales are tipped in the adversaries' favour. Even a 0.1% success rate could mean access to thousands of accounts.

The question can be simplified further. Since email addresses have become the de facto username for most webservices, it really becomes a question about password reuse. And unfortunately for organisations, people do not have the best track record when it comes to password hygiene. Studies in recent years by the likes of Google have measured password reuse at rates upwards of 65%. This is understandable – people have far too many online accounts to remember unique passwords for them

Netacea reports

all, so they fall back to using familiar passwords. More worryingly, according to LastPass' 2021 report on the Psychology of Passwords, 45% of survey respondents had not changed their passwords in the past year – even following a breach.

With minimal investment required, easily accessible tools, an ever-increasing pool of leaked credentials and multiple avenues for monetisation, it is no surprise that credential stuffing is such a popular attack.

This is unlikely to stop soon. Recent developments, such as the rollout of open banking, have increased the attack surface for adversaries, who can attack financial services organisations by targeting third parties and APIs. We found that on average, financial services organisations had 4.9% of their customer accounts breached due to credential stuffing attacks.

Successful attacks can have a severe impact on both the organisation and its customers. Customers whose accounts are breached can find themselves locked out of said accounts, charged for purchases they did not make, or targeted for further identity theft as their personal data is sold on. Whilst chargebacks or refunds provide mechanisms for customers to recover their financial losses, these do not compensate for their distress, or the time and effort they expend.

For organisations, conversely, there are costs incurred processing and paying out said chargebacks and refund requests. Customer trust and loyalty, vitally important assets for businesses operating in the digital economy, will also likely be irreversibly damaged. We found 76% of organisations had seen a reduction in customer satisfaction following a credential stuffing attack, and 83% had lost customers or business to competitors. There are also regulatory implications for organisations, who could find themselves liable to fines under data protection legislation for failing their duty to protect their customer's personal information.

Our research indicates that on average, organisations lose 3.7% of their annual online revenue to credential stuffing attacks – this equates to at least $250 million every year for the top quarter of targeted businesses.

Addressing the root cause, peoples' tendency to reuse passwords, is not a practical solution as it requires effecting large-scale cultural change.

How to prevent credential stuffing attacks

Many organisations rely on IP blocking and CAPTCHAs, and whilst these have their merits, they are insufficient in as of themselves. IP blocking or limiting may hamper unsophisticated attacks but is easily defeated by residential proxies. CAPTCHAs increase the cost factor for adversaries, who in turn farm the challenges out to specialist CAPTCHA solving services, but also frustrate legitimate customers.

True multi-factor authentication (MFA), where the validity of the username and password is not confirmed separately to the additional factor, provides strong protection. It not only prevents the adversary from accessing the account without additional verification but has the added benefit of providing no further information to the adversary about the existence of the account. This reduces their ability to resell validated credentials for a profit or orchestrate targeted social engineering campaigns against the account. However, as with CAPTCHAs, MFA can also add friction to the customer journey and may not be feasible for all organisations.

And herein lies the challenge for organisations – securing accounts without impacting the customer. Can you differentiate between human and bot behaviour in real time, so that legitimate customers do not have to jump over the same hurdles as bots do? Client-side device validation scripts attempt to do this but are vulnerable to being studied and circumvented by adversaries.

Netacea takes a different approach. We understand bot behaviour better than anyone else, thanks to our pioneering server-side approach to detection and mitigation.

Our approach guarantees quick and easy implementation of our technology and enables us to support a wide range of integrations. This ensures comprehensive coverage against malicious bots across your website, mobile apps and APIs, without detriment to your website infrastructure, reliance on hardware or disruptive code changes.

We quickly distinguish automated bots from humans to prioritise genuine users, with our team of experts and revolutionary, machine learning powered Intent Analytics™ engine at the heart of the solution. Netacea works hands-in-hand with your in-house security functions from implementation, through to providing accurate detection and empowering you with actionable threat intelligence.

The odds have been in the cybercriminals' favour for too long. It's time to tip the scales. □

Next-level customer experiences are built on digital trust

What consumers expect from businesses that sell products and deliver services online is radically different today than it was even one or two short years ago.

Joe Diamond reports

When pandemic-related shutdowns forced employers to embrace remote work, educators to adapt to distance learning, and shoppers to turn to digital channels, we *all* learned that we're more flexible than we'd previously thought. We also learned that our world is ready to capitalise on the benefits of technology-driven transformation

Today's consumers are spending more time and money in the digital space, and they're more comfortable sharing their personal data with public and private sector organisations. As our research reveals, they're also more cognisant of the value of that data.

As a result, people are now more likely to think that the companies they buy from have a strong responsibility to protect the customer information that's shared with them. Increasingly, doing business online is an act of trust.

To earn and retain that trust, organisations must do three things well. One is to provide the seamless, convenient digital experiences that consumers are always looking for when they turn to digital platforms and services. Another is to put robust security in place to ensure that the data with which they've been entrusted isn't vulnerable to compromise or theft. The third is to respect customers' privacy: according to Gartner, 65% of the world's population will have its personal data covered by privacy regulations by 2023, a rapid increase that reflects growing insistence that businesses handle customer data responsibly and ethically.

The key to modern digital business success lies at the intersection of customer experience (CX), privacy and security. And it's absolutely essential to get all three of these things right: over-emphasising any one part of the triad at the expense of the others will mean that you won't be able to satisfy consumer expectations in today's world. Security protections must be present, but they shouldn't be onerous, and they shouldn't make it harder for customers to complete their transaction or interact with your organisation.

How can you create these kinds of seamless, friction-free digital experiences? What does your organisation need to do in order to promote customer loyalty and earn trust?

Identity is the key to the modern customer journey

The modern customer journey is built on a technology backbone that facilitates interoperability and the seamless sharing of data between traditionally disparate business units and development teams. A secure identity solution enables all of these capabilities, forming the foundations of digital trust.

Every digital customer journey begins with sign-up. Sign-up should be frictionless, and the information gathered from the customer should be used to provide a 360° view of that individual user – a unified view that can serve as a single source of truth across all platforms and touchpoints in the modern omnichannel ecosystem, allowing you to tailor the experience to that customer's preferences and give them exactly what they're looking for. At the same time, security and privacy should be front-and-centre throughout the entirety of the customer journey, with risk-based detection used to secure logins and transactions, and consent and privacy requests handled automatically and centrally.

Identity underpins every aspect of this digital customer journey. When a secure identity service is fully integrated into your technology ecosystem, it provides core functionalities that stakeholders across the business need – from digital and product teams to marketers, and from DevOps practitioners to IT and security professionals. And it ensures that you're able to deliver the security, privacy and CX that today's consumers demand.

The 4 pillars of digital trust

When people shop or consume services online, they do so primarily because they're looking for ease and convenience. Being able to provide that ease and convenience – and doing so consistently and efficiently across an increasingly complex technology landscape – is what enables leading brands to earn and retain the trust of today's consumers.

Having a secure identity service positions an organisation to win market share, unlock competitive advantage and boost its ability to innovate. It does so by supplying four core capabilities that make it possible to give your customers the trustworthy experiences they crave with the real-world resources that you have on hand.

You can earn the trust of your customers by providing consistent, reliable login experiences that extend strong user authentication across all of your digital properties, no matter what devices are being used.

These pillars are:

- *Frictionless experiences.* You can earn the trust of your customers by providing consistent, reliable login experiences that extend strong user authentication across all of your digital properties, no matter what devices are being used. By making registration and authentication simple, you save time and remove roadblocks for your users. With adaptive, context-aware access policies, you can reduce friction for users leveraging single sign-on (SSO) or using known devices, while stepping up requests for additional assurance factors when more risk is present.
- *Robust, modern security.* Protect your customers – and their valuable data – across the entirety of the identity lifecycle for all of your apps. Secure accounts at registration and authentication as well as during in-app activities to prevent breaches, mitigate fraud risk and meet compliance requirements. When customers are able to interact with your business online without the worry of identity threats, you'll earn their trust throughout the entire customer journey.
- *Centralised management.* Centralising access management company-wide empowers your IT and security teams to work more efficiently by providing enhanced visibility and control across the extended enterprise. This allows you to bring user profiles from multiple identity sources together in one place, which serves as a single source of truth for the entire organisation. It's a place where policies can be enforced, passwords and user attributes managed, and monitoring and reporting capabilities maintained – and where you can automate a full complement of identity-centric workflows. In turn, this speeds ROI and decreases total cost of ownership.
- *Speed-to-market.* In today's fast-moving digital business ecosystem, a secure identity service that enhances efficiency can also unlock your ability to innovate. Customers expect modern digital businesses to deliver new features and services at an accelerating pace. Integrating the right identity solutions into your technology environment will free your development teams to focus on your core business, so that they can work more efficiently, maximise productivity, and meet project timelines.

Nowadays, identity touches on nearly every aspect of the customer journey. To reduce friction while enabling the right access to the right resources at the right time, you need to integrate data and insights from the entirety of your technology ecosystem. This includes everything from business, marketing and customer relationship management (CRM) tools to security and fraud prevention solutions all the way through the components in your DevOps toolchain.

At the heart of digital trust is consistent, top-notch customer experience. Being able to deliver this requires extensive pre-built integrations. It also demands low code, no code and pro code development options to suit the needs of diverse teams.

Want to learn more about how Okta Customer Identity solutions are helping organisations cultivate digital trust in the real world?

We're leading the way with a secure customer identity & access management solution that more than 14,000 customers trust to help them deliver digital customer and workforce experiences that stand out from the crowd. You can also download our new report, Identity: The Digital Trust Accelerator, to explore more of our research findings. □

Joe Diamond is Vice President, Product Marketing at Okta. As the Vice President of Product Marketing, Joe Diamond is responsible for all things go-to-market strategy for both Workforce and Customer Identity. His team's charter includes product marketing, solution marketing, technical marketing, pricing and competitive intelligence.

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

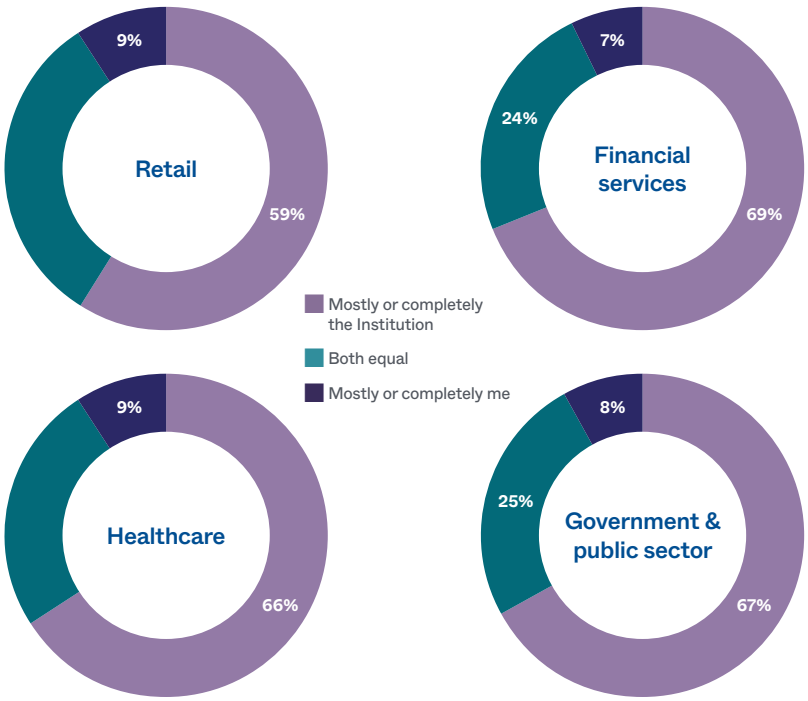
okta

Build trusted digital experiences with Okta

Customers hold you responsible for their personal data.

Find out how building trusted digital experiences can meet their expectations.

‘Identity. The Digital Trust Accelerator’ at **okta.com/uk/digitaltrust**



illumio

Stop Ransomware. Isolate Cyberattacks. Reduce Risk.

Segment in minutes on your path to Zero Trust.

Real-time visibility and Zero Trust segmentation from Illumio allow you to see and secure your most important data and applications across clouds, containers, data centers and endpoints.

90%
Simpler
Eliminate manual network segmentation

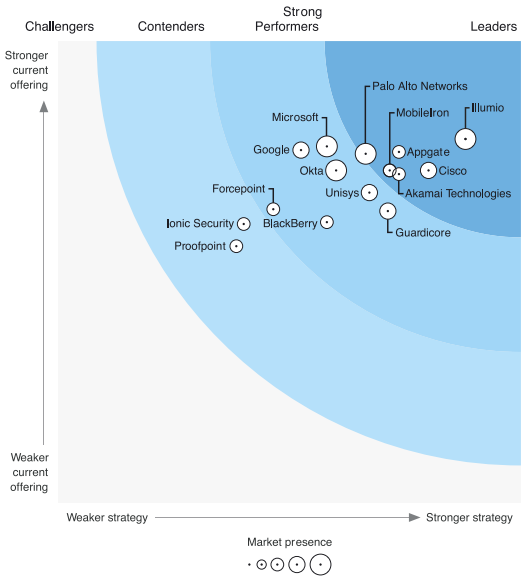
5x
Faster
Segment at the speed of business

100%
Confidence
Reduce risk and increase uptime

FORRESTER®

Illumio named a Leader in The Forrester Wave™ for Zero Trust

Highest scores in three primary categories: current offering, strategy and market presence.



Learn more at illumio.com

Our top 5 segmentation tips for a more secure organisation

Five tips to limit damage from ransomware and other cyber-attacks.

Raghu Nandakumara reports

At Illumio, we believe that Zero Trust segmentation is foundational to helping organisations become more secure. The better an organisation is at isolating and protecting its key assets from infiltration, the safer it will be. This post provides five tips for better protecting organisations to limit damage from ransomware and other cyber-attacks.

CYBERSECURITY IS STILL LAGGING BEHIND

Gartner forecasted that $150 billion will be spent on cyber and risk management in 2021, up from around $134 billion in the previous year. Yet breaches are still happening on a massive scale. By September 2021, the number of reported data breaches in the United States had already surpassed the entire 2020 figure. Ransomware is an increasingly major driver, costing some organisations tens of millions of dollars in damages.

Currently, it takes an average of 287 days to identify and contain a data breach. Clearly, cybersecurity is not yet good enough to ensure organisations can identify their risks and have the means to contain any attack.

To improve their chances of successful prevention, detection and response, security executives must adopt an offensive approach when designing security controls. Start from the assumption that the organisation has been breached, then think about how an attacker would propagate an attack.

Lateral movement is often one of the key methods for propagation. Gaining visibility into this traffic and enforcing segmentation are security best practices to limit an attacker's reach and drastically reduce the impact of a breach. Here's how to get started.

1. Identify your most valuable digital assets

Applications are the number one growth driver of modern organisations. So, the first step in any Zero Trust segmentation strategy must be to identify the most important applications, and then map how applications and workloads interact and interconnect in the data centre or cloud.

To improve their chances of successful prevention, detection and response, security executives must adopt an offensive approach when designing security controls.

From here, you'll be able to build out the solution by setting policies that only allow trusted communications between those applications. That means, if an attacker gains access to the network and tries to move laterally to exploit those 'crown jewel' assets, it will be stopped in its tracks.

2. Consult the right experts

While Zero Trust segmentation is an essential capability when pursuing best practice cybersecurity, it is crucial that key stakeholders, such as application owners, understand its importance and value – after all, it is their applications that will be benefiting from the protection segmentation provides.

Segmentation is a team sport. The best teams are those that involve:

1. An expert on the application (they know their application and its associated dependencies the best)
2. Someone from the infrastructure team who understands core services
3. A security consultant who can guide on best practice

There may be others who wish to be involved. But these three roles, armed with the right tools and mandate to adopt segmentation, are critical to making the effort a success.

3. More context leads to better decisions

Imagine randomly finding a train ticket lying on the ground that only tells you that the ticket is for a journey from station X to station Y at date and time Z. You know that someone attempted that journey – in fact, all you know is that they bought a ticket for that journey. But you don't know who made the journey, why they made it, or where it originated. The train ticket on its own, without the additional contextual data, is of limited value.

Traffic data from the network is similar to that train ticket: it is useful but, without context, has limited value. And if you're trying to make decisions around protecting your applications, having such little context makes it challenging to work with and to make progress.

Zero Trust segmentation is not a silver bullet. There's no such thing in security. But as a key enabler of defence-in-depth and mitigator of breach incidents, it's increasingly regarded as a best practice foundation for risk-based security.

For this reason, enriching traffic data with context about the workloads involved – e.g., role performed, application serviced, and hosting location – helps you understand the flows more clearly. Instead of now seeing individual flows between specific workloads, you can look at relationships between groups of workloads that share a specific context. So, rather than talking about Server A talking to Server B, you can instead discuss the Web Server in the Payments App talking to the Database in the Clearing App – and that makes the flow much easier to decipher. The app owner (on your team of experts) can use that context to determine whether it is a relevant relationship. The security reviewer can quickly determine what security controls are appropriate.

And the source of context could be anything that is a source of truth in that organisation – it could be a dedicated configuration management database (CMDB) solution, tags from an IaaS platform, or even a CSV file. As long as it's a trusted source, it doesn't matter how that data is stored.

And if this context can be used to understand flows, it can also be used to build policies.

4. Be strategic and don't boil the ocean

To stand the best chance of success with a multi-year, all-encompassing project like Zero Trust segmentation, prioritisation is important. Business buy-in is essential for long-term success, so start small and gain early wins to get executives and users on board for later phases.

Start with your most valuable assets or crown jewels. Critical applications with an immediate need for internal or external audit are a particularly good place to start. Also consider applications with a business need for ongoing change, like a new version or feature deployment.

The intention here is to show continuous, real progress in improving the protection of applications, thus reducing the cyber-risk to the business.

Also, the process should be adaptive. Learnings from each step or milestone should help you improve the process as you go.

5. Make time for sustainment

Once you have a visible topology of workload and application communications and segmented protections in place, you've finally reached operational mode. Congratulations! Yet, it's still not time to put your feet up. A segmentation deployment requires continual fine-tuning to sustain all the time, money and effort placed into it.

The bottom line is that Zero Trust segmentation is not a silver bullet. There's no such thing in security. But as a key enabler of defence-in-depth and mitigator of breach incidents, it's increasingly regarded as a best practice foundation for risk-based security. □

Raghu Nandakumara is Head of Industry Solutions at Illumio.

To learn more about each of these tips, check out our ebook, Secure Beyond Breach: **www.illumio.com/resource-center/guide-secure-beyond-breach]**

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

The who, what and why of Highly Evasive Adaptive Threats (HEAT)

In dealing with HEAT, prevention is the best policy.

Jonathan Lee reports

One of the single greatest problems in security today is the continued reliance on legacy solutions.

Old methods rarely solve modern problems. As cybercrime has continued to advance and evolve, the security practices adopted by firms have all too often either progressed at a crawl or completely stood still.

It is therefore of little surprise that we continue to see weekly headlines of new attacks ravaging global businesses, government agencies, and individuals globally. Mindsets remain cemented in detection and response – and criminals know this.

Take ransomware, for example. The fastest growing kind of cyber-attack, the US Department of Justice revealed that there have been 4,000 such attacks daily in the US since 2016. The pandemic has only served to pour gasoline onto the already raging ransomware fire.

Indeed, analysis from the Washington Post reveals that ransomware attacks doubled year on year in 2020, owing to the mass transition of business models – data, users and applications – to the cloud. This shift made the browser the primary place of work to enable the continuance of operations on a remote basis during lockdowns. Yet when it comes to the cloud, those same on-prem security measures that are still heavily relied upon today are no longer adequate.

What is HEAT?

To capitalise on this new landscape, threat actors are targeting web browsers with a category of threats, known as Highly Evasive Adaptive Threats (HEAT).

HEAT attacks make web browsers the primary attack vector, deploying various methods to evade multiple layers of detection in legacy security stacks. This enables them to bypass traditional web security protection, and leverage the standard capabilities of modern web browsers to deliver malware or compromise credentials.

HEAT are unfortunately real and growing threats. When analysing approximately half a million malicious URLs, the Menlo Labs research team found that 69% leveraged HEAT tactics, while also observing a 224% increase in HEAT attacks during the latter half of 2021.

Given that many employees now spend three-quarters of their working day using a web browser, it is an obvious avenue to target. Indeed, HEAT attacks are being used very effectively by a number of renowned organised cybercriminal gangs.

One recent example was the Astaroth banking Trojan, which made use of HTML smuggling to sneak malicious payloads past network-based detection solutions. Meanwhile, the Gootloader campaign leveraged SEO poisoning to generate high-level page rankings for compromised websites, while Nobelium, the Russian state-sanctioned outfit behind the SolarWinds supply chain attack in 2020, is another known HEAT adopter.

Infection vectors: The four characteristics of HEAT attacks

HEAT attacks typically will leverage one or more of four evasive techniques capable of bypassing legacy network security defences:

1. **Evade static and dynamic content inspection**

To bypass static and dynamic content inspection engines, HTML smuggling and/or JavaScript trickery is often executed inside the browser session to deliver malicious payloads to endpoints. In doing so, the malicious file is dynamically constructed at the browser with no request for a remote file that can be inspected, bypassing various firewalls and network security solutions. Equally, file types assumed to be blocked by Secure Web Gateway (SWG) policies can still make it to endpoints without any user interaction.

2. **Evade malicious link analysis**

Malicious links, meanwhile, are often sent to users via communication mediums outside of email – think social media, SMS, shared documents, and more – with the intention of stealing corporate credentials to deliver malware to corporate endpoints. When these methods are combined with HTML smuggling, a sandbox that analyses files and content being downloaded is blind to the potential risk – it does not see the dynamic generation of a file within the browser once it is past the network security control point.

3. **Offline categorisation and threat detection**

HEAT attacks can also use benign websites to dodge URL categorisation. We refer to these as 'Good2Bad' websites – once activated they serve malicious

SASE is highly capable in managing HEAT as it ensures security is built around users, key applications and company data at the edge by converging connectivity and security stacks.

content for brief periods before reverting back to a benign state later. Between 2019 and 2021, Menlo Labs witnessed a 958% increase in the use of Good2Bad sites, with the recent critical Internet zero day attack discovered in Log4j likely to exacerbate this growing challenge further.

4. Evade HTTP traffic inspection

HTTP traffic inspection begins with the use of malicious content, such as browser exploits, crypto-mining code, phishing kit code, and images impersonating trusted brand logos that can be generated using JavaScript in the browser by its rendering engine, once the initial page load is complete. In essence, this makes any detection technique prior to the web page execution or rendering useless. Such HEAT attacks avoid detection from static signatures that examine web page source code and HTTP traffic.

The need for Zero Trust and SASE

Be it file inspections performed by SWG anti-virus engines and sandboxes, network and HTTP-level inspections, malicious link analysis, offline domain analysis, or indicator of compromise (IOC) feeds, many legacy defences are rendered near useless when confronted with these evasive techniques.

A significant part of the challenge lies in the fact that HEAT characteristics equally have genuine uses. Therefore, they cannot simply be blocked at the function level – rather, they need to be prevented.

To achieve this, a mindset shift and updated security posture is required. Trying to overcome the challenges of web security with endpoint security creates a square peg in a round hole scenario – it simply does not guarantee protection.

Critically, endpoint security only detects a threat once it is written to the file system, at which point your network will likely have been compromised already. Further, it is not able to protect unmanaged devices, while also harbouring a high chance of inundating the security operations centre (SOC) with too many alerts.

In dealing with HEAT, prevention is the best policy. Not only can it help to alleviate pressures on endpoints, but it can also make the already tricky lives of SOC teams much easier, creating a more sustainable environment of investigation, escalation and resolution.

This shift needs to begin with a thorough review of an existing security posture. Those that still remain built around a central policy pillar of detection and response will need to be updated, adapted and enhanced so that they are fit for purpose in the modern working environment. Namely, they must lead with prevention.

Here, we recommend a Zero Trust approach, backed by the Secure Access Service Edge (SASE) framework, featuring key security technology components that cater to today's remote and hybrid workforces.

SASE is highly capable in managing HEAT as it ensures security is built around users, key applications and company data at the edge by converging connectivity and security stacks. No longer are security stacks on the outside looking in – they are instead ingrained and integrated within the cloud.

By creating the perfect cocktail of SASE and Zero Trust, all content becomes a potential suspect, leaving no stone unturned in the pursuit of security by creating a preventative outlook that directly combats modern challenges with modern solutions. □

Jonathan Lee is Senior Product Manager at Menlo Security.

To learn more on the anatomy of recent browser-based attacks, why network security today is broken, and the technology approach proven to eliminate these threats, please visit: **www.menlosecurity.com/blog/two-minutes-onhighly-evasive-adaptive-threats-heat/**

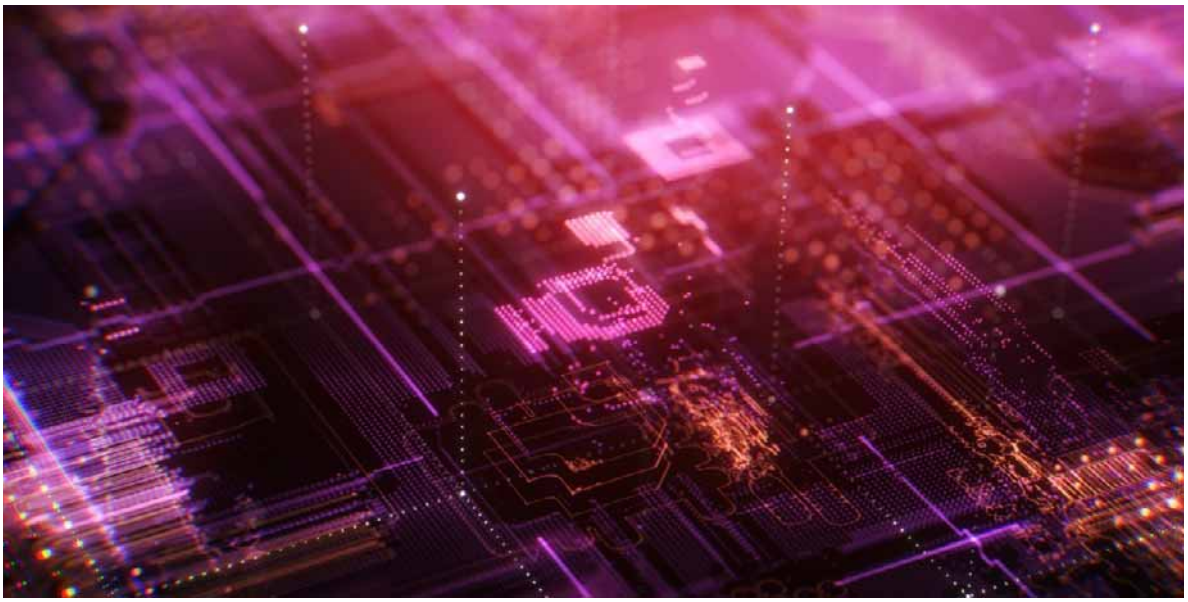
Too hot to handle:
Why modern work has given rise to HEAT attacks

MENLO SECURITY

Learn how at menlosecurity.com/why

The future of cybersecurity: Ransomware groups aim for maximum disruption

Cyber-attackers will continue evolving techniques in 2022.



Marcus Fowler reports

In parallel to the global COVID-19 pandemic, there has been a growing ransomware pandemic. Darktrace researchers discovered that ransomware attacks on US organisations tripled in 2021 compared to 2020, and attacks on UK organisations doubled.

This crisis brought 30 nations together to discuss a counter-ransomware initiative focused on cryptocurrency regulation, security resilience, attack disruption, and international cyber-diplomacy. Despite these landmark policies and law enforcement efforts, it's safe to say that ransomware will remain as a top priority threat and is not going anywhere.

As ransomware permeates, cyber-attackers will continue evolving techniques in 2022

Ransomware gangs are becoming more sophisticated in how they select targets and how they carry out attacks. Many organisations think that ransomware shouldn't be a serious concern if they have backups in place because they can quickly bring business operations back online. But modern attacks are about more than encryption or data exfiltration; they focus on maximising disruption to business operations, including targeting backups for encryption and deletion. In 2022, we could see ransomware gangs target cloud service providers as well as backup and archiving providers.

Critical infrastructure organisations and businesses will continue to assess how quickly they can restore operations in the aftermath of an attack and how extensively they will be able to rely on, and the costs required for cyber-insurers to cover entire ransom payments and costly systems repairs.

In early January, Microsoft researchers found evidence of malware targeting multiple Ukrainian organisations deploying what appeared to be ransomware but was actually a wiper. The malware displays a ransom note then executes the wiper when the target device is powered down. If adopted by other non-state actors, this evolution goes beyond ransomware, and some organisations won't be able to survive these types of attacks.

Sophisticated ransomware gangs will expand their detailed targeting efforts from only 'big game hunting,' where they target large and well-known targets, to use more resources directly targeting midsize and smaller organisations. With increased scalability through automation and leveraging supply chain attacks, ransomware gangs will have the resources to expand their operations. Large organisations have more substantial budgets and more people, and they can prioritise resources to deal with ransomware's effects – it will be far more difficult for small businesses.

Not only are ransomware operators expanding whom they can target, but the group of cyber-attackers able to execute attacks is expanding.

Figure 1: Darktrace breaks down the stages of a BlackMatter ransomware attack targeting a marketing firm in the US

The rise of Ransomware-as-a-Service (RaaS) gives low-skilled threat actors access to sophisticated malware strains, lowering the barrier to entry for attackers. RaaS has expanded the criminal ecosystem to include lower-level threat actors who find and attack the targets before installing the malicious software. Threat actors are increasingly using bots to automate the initial attack that gets them a foothold in the system.

There is also a varying degree of professionalism amongst cybercriminals, from seasoned veterans (with current or previous nation-state experience) to 'script kiddies' with little expertise. This array translates to greater potential for untested or reckless use of sophisticated tools by unsophisticated actors.

Ransomware groups will bounce back

Ransomware groups are resilient. Even if government pressures force ransomware groups to disband or criminally charge them, they will continue to rebrand and crop back up. For example, Darkside, confirmed by the FBI to be behind the attack on Colonial Pipeline, shut down a week after the attack. Shortly after, BlackMatter emerged, widely believed to be a rebranded version of the same cybercrime group.

Earlier this year, Russia's security agency announced that it had arrested several members belonging to the notorious REvil ransomware gang and neutralised its operations. While this is a significant step against a major group, it is unlikely to reflect a long-term change in Russian policy towards cybercriminal gangs. These arrests almost certainly do not mark the end of REvil.

Five ransomware groups have formed a cartel to exchange data and 'best' practices. These groups include Wizard Spider (linked to the Ryuk and Conti ransomware strains), Twisted Spider (which developed Maze and uses Egregor), Viking Spider (the group behind Ragnar), and LockBit.

Even if government pressures force ransomware groups to disband or criminally charge ransomware gangs, these groups will continue to rebrand and crop back up with even more sophisticated techniques and capabilities.

A static 'hardened' perimeter defence isn't the answer – a dynamic self-defending one is

For organisations to build systems to withstand cyber-attacks, security leaders need to think and, more importantly, defend **beyond** the initial breach to maximise continuity of business operations. Security defences like firewalls centred on defending the cyber-perimeter are not enough to protect against evolving threats.

A truly dynamic defence is achievable. Organisations need to actively enforce 'normal' for businesses and disrupt attacks at the earliest indicators of malicious anomalous behaviour, such as file encryption or data exfiltration. Security technology needs to learn, make micro-decisions, and take proportional responses to detect and stop attacks early enough before data exfiltration or encryption occurs.

Attackers are acutely aware of threat intelligence-reliant defensive tools they need to evade and know the limitations of the legacy, siloed approach many organisations employ. Attackers are finding valuable information, exfiltrating the files, and encrypting the data in a short period. The race condition and response window for defenders to detect and stop attacks is getting smaller; security teams and solution responses must get faster.

Cybersecurity is no longer a human-scale problem. Organisations need to adopt AI-based protections that can defend against increasingly automated ransomware attacks. In an era of fast-moving cyber-attacks, and with threat actors deliberately striking when security teams are out of the office, AI technologies have become essential in taking targeted action to contain attacks without interrupting normal business. □

Marcus Fowler is Director of Strategic Threat at Darktrace.

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

DARKTRACE

Don't pay a king's ransom: best practice against ransomware

What strategies organisations can implement to insulate themselves from this threat.

From WannaCry to SamSam, numerous high-profile ransomware attacks in very recent memory have demonstrated that this attack vector is an increasingly prominent threat to businesses. With significant financial and reputational costs at stake, there is a pressing need for UK organisations to review what strategy they have in place against ransomware regardless of their scale. Issues surrounding ransomware are a growing consideration recognised by UK organisations, according to CrowdStrike's latest Global Security Attitude Survey which found that 55% of organisations consider ransomware to be a 'top concern'. Bearing this in mind, this article will offer insight into what strategies organisations can implement to insulate themselves from this comprehensive threat.

The Europol Internet Organised Crime Threat Assessment warns that ransomware attacks are increasingly destructive. The law enforcement agency explains that the effectiveness of ransomware relies on the fact that it can be deployed by malicious actors via a range of different methods that give it an increased chance of going undetected by security teams or infrastructure. At its core, ransomware always operates by the same principle – accessing personal or system files and withholding them on demand of payment, usually in the form of cryptocurrency. This is often within a certain period of time and sometimes for an increasing amount after a missed deadline. The danger posed by this threat is compounded by the fact that victims who do pay are frequently targeted again and that one ransomware infection can spread laterally throughout an entire organisation.

'Beware' of Greeks bearing gifts

The traditional and most common way for ransomware to infect a system is via spam or phishing emails. However, as organisations have made an increasing effort to defend from this known method, attackers have deployed more novel and advanced methods. One such method is the use of exploit kits to take advantage of a security hole in a system or program. We've seen the success of this in the infamous WannaCry attack that crippled hundreds of thousands of computers via a Microsoft exploit. This method has evolved into forms that present malware as a fake software update, prompting users to enable admin capabilities and install malicious code.

The effectiveness of ransomware relies on the fact that it can be deployed by malicious actors via a range of different methods that give it an increased chance of going undetected by security teams or infrastructure.

Another popular method that has seen wider usage in the last year, as noted by CrowdStrike's Mobile Threat Report, is mobile ransomware which is often used to infect users' apps. Like most malware, ransomware attacks have the potential to disable mobile devices, however, the classic file encryption technique often fails. Due to the universal adoption of cloud storage, combined with the limitations of mobile battery life and mobile CPUs, file encryption is many times not the most effective approach for mobile ransomware. Instead, ransomware has been developed to 'lock' devices and display a message that will not accept any other activity unless the correct code is inputted.

The proliferation of ransomware is not going to slow down, and as revealed by the 2020 Global Threat Report, e-criminals have discovered an even more effective way of creating monetary gain. Ransomware-as-a-service allowed the pioneering group PINCHY SPIDER to continually make profits off its deployment by others. The group began helping and encouraging others to adopt their Big Game Hunting practices, retiring GandCrab for REvil. REvil was tracked making demands of $10 million – showing the impact it could have on a victim business. In December 2019, a total of 699 unique cases of REvil had been tracked, showing the virality with which e-criminals are using the ransomware.

Protecting against ransomware

Once the ransomware has made itself known, around 90 days later after initial infection, or is discovered on your device, it is often too late. Access to the hard drive is usually prohibited and files are encrypted. While you may be able to remove the malware and restore your system to a previous version, the encrypted files will have been made unreadable without the attacker's key. In some cases, a victim

CrowdStrike reports

Another consideration for security teams is infrastructure visibility. With a comprehensive view of your devices, the number of potential blindspots where malware can enter or hide within the system is reduced.

may believe that the quickest way to get their network back up and running and have access to those encrypted files is simply pay the ransom. This is not always the best first step as victims need to remember that they also need to make sure they officially kick out the actor, clean up any open vulnerabilities, any persistence mechanisms and then get the network up and running. Steps that are not easily completed and can take a considerable amount of time and expense.

As such, the best defence from ransomware is a strategy that allows for proactive prevention. A good foundation to build from is a comprehensive backup system that allows for data to be retained even if a device is rendered useless by ransomware. However, with ransomware evolving so rapidly that newer variants are capable of deleting backups, security teams need to develop a proactive strategy that can stay one step ahead of bad actors.

Good cybersecurity strategy is built from the ground up. As such, ensuring that all your employees follow basic cyber-hygiene is essential. This includes practices like using strong passwords, multi-factor authentication, secure Wi-Fi, and being aware of the signs and risks of phishing emails, in addition to ensuring physical devices and office space remain secure. In the same vein, it is likewise important to constantly monitor your operating system for potential holes or backdoors to exploit. By constantly keeping your software up to date, this risk is mitigated. Another consideration for security teams is infrastructure visibility. With a comprehensive view of your devices, the number of potential blindspots where malware can enter or hide within the system is reduced.

While ransomware presents a broad threat to UK organisations there are many basic hygiene measures yet to be put in place that can counter this risk. By focusing on the right training and implementing the necessary strategy the extensive danger to organisations presented by ransomware can be mitigated. However, it's important that organisations recognise that these practices are a combination of technical infrastructure as well as educating employees into overcoming some very human mistakes. □

CROWDSTRIKE

BUILT TO STOP BREACHES

CAN'T STOP TODAY'S CYBER ATTACKS?
CROWDSTRIKE FALCON CAN.

FIND OUT MORE AT
CROWDSTRIKE.COM/SEEDEMO


Attackers start with people.
Your protection should, too.
Proofpoint protects your people, data and systems by stopping threats, training users and securing information everywhere it lives.
proofpoint/uk
proofpoint.
Protection starts with people.

Protect people, protect your organisation

Combatting modern cyber-threats, in a diverse landscape.

Over the past two years, cybersecurity teams around the world were challenged to enhance their security posture in this ever-changing landscape. This required – and still does require – creating a balance between supporting remote and hybrid work and avoiding business interruption, while securing those environments from external and internal attacks. With the future of work becoming increasingly flexible for the foreseeable, this challenge now extends into next year and beyond.

The good news is that CISOs in the UK are on high alert of the range of threats they face, perhaps more so than their global counterparts. Proofpoint's Voice of the CISO report revealed that 81% of surveyed UK CISOs feel at risk of suffering a material cyber-attack in the next 12 months, the highest percentage across the 14 countries surveyed globally. While this strong understanding of risk is positive, what remains a concern is that over half of UK CISOs – 68% – feel their organisation is unprepared to cope with a targeted cyber-attack.

We may now be in 2022, but the events of 2020 will echo around the cybersecurity space for some time yet. Cybercriminals, consistently leveraging the widespread disruption and hybrid teams, shifted their efforts, hitting organisations with a multitude of threats new and old. But whatever the tactic, most attacks shared a common trait – they were squarely targeted at people rather than infrastructure.

With so many common threats requiring human interaction, the modern cybercriminal no longer needs to hack into an organisation. Much of the time, once they've gained access to the data they require, they can simply log in.

With this in mind, let's review some of the most prevalent types of people-focused attacks right now and what you can do to defend against them.

With so many common threats requiring human interaction, the modern cybercriminal no longer needs to hack into an organisation. Much of the time, once they've gained access to the data they require, they can simply log in.

The rise of ransomware

Ransomware attacks increased significantly last year – 300% to be precise, with email still commonly used as the point of entry. Despite the fact these ransomware attacks also drove many global news headlines, it remains alarmingly low on the list of concerns for CISOs in the UK. In fact, less than a third – 30% – consider this as their biggest cybersecurity concern for the next year.

The modern ransomware attack looks a little different today. Where once malicious payloads would drop into your inbox, they now often present as two-stage attacks.

Email remains a primary point of entry, however, so this is still very much an attack on your people. Today, the email delivers first-stage malware that acts as a backdoor for a further payload, usually delivered via a remote desktop protocol (RDP) and virtual private network (VPN) access.

As phishing and spam email is still the main gateway for ransomware distribution, it's imperative that all organisations place a priority on securing inboxes with advanced filtering and threat detection. Your solution should detect and quarantine malicious attachments, documents, and URLs before they reach the user.

Email remains the number one threat vector

Whatever the method and level of sophistication, modern cyber-attacks tend to share one common trait – they target the inbox. As recently reported in the FBI's Internet Crime Report, email remains the number one point of entry for cybercriminals.

The trend toward more sophisticated, targeted email attacks is unlikely to slow any time soon, for one good reason – it works.

Whether ransomware, phishing, Business Email Compromise (BEC) or any other threat, attacks on the inbox work because they are designed to fit in. A successfully crafted email can bypass perimeter defences in one click without raising suspicion, leaving employees as the last line of defence between the organisation and those looking to cause it harm.

BEC attacks are nothing new, but they have quickly become one of the most expensive cyber-problems, making them a top cyber concern for 30% of UK CISOs. Such attacks were already firmly on the radar

Proofpoint reports

Security is a shared responsibility. We must empower people, at all levels within our organisations, to understand security and the risky behaviours that can lead to breaches. Training and awareness programmes are crucial, but one size does not fit all.

of the FBI back in 2016 when they were estimated to have cost global businesses around $3.1 billion. Responsible for 44% of all cybercrime losses, it cost victims almost $2 billion in reported losses last year alone.

This marked increase in estimated losses is indicative of a broader trend. Attacks are not necessarily increasing in volume, but they are become more focused – and targeting higher returns. In more elaborate attacks, threat actors are spoofing C-level domain names to instruct victims to transfer vast sums of money. It only needs to work once to be a highly profitable endeavour.

Tackling payload-less threats like BEC requires visibility. It requires a broad and deep set of data and human threat expertise to train machine-learning models to accurately detect and stop bad messages without misidentifying and blocking good messages. You should look for a solution that combines machine learning with extensive threat data and threat analyst expertise to block targeted email fraud attacks as they continue to evolve.

Solving the people problem

Naturally, the cyber-challenges facing organisations today are not focused on one front. Those on the receiving end of cyber-attacks are of just as much concern as those behind them.

Whatever the physical or virtual characteristics of the workplace, people will always be at its centre. And, wherever they are, they are likely to remain squarely in the crosshairs of cybercriminals – with over 90% of cyber-attacks requiring human interaction to succeed.

With this in mind, it's easy to see why 62% of UK CISOs consider human error their organisation's biggest cyber-vulnerability as hybrid workforce presents new challenges for cybersecurity teams. Just like the threats from the outside, there are several causing concern from within. Human error, criminal insider attacks and employees falling victim to phishing emails are just some of the issues keeping CISOs up at night.

To solve this, a modern cyber-strategy must have security awareness training at its heart. And, for maximum impact, this training needs to be tailored and adaptive – not just to certain threats but also to the users who are on the front line. A lack of understanding about your most vulnerable users and the types of attacks they are likely to face makes it very difficult to prioritise a cyber-defence strategy. And with hybrid working, flexible hours, and multiple access points now the norm, gaining that understanding is increasingly difficult.

The good news is that CISOs are recognising this and taking the required steps. Proofpoint's report revealed that the top three priorities across the board for UK CISOs over the next two years are: improving employee cybersecurity awareness (44%), enhancing core security controls (36%), and supporting remote working (34%). This illustrates that a robust cybersecurity posture requires a multi-pronged approach. One that combines people, process, and technical controls.

Criminals are continually targeting humans to expose confidential data, compromise networks, and even wire money. Through a technical combination of email gateway rules, advanced threat analysis, email authentication, and visibility into cloud applications, we can block the majority of targeted attacks before they reach employees. But we can't rely solely on technical controls because as we've seen, this is a people problem.

Security is a shared responsibility. We must empower people, at all levels within our organisations, to understand security and the risky behaviours that can lead to breaches. Training and awareness programmes are crucial, but one size does not fit all. Make sure your programme is from the perspective of the user – make it relevant to their work and personal lives.

We must also bring people into our security fold. Provide simple ways for users to report back to the security team. For example, single click buttons that automatically send potential phishing emails to the security team to analyse – in this case, false positives are a good problem to have. □

Cost of passwords: Resets, breaches, and more

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

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 reports

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. □

Bots, zombies, and shadows: The API risks every developer needs to know

APIs are increasingly being targeted by hackers and many are extremely vulnerable.

Chris Waynforth reports

Who's responsible for the security of your development and production environments? It's a simple question, but for some businesses, the answer can be very complicated. In many instances, responsibility can fall to developers rather than security teams alone. The growth of developer-led security has been happening for a while, driven largely by the inability of security to keep up with the scale and pace of DevOps, and is unlikely to change in the foreseeable future.

One of the most critical areas that developers are taking on security responsibilities is around APIs, the connective tissue that ties DevOps together. APIs are increasingly being targeted by hackers and many are extremely vulnerable. Indeed, by 2024 it's estimated that abuses of APIs – and related data breaches – will almost double in volume.

The problem is, while APIs play an essential role in the way that cloud native applications are architected, they also pose huge potential risks to organisations. In fact, research found that the number of new API vulnerabilities grew in 2020, with sensitive data exposure ranking as the most common vulnerability. If developers are going to be effective cybersecurity defenders for their organisation, they need to understand the types of API-related threats they are facing and what can be done to mitigate the risks.

1. Shadow APIs

How many APIs does your organisation have? Research by Aite Group suggests that the majority of businesses don't know, while those that do have an up-to-date API inventory put the average number at 620 per organisation.

Now, how many APIs are there that you are unaware of? The challenge of shadow APIs is not new but, as the number of APIs continues to rise, it's set to become a much greater source of risk in the coming years.

If developers are going to be effective cybersecurity defenders for their organisation, they need to understand the types of API-related threats they are facing and what can be done to mitigate the risks.

It's easy to see how shadow APIs get created in a fast-paced DevOps environment. However, if APIs are published without security review or controls, they are essentially invisible to security teams and API gateway. Alternatively, APIs can get published outside of a defined process or after the API structure changes with the update of an application. In some cases, developers might not even be aware of a publication process and press on, assuming they have autonomy to publish the API into production.

Finally, there's also plain old human error. If a developer applies the Backends For Frontends (BFF) pattern in their application design, it can result in backend services – usually meant to be accessed only by internal services – being exposed to direct pass-through access from external, client API calls.

The problem is that shadow APIs still have access to the same sensitive information that published, secured APIs do, even if nobody knows where they exist or what they're connected to. As a result, it's easy to see how the presence of shadow APIs can lead to major compliance violations and regulatory fines – or worse, cybercriminals using them to access your organisation's sensitive data.

2. Automated bot attacks

The plague of automated bot attacks isn't confined to any one specific industry – it's an issue that is impacting every business that has a website, mobile app or public-facing API. Web applications in particular are a rich target for botnet operators, because they offer a direct path to the sensitive data that can be scraped and shared or sold on the Dark Web.

Such attacks are very difficult to prevent because the bots have been designed to mimic legitimate human behaviour in order to evade detection. Unlike other types of attacks, botnets can operate 24/7 and are purposefully designed to carry on repetitive tasks that are harder for humans to maintain. When successful, bot attacks on APIs can lead to the loss of personally identifiable information (PII), data leakage and more.

Many organisations struggle to ensure the security of their APIs because they rely on simple authentication tokens or basic IP rate-limiting. Unlike the authentication of human users through multi-factor authentication, API tokens are often a single factor

As attacks are becoming more complex, the solution should combine bot detection that can identify good bot from bad bot, and a bot from a legitimate human user.

authenticating an API call. For developers without formal information security training, this can be a very tricky threat to combat.

3. Deprecated or zombie API

Deprecation is a natural part of the API lifecycle. However, if and when an API hasn't been properly disabled, it becomes the perfect platform for malicious hacker activity – all too often out of sight of developer and security operations.

Having unmonitored APIs left unattended is similar to having an unlocked window on your house. A dedicated hacker can use them to gain access to data without being detected, or even execute more sophisticated attacks – often without the developer or security team being any the wiser! This is a huge underlying risk factor that can become a software supply chain attack.

One reason that deprecated APIs are often left unaddressed is because they get overlooked and aren't included as part of regular software updates. As a result, the API can be exploited for account takeover, fraudulent transactions, or data extraction, and other nefarious purposes.

Look for an advanced solution to stop an advancing problem

Today, the majority of organisations use an API gateway solution, however this technology is far from being a silver bullet for growing API security risks. Gateways are great for delivery and access management, but lack the sophistication to stop complex attacks.

Approaches like gRPC, MQTT and GraphQL are increasing in popularity as businesses demand more diverse engineering models. But, as these are deployed more widely, businesses will also be exposed to more sophisticated attacks on APIs. Therefore, it's essential to adopt a baseline of governance standards and security tools for API protocols.

While the move towards DevSecOps is an important industry effort, this mentality alone cannot stop business logic attacks – the concentrated abuse of rules that dictate how an application operates. The challenge is that runtime protection policies that protect business logic cannot be easily shifted left. Instead, organisations should seek out security tools that not only provide runtime protection, but also seamlessly embed into the application development process.

Developers and security operations can start addressing today's top API attack risks by first having a clear assessment of such risks. The assessment starts with automated discovery and keeping an API catalog up-to-date. As attacks are becoming more complex, the solution should combine bot detection that can identify good bot from bad bot, and a bot from a legitimate human user. Lastly, to address the issue of deprecated APIs, a solution also needs to monitor the lifecycle of API tokens along with versions of APIs. Together, this approach will enable developers to adequately address API security risks without slowing down their innovation agenda. □

Chris Waynforth is Area VP – EMEA North at Imperva.

Imperva is the cybersecurity leader whose mission is to help organisations protect their data and all paths to it. Customers around the world trust Imperva to protect their applications, data and websites from cyber-attacks. With an integrated approach combining edge, application security and data security, Imperva protects companies through all stages of their digital journey. Imperva Research Labs and our global intelligence community enable Imperva to stay ahead of the threat landscape and seamlessly integrate the latest security, privacy and compliance expertise into our solutions.

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

imperva

Cyber-threat landscape, nothing but the same old story

This article will consider two of the significant issues of interest for professionals involved in assessing and/or addressing cyber-threats.

Red Sift reports

In late October this year, the European Union Agency for Cybersecurity, ENISA, published their Threat Landscape Report.

Now, in its 9th edition the 2021 report is, or ought to be, considered primary source material for businesses who are serious about addressing cyber-threats and mitigating cyber-risk.

The report contains a number of significant issues of interest for professionals involved in assessing and/or addressing cyber-threats. This article will only consider two.

1. E-mail-related threats – the one that fools the human

The report distinguishes between email-related threats that exploit weaknesses in the human psyche versus technical vulnerabilities in information systems.

Familiarity with awareness and training programmes has been heightened this year as unsavoury phishing training practises hit the headlines in the United States and the United Kingdom.

In the UK, West Midlands Train suffered significant public backlash for entrapping their staff with an email containing a lure that promised a bonus to staff for their loyalty during the pandemic. In the US, 'The Tribune Publishing Company' faced similar backlash for a similar stunt.[1]

But the damaging headlines don't end there. In other news, related to phishing training, ProofPoint finally agreed to transfer a series of disputed web domains to Facebook.

ProofPoints' phishing awareness training platform ThreatSim had used facbook-login.com, facbook-login.net as well as other lookalike domains related to instagram. The decision to transfer domains back to Facebook was a sensible choice given it had all the hallmarks of a clear case of trademark infringement. But it does raise the question, if a training company cannot use lookalikes because of trademark infringement then what good are they?

Familiarity with awareness and training programmes has been heightened this year as unsavoury phishing training practises hit the headlines in the United States and the United Kingdom.

What good indeed? The authors of the ENISA Threat Landscape report put it rather more diplomatically

> *'... despite the many awareness and education campaigns against these types of attacks, the threat persists to a notable degree'.*

In other words, phishing training does not appear to be materially benefitting businesses by providing long-term defensive measures. Certainly nothing that can be measured.

2. Prime threats – only the names have changed

The second issue of note is that while the names of cyber-threats have changed over the years, the underlying problems remain the same.

To sense check this proposition, I undertook a review of the reports dating back to 2012. This is what I learned. In the 2020 report, ENISA identified nine prime threats, I focussed on the top two: ransomware and malware.

On the ENISA threat landscape webpage, I was able to locate the reports for 2012–2018, 2019 was not discoverable.

2018–2015, ransomware and malware were reported as prime threats. So no change there then.

In 2014, ransomware, and malicious code: i.e. trojans & worms were identified as prime threats. Malicious code: trojans & worms are what we today call malware. So again no change there then.

In 2013, there were differences but these were again slight and not substantial. ENISA warned about ransomware and included the terms (a) rogueware & (b) scareware and (iii) malicious code: worms & trojans (aka malware).

The previous year 2012, the word ransomware wasn't yet part of the lexicon of cyber-threats, it was simply

referred to as rogueware or scareware. Malware was simply worms & trojans.

To put it simply, the story since 2012 remains the same. Only the names have changed.

This should give firms comfort that despite the widespread reports of novel or zero day attacks, the prime threats to businesses continue to be the same threats that we have seen for the best part of the last decade.

Moreover and perhaps most importantly, key trends identified in the report place compromise through phishing emails and brute-forcing on Remote Desktop Services (RDP) as the two most common ransomware infection vectors.

Oxford University Professor of Government, Ciaran Martin, formerly the founding executive of the UK's National Cyber Security Centre and its first CEO, has frequently been quoted as saying; 'the problems we face are chronic and not catastrophic.'

This view is borne out with this simple literature review. This should both be a source of comfort and alarm to the businesses that are listening today.

So why is it important to establish that the threats are not novel but remain the same?

Firstly, directors have a duty to exercise reasonable care, skill and diligence.

This legal obligation can be found in the Companies Act in both the UK and Ireland but it can also be found throughout the common law world including the US, Canada, Australia, and New Zealand.

Civil law countries have a similar requirement, the Germans adopted this duty of care into the AKTG that is the set of laws that governs companies noted at the stock exchange. It reads:

> *'...in managing the affairs of the company, the members of the management board are to exercise the due care of a prudent manager faithfully complying with his duties.'*

Similar legal obligations exist in other jurisdictions. The question that businesses, their board, shareholders and other stakeholders should ask is:

> *Are directors meeting their obligations to the company if they do not address the most significant known threats to their business?*

Threats that, let's be clear, businesses have been warned about year on year from trusted, independent experts.

Threats that are more than reasonably identifiable but that are easily identifiable.

This brings me to the 2nd reason *why is it important to establish that the threats are not novel but remain the same year on year.*

In the event of a cyber-attack where the business operations are disrupted, the reputation is damaged due to leaks, or the share price suffers a shock on the news and the firm needs to defend itself, a solid defence available for firms and their directors is that the threat was not reasonably identifiable.

The courts do not expect directors to see around corners but they do expect them to read the writing on the wall. This is all the more pressing, when that writing has been on the wall since at least as early as 2012.

How do you protect your firm?

One way would be to make sure that your business has sensible responses to the same questions that the courts will ask:

1. Is the threat well known and understood?
2. Is the solution known and understood?
3. Is that solution reasonable, and affordable (this will depend on the type of business that you are managing) and
4. Finally, would a reasonable director implement it?

Answering yes to all but taking no action means that your business has limited the defences available to it and could prove an expensive lesson.

To put it simply, if a threat is reasonably foreseeable and avoidable, it is incumbent on the directors and officers to manage it.

Comfortingly, however, the recommendations do include well known solutions that are known to work, including the recommendation to '[p]ut security controls into place on the email gateway to reduce the frequency or possibility of the lures arriving to your employees' inboxes' and to implement one of the standards for reducing spam emails, specifically calling out DMARC. That's certainly reassuring as this year, the DMARC protocol will be 10 years old! □

[1] https://www.nytimes.com/2021/05/13/world/europe/phishing-test-covid-bonus.html

RED SIFT

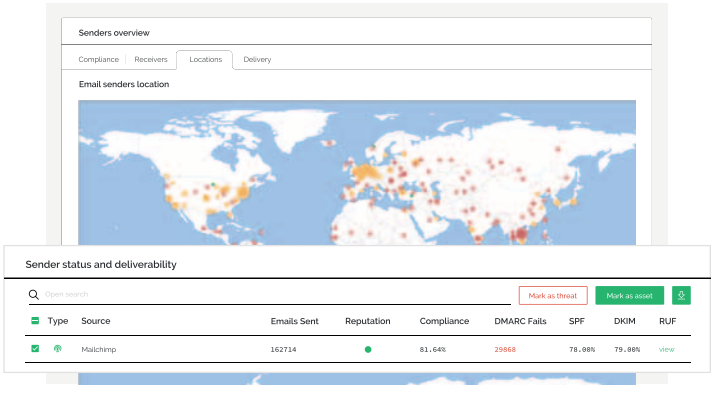
It's **400x more expensive** to stop a cyber attack than it is to start one.

We exist to **change** that.

Red Sift delivers **scalable inbound** and **outbound** email protection for less than you think.

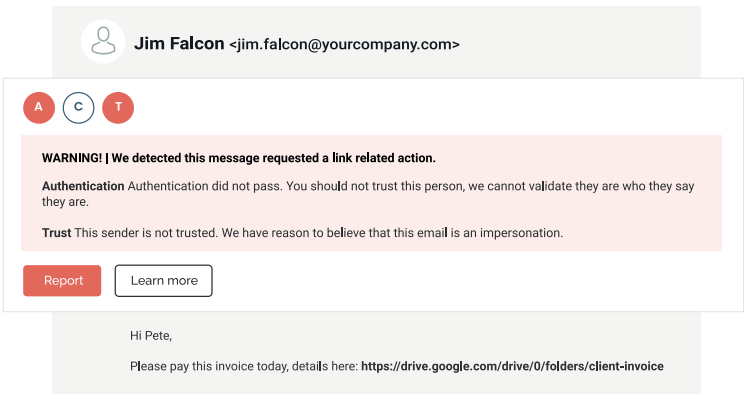
ONDMARC

Protect your domain from email impersonation



ONINBOX

Intelligent email threat detection



Trusted by: Telefónica, WISE, pipedrive, itv, Domino's

Email a member of the team to find out more about our cybersecurity solutions | contact@redsift.com

Automatically stops data breaches and security threats caused by employees

Your Data + Tessian Technology = Human Layer Security for Email

TESSIAN

Legacy secure email gateways are no match for the cyber-threats of tomorrow

Security leaders are starting to question whether standalone SEGs have a place in today's cybersecurity stack.

Tessian reports

Email represents the greatest threat vector, responsible for 96% of cybersecurity breaches. And legacy email security solutions that rely on Secure Email Gateways (SEGs) and rule-based controls are simply not up to the task of mitigating increasingly advanced and evolving cyber-threats.

In fact, between July 2020 and July 2021, Tessian detected 2 million malicious emails that bypassed SEGs. This declining security effectiveness is the principal reason why security leaders are starting to question whether standalone SEGs have a place in today's cybersecurity stack.

Combined with growing alert fatigue, and an increasing level of redundancy as organisations adopt SaaS offerings like Microsoft 365 with SEG capabilities natively included, the calls for ripping and replacing SEGs are growing louder. Echoing this shift in the email security landscape, Gartner predicts by 2023, 40% of organisations will be using a cloud email security solution like Tessian in place of a SEG.

Static vs. dynamic protection

The vast majority of organisations still rely on SEGs as the main method of filtering out malicious email-based attacks. Developed in 2004 and designed in the era of on-premise email servers, one of several shortcomings of SEGs is the reliance on an overly manual, rule-based approach, based on threat intelligence.

By using threat intelligence-derived deny lists, creating allow lists, or using signatures for message authentication, SEG-based email security controls are reactively geared to protect your company's email and data – but only from *known* threats.

The SEG-based approach offers no protection against zero day attacks, which is a significant and *growing* threat vector – with zero day discoveries up by 100% in 2021. SEG solutions also fall short against attackers that have invested resources and effort into advanced social engineering campaigns, which are able to circumvent the static, rule-based controls. The greatest attack types that SEGs fail to prevent include Business Email Compromise (BEC), Account Takeover (ATO) and advanced spear phishing attacks.

Threat actors are able to bypass SEGs by leveraging intricate social engineering exploit kits procured on the dark web. They'll even go so far as to recruit unsuspecting cybersecurity professionals to carry out attacks.

Email threats are on the rise

All it takes is *one* malicious email to bypass your existing security controls. And as Tessian research has demonstrated, malicious email bypassing SEGs and native tools is extremely common today. This is why BEC is seen as one of the leading threat vectors to organisations, resulting in $1.8 billion in losses in 2020.

Cybercrime is also steadily becoming more organised, with cybercriminals offering professionalised 'Cybercrime-as-a-Service' offerings. Threat actors are able to bypass SEGs by leveraging intricate social engineering exploit kits procured on the dark web. They'll even go so far as to recruit unsuspecting cybersecurity professionals to carry out attacks. Spear phishing and ATO are common methods for either perpetrating cyber-fraud, data exfiltration, or even more worryingly, deploying ransomware.

The growing prominence of zero day attacks and ransomware is of particular concern. International law enforcement agencies note remote workers are being targeted with phishing emails carrying malicious payloads, including ransomware. With the frequency of attacks doubling in the past year, ransomware attacks are now seen as the foremost threat faced by organisations.

Why organisations are ripping and replacing their SEGs

Only by shifting the focus from securing machines to securing the human layer will email-based threats be significantly mitigated. This is where best-in-breed email security solutions like Tessian come into play.

Relying on machine learning and behavioural intelligence, Tessian is able to detect and prevent anomalous and malicious inbound and outbound email traffic, including preventing data loss. Unlike

"Continued increases in the volume and success of phishing attacks and migration to cloud email require a reevaluation of email security controls and processes. Security and risk management leaders must ensure that their existing solution remains appropriate for the changing landscape."

2021 GARTNER MARKET GUIDE TO EMAIL SECURITY

SEGs, Tessian also offers protection against numerous collaboration platform entry points like Microsoft SharePoint, OneDrive and ShareFile.

And with over 70% of enterprises now hosted in one or more public clouds and utilising SaaS productivity suites such as Microsoft 365 or Google Suite, which include native SEG capabilities such as sender reputation and authentication, spam filtering and custom routing rules, is yet another reason why standalone SEG solutions are redundant.

If you combine these native capabilities with an intelligent inbound and outbound solution like Tessian, robust email security protection is guaranteed.

Some of the standout features offered by Tessian include advanced Attachment and URL Protection (behavioural analysis and threat intelligence), as well as a range of impersonation attack defence capabilities, such as:

- Internal impersonation & CEO fraud
- Advanced spoof detection
- Counterparty & vendor impersonation
- Brand impersonation
- External account takeover
- Invoice fraud
- Credential theft

Tessian also offers protection against malicious data loss enabled through a successful social engineering campaign, or accidental, for example, an employee sending sensitive company data to a personal email address. Other unique features include in-the-moment security awareness training for suspected phishing email, as well as in-the-moment DLP pop-ups.

Combined with Microsoft 365 or Google Workspace, Tessian's ability to address sophisticated inbound email security threats across expanding entry points places it into the best-of-breed inbound email security solution category. But when combined with Tessian's advanced DLP capability, it becomes undeniable that it's time to replace your SEG for the next generation of unrivalled email security. And this is why Tessian was recognised as a representative vendor for Integrated Cloud Email Security in the 2021 Gartner Market Guide to Email Security. □

Sponsors and exhibitors

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

Beyond Identity | Strategic Sponsor

For more information please visit www.beyondidentity.com

CrowdStrike | Strategic Sponsor

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph, CrowdStrike Falcon correlates over 5 billions endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

Learn more at www.crowdstrike.com

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

Illumio | Strategic Sponsor

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber-disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centres, and endpoints, enabling the world's leading organisations to strengthen their cyber-resiliency and reduce risk.

For more information, please visit www.illumio.com

Imperva | Strategic Sponsor

Imperva champions the fight to secure data and applications wherever they reside. In today's fast-moving landscape, your assets require constant protection, but analysing every emerging threat is a burden on time and resources. Imperva offer solutions to protect your data and applications wherever you are on your cloud evolution journey. For security to work, it has to work for you. With complex and ever-changing threats, it's more important than ever to gain visibility across your data and applications. Imperva distill millions of data points into the critical risks that are most important, so you have the actionable insights and ability to automate the responses you need to protect your business. By accurately detecting and effectively blocking incoming threats, they empower you to manage critical risks, so you never have to choose between innovating for your customers and protecting what matters most. At Imperva, they innovate using data, analytics, and through a community of experts to deliver simple, effective and enduring solutions that protect our customers from cybercriminals. They tirelessly defend your business as it grows, giving you clarity for today and confidence for tomorrow. Imperva – Protect the pulse of your business.

For more information, please visit www.imperva.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

Netacea | Strategic Sponsor

Netacea protects your websites, mobile apps and APIs from malicious bots and the growing threats from scraping, credential stuffing and account takeover. Netacea understands bot behaviour better than anyone else, thanks to a pioneering approach to detection and mitigation. Our Intent Analytics™ engine focuses on what the bots are doing (not how they're doing it), so genuine users are always prioritised while malicious bots are prevented from compromising your business. Powered by machine learning, Netacea's multidimensional approach continuously monitors your web traffic to pinpoint the difference in automated bot activity vs genuine visitors, keeping you ahead of evolving bot threats. With incredible speed, accuracy and transparency, you'll have the actionable intelligence you need, when you need it, so you're empowered to make smarter decisions about your traffic. Welcome to a new era of bot mitigation.

For more information, please visit www.netacea.com

Okta | Strategic Sponsor

Okta is the leading independent provider of identity for the enterprise, and the Okta Identity Cloud enables organisations to both secure and manage their extended enterprise, and transform their customers' experiences.

With over 5,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely adopt the technologies they need to fulfill their missions. Over 5,600 organisations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to securely connect their people and technology.

For more information, please visit www.okta.com

Proofpoint | Strategic Sponsor

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber-attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com

Recorded Future | Strategic Sponsor

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organisations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organisations around the world.

Learn more at recordedfuture.com

Red Sift | Strategic Sponsor

Founded in 2015, Red Sift is a global company providing cybersecurity services to organisations such as Wise (previously Transferwise), Telefonica, Pipedrive, ITV and top global law firms.

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. Products on the Red Sift platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analysing the security of inbound communications for company-wide email threat intelligence.

Find out how Red Sift is delivering actionable cybersecurity insights to its global customers at www.redsift.com

SenseOn | Strategic Sponsor

Founded in 2017 by David Atkinson, the first cyber-specialist in the United Kingdom's specialist military units, SenseOn brings together cybersecurity experts, former government cyber-operatives and applied machine learning specialists. SenseOn was named the 'Cybersecurity Innovation of 2019' by the Institute of Engineering and Technology (IET) and a World Economic Forum (WEF) Technology Pioneer in June 2021. SenseOn improves cyber-team productivity with more effective and faster investigations, and it also reduces costs for its clients by consolidating point solutions and deploying 15x faster than legacy security architectures. SenseOn combines broad detection and response capabilities across traditionally siloed security domains with AI-based automation. Its unified platform proactively detects and shuts down threats including ransomware, hacking/data theft and malicious insiders, solving critical security challenges in a rapidly evolving IT landscape. It's also uniquely suited to hybrid and remote work settings as it can be rapidly deployed across any endpoint or network inside and outside the traditional perimeter. In addition, SenseOn's new live incident response feature, Remeda, leverages cutting-edge technology with highly skilled cyber-analysts to respond and remediate against threats and attacks in real time.

For more information, please visit www.senseon.io

Tessian | Strategic 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

4Data Solutions | Education Seminar Sponsor

The explosion in data consumption, acceleration in digital transformation, rapid shift to the public cloud and evolving threat landscape, which have been exacerbated by the pandemic, present today's organisations with substantial challenges.

Businesses need to lock down the cloud, ensure the right skills are in place, and stay compliant. The shift to multicloud and concerns over vendor lock-in add further complexity.

As organisations look to build-out and rationalise their cloud environments, monitoring and managing threats on premise must also be tackled, preferably with modern, flexible and cost efficient tools and approaches.

4Data Solutions can help.

We provide:

- Unified multi-cloud security management (from C3M) giving you complete visibility and control of your public cloud estate.
- Next-gen SIEM & SOAR solutions (from Logsign) giving you comprehensive visibility and control of your data and enabling you to automate and orchestrate detection and response processes for reduced MTTR and improved workforce efficiency.
- Monitoring for breaches to 3rd party applications and leaked data (from Threat Status). Processing copious quantities of data, extracting useful information and comparing it to all other data gathered when reporting back on the level of threat.
- Technology (from Cribl) that allows you to efficiently and effectively manage your data for security and compliance purposes.

We are a team of technology experts highly experienced in helping organisations maximise value from data by making it available, observable, secure and compliant. We are straight-talking, conscientious, ethical and focused on earning the trust of our clients.

4Data Solutions is based in the UK, with offices in Germany and South Africa.

For more information, please visit www.4datasolutions.com, call +44 (0)330 128 9180 or email info@4datasolutions.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.

For more information, please visit www.cequence.ai

Cofense | Education Seminar Sponsor

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.

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

CybelAngel | Education Seminar Sponsor

CybelAngel provides an innovative solution of data leaks detection on the Internet.

We monitor the Dark Web and the Internet of Things to identify threats that could adversely affect our customers. We identify, in real time, the new risks on the web that target large companies. Every day we detect sensitive data circulating via the Internet without any protection such as passwords, credit cards, confidential documents, etc.

We have automated the entire information search process. This allows us to monitor a large number of sources at a high frequency. When a risk is identified, we perform a detailed human analysis to supplement the detected information. Having eliminated false positives, we then alert the companies, providing them with a precise analysis of the existing risk so they can take appropriate remedial steps.

We offer a service that can be easily integrated into existing security solutions. This service is non-intrusive, does not need to be installed on our customers' IT infrastructure and is based on a list of keywords that includes in particular domain names, IP addresses as well as subsidiary, brand and product names.

When a risk is detected, we alert our customers via a secure interface. This interface makes it possible to manage threats effectively. A control panel facilitates the monitoring of alerts over time, from the detection to the resolution of threats.

For more information, please visit www.cybelangel.com

Cybersixgill | Education Seminar Sponsor

Cybersixgill's fully automated threat intelligence solutions help organisations fight cybercrime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response – in real-time. The Sixgill Investigative Portal empowers security teams with contextual and actionable alerts along with the ability to conduct real-time, covert investigations. Rich intelligence streams such as Cybersixgill Darkfeed™ harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organisations' existing security systems to help proactively block threats. Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

For more information, please visit www.cybersixgill.com

Devo | Education Seminar Sponsor

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organisation today and tomorrow.

Learn more at www.devo.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

HelpSystems | Education Seminar Sponsor

HelpSystems is a software company focused on helping exceptional organisations Build a Better IT™. Our cybersecurity and automation software simplifies critical IT processes to give our customers peace of mind. HelpSystems offers a comprehensive, powerful data security suite designed for today's hybrid IT reality.

We partner with organisations to provide layered data protection where you need it most. From understanding what data you have to controlling its access and sharing it securely, we can help minimise threats and maintain compliance – wherever data is stored or moved. Our complete solution set includes data classification, DLP, email security, managed file transfer, encryption, and digital rights management for ultimate, data-centric security from one trusted vendor.

Learn more at www.helpsystems.com

Intel 471 | Education Seminar Sponsor

Intel 471 empowers enterprises, government agencies, and other organisations to win the cybersecurity war using near-real-time insights into the latest malicious actors, relationships, threat patterns, and imminent attacks relevant to their businesses. Our TITAN platform collects, interprets, structures, and validates human-led, automation-enhanced results. Clients across the globe leverage this threat intelligence with our proprietary framework to map the criminal underground, zero in on key activity, and align their resources and reporting to business requirements. Intel 471 serves as a trusted advisor to security teams, offering ongoing trend analysis and supporting your use of the platform.

Learn more at intel471.com

Kenna Security | Education Seminar Sponsor

Kenna Security is the enterprise leader in risk-based vulnerability management (RBVM). Using the Kenna Security Platform, organisations can work cross-functionally to determine and remediate cyber-risks. Kenna leverages machine learning and data science to track and predict real-world exploitations so security teams can focus on what matters most. Kenna serves nearly every major industry and counts CVS, KPMG, and many other Fortune 100 companies among its customers.

Kenna Risk Scores, another pioneering RBVM innovation, give security, IT, executives, board members, and other stakeholders a simple and effective way to assess the relative risk of a specific vulnerability, asset class, workgroup, and organisations as a whole.

Recently acquired by Cisco, Kenna Security's acclaimed risk-based vulnerability management will be combined with SecureX, the platform that connects the industry's broadest and most integrated security portfolio, providing global organisations the ability to hunt down and assess threats, identify the vulnerabilities most likely to pose a risk, and give remediation teams clear guidance about what to fix first.

Cisco SecureX will layer in additional capabilities by integrating enterprise security management solutions into one centralised location, giving teams a comprehensive way to break down silos, extend detection and response capabilities, and orchestrate and remediate with confidence.

By integrating Kenna Security into SecureX, companies will solve a notoriously difficult piece of the security puzzle and deliver Kenna's pioneering RBVM platform to more than 7,000 customers using Cisco SecureX today.

All of this reflects Cisco's determination to streamline and simplify security management through a highly integrated, open platform that brings together threat and vulnerability management.

For more information, please check out the latest news and visit kennasecurity.com

ManageEngine | Education Seminar Sponsor

As the IT management division of Zoho Corporation, ManageEngine prioritises flexible solutions that work for all businesses, regardless of size or budget. ManageEngine crafts comprehensive IT management software with a focus on making your job easier. With our 90+ products and free tools cover everything your IT needs, you can take complete control of your IT infrastructure and services – both on-premises and in the cloud.

For more information, visit www.manageengine.com

OPSWAT | Education Seminar Sponsor

OPSWAT is a global leader in critical infrastructure cybersecurity that helps protect the world's mission-critical organisations from malware and zero-day attacks. To minimise the risk of compromise, OPSWAT Critical Infrastructure Protection solutions enable both public and private organisations to implement processes that ensure the secure transfer of files and devices to and from critical networks. More than 1,000 organisations worldwide spanning financial services, defence, manufacturing, energy, aerospace, and transportation systems trust OPSWAT to secure their files and devices; ensure compliance with industry and government-driven policies and regulations, and protect their reputation, finances, employees and relationships from cyber-driven disruption.

For more information on OPSWAT, visit www.opswat.com

Picus Security | Education Seminar Sponsor

Picus Security is a leading Breach and Attack Simulation (BAS) vendor, enabling organisations to test, measure and improve the effectiveness of their cyber security controls through automated and continuous offensive and defensive security testing.

Picus' complete security control validation platform challenges organisations' cybersecurity controls at prevention and detection layers by simulating over 10,000 threats and attack scenarios. This includes the latest types of malware and ransomware as well as MITRE ATT&CK techniques.

Crucially, the Picus platform not only identifies defensive weaknesses as well as threat coverage and visibility gaps, it supplies content to help mitigate them too. This includes prevention signatures as well as detection rules for SIEM and EDR tools – removing the need for security teams to create and test their own.

Unlike other tools and assessments, Picus enables security leaders to understand and measure an organisation's cybersecurity posture at any moment in time. It provides insights into the impact of infrastructure changes and security improvements, and helps guide and prioritise future investment decisions.

Gartner, which lists Breach and Attack Simulation as a Top Security and Risk Management Trend for 2021, has named Picus a 'Cool Vendor'. The company is cited by Frost & Sullivan as one of the most innovative players in the BAS market.

Picus has hundreds of clients worldwide, with offices in EMEA, North America and APAC. Its technology partners include Cisco, IBM, Fortinet, Microsoft, Splunk and VMware.

For more information, please visit www.picussecurity.com

Synack | Education Seminar Sponsor

Synack, the most trusted crowdsourced security testing platform, delivers on-demand security testing, intelligence, and operations through a continuous, offensive SaaS platform with crowdsourced talent. The company combines the world's most skilled and trusted ethical hackers with AI-enabled technology to create a scalable, effective security solution. Headquartered in Silicon Valley with regional offices around the world, Synack protects leading global banks, the top 10 global consulting firms and security companies, DoD classified assets, and over $2 trillion in Fortune 500 revenue. Synack was founded in 2013 by former NSA security experts Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

For more information, please visit us at www.synack.com

Vectra | Education Seminar Sponsor

Vectra® protects business by detecting and stopping cyber-attacks. As a leader in network detection and response (NDR), Vectra® protects your data, systems, and infrastructure. Vectra enables your SOC team to quickly discover and respond to would-be attackers – before they act. No business or organisation is impervious to cyber-attacks. Your existing security tools will prevent 99% of those attacks. But with enough time, bad actors can get past even the most secure barriers. With Vectra, you stop them in their tracks. Vectra gives security analysts the ability to rapidly identify suspicious behaviour and activity on your extended network. Whether that activity originates outside the firewall or from within, whether an attack is directed against an on-prem data centre or the cloud, Vectra will find it, flag it, and alert security personnel so they can respond before the damage is done. Vectra is Security that thinks®. It uses artificial intelligence and machine learning to improve detection and response over time, eliminating false positives so you can focus on real threats. The result of an unparalleled marriage of security research and data science, Vectra will change the way you think about cybersecurity.

For more information, please visit www.vectra.ai

C2 Cyber Ltd | Branding sponsor

For more information please visit ww.c2cyber.com

Orchestra | Branding Sponsor

Orchestra Group's mission is to address the major roadblocks that make it difficult for CISO, CIO, and their teams to manage cybersecurity, such as:

1. Fragmented technologies using different paradigms for each slice of the cybersecurity puzzle leading to a cyber-stack of between 25 to120 different technologies in every large organisation.
2. Lack of standard metrics to measure, manage, and benchmark cyber-defence. This is crucial to drive efficiency, effectiveness, and continuous improvement of organisations' security.
3. Constant change is now the norm for business and IT. Cybersecurity requires constant tuning of the trade-offs between shifting IT\Business needs and cyber-risk.

Orchestra Group is promoting the following solutions:

- Harmony IoT – a unique solution that provides an airspace dome around the organisation to monitor, detect threats and mitigate cyber-attacks through the attack surface of WiFi and Bluetooth protocols, and smart-connected devices & IoTs using them.

  It delivers visibility, continuous monitoring and real time attack mitigation.

  What makes it different from traditional network access control (NAC) and mobile device management (MDM) is it monitors the airspace rather than the devices.

  Its policy engine makes it easy to establish effective airspace security hygiene to ensure the devices operating in your airspace are configured to meet your wireless security standards.

- Harmony Purple – a next-generation Automated Purple team tool that continuously showcases validated, global, multi-vector, Attack Path Scenarios™ (APS) and creates risk modelling-based prioritisation, so red and blue teams can focus their time and resources on those vulnerabilities that threaten critical assets and business processes.

  It unifies scanning, penetration testing, network analysis, risk prioritisation and remediation. It's easy to use and automated – and because it is low impact, scans can be run anytime on production systems.

  Harmony Purple delivers a manageable set of remediation recommendations that deliver better security with less work.

For more information, please visit orchestragroup.com

Telesoft | Branding Sponsor

Telesoft Technologies is an independent, privately owned global provider of cutting-edge cybersecurity, telecoms mobile products and services and government infrastructure. We work with integrators and service providers to develop, manufacture and support systems that generate revenue, keep critical infrastructure operational and important data safe on high-density multi 100Gbps and beyond 1Tbps networks.

We are headquartered in the UK, which includes engineering, research, and development with local offices for sales and support in USA and India.

Today we develop and customise network monitoring and recording systems for cybersecurity incident response, network performance management and national security at scale to cover entire countries and retention of data beyond 12 months. This enables comprehensive threat hunting to be carried out over several months, increasing the likelihood of detecting threat actors hiding within the network.

Telesoft provides an optional 24/7 threat hunting service for round the clock network security monitoring, threat detection, and intrusion alerting. Our team of expert analysts will provide your business with full network visibility to help detect malicious activities and increase overall protection, whilst decreasing risk. Comprised of highly trained security analysts, supporting personnel and toolsets, our service will monitor and detect threats within the network, alerting security teams to the activity to enable a response.

For more information, please visit www.telesoft-technologies.com

Vulnerability intel + Data science = Insight you can act on.

Risk-based Vulnerability Management

Focus on the threats that matter most.

Remediate faster and more efficiently with data-driven risk prioritization.

www.kennasecurity.com

cisco | KENNA Security

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **Securing the citizen (patient, employee, tax-payer…..)**

Eleanor Fairford, Deputy Director for Incident Management, NCSC

- The current threat level and significant threat types/actors
- Lessons learned from the attacks of 2021
- Advice for public and private sector organisations looking to improve their cyber-resilience

09:20 **The path to zero trust with least privilege & secure remote access**

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

- What zero trust is and how NIST defines it
- The goals of zero trust
- Roadblocks to zero trust (legacy architectures and technologies)
- How Privileged Access Management aligns with and enables zero trust

09:40 **Following threat actor bread crumbs**

James Burchell, Senior Security Engineer, CrowdStrike

The e-crime ecosystem is an active and diverse economy of financially motivated threat actors that engage in a myriad of criminal activities in order to generate revenue. Join this session to:

- Take a deep dive into notable shifts in advanced adversary operations
- Get an understanding of how monitoring of this malicious ecosystem is critical for
  - Early detection
  - Preventing expensive data compromises and ransomware incidents…

…No matter how big or small your security team is

10:00 **The real battleground of cybersecurity**

Ciaran Martin, Professor of Practice in the Management of Public Organisations, Blavatnik School of Government at Oxford University

- What government defences can stop and what they cannot (so what is left for private sector CISOs to deal with)
- How the national security response is evolving and how our cybersecurity as a nation is improving/getting worse
- How our cybersecurity resilience is impacted by reliance on a few foreign providers of core infrastructure (Cloud)
- The level of cybersecurity investment by government and the private sector – adequate/inadequate?
- How private sector security solutions are/are not helping improve security and resilience

10:20 **Education Seminars | Session 1** **See pages 52 to 59 for more details**

Beyond Identity	**Beyond Identity's Passwordless MFA: The only way to positively verify user identity at login** **Chris Robins,** Senior Sales Engineer, EMEA, Beyond Identity
Devo	**Single source of truth – the fundamental building blocks for an effective security operations centre** **Nipun Gupta,** Cybersecurity Specialist, Devo Inc
Imperva	**APIs as your ultimate honeypot** **Pal Balint,** Senior Sales Engineer, Imperva
Netacea	**BLADE: Cutting through the complexity of business logic attacks** **Matthew Gracey-McMinn,** Head of Threat Research, Netacea, & **Cyril Noel-Tagoe,** Cyber Threat Evangelist, Netacea
Recorded Future	**The business of fraud: Sales of PII and PHI** **Lewis Brand,** Senior Sales Engineer, Recorded Future
Red Sift	**Why building a people-first security culture is the key to cyber-defence in 2022** **Engin Yilmaz,** Product Director, Red Sift
SenseOn	**Root cause analysis in moments, not days** **Brad Freeman,** Director of Technology, SenseOn

11:00 Networking and refreshments

11:30 **Building the UK as a global responsible cyber-power – the part industry plays**

Mary Haigh, CISO, BAE Systems

- The importance of agility and creativity in cybersecurity. To achieve stable, robust growth through digital transformation we must have resilient infrastructure that is secure by design. I will explore what this means in reality and how we can address the 'responsible' aspect of cyber-power in industry
- Agility and creativity requires a higher level of digital literacy and cyber-expertise. I will look at how that can be nurtured in organisations
- The challenge of delivering cybersecurity in large organisations. Building scalable systems requires a careful balance of central visibility and control with agile local decision making

11:50 **Stopping ransomware with Autonomous Response**

Toby Lewis, Head of Threat Analysis, Darktrace

- Recent ransomware threat trends, including double extortion and RDP attacks
- How Autonomous Response takes action to contain an emerging attack, even when security teams are out of office
- Real-world examples of ransomware detected by Darktrace AI – including a zero-day and an attack initiated on Christmas Day

12:10 **Accelerating digital transformation: How to reduce friction in every digital experience**

Ian Lowe, Director of Solutions Marketing, EMEA, Okta

- Find out how to strengthen your security posture
- Learn about the challenges we are facing when it comes to securing a dynamic workforce
- Deep dive into current case studies on how to reduce IT friction in identity

12:30 **Protecting people: The new perimeter**

Alistair Mills, Director, Sales Engineering, Northern Europe, Proofpoint

- Why social engineering dominates among today's cyber-threat actors
- How remote work and the move to the cloud has changed the nature of threats
- The ways organisations are building controls to better understand and protect people

12:50 **Education Seminars | Session 2** See pages 52 to 59 for more details

ManageEngine	**How to use the MITRE ATT&CK framework to stop ransomware** **Ram Vaidyanathan,** Cyber Risk and Security Expert, ManageEngine
Okta	**How identity can accelerate digital trust** **Ian Lowe,** Director of Solutions Marketing, EMEA, Okta
Picus Security	**The CISO's challenge – how to be more proactive with less** **Tim Ager,** VP of Sales, EMEA, Picus Security
Synack	**Hacking for the greater good: Using hackers to beat hackers** **Justin Shaw-Gray,** Sales Director for UKI and South Africa, Synack, & **Mark Walmsley,** Chief Information Security Officer (CISO), Freshfields Bruckhaus Deringer LLP
Tessian	**Master defence in depth: Supercharging the security of your Microsoft email environment** **Neil McRae,** Solution Engineer, Tessian
Vectra	**How AI-based 'Threat Detection & Response' finds and stops ransomware** **Steve Cottrell,** EMEA CTO, Vectra

13:30 Lunch and networking

14:30 **EXECUTIVE PANEL DISCUSSION** **Getting cybersecurity regulation right**

Andy Ng, Partner, Cyber, EY Consulting; **Fred Langford,** Director Online Technology, OFCOM; **Elaine Bucknor,** Group CISO and Group Director, Technology Strategic Services, Sky Plc; **Federico Iaschi,** BISO, Virgin Media O2

- Should regulators create more cybersecurity specific regulations instead of the current focus on data privacy?
- Is regulating the resilience of CNI perhaps a better way to address the problem of cybersecurity?
- What about the IoT? Is regulating operational technology feasible?
- How can regulators work more closely with both legislators and industry to come up with useful standards to help secure economies and society?

14:50 **Why human layer security is the missing link in enterprise security**

Ed Bishop, Chief Technology Officer and Co-founder, Tessian

- Email is every bit as crucial an environment to protect as the network and databases; once compromised, there can be lasting, costly, and damaging effects. Leaning on built in security controls of email platforms or legacy technology are insufficient in providing comprehensive protection against human-related threats over email
- Over 75% of firms report that 20% or more of email security incidents get past their existing security controls
- The findings from the commissioned study conducted by Forrester Consulting on behalf of Tessian recommends that organisations consider human layer security to be used
- Learn how human layer security technology will help you to feel more prepared to face email security threats and data loss incidents (accidental, negligent, or malicious) and demonstrate a higher level of maturity when it comes to readiness to prevent these damaging threats
- Learn how human layer security technology will increase your visibility into risky behaviour, automate threat detection and prevention, save your organisation from reputation damaging data breaches and hours of resource time monthly, and set you up for email security success with a focus on in-the-moment security coaching and preventative technology

15:10 **HEAT attacks: Examining the next class of evasive, adaptive web threats**

Jonathan Lee, Senior Product Manager, Menlo Security

- How has modern work given rise to HEAT attacks?
- What delivery mechanisms do these attacks leverage to evade detection?
- The impact of HEAT attacks on organisations of all sizes and sectors
- What can organisations do to prevent HEAT attacks?

15:30 **Education Seminars | Session 3** See pages 52 to 59 for more details

CrowdStrike	**How to reveal secrets from criminal forums and interrupt adversaries in their tracks** **James Burchell,** Senior Security Engineer, CrowdStrike
CybelAngel	**Finding the leaky data links in your supply chains – data security beyond perimeters** **Vijay Kishnani,** Lead Cyber Security Engineer, CybelAngel
HelpSystems	**HelpSystems Data Security Suite: Protecting your data with layered security solutions** **Nick Hogg,** Director of Technical Training, HelpSystems
Kenna Security	**Cisco SecureX + Kenna Security: Radical simplification in the new era of cybersecurity** **Stephen Roostan,** VP, EMEA, Kenna Security
OPSWAT	**File upload protection: A critical gap in web app security** **Adam Gurney,** Sales Engineer, OPSWAT

16:10 Networking and refreshments

16:30 **EXECUTIVE PANEL DISCUSSION** **CISO priorities for 2022**

Danielle Sudai, Cloud Security Operations Lead, Deliveroo; **Prakhar Chandra,** BISO, News UK; **Greig Sharman,** Chief Technology Officer, NSPCC; **Isaac Ng,** CISO, Southeastern Railway; **Neil Johnson,** Head of Security and Threat Solutions, TikTok

- Data privacy or security? How will companies view 'security' in the post-pandemic world?
- Hybrid working: problem solved or problem postponed?
- Is 2022 the year of Cloud? And have the security implications of Cloud been exaggerated?
- The future of the security stack

16:50 **Towards better cyber-resiliency: Digital transformation with risk reduction**

Raghu Nandakumara, Head of Industry Solutions, Illumio

- See how the attack surface is growing as technology use is changing
- Understand why a Zero Trust approach is essential to reducing this risk
- Identify how better security can be incorporated into your transformation

17:10 **Engaging with the board – getting the backing, finding the finance**

Lee Whatford, CISO, Domino's Pizza

- Why it's all about risk, or is it? Using the right language
- Shifting the tone – from IT security to business risk management
- Framework ideas – quantifying the ask

17:30 Networking and drinks reception **18:30** End of day one

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **Driving change at scale**

Pete Cooper, Deputy Director Cyber Defence, UK Cabinet Office

Pete has led and worked across global communities and driven change at scale, most recently on the first ever Government Cyber Security Strategy. In this talk he will walk through:

- The key approaches to success at scale
- Managing sectoral changes
- Developing scalable cybersecurity strategies

09:20 **Malicious bot attacks are becoming ever more frequent, and high profile**

Matthew Gracey-McMinn, Head of Threat Research, Netacea, & **Cyril Noel-Tagoe,** Cyber Threat Evangelist, Netacea

- Malicious bot attacks are becoming more frequent and high profile, with a slew of scalper bot attacks hitting the headlines since 2020, as attackers target in-demand items such as the Playstation 5 and even Covid-19 vaccine appointments
- According to Netacea's recent survey, 46% of enterprise organisations had experienced an account takeover attack in 2020. 58% of these businesses stated that the attacks had a known financial impact
- During our session, we will explore the scale of the account takeover attack problem, zoning in on credential stuffing and how these attacks are executed, with a live demonstration using real attacker tools
- We will then walk through the makeup of attacker tooling, explaining how they bypass defences and how they maximise the efficiency of their attacks
- We will discuss the impact on various sectors, including retail, telecommunications and financial services

09:40 **Why SOCs fail**

Brad Freeman, Director of Technology, SenseOn

- Poor SOC technology implementations critically hamper both people and processes, which leads to SOC failure
- Developing an efficient SOC is an engineering challenge. Bringing together tools, data and in house engineering to deliver a tailored solution specific business outcomes
- Hard learned lessons of implementing security operations. Insights into when they work well, when they don't, and why they don't
- Reveal of technology innovations relating to breakthroughs of unified telemetry and how it can change security operations

10:00 **Defence perspectives on future trends of cyber and e-crime**

Major General Ben Kite, Director of Intelligence Interoperability, Ministry of Defence

- Introduction and exploration of the breeding grounds for cyber-actors and threats they pose
- The unique cyber-challenges for defence
- How will technology change criminal behaviour?

10:20 **Education Seminars | Session 4** **See pages 52 to 59 for more details**

4Data Solutions	**Observability; a data driven approach to cloud security** **Ian Tinney,** CEO, 4Data Solutions
Cequence Security	**Frictionless API security strategies** **James Sherlow,** Systems Engineering Manager, EMEA, Cequence Security
Cofense	**Adaptive email security architecture: Moving from incident response to continuous response** **Alain Salesse,** Senior Sales Engineer, Cofense
Cybersixgill	**Chihuahuas VS. muffins: Developing AI solutions for threat intelligence problems** **Benjamin Preminger,** Product Manager, Cybersixgill
Darktrace	**Fast and furious attacks: Using AI to surgically respond** **Toby Lewis,** Head of Threat Analysis, Darktrace
Intel 471	**Back to the future** **Maurits Lucas,** Director of Product Marketing, Intel 471

11:00 Networking and refreshments

11:30 **'Threatcasting' looking and preparing for threats up to 10 years out**

Nick Coleman, Chief Security Officer for Real-Time Payments, Mastercard

- The Mastercard approach to threat forecasting
- How threatcasting works – an in-depth look
- An insight of recent threatcasts

11:50 **An inside look at the attack lifecycle**

Jason Steer, Principal Security Strategist, Recorded Future

- Learn how to monitor and alert on unusual or potentially malicious activity inside your organisation
- Specifically understand how credentials for your users can be stolen and sold
- Specifically understand how Initial Access Broker posts can be reviewed to protect your organisation
- Discover how using threat intelligence can provide insights to help your organisation detect potential events before they cause serious business impact

12:10 **DORA: Your framework for smart thinking**

Dr Rois Ni Thuama, Head of Cyber Governance, Red Sift

During this session, Rois will explore:

- Why you should listen to the FBI's warnings
- Promoting smarter thinking with DORA
- How DORA will reduce business disruption
- The cost of doing nothing… from civil litigation and fines to criminal penalties

12:30 **EXECUTIVE PANEL DISCUSSION** **Future-proofing the CISO**

Helen Rabe, CISO, Abcam; **David Whitelegg,** European Security Officer, Compass Group; **Zibby Kwecka,** Head of Information Security, Heineken UK; **Jon Townsend,** CIO, National Trust; **Simon Goldsmith,** Director for Information Security, OVO Energy

- How has the evolution of the threatscape and security technology affected the role of the CISO in the last five years?
- What are the most important skills and qualities CISOs will need to possess over the next five years?
- How must the organisation and staffing of cybersecurity teams change? (bigger, smaller, skillsets, diversity?)

12:50 **Education Seminars | Session 5** **See pages 52 to 59 for more details**

BeyondTrust	**The seven perils of privilege** **Brian Chappell,** Chief Security Strategist (CSS), EMEIA & APAC, BeyondTrust
FireMon	**Improving security outcomes and eliminating security headaches through a threat-led approach** **Bryan Littlefair,** CISO & Cybersecurity Consultant, presenting on behalf of FireMon
Illumio	**How isolation stops the spread of ransomware** **Trevor Dearing,** Director of Critical Infrastructure Solutions, Illumio
Menlo Security	**The next class of browser-based attacks** **Brett Raybould,** Head of Solutions (EMEA), Menlo Security
Proofpoint	**Ransomware: One of your biggest risks – don't let it in** **Alistair Mills,** Director, Sales Engineering, Northern Europe, Proofpoint

13:30 Lunch and networking break

14:30 **EXECUTIVE PANEL DISCUSSION** **Securing financial services**

Crawford Thomas, Global Head of Cyber Threat Intelligence, Credit Suisse; **Ruth Anderson,** Director Group Operational Resilience and Security, Lloyds Banking Group; **Jill Robertson,** Head of Information Security Change Team, Metro Bank

- How do new resilience regulations help in the battle against cybercriminals?
- Does cybersecurity fit naturally into the three lines of defence model?
- Third-party dependency: do we need to talk about Cloud oligopoly?
- How can we collaborate when regulators and legislators make it so hard?

14:50 **Supply chain cybersecurity: Reduce your risk**

Chris Waynforth, Area VP, EMEA North, Imperva

Why supply chain attacks affect every business and protecting against them is everyone's business – not just security. Hear

- How to minimise the software supply chain risk, without business impact
- How to protect the application layer – a key attack vector
- What new technologies exist to defend against this critical risk

15:10 **Why your MFA will not keep the bad guys out**

Chris Robins, Senior Sales Engineer, EMEA, Beyond Identity

- MFA requirements have changed
- Cybercriminals have become more sophisticated in their attacks, and traditional MFA that relies on passwords and other weak factors can't keep up
- Remote working has expanded and rapid cloud adoption demands that companies ensure the identity of the user behind every device, and assess the level of risk before access
- Unlike traditional MFA, Beyond Identity can protect your data from advanced attacks
- Traditional MFA relies on weak factors like passwords and one-time codes. Beyond Identity eliminates passwords and only uses strong factors like asymmetric cryptography and biometrics to protect your organisation from phishing, ransomware attacks, and other password-based attacks

15:30 Networking and refreshments

15:50 **The FBI's overseas posture**

Eric Smithmier, Assistant Legal Attaché, FBI London, Cyber Division, & **Jensen Penalosa,** Assistant Legal Attaché, FBI

- Coordination with UKIC partners
- Public/private sector engagement
- Cyber-threat intelligence sharing

16:10 **Cybersecurity, achieving security convergence in interesting times**

Ian Shaw, Head of Risk and Security, South East Coast Ambulance Service, NHS Foundation Trust

- The challenge of truly integrating security and creating a converged solution
- The human component within cybersecurity, why EQ is as critical as IQ
- Early observations on how COVID has skewed risk perception

16:30 Chairman's closing remarks and Congress close

Education seminars

Over two days 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: 2nd March | 10:20–11:00

Beyond Identity

SESSION 1
2nd March
10:20–11:00

Beyond Identity's passwordless MFA: The only way to positively verify user identity at login

Chris Robins, Senior Sales Engineer, EMEA, Beyond Identity

MFA requirements have changed. Cybercriminals have become more sophisticated in their attacks, and traditional MFA that relies on passwords and other weak factors can't keep up. Remote working has expanded and rapid cloud adoption demands that companies ensure the identity of the user behind every device, and assess the level of risk before access. Traditional MFA relies on weak factors like passwords and one-time codes, Beyond Identity eliminates passwords and only uses strong factors like asymmetric cryptography and biometrics to protect your organisation from phishing, ransomware attacks, and other password-based attacks.

In this seminar you'll learn how to:

- Stop unknown users and devices from authenticating – block malevolent access attempt
- Enforce and prove compliance – force adherence to regulations
- Simplify roll out, empower your users – deploys within minutes, allows users to self enroll
- Remove productivity killers – no need to locate a 2nd device, fish out a code or link
- Reduce cost – no more forgotten password lock outs!

Devo

SESSION 1
2nd March
10:20–11:00

Single source of truth – the fundamental building blocks for an effective security operations centre

Nipun Gupta, Cybersecurity Specialist, Devo Inc.

How effective is your security operations and your ability to gather evidence, investigate and find source data?

If unsure, you're not alone. Combating today's threats requires new approaches to how your SOC manages its data, analytics, and expertise.

Join Devo as we explore innovative ways your security team can thrive in the era of massive data growth, talent shortage, and constantly evolving threats.

- Cloud-based solutions scale to achieve the critical full visibility into threats, giving you a single source of truth
- Analytics that use automation and machine learning uplift analysts' performance, saving your security team valuable time
- Community expertise augments your tribal knowledge to quickly resolve threats, helping you bridge the industry talent gap

Imperva

SESSION 1
2nd March
10:20–11:00

APIs as your ultimate honeypot

Pal Balint, Senior Sales Engineer, Imperva

How the use of the accelerator of all modern web applications goes horribly wrong, and what to do to prevent it.

- What are some of the popular API security measures and why they are not enough?
- How to recognise data leakages and what to do to counter them
- How to spot irregular behaviour in both B2B and B2C APIs

Netacea

SESSION 1
2nd March
10:20–11:00

BLADE: Cutting through the complexity of business logic attacks

Matthew Gracey-McMinn, Head of Threat Research, Netacea, &
Cyril Noel-Tagoe, Cyber Threat Evangelist, Netacea

The bot attack landscape is growing in maturity, and as it does it's crucial that bot management vendors develop and implement sophisticated bot defence systems to combat the growing threat. To facilitate this next phase of bot defence, we have developed a bot

management framework, built with the combined input of vendors and influencers throughout the industry.

- Taking inspiration from the MITRE ATT&CK Framework, the Business Logic Attack Definition (BLADE) Framework captures all automated bot threats and their life cycle in a series of comprehensive kill chains
- The BLADE Framework enables all bot vendors to take a proactive approach to tackling the malicious bot threat, with a greater shared understanding and knowledge that ultimately empowers businesses
- During this Educational Seminar, we will introduce the BLADE Framework, discussing how it captures automated bot threats using a series of kill chains, and how a bot framework will help businesses fight sophisticated bots and protect customers from automated threats
- We will draw upon use cases where other organisations have successfully employed the framework

Recorded Future

SESSION 1
2nd March
10:20–11:00

The business of fraud: Sales of PII and PHI

Lewis Brand, Senior Sales Engineer, Recorded Future

- Gain knowledge on how personally identifiable information (PII) and patient health information (PHI) are highly sought after data across criminal sources, both on the clearnet and dark web
- Learn how our research identified that threat actors use various attack vectors, including social engineering and infostealer malware variants, to obtain victim PII or PHI
- Understand how, once this data has been harvested, threat actors monetise it through traditional cybercriminal sources (dark web, including forums, marketplaces, and shops) and messaging platforms
- Discover how threat actors interested in buying and selling PII and PHI data continue to improve their tactics, techniques, and procedures (TTPs), with vendors selling customised services and methods that include access to accounts with sensitive user data, methods to defeat security measures, and counterfeit documentation

Red Sift

SESSION 1
2nd March
10:20–11:00

Why building a people-first security culture is the key to cyber-defence in 2022

Engin Yilmaz, Product Director, Red Sift

2022 looks set to be another year where organisations will face an onslaught of cyber-attacks. With phishing attacks still the number one cause of security breaches, and 85% involving the human element, businesses need clear, concrete advice on how to act.

- The importance of building a people-first cybersecurity culture
- Why phishing awareness training and Secure Email Gateways aren't enough
- How new 'in the moment' threat intelligence products can help to mitigate human error

SenseOn

SESSION 1
2nd March
10:20–11:00

Root cause analysis in moments, not days

Brad Freeman, Director of Technology, SenseOn

Identifying the root cause of security events quickly and accurately is a critical success factor for security operations. By not relying on true root cause analysis, we hold significant compound risk every time we are 'almost certain' that an event was benign. This education seminar discusses key operational problems with strategic impact in existing security operations teams including how they can be measured, how this can be used as a basis for threat hunting, and how it can help with SOC efficiency improvements.

In this session you will:

- Understand why root cause analysis is important for process improvement and risk reduction.
- Consider new metrics and different methods of measuring SOC efficiency beyond existing detection and response metrics such as MTTR & MTTD.
- Apply root cause analysis as the basis of threat hunts across complex networks and as a driver for security improvements

Session 2: 2nd March | 12:50–13:30

ManageEngine

SESSION 2
2nd March
12:50–13:30

How to use the MITRE ATT&CK framework to stop ransomware

Ram Vaidyanathan, Cyber Risk and Security Expert, ManageEngine

With the MITRE ATT&CK framework, you can understand the modus operandi of potential attackers. But how exactly can you use this framework to stop ransomware?

A typical ransomware attack has five stages: Initial exploitation, installation, backup destruction, encryption, and extortion. In this talk, I will try to map each

of these stages to the different tactics and techniques identified in the MITRE ATT&CK. The objective is to understand the intricacies of ransomware so that you can defend against it effectively.

Key learnings:
- Tactics, techniques and procedures covered in the MITRE ATT&CK framework
- What makes ransomware such a big threat for organisations?
- Mapping the 5 stages of ransomware to the MITRE ATT&CK
- Tips for effective defence

Okta

SESSION 2
2nd March
12:50–13:30

How identity can accelerate digital trust

Ian Lowe, Director of Solutions Marketing, EMEA, Okta

In today's digital-first world, customers and citizens are being asked to share their data in new ways and for new purposes. While most are increasingly comfortable interacting online they expect secure, consistent services in return for their valuable personal information. Seamless digital experiences are critical to securing our trust – and this starts with identity

In this session we will look at:
- What are the top drivers of trust online?
- Whether digital IDs are winning acceptance
- Who's responsible for protecting personal digital identity

Picus Security

SESSION 2
2nd March
12:50–13:30

The CISO's challenge – how to be more proactive with less

Tim Ager, VP of Sales, EMEA, Picus Security

In cybersecurity, being proactive is often easier said than done. With so much to do to manage your organisation's security posture day-to-day, it can be almost impossible to find the time to stay on top of the latest threat intelligence and apply it to improve your defence.

Join Tim Ager, VP at Picus Security, to learn how Breach and Attack Simulation (BAS) technology is helping CISOs to address this very challenge by automatically validating the effectiveness of security controls and by reducing the strain on security operations.

Learn how BAS is helping security teams to:
- Validate preparedness against the latest threats
- Swiftly address prevention and detection gaps
- Measure and benchmark threat coverage and visibility
- Rationalise investments to improve efficiency and value
- Demonstrate assurance to the boardroom

Synack

SESSION 2
2nd March
12:50–13:30

Hacking for the greater good: Using hackers to beat hackers

Justin Shaw-Gray, Sales Director for UKI and South Africa, Synack Inc, & **Mark Walmsley,** Chief Information Security Officer (CISO), Freshfields Bruckhaus Deringer LLP

For CISOs, designing security for a decentralised workforce requires revisiting where and how security and risk management leaders direct their efforts. In this session, Synack's Justin Shaw-Gray and Mark Walmsley, CISO, Freshfields Bruckhaus Deringer LLP. will discuss the security challenges CISOs are facing in today's business climate and how Synack's innovative crowdsourced security model and continuous pen testing offering address these challenges.

Attendees will learn
- How concerns and security implications for organisations and their remote workforce have played a role in security decisions
- How to secure your organisation while managing a remote workforce from the executive's perspective
- How agile businesses are able to respond quickly to opportunities or threats
- How security researchers are playing a pivotal role in securing company's assets

Tessian

SESSION 2
2nd March
12:50–13:30

Master defence in depth: Supercharging the security of your Microsoft email environment

Neil McRae, Solution Engineer, Tessian

- Hear about the benefits of joining forces between machine learning and threat intel to bring you closer to becoming a master of defence in depth!
- We will discuss how to build high impact defence augmenting Microsoft with behavioural technologies
- How threat attackers are actively deploying new BEC, ransomware, and ATO attacks to target enterprise companies
- How to own the best practices of multi-layered security to fulfil the security requirements of cloud API architecture

Vectra

SESSION 2
2nd March
12:50–13:30

How AI-based 'Threat Detection & Response' finds and stops ransomware

Steve Cottrell, EMEA CTO, Vectra

Cybercriminals are always looking for easy targets and opportunities to steal personal information. With no application, network, or data centre being invulnerable, decision-makers often harbour a false sense of security about their ability to fend off hackers – especially when they're not armed with the necessary tools to succeed.

During our presentation we will cover:

- How prepared your organisation is to detect and respond to a ransomware attack
- What approaches other organisations are taking to stop ransomware gangs
- How to detect and respond to Ransomware before it impacts you

Session 3: 2nd March | 15:30–16:10

CrowdStrike

SESSION 3
2nd March
15:30–16:10

How to reveal secrets from criminal forums and interrupt adversaries in their tracks

James Burchell, Senior Security Engineer, CrowdStrike

A thriving e-Crime ecosystem of services, distribution, and monetisation makes it easy for malicious operators to 'set up shop', join the cybercrime scene, and target victims. In this session, we will focus on one specific use case of monitoring access brokers, following the bread crumbs they leave behind, and identifying critical threat activity in a high-noise, fast-moving criminal ecosystem.

- Understand threat actor operations and value chains of specialised services
- Identify and interpret the bread crumbs operators leave behind when selling illegitimate merchandise
- Refine high noise and difficult to access environments to actionable insights
- Learn steps to form a monitoring strategy that follow the bread crumbs

CybelAngel

SESSION 3
2nd March
15:30–16:10

Finding the leaky data links in your supply chains – data security beyond perimeters

Vijay Kishnani, Lead Cyber Security Engineer, CybelAngel

Ask yourself, where is the risk in sharing data with third parties? Is the risk the third party, or is the risk having your data leak? The real danger is the data leak! The leak being at a third party just makes it more challenging to locate. Instead of making third parties jump through long and sometimes unproductive audits, a new perspective is needed – a data risk first approach.

A data risk first approach focuses on locating whatever data matches your organisation's regardless of where it appears. By focusing on which data matches, you gain visibility and protection far beyond a company's perimeter into third, fourth, and fifth parties. This increase in visibility frees cybersecurity teams from choosing which partners get monitoring.

You will learn:

- Why your risk is with the data, not third parties
- What is a data risk first approach?
- How DRPS tools can assist in a data risk first approach

HelpSystems

SESSION 3
2nd March
15:30–16:10

HelpSystems Data Security Suite: Protecting you data with layered security solutions

Nick Hogg, Director of Technical Training, HelpSystems

Today's organisations have to protect their data from a host of external threats and internal risks. Using a layered approach to our data security still makes a huge amount of sense, even as we move more of our data to the cloud.

By using different detection and mitigation techniques, we provide resilience for those instances when a system or manual process becomes compromised, because you have other systems there to catch and prevent the breach.

This session will cover:

- The data security challenges that organisations face
- How people, processes and technology can be used in order to protect data throughout its entire lifecycle

- How the HelpSystems Data Security Suite can assist with protecting your sensitive data
- How organisations can regain control of their data by identifying and classifying sensitive data
- Attend this session for inspiration and ideas on how to more effectively protect your data and get the most out of your data security investments

Kenna Security

SESSION 3
2nd March
15:30–16:10

Cisco SecureX + Kenna Security: Radical simplification in the new era of cybersecurity

Stephen Roostan, VP, EMEA, Kenna Security

Cybersecurity is a complex challenge. What's needed is a way to radically simplify security operations to be simple, automated, and democratised. So, no matter the complexity of your IT environment, and how many threats may be targeting your organisation, protecting it shouldn't be difficult.

Cisco recognises this need and is defining a path forward. By integrating Kenna Security's acclaimed risk-based vulnerability management platform, Cisco's SecureX will help organisations solve a notoriously difficult piece of the security puzzle to accelerate response time for cyber-readiness.

In this session, Stephen Roostan, Vice President for EMEA at Kenna Security, now part of Cisco, details why Cisco's acquisition of Kenna is a pivotal move for customers and the industry as a whole.

- Real-world threat intel, machine learning, and predictive analytics help teams identify and prioritise their riskiest vulnerabilities
- Remediation teams will know what to patch and when, saving time, money, and resources
- Integrating enterprise security management solutions into one centralised location breaks down silos and extends detection and response capabilities
- Automated workflows help lower organisational risk profiles, improve collaboration between Security and IT, and shrink their attack surfaces
- Kenna Risk Scores help stakeholders clearly assess the relative risk of a specific vulnerability, asset class, workgroup, or organisation as a whole
- To speed decision making with prioritisation of vulnerability data based on threat intelligence and asset business value
- Adding Kenna Security to SecureX extends the broadest XDR capabilities in the industry

OPSWAT

SESSION 3
2nd March
15:30–16:10

File upload protection: A critical gap in web app security

Adam Gurney, Sales Engineer, OPSWAT

Digital transformation is a must for today's organisations, resulting in a migration from paper-based to digital documents. Millions of documents are now being shared among collaborators weekly and monthly – uploaded to either a web portal, customer portal (insurance or mortgage applications) or support portal (attaching files to your support ticket). At the same time, an enormous amount of effort is invested into building high-availability, fault-tolerant systems and securing them. However, file upload remains a major attack vector and far too often is not covered by traditional web application defences.

In this seminar, Adam Gurney, Sales Engineer at OPSWAT will cover three types of risks to web applications and how to apply a Zero Trust model to both users and the files they upload and the devices from which these uploaded files originate. Risks from:

- Threat actors who submit malicious files to gain access to the organisation's IT infrastructure
- User who submits sensitive data in violation of an application's terms of service
- Inadvertent hosting and distributing malicious files uploaded by a threat actor

Session 4: 3rd March | 10:20–11:00

4Data Solutions

SESSION 4
3rd March
10:20–11:00

Observability; a data driven approach to cloud security

Ian Tinney, CEO, 4Data Solutions

Securing cloud data is a sizable challenge. Doing it properly means processing huge amounts of data – which, given the associated cost, can become unviable.

Being smart with your data by being able to source, reduce, shape, enrich and route it with complete flexibility and agility enables you to overcome this problem and make full data security viable for your organisation.

We explore this security challenge in more detail looking at:

- Building an inventory
- Recording the state

- Monitoring for change
- Securing user accounts
- Curating data
- Observing

And what technologies will help deliver all of this.

What you will learn:
- Dealing with the 'analysis versus privacy' dilemma
- Cloud adoption drivers; the electric car of the data world (doing it for the greater good)
- Securing data – the need for flexibility, prioritisation and protection
- Borrowing from APM – taking an observability approach to security data
- Data use cases – different storage for different data needs
- Organisational security – insights into a data driven approach to cybersecurity

Cequence Security

SESSION 4
3rd March
10:20–11:00

Frictionless API security strategies

James Sherlow, Systems Engineering Manager, EMEA, Cequence Security

Organisations are rapidly adopting an API-first development strategy and methodology because of the power, flexibility and efficiency that APIs provide. The shopping, finance, manufacturing or marketing apps we use every day are all based on APIs, connecting back to compute resources located elsewhere – be it the cloud, the data centre or both. Critically, threat actors leverage APIs for the exact same reasons that developers do. APIs are susceptible to a range of automated attacks and vulnerability exploits that can lead to data loss and system compromise.

To protect existing and future APIs, organisations need to implement forward-looking API security strategies that are frictionless and transparent to the development team. This session will delve into the different approaches to protecting APIs from various security risks and how security teams can make strategic decisions on the depth of protection deployed.

- Discover: Complete visibility of public-facing APIs, their location & service categories
- Detect: Identification of sophisticated API attacks targeting apps & data
- Defend: Ability to respond in real-time & block attacks

Cofense

SESSION 4
3rd March
10:20–11:00

Adaptive email security architecture: Moving from incident response to continuous response

Alain Salesse, Senior Sales Engineer, Cofense

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.

Join us for this informative session that walks through the benefits of implementing an adaptive security architecture and risk framework, and how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity.

This session will cover:
- What is adaptive security architecture
- Objectives of adaptive security architecture
- Risk framework
- The current situation in email and phishing security
- Implementing adaptive security architecture and risk framework with Cofense

Cybersixgill

SESSION 4
3rd March
10:20–11:00

Chihuahuas VS. muffins: Developing AI solutions for threat intelligence problems

Benjamin Preminger, Product Manager, Cybersixgill

AI and automation are well-known industry buzzwords, but how can they actually benefit modern threat intelligence practices and capabilities? In this interactive workshop we will quickly run through high-level concepts in AI/ML and automation, and then deep-dive into some of the practical challenges and opportunities AI offers to combat cyber-threats. Leveraging the speaker's real-world experience of developing home-grown AI solutions, the workshop will strive to answer key questions such as:

- How can organisations prioritise work on AI initiatives?
- What challenges can I expect in developing AI?
- Is it worth it?

Darktrace

SESSION 4
3rd March
10:20–11:00

Fast and furious attacks: Using AI to surgically respond

Toby Lewis, Head of Threat Analysis, Darktrace

Fast-moving cyber-attacks like ransomware can strike at any time, and security teams are often unable to react quickly enough. Join Toby Lewis, Head of Threat Analysis at Darktrace, to learn how Autonomous Response uses Self-Learning AI's understanding of 'self' to take targeted action to stop in-progress attacks, without disrupting your business.

- 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

Intel 471

SESSION 4
3rd March
10:20–11:00

Back to the future

Maurits Lucas, Director of Product Marketing, Intel 471

Those who do not learn from history are doomed to repeat it, the saying goes. On this, the 20th edition of the e-Crime Congress, join us in this session as we look at the lessons from the past to predict the near future.

From the first case of nation-state hacking – which happened earlier than you may think – to the rise of financially motivated cybercrime and the ecosystem of products, services and goods that arose to facilitate it, we'll plot the trends and use them to predict the future.

From banking botnets to WhatsApp fraud, Ransomware-as-a-Service, cryptocurrencies and the blurring lines between nation-state and cybercriminals to IoT and everything as a service: the future is already here! How about our understanding of its threats?

Key takeaways:

- How far we've come from humble beginnings both in the type of attacks but also in the tooling we have at our disposal
- First, there were nation-state actors and cybercriminals — now the two are mixing and blurring that it is hard to tell which is which anymore. Sometimes they don't even seem to know themselves!
- The impacts of attacks are increasing, but at the same time over the past 6 months, some new ground rules have started to emerge
- What future trends we can distil from recent events. No matter what happens, fundamental changes have occurred that come with consequences

Session 5: 3rd March | 12:50–13:30

BeyondTrust

SESSION 5
3rd March
12:50–13:30

The seven perils of privilege

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

Cybercriminals are opportunistic and merciless. They will target security vulnerabilities such as weak passwords or unnecessary administrator rights. The National Cyber Security Centre recently found that 23.2 million victim accounts worldwide used 123456 as the password, and many companies still provide full admin rights to employees, despite the widely known risks involved. In this session, we will cover the 'Seven perils of privilege' – addressing what they are, their causes, the effects of leaving them unaddressed, and (most importantly) solutions.

Join us to learn:

- What the seven perils of privilege are and why they matter
- Why poor password practices, lax cloud security (and much more) create risk
- How to mitigate these risks and protect your organisation

FireMon

SESSION 5
3rd March
12:50–13:30

Improving security outcomes and eliminating security headaches through a threat-led approach

Bryan Littlefair, CISO & Cybersecurity Consultant, presenting on behalf of FireMon

The world has changed. And so has the threat landscape. Organisations are facing a landscape of scarce security resources, increased pressure from regulators, and an unprecedented volume of threats. And the reality is, we can no longer rely on the 'old way' of managing security. Change brings challenges, and this is being felt from the boardroom down.

For organisations to improve security outcomes, they need to improve security operations, and that starts with a threat-led approach.

Join us as we explore:

- The global threat of change: The real-life impacts to businesses right now
- A threat-led approach: Best practices in how to improve your security operations and improve your security outcomes
- Avoid violations. Avoid risk. Avoid fines. How to get a real handle on your risk profile by adopting a threat-led approach to security

Illumio

SESSION 5
3rd March
12:50–13:30

How isolation stops the spread of ransomware

Trevor Dearing, Director of Critical Infrastructure Solutions, Illumio

- See how to stop the propagation of ransomware
- Identify the potential weaknesses in your infrastructure
- Build a more resilient defence against future threats

Menlo Security

SESSION 5
3rd March
12:50–13:30

The next class of browser-based attacks

Brett Raybould, Head of Solutions (EMEA), Menlo Security

There are two distinct characteristics that all threat actors tend to share. First, they focus on avoiding detection by any means. Second, while some go after specific targets, many opt to aim their tactics at the vectors that will reap the greatest rewards. After all, a big pond with many fish increases everyone's chances of success.

Between July and December 2021, there was a 224% increase in highly evasive adaptive threats (HEAT) attacks – a class of cyber-threats targeting web browsers as the attack vector. While malware once had to be downloaded to pose a real risk, now, it's a dynamically generated threat toolkit built in the web where employees are productive.

In this session you will:

- Discover the anatomy of recent browser-based attacks
- Learn why network security today is broken
- Experience a live demo that enables you to discover the technology approach proven to eliminate these threats

Proofpoint

SESSION 5
3rd March
12:50–13:30

Ransomware: One of your biggest risks – don't let it in

Alistair Mills, Director, Sales Engineering, Northern Europe, Proofpoint

Mitigating the risk of ransomware to your business has become the job of every security product and service available today. But measuring the impact of technology on the risk of exposure is rarely achievable until it's too late.

Endpoint security and EDR solutions will help you respond once you already have a ransomware problem. So how do you measurably reduce the risk of the problem occurring before it's too late?

- What are the common attack vectors for ransomware?
- How you can quickly reduce your risk □

Speakers and panellists

Tim Ager

VP of Sales, EMEA, Picus Security

Tim has been working in the cybersecurity industry for over 20 years and has a passion for helping organisations defend against the latest cyber-threats. He is an advocate of continuous security validation and how it empowers security teams to better understand, measure and mitigate risks.

Ruth Anderson

Director, Group Operational Resilience and Security, Lloyds Banking Group

Ruth currently leads the Group's Operational Resilience and Security teams, delivering security and identity and access management policies/controls, security education and awareness, operational resilience policy and framework, and leading the Group's response to the new regulatory requirements for operational resilience. Ruth has been with LBG for five years in both operational and 2LoD roles. Ruth has extensive experience of working to address security and operational resilience risks across financial services including developing risk management frameworks, leading education and awareness campaigns, building 3rd party assurance activities, establishing maturity models and leading the delivery of penetration testing and red teaming exercises.

Prior to joining Lloyds Banking Group, Ruth worked for five years in KPMG leading a successful global practise in cyber-maturity and third-party risk assessments and worked with a range of financial services clients. Ruth began her career in the military spending seven years in the Intelligence Corps including seeing active service in the Middle East before joining law enforcement as part of the Child Exploitation and Online Protection Centre where she led the first national intelligence function supporting operations against online child sexual exploitation. She was involved in ground breaking work, coordinating activity across international law enforcement, intelligence agencies, children's charities and industry in order to address the increasing problem of child sexual exploitation.

Pal Balint

Senior Professional Services Consultant, Imperva

Pal Balint is a combat trained security architect with strong engineering background that he had gathered during his 15 years of service in the field. Being a Datasec and Appsec SME, Pal's view has always been that one cannot exist without the other and that end-to-end threat modelling is the key to securing each artefact of a system appropriately.

Ed Bishop

Chief Technology Officer and Co-founder, Tessian

Ed is the Chief Technology Officer and Co-founder of human layer security company Tessian. He is responsible for leading the engineering, product and data science teams. Following a career in M&A, Ed co-founded the company and built the early platform that uses machine learning to protect people from risks on email like data exfiltration, accidental data loss and phishing.

Lewis Brand

Senior Sales Engineer, Recorded Future

Lewis Brand, Senior Sales Engineer at Recorded Future, has over eight years in the IT industry, where he has specialised in liaising with enterprise customers across EMEA. Before his career at Recorded Future, Lewis operated as a Sales Engineer at Tenable, with his primary focus centred around vulnerability management.

He has previously provided continuous IT support for SMBs, which gave him a unique perspective when engaging with customers by providing insight from both a vendor and end-user viewpoint. Lewis most recently passed his SANS GPEN certification on Ethical Hacking and Network Penetration.

Elaine Bucknor

Group CISO and Group Director, Technology Strategic Services, Sky Plc

Elaine is Sky Plc's Group Chief Information Security Officer and a Group Director in its Technology Executive team. She has overall responsibility for cybersecurity at Sky, covering all aspects of information security strategy, governance, risk and compliance. Alongside this critical role, she leads a core team of technology specialists who work across the 5,000+ people in the Technology Group to define a cohesive technology strategy and operating model. Her team ensures the development and delivery of Sky's large-scale international technology programmes across digital platforms, networks, infrastructure and IT. With over 20 years in operational and strategic technology consultancy roles, Elaine has worked across numerous sectors from defence to financial services media and telecommunications. Beginning her career writing code and designing and architecting technology platforms and systems, she then moved onto consulting in business change and technology, directing and delivering major programmes of work, before joining Sky's senior leadership team. Elaine is a key sponsor in Sky's drive to encourage women into technology-based careers. She has been at the forefront of Sky's Get into Tech initiative and serves as a mentor to many women looking to progress to more senior roles. She is also a member of a number of industry councils in the technology and cybersecurity sectors as well as holding two non-executive positions.

James Burchell

Senior Security Engineer, CrowdStrike

James is a passionate, multidisciplinary security specialist who has the ability to de-mystify the complexity that shrouds many IT security challenges. With many years of experience in both military and corporate cybersecurity worlds, he has the knowledge to help you protect your brand's reputation, data and intellectual property. The battle for IT security won't end any time soon, James strives to make sure that everyone understands the challenges and are equipped to protect themselves from the most advanced modern threats.

Prakhar Chandra

Director of Cyber Risk, News UK

Prakhar is the Director of Cyber Risk for News UK. As part of his role, he looks after the cybersecurity and risks associated with one of the largest media organisations in the UK, with interests in print, digital and broadcasting. He has almost a decade of experience across the cybersecurity, risk, audit, and data protection domains. He is a trusted advisor to the NUK Executive Board on matters relating to cybersecurity, including but not limited to third-party management, risk management and compliance.

Prior to joining News UK, he worked with a British cybersecurity boutique firm and worked on a variety of projects assessing third-party risk, organisational security risk, 5G security as well as conducting secure code reviews in multiple countries across Europe and Asia. Prior to this, Prakhar worked for two of the Big 4 accounting firms. He is an engineer by education and also has two masters degrees in Information Security and Digital Signal Processing.

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.

Nick Coleman

Chief Security Officer for Real-Time Payments, Mastercard

Nick Coleman is the Chief Security Officer for Real-Time Payments at Mastercard. Mr Coleman was formerly the National Reviewer of Security for the UK Government and authored 'The Coleman Report' published in the Houses of Parliament.

He previously also worked at IBM where he was Global Cloud Security Leader. He is a Visiting Professor at Lancaster University. He has served on the World Economic Forum Global Future Council and recently led work for the forum on securing the future of Artificial Intelligence. He holds an MBA with distinction from Manchester Business School.

Pete Cooper

Deputy Director Cyber Defence, UK Cabinet Office

Pete is Deputy Director Cyber Defence within the Government Security Group in the UK Cabinet Office where he looks over the whole of the Government sector and is responsible for the Government Cyber Security Strategy, standards, assurance and policies as well as responding to serious or cross government cyber-incidents. Across a diverse military, private sector and government background, he has worked on everything ranging from cyber-operations, global cybersecurity strategies and advising on the nature of state vs state cyber-conflict.

His leadership efforts across industry, public sector and the global hacker community include founding and leading the Aerospace Village at DEF CON, the world's largest hacker conference and Cyber 9/12 UK, the UK's first national cyber-strategy competition. He has a post grad in Cyberspace Operations from Cranfield University, is a Non-Resident Senior Fellow at the Cyber Statecraft Initiative of the Scowcroft Centre for Strategy and Security at the Atlantic Council and a Visiting Senior Research Fellow in the Dept of War Studies, King's College London.

Steve Cottrell

EMEA CTO, Vectra

As the EMEA CTO at Vectra, Steve Cottrell assists customers, prospects, and security communities to identify key security pain points, while helping evolve security strategies in support of digital transformation and cloud adoption. Steve has worked as a CISO in large enterprises for the past 15 years, bringing a wealth of experience to the Vectra team from key sectors including communications, telecoms, and insurance. Prior to working at Vectra, Steve undertook CISO roles at Fujitsu, Vodafone, Aviva, and Admiral Insurance. Before this, he was a security specialist at Intel.

Trevor Dearing

Director of Critical Infrastructure Solutions, Illumio

Trevor is an experienced technology expert, who has been at the forefront of new technologies for nearly 40 years. From the first PCs through the development of multi-protocol to SNA gateways, initiating the deployment of resilient token ring in DC networks and some of the earliest use of firewalls. Working for companies like Bay Networks, Juniper and Palo Alto Networks, he has led the evangelisation of new technology. Now at Illumio, he is working on the simplification of segmentation in Zero Trust and highly regulated environments.

Eleanor Fairford

Deputy Director for Incident Response, NCSC

A generalist civil servant for the past 18 years, Eleanor has undertaken a range of policy and security roles at home and overseas in immigration, security policy and corporate services. Joining the NCSC when it began, Eleanor was responsible for the cyber-assessment function providing reports on the cyber-threat landscape for strategic decision makers in government. Eleanor took on the leadership of the Incident Management function within the NCSC and is responsible for leading the organisation's response to cyber-incidents.

Brad Freeman

Director of Technology, SenseOn

Brad has over a decade of experience in conducting national cybersecurity investigations across critical national infrastructure and telecommunications sectors. He has led threat hunting teams at corporations such as BT, managed security operations at EE as well as performing incident response on offshore oil & gas platforms. Drawing upon his extensive experience and knowledge, including CISSP & CISM certifications, Brad leads the threat analytics team at SenseOn. He applies ML and AI to automate the process of detecting and investigating cyber-adversaries, overall specialises in uncovering advanced actors within customer environments. Brad was named 'Security Specialist of the Year' in 2019 for his work developing the SenseOn threat detection platform.

Simon Goldsmith

Director for Information Security, OVO Energy

Simon is the Director for Information Security at OVO Energy. His background is in systems engineering in military and national security. Over 20 years, he has built information security and counter financial crime solutions and programmes in government, financial services, energy and global retail. Simon has lived and worked in UK, mainland Europe, Middle East and Asia. Simon believes security is a team sport and often draws on his experiences in professional rugby for inspiration in his work on cybersecurity and resilience.

Matthew Gracey-McMinn

Head of Threat Research, Netacea

Matthew Gracey-McMinn is an experienced Cyber-Threat Intelligence professional with an MPhil from the University of Oxford. In his current role at Netacea, he researches and investigates the impact of malicious bots on online businesses and their customers, having previously worked for ReliaQuest with the world's largest companies responding to global cybersecurity incidents.

Nipun Gupta

Cybersecurity Specialist, Devo

Nipun Gupta is a senior security leader leading Devo's product and growth strategy for partnerships, and is based in London, UK. Prior to joining Devo, he served as the Vice President, Global Cyber Security Strategy & Innovation Lead at Deutsche Bank in their Silicon Valley office. He led the bank's cybersecurity transformation efforts and provided strategic advice to tech leadership while sourcing/implementing early-stage solutions. He works closely on product and GTM strategy with the brightest founders, startups and peers in security. Prior to working in financial services, he was at Deloitte solving complex security challenges faced by Fortune 500 customers. He co-founded and led Deloitte's cyber-innovation ecosystem strategy, working in partnership with VCs, accelerators and cutting-edge security companies to solve futuristic customer challenges. He was instrumental in Deloitte's decision to invest in Maryland-based cybersecurity startup studio DataTribe, and advised portfolio companies on enterprise-focused product management, marketing and business development activities. He is a reformed penetration tester and frequents Defcon, BlackHat, and RSA conferences to connect with the community. Nipun holds a bachelor's in Electronics & Communications Engineering from Panjab University in India and a master's in Information Security from Carnegie Mellon University in the US.

Adam Gurney

Sales Engineer, OPSWAT

Adam Gurney is a Sales Engineer covering the EMEA region at OPSWAT, focusing on securing Critical National Infrastructure. An experienced technical engineer and sales professional, Adam has over 15 years' industry experience, working with the UK's largest MSPs and security vendors, developing a key understanding of the demands organisations of all sizes face in today's threat landscape. He works with key organisations across government, defence, energy and finance industries

Mary Haigh

CISO, BAE Systems

Mary is the CISO for BAE Systems plc. She joined the company in January 2015. Since joining BAE Systems, she has held a number of roles including Director of Cyber for BAE Systems Applied Intelligence, responsible for developing the cyber-vision and strategy, as well as the roadmap and go to market strategy for the cyber-products and services. Prior to that, Mary was Product Director for the Managed Cloud and Security Services business. Previously, Mary led the Technical Roadmap for the Cybersecurity Division in QinetiQ having had various roles since 2001, including heading up the Cybersecurity Services business group and the Cross Domain Products business group. Mary has worked in the cybersecurity domain since 2009, prior to that working in semiconductors research and then specialising in intellectual property management. Her PhD was in Semiconductor Physics.

Nick Hogg

Director of Technical Training, Clearswift

Nick has over 25 years of experience of developing and delivering training courses. Twenty years of that have been spent developing partner sales, pre-sales, and technical training, along with end-user courses for cybersecurity organisations. At Clearswift, Nick is focused on ensuring that our customers get the best value from their solutions by understanding how they can address their key cybersecurity business issues.

Federico Iaschi

Business Information Security Officer, Virgin Media 02

Federico is an information security and compliance practitioner with a combination of leadership, managerial and technical experience developed over 20 years within private and public sector enterprises, with both global and local companies.

Neil Johnson

Head of Security and Threat Solutions, TikTok

Over 20 years of experience in various roles within security, can be seen as a 'man of many hats'.

Currently working for TikTok helping secure 'the last sunny corner of the internet' as the Head of Security and Threat Solutions where the team models threats and designs mitigating security controls. Has previously worked for NYSE, Diageo, EMC, Evercore and through some start ups at build stage. Was chosen as one of Time's Person of the Year 2006.

Vijay Kishnani

Lead Cyber Security Engineer, CybelAngel

Vijay Kishnani is the Lead Cyber Security Engineer at CybelAngel. His team focuses on demonstrating the value of CybelAngel to prospective customers by leveraging our technology to identify live data leaks that can be found inside the supply chain. Vijay Kishnani has previously worked with PricewaterhouseCoopers, Merrill Lynch, and Goldman Sachs.

Major General Ben Kite

Director of Intelligence Interoperability, Ministry of Defence

Ben Kite is a serving, senior British Army Officer and author; he attended the Royal Military Academy Sandhurst in 1989 and was commissioned into the Intelligence Corps. He has completed operational deployments in Belize, Bosnia, Kurdistan, Kosovo, Iraq and Afghanistan as well as helping to integrate ANC soldiers into the post-apartheid South African National Defence Forces and instructing Sandhurst. Ben has a broad military background serving in armoured, infantry and airmobile units as well as with the Royal Air Force and Special Boat Service. He also remembers, with great affection, his time spent with US forces in Iraq, Afghanistan and at US Cyber Command. Ben Kite is a graduate of the Higher Command and Staff College and has led many organisations and teams including 4 Military Intelligence Battalion, for whose work in Afghanistan he was awarded the OBE.

More recently, he commanded the 2,500 strong UK's Joint Force Intelligence Group from 2016–2019, a high-profile organisation delivering global intelligence operations and is currently Director Intelligence Interoperability in Defence Intelligence. Ben Kite is an author in his spare time, publishing his first book the widely acclaimed 'Stout Hearts – The British and Canadians in Normandy 1944' in 2014. His new two-part work is Britain and the Commonwealth's War in the Air 1939-45', Volume 1 of which was published in November 2019 and Volume 2 in June of 2021. He is a Fellow of the Royal Historical Society and is a regular international public speaker on intelligence, military, leadership and historical subjects for organisations as diverse as the Harvard Business School, the Royal New Zealand College of General Practitioners, Moody's and the Chalke Valley History Festival.

Zibby Kwecka

Head of Information Security, Heineken UK

Zibby progressed from electronics, through advanced networking, and research in privacy-preserving cryptographic techniques, to helping some of the biggest organisations secure by design and defend their assets. On this journey, he has inspired further development of covert-channel analysis and crypto solutions, assisted in forming one of the first CSOCs in UK, designed card data tokenisation solutions, and played cameo role in securing a banking grade distributed ledger system. Now, Head of Information Security in Heineken UK, Zibby continues to collaborate with CISOs, the cybersecurity industry and academia.

Fred Langford

Director of Online Technology, Ofcom

Fred has 30 years' experience across a variety of sectors focusing on the Internet, its technology, governance, security, safety and regulation. Fred joined online harms regulator Ofcom in November 2020 and is the Director of Online Technology. His work focuses on directing Ofcom's technical function and research in relation to Ofcom's current and future roles in Internet regulation.

Prior to joining Ofcom Fred was Deputy CEO and Chief Technology Officer at Internet Watch Foundation (IWF – https://www.iwf.org.uk/), the UK Child Sexual Abuse Material hotline. Fred is also a Board Member of Video Standards Council (https://videostandards.org.uk/RatingBoard/), Member of the INHOPE Advisory Board (https://www.inhope.org/EN), Former Chair of the UK Council for Internet Safety, Technical Working Group (UKCIS TWG – https://www.gov.uk/government/organisations/uk-council-for-internet-safety), Member of the National Crime Agency (NCA) Prevent Strategic Board, a founding Director of the UK Safer Internet Centre (https://saferinternet.org.uk/) and is an expert advisor to UK and other Governments, Parliamentarians, The Commonwealth, Police and NGOs approaches to Online Safety. Fred is also a Chartered Director (www.iod.com) and is passionate about influencing how Internet technologies impact society.

Jonathan Lee

Sr. Product Manager, Menlo Security

Jonathan Lee is a Senior Product Manager at Menlo Security, a leader in cloud security. In this role, he serves as a trusted advisor to enterprise customers, and works closely with analysts and industry experts to identify market needs and requirements, and establish Menlo Security as a thought leader in the Secure Web Gateway (SWG) and Secure Access Service Edge (SASE) space. Experienced in leading the ideation, technical development, launch and adoption of innovative security products, including email security, data loss prevention and end point security,

Jonathan previously worked for ProofPoint and Websense. As an industry expert, media commentator and speaker, Jonathan is well versed in data protection, threat analysis, networking, Internet isolation technologies, and cloud-delivered security.

Toby Lewis

Head of Threat Analysis, Darktrace

Prior to joining Darktrace, Toby spent 15 years in the UK Government's cybersecurity threats response unit, including as the UK National Cyber Security Centre's Deputy Technical Director for Incident Management. He has specialist expertise in security operations, having worked across cyber-threat intelligence, incident management, and threat hunting. He has presented at several high-profile events, including the NCSC's flagship conference, CyberUK, the SANS CyberThreat conference, and the Cheltenham Science Festival. He was a lead contributor to the first CyberFirst Girls Competition, championing greater gender diversity in STEM and cybersecurity. Toby is a Certified Information Systems Security Professional (CISSP) and holds a master's in Engineering from the University of Bristol.

Bryan Littlefair

CISO & Cybersecurity Consultant, presenting on behalf of FireMon

Bryan Littlefair is a CISO and Cybersecurity Consultant, with over 20 years' experience leading teams within information and cybersecurity. He specialises in advising executive teams and boards of some of the world's largest organisations on their security strategy as well as providing security consultancy, guidance and mentorship to the Chief Information Security Officer community.

Bryan is also very active in the start-up community working with both the London Office for Rapid Cyber Acceleration (LORCA) and Cyber London (Cylon) working with the start-ups and scaleups to ensure they have the right approach to cybersecurity, as well as working with more mature start-ups on embedding an effective but practical approach to cybersecurity with the supporting policies and governance. He has most recently been the Global Chief Information Security Officer at the Multinational Insurer Aviva, transforming their security capability as the organisation changed to a fully digital way of interacting with its client base.

Before Aviva, Bryan was the Global Chief Information Security Officer at Vodafone Group where he created the Information Security function within the global telco, created and embedded their security strategy and oversaw day to day security operations for over seven years. He also directed the Security Research Lab for British Telecom, participating in Global, EU and academic based research studies as well as driving relevant business transformation studies on behalf of BT. He advises at an executive and non-executive level both venture capital funds and security start-ups on their security strategy and product visions to ensure as well as working with several universities on both the academic and research aspects. Bryan holds several patents in the information security space and is a regular keynote speaker at security events.

Ian Lowe

Director of Solutions Marketing, EMEA, Okta

Ian Lowe is Okta's Director of Solutions Marketing for EMEA. In his 19-year career, Ian has become a recognised product marketing and sales enablement leader having created and launched successful cloud-based security solutions that are used by top technology firms, financial services organisations and Governments around the world today; including but not limited to the White House, Microsoft and HSBC.

Maurits Lucas

Director of Intelligence Solutions, Intel 471

Maurits Lucas is Director of Intelligence Solutions at Intel 471, where he specialises in bridging the gap between technology and business. Maurits has held various positions in cyber-threat intelligence and IT security over the past 17 years and is a subject matter expert on cybercrime, presenting his research and providing his thought-leadership to distinguished audiences around the world.

Ciaran Martin

Professor of Practice in the Management of Public Organisations, Blavatnik School of Government at Oxford University

Ciaran Martin is Professor of Practice in the Management of Public Organisations at the Blavatnik School of Government, part of Oxford University. Prior to joining the School, Ciaran was the founding Chief Executive of the National Cyber Security Centre, part of GCHQ. Ciaran led a fundamental shift in the UK's approach to cybersecurity in the second half of the last decade. He successfully advocated for a wholesale change of approach towards a more interventionist posture and this was adopted by the Government in the 2015 National Security Strategy, leading to the creation of the NCSC in 2016 under his leadership. Over the same timeframe, the UK has moved from joint eighth to first in the International Telecommunications Union's Global Cybersecurity Index and the NCSC model has been studied widely and adopted in countries like Canada and Australia.

The NCSC's approach has been lauded for responding quickly to incidents and giving the British public clear and prompt advice on responding to them, putting previously classified information in the hands of industry so that companies can defend themselves more effectively, major improvements in automatic cybersecurity like countering brand spoofing and rapidly taking down malicious sites, and projecting the UK's leadership in cybersecurity across the world. Ciaran's work, which led to him being appointed CB in the 2020 New Year's Honour's list, has also been recognised and honoured in the United States and elsewhere across the world.

In his 23-year career in the UK civil service, Ciaran held senior roles within the Cabinet Office, including Constitution Director (2011–2014), which included negotiating the basis of the Scottish Referendum with the Scottish Government and spearheading the equalising of the Royal Succession laws between males and females in the line; and director of Security and Intelligence at the Cabinet Office (2008–2011). Between 2002 and 2008 he was Principal Private Secretary to the Cabinet Secretary and Head of the Civil Service and Private Secretary to the Permanent Secretary to HM Treasury.

Neil McRae

Solution Engineer, Tessian

Neil McRae is an experienced Solution Engineer with a demonstrated history of working in the computer and network security industry. Having previously worked for Fortinet, Extreme Networks and Sky, a strong professional who likes to keep up with the latest trends, challenges and threats in today's cybersecurity landscape. At Tessian, Neil is responsible for demonstrating Tessian's products to prospects and customers and helping them to understand the full capabilities of the Tessian Human Layer Risk Hub.

Alistair Mills

Director, Sales Engineering, Northern Europe, Proofpoint

Alistair Mills is a Cybersecurity Expert with over 15 years' experience. He enjoys the challenge of running teams who work on complex technical solutions that help organisations to secure their data. Prior to Proofpoint, Alistair worked at Forcepoint, Symantec and Sophos.

Raghu Nandakumara

Head of Industry Solutions, Illumio

Raghu Nandakumara is the Head of Industry Solutions at Illumio, where he leads the strategy and execution for Illumio's solutions catering to key vertical industries. Prior to that, he was Field CTO for EMEA/APAC and was responsible for helping customers and prospects through their segmentation journeys. Previously, Raghu spent 15 years at Citibank, where he held a number of network security operations and engineering roles. Most recently, he served as a Senior Vice President, where he was responsible for defining strategy, engineering, and delivery of solutions to secure Citi's private, public, and hybrid cloud environments. Raghu holds an undergraduate degree in Mathematics and Computer Science from the University of Cambridge, and a master's degree in Advanced Computing from Imperial College London.

Andy Ng

Partner, Cyber, EY Consulting

As EY EMEIA Data Protection & Privacy Consulting Leader, Andy is responsible for an area of cybersecurity that helps clients make more informed decisions about their information assets, including strategic areas of data loss prevention (DLP), Cloud Access Security Broker (CASB), Information Centric Security and Alliances. With more than 15 years of experience in the cybersecurity space, he previously led information protection and alliances capabilities across EMEA for a professional services organisation, building a market-leading business in both areas. Prior

to that role, he was responsible for identity and information protection solutions for financial services at a software company. Andy is a recognised thought leader in DLP and developed methodologies and leading practices that have been adopted by the market globally.

Isaac Ng

CISO,
Southeastern Railway

Experienced Security Consultant with a demonstrated history of working in the computer networking industry. Strong engineering professional with a Bachelor of Applied Science (B.A.Sc.) focused in Cyber Forensics, Information Security and Management & Business Information Systems from Murdoch University. Skilled in analytical skills, technical support, customer relationship management (CRM), and computer forensics.

Rois Ni Thuama

Head of Cybersecurity Governance & Legal Partnerships, Red Sift

A doctor of law and an expert in the field of cyber-governance and risk mitigation, Rois is highly experienced in her role as Head of Cybersecurity governance at Red Sift. She works with key clients across a wide range of industries including legal, finance, banking and oil & gas, and regularly writes and presents content focussed on significant cyber-threats, the latest trends and risk management.

Cyril Noel-Tagoe

Cyber Threat Evangelist,
Netacea

Cyril Noel-Tagoe is an experienced information security professional. He recently joined Netacea's threat research team, where he spends his time researching, speaking and writing about malicious bots and other cybersecurity topics. He comes from a consulting background, having advised financial services organisations on a range of technical and non-technical cybersecurity domains in a previous life.

Jensen Penalosa

Assistant Legal Attaché,
FBI

Assistant Legal Attaché (ALAT) Jensen Penalosa has been a Special Agent with the FBI since 2005. ALAT Penalosa is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (C|EH) with a Bachelor of Science degree in Computer Science. Prior to entering on duty with the FBI, ALAT Penalosa was employed as a Software Engineer. From 2012 to 2017, ALAT Penalosa supervised Cyber Crime Squads responsible for conducting counterintelligence and criminal cyber-investigations in the Los Angeles area. In 2017, ALAT Penalosa was named the FBI Liaison Officer to Department of Defense partners in Hawaii. In 2019, ALAT Penalosa was assigned to the FBI Legal Attaché office in London where he coordinates the investigative and intelligence activities between the FBI and international partners.

Benjamin Preminger

Product Manager,
Cybersixgill

As Product Manager at Cybersixgill, Benjamin Preminger leads innovation and product development across a variety of cyber-threat intelligence offerings. He has deep experience working at the intersection of threat intelligence and AI, including the creation of an in-house, multi-lingual data analyst team that supports that company's mission to provide scalable, AI-driven solutions. Having previously been part of the company's intelligence group, Benjamin leverages his deep understanding of the cyber-underground to create cutting-edge technological solutions to real-world intelligence problems. A graduate of Yale and Johns Hopkins SAIS, Benjamin is a frequent commentator on the intersection of crime, foreign policy, and the cyber-underground. His research appeared in leading publications around the world, including USA Today, The Independent, Variety, Fox News, and Forbes.

Helen Rabe

CISO,
Abcam

An internationally experienced information security professional who specialises in complex strategic deliveries with a strong emphasis on security service management delivery across a broad range of industry and technology sectors. She holds a strong work ethic applying high levels of accuracy, dedication and professionalism at all times. Helen thrives within high-pressure, fast-paced environments, while managing strategic security programmes and large operational budget assignments within strict constraints. Possessing excellent communication skills, she is adept at developing and harnessing constructive relationships between business leaders and multi disciplined technical teams. Helen is accomplished in delivering engaging presentations as well as compiling and presenting comprehensive reports to board level. Experienced in multiple system methodologies, she

is quick to grasp new ideas, technologies and concepts. Her strengths lie in rapidly adapting to environments that demand critical path delivery and management, subsequently delivering accelerated value add to my clients. She has an earned reputation for strong leadership and delivery skills in matrix environments, coupled with significant expertise in managing globally dispersed teams across business and IT offshore divisions, and providing consultative services to core stakeholders, up to and including Partner, C-Suite and Board level. She readily engages trust and confidence with her clients and peers.

Brett Raybould

EMEA Solutions Architect,
Menlo Security

Brett Raybould is EMEA Solutions Architect at Menlo Security, a leader in cloud security. In this role, he is responsible for technical sales, product demonstrations, installations, solution proposals and evaluations. Brett joined Menlo Security in 2016 and discovered how isolation technology provides a new approach to solving the problems that detection-based systems continue to struggle with. Passionate about security, Brett has worked for over 15 years for some of the leading vendors specialising in the detection of inbound threats across web and email, and data loss prevention (DLP) including FireEye and Websense. He has represented Menlo Security as a speaker at industry events, including e-Crime & Cybersecurity Congress and Cloud Security Expo.

Jill Robertson

Head of Information Security
Change Team, Metro Bank

Jill has had a number of roles in IT within financial services and consultancy sectors in the areas of development, change management and then specialising in information security. She now runs the Information Security Change team at Metro Bank, advising on initiatives across the organisation, including regulatory implementations, of their InfoSec requirements and risks. Companies she has worked at include MBNA, RBS, LBG and F-Secure. In her spare time, she enjoys taking to the mountains skiing and hill walking.

Chris Robins

Senior Sales Engineer, EMEA,
Beyond Identity

Chris Robins is a Senior Sales Engineer for the EMEA region at Beyond Identity. He is an experienced security sales professional who has worked for several of the world's top cybersecurity companies over his 20-year career. In his present position, he is charged with helping organisations change the way users validate their identity, be it for workforce applications, DevOps code signing or customer identity access management.

Stephen Roostan

VP EMEA,
Kenna Security

Roostan has over a decade of experience in cybersecurity and transformation projects. His role at Kenna is to rapidly grow the EMEA organisation to meet the customer demand for risk-based vulnerability management. Prior to Kenna, he held senior sales roles at Forcepoint, Citrix and Imperva, focusing on IT solutions for complex, enterprise requirements. Roostan has a passion for driving equality alongside enabling flexibility at work for modern lifestyles. He has held steering committee roles in companies looking to close the gender pay gap and develop careers for working parents, and strives to find and support equality initiatives across the workplace and industry. He believes that creating a collaborative and supportive working culture is hugely productive for both an organisation and its employees.

Alain Salesse

Senior Sales Engineer,
Cofense

Alain Salesse is a Senior Sales Engineer at Cofense. Alain has spent 25 years working for and with large enterprises and service providers to improve the efficiency and value of their IT operations and security services through the effective use of systems management technologies. In his current position, Alain helps organisations to better protect themselves against phishing attacks.

Greig Sharman

Chief Technology Officer,
NSPCC

A high-performing strategic business change and digital leader who has proven experience of delivering change and transformation in a number of private and public sector organisations. Greig is highly experienced across IT operations, business strategy, enterprise architecture, software and service development, data capabilities, business change, portfolio and programme delivery. With many years' experience of managing and leading large teams, he is a technology and data innovator, embedding the necessary structures, skills, capabilities and ways of working to bring a fully digital vision to life.

Ian Shaw

Head of Risk and Security, South East Coast Ambulance Service, NHS Foundation Trust

From the start of my military career, I have honed my operational, leadership, risk and security capabilities, then applied these successfully to a corporate environment, driving organisational resilience, security and risk for major institutions, including The Bank of England and the UK Civil Aviation Authority. I build strength and durability across all levels. I recognise the need for companies to evolve and grow into today's global marketplace, and pride myself on the protection of people and assets to ensure a safe, secure and supportive environment. As a confident and motivational leader, I invest in others, sharing best practice and encouraging individuals to become more aware of their part in operational security. Throughout my career, I have pioneered concepts such as the UK's first Aviation Security Management System that utilises insights and intelligence to improve security decision making. I cultivate relationships with key stakeholders up to board level, influencing policies, making recommendations and spearheading cultural and organisational changes. Enabling rapid responses to threats and situations is key to continuity: I promote security convergence and set out flexible operating models, security strategies and systems to revolutionise corporate landscapes. I promote smarter ways of working, innovation and creative thinking, discussing benchmarks in global security forums.

Justin Shaw-Gray

Sales Director, UKI and South Africa, Synack, Inc.

In 2018, shortly after joining Synack, Justin was awarded SC Media's Runner Up for Best Cybersecurity Sales Leader. Prior to Synack Justin held senior roles at Netscope, Zscaler, and Riverbed. Justin is originally from Zimbabwe where he was Founder and Human Rights Activist for the Restoration of Human Rights Zimbabwe. Justin is an avid runner and lives in London with his wife and three young children.

James Sherlow

Systems Engineering Manager, 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.

Eric Smithmier

Assistant Legal Attaché, FBI London, Cyber Division

Eric Smithmier was born in Detroit, MI. He received an MS in Law Enforcement Intelligence & Analysis from Michigan State University in 2012 and a BA in Computer Science from Coe College in 2000. Prior to working for the FBI, Mr Smithmier was a Network Engineer employed by Communications Engineering Company in Iowa City, IA. Eric Smithmier entered on duty as a Special Agent (SA) of the FBI on February 9, 2003. From 2003 through 2006, SA Smithmier was assigned to the Minneapolis Division, where he worked Theft of Intellectual Property, Crimes Against Children, and Criminal Computer Intrusions. In 2006, SA Smithmier transferred to the Houston Division where he was assigned to the Houston Area Cyber Crime Task Force focusing on Criminal and National Security Cyber investigations. In 2007, SA Smithmier was selected as a member of the FBI's Cyber Action Team (CAT), a highly trained technical response unit responsible for domestic and international rapid deployment. In 2009, SA Smithmier was promoted to a Supervisory Special Agent (SSA) position in the Eurasian Cyber Unit at Cyber Division where he created and chaired the Industrial Control Systems Threat Focus Cell and led the FBI's participation in Cyber Storm III, a national-level cyber-exercise. In 2011, SA Smithmier returned to Houston and in 2013 was promoted to SSA of a Cyber Squad responsible for Cyber Criminal and Cyber National Security matters where he also maintained program and task force coordinator responsibilities. In 2019, SSA Smithmier reported to London, United Kingdon as an Assistant Legal Attaché where he oversees the FBI's Cyber National Security portfolio. ALAT Smithmier is responsible for the coordination of all cyber national security matters between the FBI and UKIC partners.

Jason Steer

Principal Security Strategist, Recorded Future

Jason is a techie at heart and has built and broken computers and networks since 1996! Jason has worked at a number of successful technology companies over the past 15 years, including IronPort, Veracode & FireEye. Jason has worked as a media expert with the BBC, CNN & Al Jazeera and has worked with both the EU and UK Governments on cybersecurity strategy.

Danielle Sudai

Cloud Security Operations Lead, Deliveroo

Danielle is a Cloud DevSecOps lead who joined the security industry when she turned 18 during her Military Service. Today, she leads Security Operations at Deliveroo, where she is responsible for the security use-cases and real-time scenarios strategy of all Deliveroo's Cloud Assets and SaaS solutions. In 2018, after working in the security software industry, Danielle started focusing on cloud security and relocated to the UK to lead compliance & visibility within GCP, AWS and Azure at HSBC. She has been consulting in her roles for various processes based on security posture and global standards, and investigating threat models to adjust response levels from an operational perspective. Danielle is also a hands-on engineer – she has co-engineered a GCP compliance & visibility scanner and cloud encryption key generation automated process.

Crawford Thomas

Global Head of Cyber Threat Intelligence, Credit Suisse

Army officer in the Scottish Infantry for 10 years in the 90s before moving to Intelligence for a further 10 years. Left the military in 2013. Began my second career in the commercial world of Cyber Threat Intelligence in 2015 as Head of Threat Intelligence at Clydesdale Bank based in Glasgow. Moved to Credit Suisse as the Global Head of Cyber Threat Intelligence in 2018, where I am currently, and based in London. Avid cyclist and wine collector.

Ian Tinney

CEO & Founder, 4Data Solutions

4Data Solutions was co-founded by Ian Tinney, who previously founded, ran, and successfully sold one of the first and most successful Splunk partners in EMEA, EQALIS Limited. Ian combines a deep knowledge of technical subjects, from IT and cloud security and regulatory compliance to data management and analytics, with a firm grasp of the challenges faced by CXOs and is able to bridge the gap between business challenges and technical solutions. Ian ensures that 4Data seeks out financially accessible, cloud-native or innovative technology solutions to meet the rapidly evolving data, cloud, security & compliance demands of today's organisations. He drives the business to put itself in the mind and shoes of the customer, and combine the latest technology solutions to provide innovative approaches to rapidly shifting challenges, where flexibility to change in a financially viable way is absolutely critical. Ian brings experience from the world of large enterprise banking combined with entrepreneurial experience with small and medium start-ups, having built and run international teams of technology consultants. Ian drives the strategy and commercial direction of the business, ensuring that 4Data continues to root itself in good ethics and a highly service-driven culture.

Jon Townsend

CIO, National Trust

Jon Townsend is a leader in technology and is the Chief Information Officer for the National Trust, where he was previously the CTO and CISO. He holds an MBA with the Open University and an MSc with Cranfield University in the Design of Information Systems. He previously held a commission as an Officer in the British Army, fulfilling a variety of technical and leadership roles culminating in Regimental command. Upon leaving the military, he became a Senior Civil Servant in the UK Central Government responsible for developing cybersecurity and intelligence capability for the Department for Work and Pensions. He is also a Certified Data Protection Practitioner with the British Computer Society, a Certified Information Security Manager with ISACA and GIAC Certified Enterprise Defender with SANS.

Ram Vaidyanathan

Cyber Risk and Security Expert, ManageEngine

Ram Vaidyanathan is a Cyber Risk and Security Expert at ManageEngine, the IT management division of Zoho Corporation. He helps security analysts better understand and solve security and compliance challenges. He keeps updated about the latest attack methods, and the most effective response techniques. This helps with the product roadmap decisions in ManageEngine Log360, which is a comprehensive SIEM solution.

Mark Walmsley

CISO,
Freshfields Bruckhaus Deringer

Mark Walmsley is an experienced Chief Information Security Officer. He studied law before joining a number of small boutique private investigation agencies. The majority of Mark's professional career has been spent within the legal industry, working within litigation before moving to business services where he managed high-value, complex programmes of work. Mark has led Freshfields' information and cybersecurity capability for the last five years. Over the past 12 months, Mark has had a part-time secondment to the National Cybersecurity Centre (part of GCHQ) where he helped manage the government and legal industry engagement.

Chris Waynforth

Area VP, EMEA North,
Imperva

Chris is part of the leadership team for Imperva EMEA as AVP for Northern Europe. Before joining Imperva, Chris worked at a number of major technology companies including RSA, Splunk, and Identiv, providing cybersecurity solutions to the UK market. In particular, he has focused on helping businesses combat fraud through analytics and cutting-edge technology. Chris has deep experience of leading both technical and customer-facing teams on an international scale. He graduated from Manchester Metropolitan with a BA in 1999 and returned to study for the High Contributors programme at the Cranfield School of Management in 2011.

Lee Whatford

CISO,
Domino's Pizza

Lee Whatford is a seasoned leader in information security and risk management. With over 25 years' experience in a variety of roles across the industry, from start-up to large vendors, consultancies and managed service providers, Lee is now CISO for a leading global brand. He is also a Founding Partner of the South East Cyber Resilience Centre helping small businesses, a strategic advisor to EC-Council and a member of Evanta's CISO Community Governing Body. Lee is a regular speaker at a variety of industry events and retains a strong interest in the start-up community, acting as a strategic advisor to several start up and growth phase companies. Outside of his infosec commitments, Lee enjoys, golf, tennis the great outdoors, photography and (when allowed) travelling.

David Whitelegg

European Security Officer,
Compass Group

David is a commercially oriented and highly experienced information security professional with over 20 years of cybersecurity leadership and management. Proven track record of driving security posture improvement within large multinational enterprises and FinTech. Responsible for securing and achieving PCI DSS compliance at one of Europe's largest payment service providers. Processing over 250 million transactions annually, the business was the first Payment Service Provider outside the United States to be listed as PCI DSS compliant by both Visa and MasterCard in 2007.

Credited with engineering Europe's first satellite VPN in 2003, which successfully enabled Pitney Bowes to continue its client's bank statement printing operations at a rural DR site following the 2005 Buncefield oil terminal explosion.

Engin Yilmaz

Product Director,
Red Sift

Engin Yilmaz is Product Director at Red Sift, one of Europe's fastest-growing cybersecurity companies. His expertise in leading Product teams has seen him work on Gmail for business and Google Workspace, the integration of the Skype mobile app into Microsoft as well as an adventure into a behavioural advertising startup. He found his way into cybersecurity via Mimecast, where he created a collaborative platform for knowledge sharing within the email archive to help businesses make better decisions through the use of their collective mind. Now at Red Sift, he remains interested in, and focused on, creating products that simultaneously keep people safe and are easy to use. □

Multicloud security: More clouds, more problems

Organisations aren't merely in the cloud – they're in many clouds resulting in more security and operational challenges.

BeyondTrust reports

Today, cloud vendor lock-in fears of the past seem overblown. Instead of choosing one cloud or another, organisations are simply choosing both, or to be more precise, many! Most organisations aren't merely in the cloud – they're in many clouds (PaaS, IaaS), and their end users regularly consume dozens, or even hundreds, of different SaaS applications. A McAfee study published in 2019 reported the average organisation used 1,935 cloud services. And that number has almost certainly ballooned further since then.

Over the past year, the great cloud migration has enabled the successes of increased remote working and is propelling the acceleration of digital transformation initiatives. Yet, more clouds can mean more security and operational challenges. Siloed identity stores (i.e. Azure ID), native, but incomplete toolsets, and conflicting shared responsibility models between cloud providers – along with all the fundamental cloud security challenges – is creating a fertile atmosphere for threat actors. Additionally, most companies are not 100% cloud – they operate with a hybrid model that includes an on-premises infrastructure, often based on legacy technology.

Inadequate privileged access security controls – often involving credentials, excessive privileged access, or misconfigurations – play a role in most breaches today across both cloud and on-premises environments. The scale of managing the exploding universe of privileges requires an integrated, universal approach, rather than relying on a stack of niche tools, each only helping to manage a slice of the privilege problem. This is especially true when the elasticity of the cloud allows for rapid changes that even traditional tools for management and governance may miss.

Many organisations already run at high risk from over-privileged IT administrators and power users. As they migrate more workloads to the cloud, the on-premises complexity doesn't vanish. Instead, they tend to end up with the hybrid, multicloud management challenge.

Lean into identity-centric security to address the most critical multicloud & hybrid IT security gaps

As environments have trended toward increasing decentralisation, identity has become the strongest foundation for security. The identity challenge is the most important security problem for organisations to solve for across cloud and on-premises environments. And no identities are more critical to protect than privileged identities – whether associated with humans or machines, employees or vendors, and whether they are persistent or ephemeral. Solving for the multicloud/hybrid identity and privilege challenges is best accomplished by standardising the management and security controls across the entire IT ecosystem.

Ultimately, your privileged access management strategy should ensure every privileged account, session, and asset is secured, managed, and monitored across your entire cloud and hybrid infrastructure. BeyondTrust Privileged Access Management (PAM) solutions protect your entire multicloud and hybrid environment via our universal privilege management model by:

- Continuously discovering and onboarding privileged accounts and cloud instances
- Enforcing credential security best practices across every human and non-human account, including implementing zero trust architectures
- Reducing the number of users with privileged access
- Restricting the privileges any user, application, service, or asset has for access and automation
- Preventing and mitigating human-based errors in privileged access
- Condensing the window of time during which privileges can be executed, and thereby abused, by applying the principle of just-in-time access
- Enforcing segmentation of the cloud environment and securing/proxying remote access to cloud management consoles/control planes and to computing resources
- Robustly managing and monitoring every privileged session and providing certification for regulatory compliance
- Providing a single, centralised platform for all privilege management activity that is architected to integrate with the rest of your security and information technology ecosystem

For a deeper dive on understanding and addressing the most pressing multicloud security risks and challenges, download our new Guide to Multicloud Privilege Management. □

BeyondTrust

UNIVERSAL PRIVILEGE MANAGEMENT

Secure and protect privileges across passwords, access, and endpoints to stop data breaches and achieve compliance

Privileged Password Management

Endpoint Privilege Management

Secure Remote Access

beyondtrust.com

The only universal security intelligence solution

Recorded Future – delivering relevant cyber-threat insights in real time.

Recorded Future reports

Who we are

Using a sophisticated combination of machine and human analysis, Recorded Future fuses the broadest set of open source, dark web, technical sources, and original research together to deliver relevant cyber-threat insights in real time. The Recorded Future Security Intelligence Platform aggregates this rich intelligence with any other threat data sources, which empowers security teams to collaborate on analysis and deliver intelligence wherever they need it most – including rapid integration with existing security solutions.

Security intelligence solutions

Security intelligence accelerates detection, decision-making, and response times by positioning comprehensive intelligence at the centre of your security workflows.

- *Threat intelligence:* Gain context on who is attacking you, their motivations and capabilities, and indicators of compromise to look for in your systems. This information is searchable in real time and presented in a single-pane-of-glass view and via customised alerts.
- *SecOps and response:* Discover previously unidentified threats and triage internal alerts in your SIEM based on rich external context and threat indicators correlated with internal threat data – so you can make faster, more confident decisions
- *Brand protection:* With real-time alerting, you can find things like leaked credentials, typosquat domains, social media accounts meant to impersonate an employee or brand, fake applications, threats to executives, and more. Takedown services go the last mile to simplify and expedite the removal of malicious content from the internet.
- *Vulnerability management:* Real-time risk scores based on real-life exploitability make it easy to prioritise where you should focus efforts and what you need to patch to prevent attacks. Real-time alerting on vulnerabilities affecting your tech stack provides new insights for effective risk reduction.
- *Third-party risk:* Make informed decisions to reduce your overall risk based on insights from real-time intelligence about the vendors and partner companies that form your business ecosystem – including vulnerable technologies, domain abuse, threats targeting the organisation, and more.

Intelligence-led security

Lead with intelligence across your security teams, processes, and workflows with security intelligence solutions from Recorded Future.

- Threat intelligence
- SecOps and response
- Brand protection
- Vulnerability management
- Third-party risk
- Geopolitical risk

- *Geopolitical risk:* Accelerate critical decision making with contextual data on threats, trends, sentiments, and evolving security situations – so you can protect your assets and understand shifting geopolitical dynamics in the geographic areas that matter to your organisation.

Innovative security intelligence technologies

Security Intelligence Graph

Recorded Future's unique ability to model all relevant security information available on the internet is what has set us apart since the beginning. With billions of indexed facts, and more added every day, the Recorded Future Security Intelligence Graph leverages a unique combination of patented machine learning and human analysis to provide you with unmatched insight into emerging threats that are relevant to your organisation.

Recorded Future Intelligence Cards™

Security teams gain instant context around suspicious observables and indicators with Recorded Future Intelligence Cards – with just one click. This innovation enables security teams to rapidly prioritise threats or dismiss false-positives using Recorded Future's dynamic risk scores. All of the evidence gathered by our Security Intelligence Graph is visible on these cards, allowing you to pivot quickly between indicators and attack methods, or vulnerabilities and exploits. □

For more information, please visit
www.recordedfuture.com

Recorded Future®

The SOC evolution answers your questions

The security industry faces a forced SOC evolution, driven by pressure from all directions. For the last decade, the security industry that powers SOCs has fixated on automation as the key to alleviating some of the pressures. But what's really changed?

Devo reports

The cyber-attack surface is growing exponentially and diversely. The environments, platforms, services, regions, and time zones that constitute modern enterprise operations and drive businesses' digital transformation continue to require increasing specialisation and expertise not available in-house. Enterprise attack surfaces are expanding past businesses' ability to provide protection.

Meanwhile, global hiring and retention of security experts continue to be challenging, and direct access to specialised security knowledge and experience is becoming increasingly difficult and costly. Also, the volume, duration, pace and sophistication of attacks continue to increase and require significant acceleration in SOC response times and durability – and subsequent autonomous response systems.

Conundrum is an understatement

The security industry faces a forced SOC evolution, driven by pressure from all directions. Plenty has happened that *tried* to look like evolution. For the last decade, the security industry that powers SOCs has fixated on automation as the key to alleviating some of the pressures. But what's really changed?

SOAR was a brief shining light that has come and mostly gone, having been absorbed back into SIEM, as legacy vendors – to make up for their shortcomings in human workflow automation – acquired dedicated SOAR vendors. This left analysts in the lurch. They faced the same automation integration challenges, only they were locked into a single vendor (where previously an 'independent' SOAR offered the prospect of multivendor connectors and flexibility to operate independently of SIEM lock-in).

Automation, on its best day, remains too playbook-oriented. To get things done, experts must, essentially, write scripts for each new system, connector and application in an enterprise. We're caught in a linear script development cycle and automation hasn't yielded the desperately needed reduction in analyst workloads.

Breaking the cycle

Two major breakthroughs will accelerate SOC evolution. First, SOCs must successfully implement and use AI 'smart' orchestration systems. Many SOC analysts and CISOs are likely jaded from past promises, but the reality is that AI and ML approaches have matured significantly during the past year, reaching the inflection point of their 'hockey stick' usefulness trajectory and the value they can bring. The industry must move past the fear of turning on automated response and protection capabilities powered by this new generation of AI and ML. By embracing it, SOCs will become much more effective at detection, which will reduce the number of distinct alerts and false positives – and reduce analysts' workloads.

The second needed breakthrough is the ability to tap a global community of contributors via marketplace ecosystems. Detection-as-code, policy-as-code, etc., have redefined content development and vendor-proprietary product-dependent content. Platform-independent content (ranging from alerts, threat detection, playbooks, etc.) is readily available from worldwide sources. The ability to tap a global pool of expertise is more prevalent than ever and it feels like the gig economy is finally coming to the security world via the SOC.

It's time to get started

Both 'smart' machine intelligence and content marketplaces directly address the pressure points mentioned previously, but it's early days for the SOC evolution. Organisations must look at their SOC and decide how they're going to reorganise and prioritise to discover and implement the people, tools and partners needed to usher in the evolution.

There are some philosophical hurdles to overcome, but business needs will drive the pace of change. At one time, penetration testing was in-house only, then it extended to trusted vendors managed under restrictive agreements, and then to industry-accredited providers. Now businesses can tap broad communities of bug-bounty-based individual contractors and cloud-based automated attack simulators. The industry successfully managed those changes, and it's reasonable it can do the same for incident response and investigation. □

For more information, please visit
www.devo.com

DEVO

Struggling to scale your security analysts and defenses to stop attackers?

Today's fast-moving threats require security teams to take a new approach to managing data, analytics and tactics.

Devo is the cloud-native logging and security analytics platform that:

- Empowers security teams to protect their organizations by closing the visibility gap
- Defends against advanced cyberthreats with quick detection and investigation
- Enables analysts to work more effectively and punch above their weight

Learn more at devo.com

Observability: A data-driven approach to cloud security

A lack of visibility continues to hamper efforts.

Ian Tinney reports

We've seen explosive cloud growth in response to the demand for more flexible, agile, and accessible infrastructure over the last two years, but the rapid rollout created a significant security vacuum, enabling e-Crime to flourish. There was a 630%[1] increase in attacks against cloud accounts during the first wave, with misconfiguration, unauthorised access and insecure interfaces listed among the top threats, while ransomware and malware were deemed to be the fastest-growing.

As we move into recovery, teams are now assessing the damage and evaluating the effectiveness of their cloud security. A lack of visibility continues to hamper efforts, however, with 64%[2] saying it can take months to detect incidents, with these often only spotted due to a spike in cloud usage (and cost). Small wonder, then, that the vast majority (72%[3]) say they are either not confident or only moderately confident in their cloud security posture.

So why is cloud security so difficult?

Much like the shift from the combustion engine to the electrically powered vehicle, migrating to the cloud is disruptive. The skillsets and equipment required are different to those used in the datacentre, with physical servers in racks replaced by code that can build entire virtual datacentres in minutes. And just as the electric vehicle will eventually give way to self-driving cars, so too are approaches to cloud security evolving and embracing automation, making it easier to see, secure and protect data through advanced techniques such as automated remediation, for example.

But what can you do today to fill the security vacuum and make your infrastructure more secure, cost-effective and futureproof? We see this as largely a data problem. There are enough clever tools but simply too much data to process cost-effectively. So, we use a data-led approach that we call organisational security. This introduces observability, which allows us to keep answering new questions as things change, and at the same time, helps us manage data more effectively.

Six steps to organisational security

While detecting attacks is good, measuring your organisational effectiveness is even better. To achieve this, you'll need a cloud security strategy that:

- *Inventories assets:* What entities do I have in the cloud? Figure out what you have (hosts, instances, software, libraries, etc.)
  TOOL: CSPM
- *Determines asset states:* How are they configured? Figure out what state these assets are in (versions, configuration, access, etc.)
  TOOL: CSPM, CWPP (or CNAPP, which combines the two)
- *Monitors for change:* What is changing? Who is using my services? Am I compliant? Check for changes in state that might affect the security posture or adherence to compliance standards.
  TOOL: CSPM, CIEM, CWPP, CNAPP
- *Protects access:* Have my accounts been compromised? Ensure user credentials are not compromised and, in the event they are, be able to detect compromise and prevent crime.
  TOOL: Credential protection/detection
- *Curates data:* How can I get, route, reduce, transform my data? Determine which data is of value, how accessible it needs to be, and which systems need it.
  TOOL: Observability pipeline
- *Observes more widely:* What trends are happening in real-time? What changed? What looks unusual? What behaviours can we determine about an entity? Applying an observability approach to security by monitoring a myriad of KPIs can provide unprecedented insight and control.
  TOOL: Security analysis tools

Organisational security means you can begin to think strategically, not just tactically, and move from a reactive to a proactive stance. Introducing an observability pipeline helps us collect more data but deal with it cost-effectively, making security affordable and achievable. □

1 Cloud Adoption and Risk report, McAfee https://www.mcafee.com/enterprise/en-us/assets/reports/rp-cloud-adoption-and-risk-report-work-from-home-edition.pdf

2 2021 State of Cloud Costs report, Anodot https://go.anodot.com/hubfs/WP,%20Guides,%20Reports/2021-State-of-Cloud-Costs-Report/2021-State-of-Cloud-Costs-Report.pdf

3 Cloud Security Report 2021, ISC(2), https://www.isc2.org/-/media/ISC2/Research/Resource-Thumbnails/Resource-Center/Research/2021-Cloud-Security-Report-FINAL.ashx?la=en&hash=365C243EC4B2196B9C4B55AF8E3C4E1EC4B0C5B6

Ian Tinney is CEO at 4Data Solutions.

For more information on how to make your cloud security posture fit for the future, please visit **4datasolutions.com**

4data SOLUTIONS

DATA-DRIVEN CLOUD SECURITY

- Gain complete visibility and control of your cloud platforms
- Maintain regulatory compliance
- Reduce financial and security risks, and prevent vendor lock-in
- Enable security analytics through better data management
- Reduce fraud through 'account takeover' and 'data leak' detection and prevention

Unlock the Potential of your Data

4datasolutions.com | info@4datasolutions.com | +44 (0) 330 128 9180

TechVets · better business act · Security Cleared · Armed Forces Covenant

Cloud Control · corelight · Cribl · Logsign · splunk> · Threat Status

The canary in the supply chain – third-party data leaks and supply chain attacks

Supply chain attacks have originated in third parties, big and small.

CybelAngel reports

What is the 'canary in the coal mine' of supply chain attacks? What characteristic or signal should cybersecurity use as a warning sign?

Some think that a vendor's size is an indicator of being the target of a supply chain attack. According to the World Economic Forum, 88% of survey respondents indicate that they are concerned about the cybersecurity of SMEs in their ecosystem. There is a logic to that fear as cybersecurity skills are expensive, and SMEs may not prioritise them.

But supply chain attacks have originated in third parties, big and small. Retail giant Target famously suffered a supply chain attack in which threat actors used an HVAC repair vendor as the initial access point. Several departments of the US Government were compromised when IT software giant SolarWinds suffered an intrusion.

So if 'size' is not the answer, what is the 'canary' of supply chain attacks?

It's third-party data leaks. Supply chain attacks do not start with businesses halting ransomware; instead, they begin by locating weak links in the supply chain that are leaking data.

An unforced data leak, caused by negligence or mistake, is the starting block for many supply chain attacks. By leaving data exposed, threat actors are informed of which links in your supply chain will be easier to target and exploit. Two prime examples of this are the SITA data breach and the Passwordstate supply chain attack.

The SITA data breach is estimated to have exposed more than 580,000 records from multiple airlines' frequent flyer programmes. The breach is believed to have started when SITA shared data with Star Alliance, which was compromised sometime earlier. From there, it spread across the entire supply chain.

A leaky third party also led to a supply chain attack against enterprise password management solution, Passwordstate. According to reports, an attacker gained access to Passwordstate's update server, which was hosted on a third-party CDN. It is suspected those who received a software update during that period were also infected with DLL malware.

An unforced data leak, caused by negligence or mistake, is the starting block for many supply chain attacks. By leaving data exposed, threat actors are informed of which links in your supply chain will be easier to target and exploit.

Both SITA and Passwordstate had their supply chain attacks proceeded by a third-party data leak. Presumably, audits were conducted and third-party risk management procedures were followed. So why were third-party leaks undetected? Because today's risk is not the same as yesterday's risk.

The reality is that a third-party's risk changes day to day. All that is needed is for the wrong security settings to be selected or for someone to rush and skip a permissions step for a data leak to occur. Constant data breach monitoring is needed, especially if the third party manages a company's data.

CybelAngel Data Breach Prevention provides constant monitoring to detect third-party data leaks. Data Breach Prevention focuses on locating whatever data matches an organisation's regardless of where it appears. By focusing on which data matches, a company gains visibility and protection far beyond a company's perimeter into third, fourth, and fifth parties. This increase in visibility frees cybersecurity teams from choosing which partners get monitoring. □

CybelAngel

CYBELANGEL.COM

SEE BEYOND PERIMETERS

External risk protection from the most critical digital threats.

- Blind spots don’t exist
- Critical insight into critical threats
- Lightning-fast detection

STOP DATA LEAKS
View your exposure

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 US 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/continuous-compliance** to see how FireMon can efficiently automate network security policies and help achieve continuous compliance.

FIREMON

FIREMON

Say goodbye to compliance worries.

Say hello to a good night's sleep.

FireMon's **Continuous Compliance** ensures you are always audit ready.

See For Yourself

firemon.com/request-a-demo/

Objects in the rear-view mirror are closer than they appear

Helping to illuminate what may lie ahead in the coming years.

Intel 471 reports

This, the 20th e-Crime Congress, is a good time to look back at how far we have come since the first recorded instances of cyber-attacks, and how far both our adversaries and our ability to defend against them has evolved. This helps illuminate what may lie ahead in the coming years.

Ever since a West German hacker attempted to steal American defence secrets documented in Clifford Stoll's 1989 book *The Cuckoo's Egg,* we have been embroiled in an arms race between attackers and defenders with no sign of letting up. Over the next decade, a host of new threats appeared including spam, malware, phishing and more.

These bad actors spurred a new underground ecosystem focused on financial gain. Banking malware botnets began targeting online banking, payment terminals and even banking gateways. On the nation-state front, we observed the RSA SecurID attack, which gave us the APT acronym, followed by Stuxnet, Flame, Gauss and the Office of Personnel Management attack.

Recently, attacks against cryptocurrency exchanges and big game ransomware attacks have netted attackers tens of millions of dollars in illicit gains and sometimes have an impact hitherto associated with nation-state attackers. This is also because nation-state and pedestrian cybercriminals are merging; not only is it hard to tell them apart, but some actors occupy both spaces at the same time or collaborate in their attacks.

Thankfully, the tooling and organisation of the defenders have come to an equally impressive distance since Clifford Stoll's book. In 1989, there were few if any tools aimed at these issues, and even fewer people listened to the danger of cyber-threats, much less understanding the gravity of these attacks. Since then, firewalls, IDS, SIEMs, Endpoint Protection and a whole host of other tools have appeared as well as SOCs, Incident Responders, CERTs, and an ecosystem of security researchers and analysts.

Forward-leaning organisations however recognised the more they protected their digital estate to keep threats out, the more important it became to proactively monitor what was happening outside their perimeter.

As the stakes increased and the threats became ever more complex and diffused, these organisations realised that building a perimeter and hoping the defences would hold when the as-yet-unknown enemy would eventually appear was not a viable strategy. This was especially relevant with the advent of digital transformation as more and more of an organisation's critical assets were located outside of the perimeter.

Cyber-threat intelligence (CTI) is key in supporting organisations to monitor and proactively defend against emerging threats outside the perimeter. CTI informs organisations to invest in the right countermeasures and deploy their limited defensive resources in areas where these will have the greatest impact in mitigating cyber- risk.

CTI takes many forms: from collecting indicators of compromise to tracking and monitoring actor communications. Tracking actor communications is both the most difficult but also yields the most in-depth and long-term insights into actor motivation and intention.

At the same time, CTI practitioners are challenged with ensuring that they are meeting the requirements of their stakeholders, and in a way that they can demonstrate ROI. At Intel 471, we developed our Cyber Underground General Intelligence Requirements Methodology (CU-GIRH) to ensure that our customers have the framework to maximise the use of our resources.

Twenty years after the first e-Crime Congress, the digital world is now part and parcel of everyday life. At the same time, the threats lurking within it have become more sophisticated and impactful. Real-time, relevant and comprehensive coverage outside of your perimeter is required now more than ever to protect your organisation and its assets. □

For more information, please visit
intel471.com

INTEL471


INTEL471
Fight Cyber Threats and Win
Your organisation deserves the best cyber threat intelligence
Your Voice of Reason and Truth
intel471.com
© 2022 Intel 471

Why your Secure Email Gateway isn't as secure as you think

Every hour of every day, phishing emails evade perimeter controls – in most cases, secure email gateways (SEGs).

Cofense reports

Once delivered to the inbox, phish tempt users to click and give up network or personal credentials, activate malware, or fall for scams. Over 50% of enterprises report that phishing emails reach the inbox roughly once a week. Since SEGs are missing so many phish, there's a good chance other technologies – firewalls, anti-virus, and EDR – also aren't spotting these threats. Such gaps can leave you vulnerable for hours or even days.

What is a SEG?

Secure email gateways – AKA email gateways or email security solutions – are the most common type of perimeter technology used to stop phish from reaching the inbox.

Unlike firewalls and other security technologies, SEGs receive no regulatory or compliance oversight. That's right, SEGs get zero validation testing against the problem they're meant to solve – phishing, the #1 global cyber-threat.

Why SEGs fail

As we've seen, SEGs can handle the basics of perimeter phishing defence. But today's attacks are anything but basic. Here are three reasons why technology fails to stop determined attackers.

1. Attackers constantly innovate

Every time you configure your SEG to thwart the latest Tactics, Techniques and Procedures (TTPs), attackers adjust. They innovate relentlessly to stay a step ahead. Some of the TTPs attackers use to sidestep defences are as follows:

- Leverage trusted cloud infrastructure
- Obfuscate or encrypt malicious content
- Inject malicious content into legitimate email conversations

2. SEG vendors are reactive

You're not the only one having trouble keeping up. As phishers refine their tactics, SEG vendors scramble too.

3. Business can't wait

Tuning your SEG to the latest TTPs takes time. But email must flow freely for your business to operate. Too often, you're forced to choose between speed and organisational security. Sooner or later, speed wins out and phish land in the inbox.

Your best defence against phishing attacks

Because SEGs are so porous you need something to back them up, a consistent way to find and remove threats that reach the inbox. We're talking defence-in-depth, combining human intuition and purpose-built automation.

Security awareness

When human attackers deliver threats to the inbox, humans need to respond. Besides educating users on phishing, your security awareness programme needs to let them practice in a real-world setting: their inboxes. Phishing simulations are your best bet. Make sure the training is positive, not punitive, and that scenarios mirror threats your organisation faces.

Email reporting

Your security teams can't stop a threat in the inbox unless it's reported. A 'Report Phishing' button on the email toolbar makes it easy. With a single click, end users get involved. As employees get more practice, both in training and real situations, they'll sharpen their intuition – something tech controls like email gateways lack.

Email analysis

When security teams try to respond manually to email reports, they usually fall behind. There are simply too many emails, most of them harmless. Automation can cut through noise and identify real threats, plus prioritise them so analysts can budget their limited time.

Search & quarantine

Thanks to well trained users and advanced automation, your SOC has identified a phishing email in a handful of inboxes. But who else received the phish? Again, you'll rely on automation to search all inboxes ASAP and quarantine the threat before lasting damage is done.

At the end of the day, attackers will continue to evolve their tactics faster than most technologies can keep up with. Your best defence against phishing attacks is a combination of technology and humans working together. □

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

We Stop Phish.

Phishing campaigns continue to evolve and innovate.

MILLIONS of attacks bypass expensive email security solutions **EVERY YEAR**.

Download the **Annual State of Phishing Report** to learn how you can avoid a breach from the phishing threats that are targeting businesses around the globe.

DOWNLOAD THE REPORT

COFENSE

Avoiding assumptions about your cybersecurity with continuous security control validation

How next-gen breach and attack simulation technology is enabling security leaders to measure risk and answer difficult questions from the boardroom.

Tim Ager reports

The constantly evolving threat landscape makes it hard for CISOs and other security professionals to confidently answer questions such as 'How secure is my organisation right now?' and 'Are our defences able to protect us against the latest ransomware?'

Continuous security control validation removes the need for assumptions, providing a powerful capability to simulate real-world attacks as well as measure and maximise the performance of tools to prevent, detect and respond to them.

The need to prove security effectiveness and value

For too long security leaders have had to rely on penetration testing and red teaming exercises to help answer tough questions concerning cyber-risk. However, as important as these assessments are to conduct, they are point-in-time engagements and the results can quickly become out of date.

Being human-led, the time it takes to complete traditional assessments means that they also tend to be narrow in scope and costly. Rarely do they supply the full and quantifiable evidence that board members now demand as proof of security effectiveness and value.

The benefits of Breach and Attack Simulation

Breach and Attack Simulation (BAS) is a rising trend in cybersecurity that is enabling organisations of all sizes to obtain a more complete and current understanding of their security posture. BAS tools address the limitations of other security assessments by safely automating real-world attacks and by measuring the performance of network, endpoint and email controls to defend critical assets against them.

Early BAS solutions were developed to validate the efficacy of firewalls and other prevention-based controls to block threats. However, more advanced platforms are now able to provide a more holistic view by also evaluating the detection capabilities of Security Incident and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools.

The need for a continuous approach

New adversarial tactics, infrastructure drift and misconfigurations mean that threats can too easily slip through the net. A key feature of the latest BAS tools is their ability to validate and report on the effectiveness of security controls continuously – ensuring that performance can be benchmarked and any weaknesses swiftly identified and addressed.

Among the performance areas that the latest BAS solutions can validate includes:

- threats being blocked by prevention controls
- logs and telemetry being captured and parsed
- security events being accurately timestamped
- correlation rules triggering alerts

Achieving the best outcomes

When evaluating BAS tools, it's important to prioritise an intelligence-led solution that is capable of simulating the latest threats as and when they emerge.

Mitigation support is also highly important. Verify that a solution offers actionable insights and vendor-specific prevention signatures and detection rules for the latest toolsets. Any supplied content will not only help to quickly address gaps but will also ease the pressure on your SOC team to develop, test and apply their own.

The reporting capabilities of a BAS platform should also be a key consideration. Ensure that the toolset you select offers easy to generate reports and dashboards to help track performance day-to-day and can map results to frameworks such as MITRE ATT&CK.

Be more proactive and threat-centric

The need for security leaders to measure risk and demonstrate the effectiveness of investments is more important than ever. Continuous security control validation with BAS helps to answer fundamental security questions being asked at the top of almost every organisation and is key to achieving a more proactive and threat-centric security programme. □

Tim Ager is VP Sales EMEA at Picus Security.

To learn how the Picus Complete Security Control Validation can help to validate, measure and optimize your security controls, please visit **www.picussecurity.com**

PICUS

PICUS

THE COMPLETE SECURITY CONTROL VALIDATION PLATFORM

AWARD-WINNING BAS TECHNOLOGY

SIMULATE

real-world threats
continuously and on-demand

VALIDATE

network security and
detection tools

MITIGATE

coverage and visibility gaps
quickly & easily

The Complete Security Control Validation Platform

- Become more proactive and threat-centric
- Strengthen your cyber resilience
- Prove security effectiveness

Request a demo today!

www.picussecurity.com

2021 Cyber Security Awards WINNER BEST SECURITY PRODUCT OF THE YEAR PICUS COMPLETE SECURITY CONTROL VALIDATION PLATFORM PICUS SECURITY

CYBERTECH100 2021
The World's Most Innovative CyberTech Companies for Financial Services

2021 Computing Security Awards WINNER
Breach and Attack Simulation Solution of the Year

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022

Thinking differently to track down ransomware

Not only are ransomware attacks becoming more commonplace, but they're also more difficult to detect. This is because there's no sign of ransomware until the very end of an attack.

Vectra reports

Solving ransomware requires a new way of thinking. That might sound obvious to some, but when you consider that 65,000 ransomware attacks are expected by the end of the year – many of the current security systems and strategies just aren't up to the task. We're no longer dealing with WannaCry and NotPetya; in fact today's attacks don't rely on malware at all – at least not until it's too late.

So, what has changed? And more importantly, how do we stop it?

Ransomware, but not like the old days

At its core, ransom has always been about an item of value being held until price demands were met. And while that remains the same, the approach these days is much different. We're no longer seeing malware doing all the work to spread throughout a network, encrypting files along the way – that's the good news. The challenge, however, is that the effort and innovation put forth by ransomware groups like REvil and Darkside make it more accessible for criminals to launch attacks.

Not only are ransomware attacks becoming more commonplace, but they're also more difficult to detect. This is because there's no sign of ransomware until the very end of an attack. Up until that point, you're just trying to uncover unusual activity inside your systems that may or may not be recon conducted by attackers. This is where traditional security measures and prevention tools fail.

Detecting in-progress attacks

While these attacks can't be prevented by traditional security measures, it is possible to detect attacker activity that exists in your environment. This can also be done in a way that will allow security teams to contain malicious events in a timely manner. Time being the key here as Dark Reading recently reported that the global dwell time attackers remain inside an environment continues to drop.

Organisations are up against the clock when it comes to detecting attackers, and the tactics many criminals use today appear just like that of authorised users. This is where AI-driven threat detection and response can lend a hand. A good example of this can be seen in the recent Vectra Spotlight Report – Vision and Visibility: Top 10 Cybersecurity Threat Detections for Microsoft Azure AD and Office 365. The data shows

Organisations are up against the clock when it comes to detecting attackers, and the tactics many criminals use today appear just like that of authorised users.

specific examples of how security teams are using AI to detect and stop abnormal or unsafe activity that could lead to costly attacks.

The report discusses the top detections that customers use to mitigate malicious activity such as suspicious download and sharing activity and even mail forwarding techniques that could be used as an exfiltration channel. It's important to recognise that attacker behaviour typically comes in multiple stages and way beyond the initial compromise or entry. This could mean privilege escalation, persistence, lateral movement, internal recon and discovery, credential access, command and control and a multitude of other tactics. All of this activity is representative of human attacker behaviour inside an environment while attacks are being set up.

The bottom line is that organisations need to account for the complexity of today's expanded attack surface. This means having coverage that accounts not just for the extended enterprise, but the sophistication of ransomware operators along with the limitations of traditional security tools and the overall shortage of cybersecurity professionals.

AI-driven threat detection and response sees the telltale signs of ransomware at its earliest stages so organisations can stop it before encryption occurs. Security teams can also leverage AI to augment workloads, optimise analyst-based investigation and automate labour intensive threat hunting activities. Get to see first-hand how Vectra can track down ransomware in your environment, take a self-guided tour today. □

For more information, please visit
www.vectra.ai

VECTRA®

FIND and STOP RANSOMWARE

Ransomware is evolving, your threat detection and response approach better keep up.

Vectra's AI-driven threat detection and response platform allows you to:

- **Detect and respond** to intent-based behavior across everything, everywhere.
- **Agentless solution** for always-on security and no business disruptions.
- **Zero rule-writing.** AI-driven detection spots all stages of ransomware attacks.

Learn how to recognize the signs.
Schedule a demo by visiting
https://www.vectra.ai/demo

VECTRA®
SECURITY THAT THINKS.®

Where to spend on security depends on business objectives

Running a security operation is now a heavier task than ever before.

Lior Marom reports

Assets are moving targets because so many employees are still working from home – some likely will be for a while – and that means more possible vulnerabilities and less control. Organisations are shoring up security by building out their tools and technology and hiring to close skills gaps. According to a recent Cybersixgill survey of 150 CISOs, 85% of CISOs have budgets of more than $1 million. A whopping 97% expect their teams to grow this year, with 56% anticipating growth of up to 10%, and a third – 34% – expecting growth of 11–20%.

How CISOs approach these technologies and hiring decisions will go a long way in determining how their security posture evolves this year and beyond. There's an important balance to strike between the two, and you can't determine the right mix without taking a step back to understand the business itself.

Which CISO are you?

CISOs are defined by how they approach key decisions like technologies to implement and hiring. There are two major philosophies: Some CISOs are optimisers and some are satisficers.

Optimisers focus more on gathering as much data as possible and building ideal scenarios (good luck with that) before making decisions. They hold out for a bigger budget to address any issues that may arise. If the right teams and tools don't exist already, an optimiser won't be ready to start building or updating a cybersecurity system until they have enough information to know they've made the best choices.

Satisficers will of course wish for those ideal conditions, but they work within the current landscape and identify more solutions than problems when considering a security plan. In this situation, a satisficing CISO can prioritise what is best for the business and optimise the budget accordingly. Especially these days, CISOs have to do the best they can with the information available.

It's no surprise that satisficing is the better approach. Still, to find the best available solution, you need to fully understand how the business operates beyond just privacy and security concerns.

Building resources

Finding the right balance between technological innovation and manpower is one of the bigger challenges for CISOs. There are fantastic, effective tools and technology, but they can't work alone. They need proper support, whether a DevOps team or a SOC team, to run and maintain these tools on a daily basis. It has become an expensive and necessary requirement and will only grow more important.

According to Gartner Inc., worldwide spending on security and risk management is expected to exceed $150 billion by the end of 2020, 12.4% more than companies spent in 2020.

Finding the right tech tools and deciding how to spend that money depends on the structure of your company. A cloud-based operation will want more automated tools for an automated process. Any company not working as much on the cloud will likely want to spend on human oversight of the technology.

Take an active approach in creating those protections. Instead of playing whack-a-mole and reacting to vulnerabilities that have already been exploited, be aware of the building blocks of your company and its operations as clues for what might be most at risk. If an operation is running on AWS, for example, be diligent about finding and tracking chatter on hacking forums about vulnerabilities with that platform. If that's something threat actors are exploiting, you'll want to know as soon as possible.

Find the mix that works for you

Ultimately, the balance you'll need to strike between hiring and technology comes down to your business objectives. Based on what your company is focused on and investing in, you can make decisions that support your CEO and CFO.

But don't look at your security infrastructure as all or nothing. While an optimiser might have an uncompromising ideal in mind for the skills and tools needed to secure the organisation, a satisficer takes a growth mindset. This year, it might make more sense to invest in threat intelligence tools. Maybe next year you negotiate for a bigger budget to build out your security team or expand the DevOps team. Instead of waiting for the ideal situation, work within the constraints you have to make the most impactful decisions around security.

The right balance between tools and skills will come down to where your company is and where it's going. For every technology you're testing, for every hire you're interviewing, always ask how that tech or that hire will advance the company's goals. □

Lior Marom is CISO at Cybersixgill
For more information, please visit **www.cybersixgill.com**

Data classification: The cornerstone of regulatory compliance

Achieving compliance can be complicated.

HelpSystems reports

The primary reason most organisations look at classifying the data they create and handle is to control access to sensitive information, driven by the need to manage security risk, and comply with data protection regulations such as GDPR, CCPA, ITAR, and more.

All organisations have to comply with the rules of their industry bodies, as well as the nation states they operate in. Achieving compliance can, therefore, be complicated. There are a myriad of tools available to support the protection and control of data, ranging from point products, to whole integrated suites.

When recently asked what mix of technologies were seen to be the optimum for a strong data protection stance, Senior Analyst at Forrester, Enza Iannoppolo responded "Gaining a good understanding of where data is and what it is that requires protection it is very important. Using technology that can help with this task, such as data discovery and classification, is a good starting point." While adding "I would say that it's important to get started with classification ahead of DLP implementation."

While compliance with data protection regulations is non-negotiable, and the penalties for failure are severe, it is a mistake to see compliance solely as an inevitable burden. With a comprehensive and proactive approach, that involves a combination of people, process and technology, organisations can pivot from viewing compliance as an expense and turn it into a positive competitive differentiator and one that, over the long term, will prove to deliver business benefits.

The key drivers for data protection when it comes to regulatory compliance often fall into the following three brackets:

1. *The need to identify sensitive data.* What sensitive data is being created and stored, where is it, and how is it managed?
2. *Mitigate data leakage.* The need to enhance data protection controls to protect identified sensitive data and reduce the risk of data loss.
3. *Simplify and automate data security.* Can these processes be automated/simplified to increase operational ease for users?

In today's highly regulated data environment, organisations need to embrace and build an effective compliance strategy, as those that do will experience positive business benefits and undoubtedly reap the rewards.

As evidenced by Forrester, intelligent data discovery and classification is important in building a strong data security strategy within an organisation. By using a business-centric approach when it comes to classification policies can be built to the required degree of granularity, meaning that the labels and metadata applied to documents and data capture the necessary business context. Using a deeper level of context, as opposed to basic classification labels, fuels more effective data protection across the business. Not only can you quickly identify the sensitive data you hold, but the business context can be used to drive downstream tools such as DLP, DRM, and encryption.

By putting these measures in place, organisations can immediately demonstrate to regulators that they are taking the necessary measures when it comes to data protection. As we know, data protection compliance is not a one-time exercise, but something that needs to be sustained, therefore, organisations need the right solutions in place to achieve compliance ongoing.

Ultimately, in today's highly regulated data environment, organisations need to embrace and build an effective compliance strategy, as those that do will experience positive business benefits and undoubtedly reap the rewards. Those with low levels of data privacy protection and data governance software adoption need to change – and change quickly. □

helpsystems

Securing your sensitive data from creation to sharing

agari by HelpSystems

boldonjames by HelpSystems

clearswift by HelpSystems

digitaldefense by HelpSystems

filecatalyst by HelpSystems

goanywhere by HelpSystems

globalscape by HelpSystems

titus by HelpSystems

www. helpsystems.com

Why seasonality factors are important to anomaly detection in cybersecurity

It's important for organisations to detect anomalies to ward off potential cyber-attacks.

ManageEngine reports

Seasonality factors need to be considered while attempting to detect behaviour anomalies of users and hosts in a network. But before we make a case for that, let's first try and understand what seasonality is by looking at a few examples from daily life:

1. *Seasonality in product sales:* Numerous products such as chocolates, summer clothes, workout gear, and Halloween costumes belong to seasonal markets. The demand for these products typically peaks for a few days or months and then tapers off. Depending upon the market, the sales that can be attributed to seasonality can vary. For instance, the sales of winter clothes during the winter months may actually eclipse the sales during the rest of the year.
2. *Seasonality in water consumption:* This is an easy example to understand: People usually consume a lot more water during the summer months.
3. *Seasonality in the stock market:* Historically, stocks have underperformed between the months of May and October but have done well from November to April. There is a popular saying that goes, "Sell in May and go away."

Is there an example of seasonality when it comes to an organisation's computer network? Yes, there is....

In an organisation's network, users and hosts may exhibit seasonal behaviour such as:

1. A database server that's heavily queried on Monday every week.
2. A user who works on alternate Saturdays.
3. A user who accesses a particular file server only once a month, particularly on the last working day of the month.

The three examples above involve relatively rare occurrences that are seasonal in nature, but they're not anomalies.

An anomaly, by definition, is something that deviates from what's expected. These three activities (and others like it), though rare, aren't anomalies because they start to become accepted as normal after they occur a few times. They're normal activities that follow a seasonal trend.

Anomaly detection in cybersecurity

It's important for organisations to detect anomalies that happen in the network to ward off potential cyber-attacks. To do this, organisations typically use a security analytics solution or a SIEM solution that has anomaly detection capabilities fuelled by machine learning algorithms. This solution creates a baseline of expected behaviour for every user and host in the network. If a user's or host's observed behaviour deviates beyond a learned threshold, it's flagged as an anomaly and the risk score is raised accordingly.

Anomaly detection with the ability to identify seasonality

The machine learning algorithms used to detect anomalies must be able to account for seasonality. They should understand seasonal effects on the behaviour of users and hosts and be able to identify a particular activity as non-anomalous even if it's rare. After accounting for seasonality, no red flags should be identified and risk scores should not be raised. So, what if the activity occurs outside of this seasonal window? That would be an anomaly, as the use case below illustrates.

A seasonality use case

Your bank operates on the first and third Saturday of every month. On the second Saturday of the month, your security analytics platform notices an employee logging in to the network. A lesser-trained system would accept this; after all, the employee was online the previous Saturday, so why not today? But yours is well-trained to spot seasonal anomalies just like this. It knows the difference between the various Saturdays of a month. An alarm goes off, and the risk score of the employee increases.

Seasonality factors are critical for calculating the real risk posed by users and hosts in your network. Without considering seasonality, there are chances of both blind spots and false negatives. The anomaly detection engine within your SIEM solution should make use of this capability to show you a more accurate picture of what's taking place. □

Avoiding storage data leaks and PII regulation noncompliance

How can you be sure that your stored information is totally safe?

OPSWAT reports

A recent data breach at a large clothing retailer led to the exposure and leakage of private data of 7 million end-users. Threat actors hacked into a backup file stored on a third-party cloud platform and stole critical PII (Personally Identifiable Information) data like credit card numbers, encrypted passwords and history, contact information – addresses, phone nos. etc. This stolen information was then shared online where other hackers could use it to target more sites.

This raises the much more serious issue of ensuring data safety when it's stored on third-party cloud storage providers. The Covid-19 situation has forced companies to use shared storage capabilities, not only as backup but also for their day-to-day storage, as they adapt to provide WFH options to their employees.

As the common joke states – 'A cloud basically means other people's computer'. How can you be sure that your stored information is totally safe? Well… you can't.

Relying on the host provider for security is both naïve and irresponsible. A good example of how responsibilities for security are shared between the customer that owns the data and the cloud storage provider can be found in Microsoft Security Best Practices for Azure storage.

One very efficient way to avoid PII data leaks is to scan files before they are uploaded to the cloud and take a few additional security measures according to their content and context. For example:

- *Use DLP* (Data Loss Protection) to identify personal data (PII) in files before they are uploaded and stored in the cloud
- *Use CDR* (Content Disarm and Reconstruction) on any file saved to the cloud to verify it does not carry any malicious 'payload' that is aimed to steal information
- *Take remediation actions* on the scanned files to:
  - Obfuscate/'mask' PII data – for example replace or mask credit card numbers with XXXXXXXXXXX
  - Encrypt all files with PII data before they are uploaded to any cloud storage

OPSWAT designed MetaDefender for Secure Storage to cover the security holes for files and data uploaded to the most common cloud storage providers like AWS(S3), OneDrive, SharePoint, Azure, Box, Dropbox, Google drive and more.

The easy to integrate solution helps you secure and protect your mission critical data (whether stored on the cloud or on-premises) before it can be targeted by hackers, and helps you meet regulatory compliance requirements. □

For more information, please visit
www.opswat.com

OPSWAT.

OPSWAT. + ARROW

Critical Infrastructure Protection Solutions

Cross-Domain Solutions
Secure Device Access
Network Access Control
File Upload Security
Malware Analysis
Email Security
Storage Security
Developer Tools

The Synack Platform expands to confront the cyber-skills gap

Providing on-demand access to a highly skilled community of security researchers.

Peter Blanks reports

At Synack, we're truly committed to making the world a safer place. We're doing that by helping organisations defend themselves against an onslaught of cyber-attacks. We're doing it by harnessing the tremendous power of the Synack Red Team, our community of the most skilled and trusted ethical hackers in the world, and through the most-advanced security tools available today.

Now, the Synack Platform is expanding to help organisations globally overcome the worldwide cybersecurity talent gap. I am excited to announce the launch of **Synack Campaigns** to provide on-demand access to the SRT, who will be available 24/7 to execute specific and unique cybersecurity tasks whenever you need them – and deliver results within hours. This new approach to executing targeted security operations tasks will fundamentally change organisations' approach to cybersecurity by providing on-demand access to this highly skilled community of security researchers.

During my time at Synack, I've seen first hand how the Synack Operations and Customer Success teams creatively engage with the SRT to address a growing range of clients' security operations tasks, in addition to our traditional vulnerability discovery and penetration testing services.

Now, we are making these targeted security activities directly available to every organisation in the form of **Synack Campaigns**, available through the new **Synack Catalog**, also launching today on the Synack Client Platform.

I know from speaking to our clients across multiple industries that security teams are struggling to keep pace with the speed of product development. At the same time, they are trying to scale defences to meet the complexity and magnitude of today's threats. Our customers ascribe challenges with their growing backlog of security tasks such as CVE checks and cloud configuration reviews. On top of all of that, there's the need to implement industry best-practice frameworks such as OWASP & Mitre Att&ck. Essentially, customer security teams are struggling with demanding workloads and have asked us for assistance in a number of areas:

- On-demand access to talented Synack Red Team members who are available 24/7 and capable of completing diverse security operations activities across a growing range of assets.
- A flexible security solution that can be configured to meet their specific needs in one centralised platform with their existing pentesting insights.
- A security solution that delivers results quickly *(hours and days, not weeks or months)* and is aligned with their agile development processes.

Synack Campaigns expands the core capabilities of the **Synack Platform**, including our trusted community of researchers, an extensive set of workflows, payment services, secure access controls and intelligent skills-based task-routing to provide customers with the ability to execute a growing catalog of cybersecurity operations.

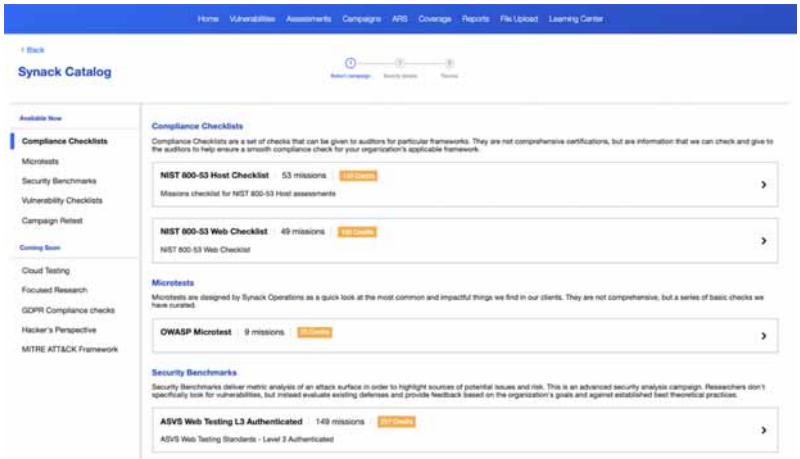
With **Synack Campaigns** our researchers can augment internal security teams by performing targeted security checks such as:

- CVE and OWASP Top 10 vulnerability checks
- Cloud configuration checks
- Compliance testing (NIST, PCI, GDPR, etc.)
- ASVS checks

Synack Campaigns are built to complement our vulnerability management and pentesting services, and help customers achieve long-term security objectives, such as application security, M&A due diligence, and vulnerability management.

We are excited for you to learn more about **Synack Campaigns** and to hear how you and your teams would like to leverage our on-demand community of researchers to address your organisation's growing operational security needs. □

The new **Synack Catalog**, where customers can discover, configure, purchase and launch **Synack Campaigns is available** now on the Synack Client Portal. Please speak with your CSM to have this feature enabled for your organisation



Peter Blanks is Chief Product Officer at Synack.

Reach out to us with your thoughts or for more information visit us at **www.synack.com**

THE MOST TRUSTED CROWDSOURCED SECURITY TESTING PLATFORM

SECURITY AT SCALE

A continuous and augmented approach that combines the best of human and machine to deliver security that is Controlled, Smart, and Efficient.

WHAT WILL YOU CHOOSE?

Traditional Pen Test:

2 Consultants, 80 Testing hours

OR

Synack:

4x higher ROI

40% faster and more impactful results using the best in human and artificial intelligence

SCALABLE. TRUSTED. PROVEN.

LEARN MORE AT WWW.SYNACK.COM

An API security balancing act: Shielding right while shifting left

The adoption of APIs is synonymous with the shift left movement where APIs are developed and released rapidly, and the speed that developers can now deploy APIs can introduce coding vulnerabilities that can lead to API security incidents.

Cequence Security reports

Organisations are rapidly adopting an API-first development methodology brought on by the power, flexibility and efficiency that APIs provide. The shopping, finance, manufacturing or marketing apps in use today are all based on APIs, connecting back to compute resources located elsewhere – be it the cloud, the datacentre or both. The adoption of APIs is synonymous with the shift left movement where APIs are developed and released rapidly, in an iterative manner and development teams are given more responsibility for security. The speed that developers can now deploy APIs can introduce coding vulnerabilities that can lead to API security incidents as seen in the past year (e.g., Peloton, John Deer, Experian). Make no mistake, shift left **is** improving API security as a whole, but developers are admittedly not security experts with some expressing frustration with the amount of time spent on fixing code. A balance must be struck where protection mechanisms are in place to prevent attacks on existing and newly released APIs. Organisations need to shield right while shifting left.

Shield right step 1:
API threat surface area discovery

Most organisations have no idea how many active APIs they have, evidenced by both customer conversations and industry research. Neither the security team nor the DevOps team can protect what they do not know exists. The first step towards effective API security is to gain a complete picture of your API attack surface area.

Shield right step 2:
API risk assessment and remediation

API Security and DevOps teams can be overwhelmed when the API discovery uncovers many shadow and unmanaged APIs. But not all APIs are created equal, some APIs are informational, posing minimal risk while others pose higher risk. Those with higher risk may be using sensitive data – PII, PCI, or PHI – or are not properly authenticated, while others may be prone to business logic attacks like account takeovers or scraping. Teams can avoid being overwhelmed by categorising APIs based on their risk exposure using customisable risk assessment and specification conformance analysis rules. Those APIs deemed high risk can then be prioritised for remediation by development.

Shield right step 3:
Native detection and mitigation

The rash of security incidents in 2021 has shown that web protection tools fall short when it comes to API security. Most APIs are not vulnerable to traditional cross-site scripting and SQL injection attacks. APIs are not designed to use session cookies; they don't follow SQL syntax to access the backend database and they use JSON or XML, not JavaScript. This means, traditional WAFs or bot prevention tools are ineffective in protecting the (newly) inventoried APIs – either natively or through integration with other tools. The result is a false sense of (API) security. API security should include the ability to natively detect threats hiding in plain sight and respond without reliance on 3rd-party tools.

Shifting left while shielding right with Cequence Security

Cequence Security can help your teams strike the perfect balance between shielding right and shifting left with the only API Security Platform that unifies runtime API visibility, security risk monitoring, and patented behavioural fingerprinting technology to natively detect and protect against ever evolving online attacks. The Platform is proven to be effective in eliminating data governance violations caused by unintended data leakage and preventing online fraud, business logic attacks, and exploits, which helps our F500 customers remain resilient in today's ever-changing business and threat landscape. □

Learn more and request your free API security assessment today.
cequence.ai/demo

CEQUENCE SECURITY

CEQUENCE® SECURITY

Protect Your APIs and Empower Your Developers

DISCOVER
your entire API attack surface area

DETECT
risks and threats hiding in plain sight

DEFEND
natively, in real time

The Most Comprehensive API Security Solution on the Planet

Organizations that rely on APIs to power their businesses trust Cequence Security to deliver the most comprehensive API Security Platform on the planet. Cequence is the only API Security Platform that unifies runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to natively detect and protect against ever evolving online attacks. The Platform is proven to be effective in eliminating data governance violations caused by unintended data leakage and preventing online fraud, business logic attacks, and exploits, which helps our F500 customers remain resilient in today's ever-changing business and threat landscape.

100+
Global Brands Protected

5B+
API Transactions Analyzed Daily

0%
Customer Churn

Request a Demo and a FREE API Security Assessment Today!

CEQUENCE.AI/DEMO

Managed threat hunting – the benefits of outsourcing

Data rates are increasing day by day. Threat actors are constantly evolving their Tactics, Techniques and Procedures (TTPs). A perfect storm is brewing for security analysts and outsourcing security elements can benefit more than just security.

Telesoft reports

Data, data, data…

It is becoming increasingly challenging to comprehensively monitor networks; the traffic generated on a daily basis is at an all-time high and threat actors are using ever more sophisticated defence evasion techniques. This helps them to not only maintain persistence in the network for a prolonged period of time, but also ensures they have sufficient time to understand their target infrastructure to exact the maximum effect. And the same is true for all networks, from small or medium enterprises, up to CSP/ISP and network operators – if we are connected to the internet, then we are a potential target, it is all a matter of time. But how can we identify these evolving TTPs if they continue to evade endpoint security solutions? More importantly, how can we identify them within our network before they carry out their malicious actions?

Sophisticated adversaries

Security needs to be considered from a more holistic approach. There is no 'one size fits all' or 'silver bullet' in cybersecurity and, consequently, a multitude of platforms and capabilities are required to provide a more complex and comprehensive security posture, creating a more challenging environment for threat actors to navigate.

Most organisations utilise a number of security solutions such as endpoint security, antivirus, firewalls and so on. Unfortunately, as we continue to witness in the news despite these security solutions, threat actors are still conducting successful operations. So, are these solutions ineffective? Of course not, but it has to be acknowledged that cybercriminals continue to evolve their understanding of our environments and defensive capabilities in order to bypass them and compromise a network more effectively. To bolster their cybersecurity, organisations should consider augmenting their existing infrastructure with tools that provide enhanced visibility that existing solutions may not provide.

Extended visibility

Network security solutions are vital in enhancing an organisations' security posture. Being able to see what is happening within a network is crucial to detecting threats, but being able to identify anomalous communications or beaconing outside of a network is vital to see what the endpoint solutions often miss.

Visibility into an organisations' network traffic enables detailed analysis to be conducted by security analysts, enabling identification of changes in traffic patterns of behaviours that could indicate malicious activity, such as communications with Command and Control (C2) servers. This can often initiate the start of an investigation into a device of interest, enabling the identification of a compromised device before malware has been able to have an effect.

This proactive identification of anomalous communications activity can help an organisation to not only identify previously unknown malicious activity within their network, but it can also help to plan a response and mitigate the attack efficiently before it can have a negative impact, reducing costs associated with remediation, reputational damage and so on.

Outsourcing

Additional tools, however, also require additional training, recruitment or upskilling existing analysts to make the most benefit from it. Consequently this leads to additional costs, making it another barrier to entry for many small to medium enterprise organisations.

Outsourcing these requirements to service providers who can provide a comprehensive network security monitoring and threat hunting solution can be an attractive and cost-effective solution for enterprise organisations. Not only does it enable an organisation to strengthen their monitoring capabilities across all the growing data volumes, but it also enables them to proactively identify malicious activity before threat actors can exploit the network. □

DO YOU HAVE EYES ON YOUR NETWORK?

OUR 24/7/365 UK BASED THREAT HUNTING SERVICE OFFERS ROUND THE CLOCK NETWORK SECURITY MONITORING, THREAT HUNTING AND INTRUSION ALERTING.

WE ARE ALWAYS WATCHING...
www.telesoft-technologies.com

TELESOFT

SECURING FINANCIAL SERVICES

6th July 2022 London

2021 sponsors included:

Strategic Sponsors

DARKTRACE
ExtraHop
FORTINET
INTSIGHTS Democratizing Threat Intelligence
proofpoint.
okta
Recorded Future

Education Seminar Sponsors

BeyondTrust
Centrify
LogRhythm
MENLO SECURITY
OneTrust GRC
RANGEFORCE
RED SIFT
virtru
zivver

SECURING THE LAW FIRM

6th July 2022 London

September 2021 sponsors included:

Strategic Sponsors

DARKTRACE
MENLO SECURITY
Recorded Future
TENEO OPENING MINDS

Education Seminar Sponsors

ankura
bitglass
Cryptshare
egress

Networking Sponsors

CyGlass by NOMINET

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

e-Crime & Cybersecurity Mid-Year Summit 2022

"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 call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

Thank you to all our sponsors

Strategic Sponsors

BeyondTrust
BEYOND IDENTITY
CROWDSTRIKE
DARKTRACE
illumio
imperva
MENLO SECURITY
NETACEA
okta
proofpoint.
Recorded Future
RED SIFT
SENSE ON
TESSIAN

Education Seminar Sponsors

data SOLUTIONS
CEQUENCE SECURITY
COFENSE
CybelAngel
cybersixgill
DEVO
FIREMON
helpsystems
INTEL471
CISCO | KENNA Security
ManageEngine
OPSWAT.
PICUS
Synack
VECTRA

Branding Sponsors

C2 CYBER LTD RESILIENCE REALISED
ORCHESTRA
TELESOFT