e-crime & cybersecurity CONGRESS

3rd and 4th March 2020
London

@eCrime_Congress
#ecrimecongress

#ecrimecongress

The age of convergence:
Can CISOs adapt?

WHEREVER YOUR BIG IDEA LIVES, EXTRAHOP SECURES IT.

Detect threats up to 95% faster with
Cloud-Native Network Detection & Response.

ExtraHop

Rise Above the Noise.

Welcome

Digital transformation is upending companies' treatment of IT, security and information risk. In the old model, as budgeting and seniority reflect, cybersecurity is not viewed as a strategic imperative, nor is it seen as a major threat to the business. But now, as companies are primarily interacting with their customers and supply chain digitally, things are starting to change. Without technology and data, there is no business.

Digital transformation turns cybersecurity into the major business risk that CISOs and vendors have been warning of and in the post-DX business, old models of security, privacy, fraud and data integrity are untenable. Cybersecurity needs to be prioritised, analysed and managed like other (often more business-critical) risks and operate according to standard risk management practices.

At the same time, intimately related activities such as fraud detection and prevention, data management, PCI DSS and data privacy are often still siloed away from each other and from security teams. Cybersecurity must enable and secure the data centralisation, analytics and visibility required to deliver truly digital services and it must be integrated into the anti-fraud effort. In short, a new level of business orientation and rigour is needed to shape a new era of cybersecurity. And the effects on CISOs, their staff, and the entire function will be profound.

The 18th anniversary edition of the flagship e-Crime & Cybersecurity Congress will address these and other key issues through strategic guidance, case studies, animated panel discussions and more from senior business leaders in the space. One of the main aims of our events is to facilitate conversation so please take the opportunity to mingle with peers and colleagues. We hope you enjoy the event, if you have any questions please don't hesitate to ask any member of the team.

Ruby Mercer | Editor

@eCrime_Congress **#ecrime20**

3rd and 4th March 2020

Park Plaza Victoria London, UK

Editor:
Ruby Mercer
e: ruby.mercer@akjassociates.com

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

Forum organiser:
AKJ Associates Ltd
27 John Street
London WC1N 2BX
t: +44 (0) 20 7242 4364
e: ruby.mercer@akjassociates.com

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

Right-sizing risk: Talking to the board about cybersecurity

Top strategies for CISOs and CIOs to have an effective board-level conversation.

As enterprises have become increasingly reliant on technology for every aspect of operations, technical executives like CIOs and CISOs have found themselves in a completely new operations centre: the boardroom. This shift is more recent for CISOs, who increasingly must demonstrate security and compliance at a board level. This move from the security operations centre can present a significant challenge. Board members are often not well-versed in technology or security best practices, let alone jargon. At the same time, CISOs (and CIOs) often lack the business experience to speak in terms that the board can understand, defaulting to technical discussions that the board can't parse.

This breakdown in communication can have a cascade effect. The board might fail to fully understand the security risks posed by a certain initiative. Or, with the growing number of costly and embarrassing security breaches, they might overemphasise caution and risk mitigation at the expense of implementing important technical advancements.

As a long-time executive in the technology industry, I've spent my fair share of time in boardrooms. I know how boards view risk, and how to effectively communicate about it.

Below are my top strategies for CISOs and CIOs to have an effective board-level conversation about right-sizing risk.

Get aligned

One of the first steps to successful board communication is getting alignment between security, IT operations, and line of business priorities. While IT operations and security operations often find themselves at odds – the former wanting to accelerate adoption and development, the latter wanting to put as many safeguards in place as possible – they ultimately represent two sides of the same coin.

Even as enterprise budgets get poured into security initiatives, at the board-level security can often be seen as a necessary evil, and sometimes an outright impediment to business operations.

The board isn't going to understand the technical nuances of why or how requiring certain security measures will impact DevOps cycles or application rollouts, but they will understand the trade-off between speed to market and security. For technical leaders planning in advance how to address these trade-offs at the business level will minimise confusion, and in the event something goes wrong in the future, it will ensure a baseline of understanding across all stakeholders.

Build a roadmap to 'yes'

Even as enterprise budgets get poured into security initiatives, at the board-level security can often be seen as a necessary evil, and sometimes an outright impediment to business operations. Almost everyone has a story about how some 'draconian' security requirement prevented them from using a technology that they needed to better perform their job. This pain point gave rise to an entire category known as 'Shadow IT' – itself a massive security headache.

For the board, these anecdotes can make it feel like security is diametrically opposed to innovation. This is why it's critical for CISOs to come prepared with a roadmap for getting to 'yes'. If CISOs, together with CIOs, can demonstrate a clear understanding of business requirements and objectives and talk about what security measures need to be in place to achieve them, it reframes the conversation around 'when' not 'if'.

With this approach, CISOs will demonstrate a strong understanding of business strategy and cross-functional implications that build trust and credibility with the board.

Demonstrate knowledge of the gaps (and how to close them)

While process and strategy are an important part of 'getting to yes', at a macro level, getting to yes also means identifying and closing the gaps in your security architecture. CISOs should be prepared to communicate their security posture in terms of the key gaps in enterprise security programs and their coverage model. This includes an overview of the technologies they have in place – such as next-gen firewall, SIEM, and end-point protection – as well as the technologies they plan to implement to close gaps in their architecture – such as cloud access

ExtraHop reports

Helping the board to understand that there is no such thing as fool-proof security but that the risks are well understood will manage their expectations about what is possible and what risks actually exist.

security brokers (CASB) and network detection and response (NDR).

Focus on risk and reward to the business

One of the most critical success factors for CISOs in a board setting is mapping the priorities of the security team to core business objectives. While the security team might consider having zero expired SSL certificates a major achievement, the board likely has no understanding of the business implications of this effort. For CISOs, presenting this information in the context of business objectives can make all the difference. In the case of SSL certificates, that means talking about the implications for consumer trust, service reliability, search engine rankings, and website engagement and conversion. Framed this way, maintaining SSL certificates is a driver of important business outcomes.

While SSL certificates are just one example, if CISOs brief the board through the lens of the organisation's top objectives and how they are supporting them, the conversation will be much more productive.

Put risk in perspective

Headline-grabbing breaches can draw a lot of attention from business stakeholders and board members who want to avoid finding themselves in similar circumstances. But not all breaches are created equal. Some breaches, like those due to misconfigured cloud services or ransomware attacks, are incredibly common. Others, like those involving service provider employee malfeasance, attract a lot of attention but are vanishingly rare.

Lead with resilience

While major breaches may be the catalyst for bringing CISOs into the board room, focusing on breach prevention is probably a losing strategy. Going in and telling the board that the organisation is 100% secure is setting the security team up to fail, and setting up the CISO for a new acronym: Career Is Soon Over.

The first step in this conversation is education. Helping the board to understand that there is no such thing as fool-proof security but that the risks are well understood will manage their expectations about what is possible and what risks actually exist.

The second step is to talk about resiliency – how the organisation will recover in the event of a breach, what measures are in place to react quickly, and how the security team can effectively investigate and use that knowledge to move forward in a more secure and intelligent way. □

Achieving security without compromise

How isolation is challenging the 'almost secure' security architecture.

Mehul Patel reports

The internet has become integral to the way people work. No longer are users chained to their desks or the data centre. They are more mobile, more collaborative, and more flexible than ever, leveraging web-based apps, rich media websites, and Software as a Service (SaaS) platforms to complete daily responsibilities and engage with customers. The internet is also a cesspool of cyber-attacks, many of which are delivered to people through everyday use of the browser and clicking on links in email.

Once confined to gateways that guarded the data centre, a company's attack surface is now unlimited and ubiquitous – basically everywhere users log in from, whether it's at a remote office, from home, at a customer site, through public Wi-Fi, or while lounging at the beach. The more tools used by an enterprise, the greater the attack surface that the security team needs to track, monitor, and secure.

According to Blissfully, enterprises with more than 1,000 employees are adopting SaaS platforms at a rapid pace, with each employee using an average of 9.5 SaaS apps as part of their daily routines.

SaaS adoption by the enterprise is no secret. Malicious actors – including cybercriminals and cyber-terrorists, insider threats, industrial spies, and hacktivists – are capitalising on this trend and are increasingly using popular SaaS platforms as an attack vector. Credential theft and malware downloads are the two most common types of attacks, and, like the original Trojan virus, these new attacks use social engineering with the intent to gather valuable data or install a backdoor to gain unauthorised access remotely.

The danger to enterprises is real – many of these services are actually whitelisted by security products, since they are approved services. This means that security products that block phishing links or user access to malware are bypassed, leaving the enterprise little or no defences against these advanced attacks.

Credential theft and malware downloads are the two most common types of attacks, and, like the original Trojan virus, these new attacks use social engineering with the intent to gather valuable data or install a backdoor to gain unauthorised access remotely.

Traditional cybersecurity solutions fall short

Unfortunately, simply moving traditional cybersecurity solutions to the cloud does not work. These solutions, designed for the data centre, are ill-equipped to deal with today's increasingly sophisticated threats.

- *Detect and respond is broken:* Today's cybersecurity threats move too fast for even the most robust threat intelligence service. Any insight is likely to come to light too late, as threat actors are able to spin up and customise out-of-the-box phishing and malware attacks from the dark web easily and cheaply with little or no coding expertise. In addition, making an allow-or-block decision at the point of click produces too many false positives, preventing users from accessing legitimate web content they need, while overwhelming the help desk. The result of these dual pain points? User productivity suffers and attackers are still able to gain a foothold on the network.
- *Scaling is cost prohibitive:* SaaS platforms, rich media websites, and powerful web apps require constant connectivity to users' machines. Office 365, for example, requires 20 persistent connections to enable real-time editing and collaboration. Unfortunately, traditional security stacks were not designed with this volume of traffic in mind, putting enormous pressure on network connectivity and bandwidth. Scaling security appliances to provide local internet breakouts on a global level is simply not something that can be done easily or cost effectively.
- *Lack of visibility into web browsing creates risk:* Another problem occurs when traditional hub-and-spoke security architecture attempts to decrypt https websites – a protocol that 90% of current websites use. Appliances and traditional security solutions simply cannot handle the increased load caused by the advanced encryption techniques that are used by https, preventing organisations from gaining visibility into https traffic to identify and block malicious content.

It's clear that cloud transformation is forcing enterprises to fundamentally rethink how to provide users with secure internet access wherever they do business.

Menlo Security's technology enables secure cloud transformation by creating near-latency-free connections to our global elastic cloud. The practice provides branch and remote users with direct-to-internet connectivity for faster SaaS response times in a worry-free web browsing environment.

Security without compromise

Rather than continuing to use an appliance-based security strategy that relies on an allow-or-block decision at the point of click, enterprises need to deliver security services through the cloud. Cloud security ensures that policies (such as isolation) follow users wherever they log in from – whether it's from corporate headquarters, a remote office, a customer site, or public Wi-Fi.

The Menlo Security product suites, powered by an Isolation Core™, provide this cloud security. It acts as the central choke point for all traffic, providing a ubiquitous and separate security layer in the cloud. It's here where malicious traffic is blocked while all other traffic is isolated far from the end user's device. It doesn't matter if there's a known or unknown vulnerability on the endpoint, because no content – whether it is malicious or not – is executed on users' browsers.

Menlo Security in action

Social engineering is a common attack used by malicious actors today. These are essentially phishing attacks designed to seem like legitimate requests that trick users into taking a risky action like opening a document, clicking on a link, or entering their credentials into a fake web form.

Often, a malicious actor will host a malicious document in a cloud storage account such as OneDrive, Google Drive, Box, or iCloud and share it with targeted users under the guise of an unpaid invoice, a statement of work, or another action that may be relevant to the target's daily responsibilities. Once the document is opened, users are encouraged to click on a link that takes them to a fake web form, funnels them to a compromised site, or tricks them into downloading a malicious document. Other times, a malicious actor will spread malware via shortened URLs hidden inside social media ads. The user clicks on the ad, thinking they are going to a branded website or microsite, but the user is instead redirected to a fake website or document.

Traditional cybersecurity solutions will not protect users from this type of attack, simply because they are not fine-tuned enough to determine legitimate from fake content purporting to be from Microsoft, Google, Amazon, Apple, or other popular social media and file sharing sites. Organisations know this and have to choose to add this type of traffic to either a whitelist or a blacklist. Blocking all traffic prevents users from accessing these sites at all, severely limiting productivity, but allowing all traffic puts the organisation at tremendous risk of this increasingly popular type of cyber-attack.

With Menlo Security's solution, no such allow-or-block decision needs to be made at the point of click or as policy. All known malicious content is blocked, while all other traffic is isolated in a remote browser in the cloud far from the end user's device. Users can click on any link in an ad, social media post, or email, and they are 100% protected. They can click with impunity, knowing that malicious content has no avenue for infecting their device. Menlo Security can also render web forms as read only, preventing anyone from inadvertently giving their credentials to malicious actors.

Menlo Security's technology enables secure cloud transformation by creating near-latency-free connections to our global elastic cloud. The practice provides branch and remote users with direct-to-internet connectivity for faster SaaS response times in a worry-free web browsing environment. This allows enterprises of all sizes to give workers ubiquitous access to the tools and information they need, wherever business takes them. □

Mehul Patel is Menlo Security's Director of Product Marketing. He has more than 20 years of experience in the cybersecurity industry. Previously, he founded Lattice Security, an enterprise data protection solution, and he has held product management leadership roles at Proofpoint, Cisco, and ScanSafe. Earlier, he worked at Deutsche Bank as an analyst, and he holds an MBA from Imperial College of London. As an industry leader in the cybersecurity space, Mehul is well-versed in data protection, threat analysis, networking, internet isolation technologies, and cloud-delivered security, as well as in finding the best pubs in London.

Menlo Security

SECURITY WITHOUT COMPROMISE

No Malware Guaranteed

Learn more at menlosecurity.com

Orange Cyberdefense

Europe's leading managed security threat detection and threat intelligence services provider.

We provide integrated solutions that assess risk, detect threats, protect our customers IT assets and respond to security incidents.

info@uk.orangecyberdefense.com
orangecyberdefense.com

The state of the threat

There are three distinct forces at play. These forces are unpredictable but always present; they are somewhat uncontrollable, but we can react accordingly if we acknowledge the impact they can have both on our business and our cybersecurity strategy.

Data breaches exposed 4.1 billion records in the first half of 2019, with total fines doled out to non GDPR-compliant companies reaching €428,545,407 by the end of last year. Amongst the victims, we saw universities, government departments, global organisations, huge corporations and smaller businesses crumble at the hands of opportunistic hackers.

As nation states lock horns on the cyber-battlefield and hackers ransack businesses for personal gain, cyberspace is starting to feel hostile. In light of clear and present danger online, organisations are largely responding in panic. Worldwide spending on cybersecurity is forecast to reach $133.7 billion in 2022, according to Gartner. But, as RSA Chief Executive Art Coviello expressed in 2017, a lot of spending today is misplaced, with strategies being driven by fear and the *perception* of threats. Security and compliance vendors often capitalise on this fear, and sell the products they *have*, rather than the solutions customers *need*.

At Orange Cyberdefense, we are committed to developing and delivering products and services that enable our customers to address *genuine* threats, with the least possible impact on financial and human resources. This starts with a more realistic look at what these genuine threats are, as well as how to identify and track them as the threat landscape inevitably shifts.

When it comes to the threat landscape (or the state of the threat) as we know it today, there are three distinct forces at play. These forces are unpredictable but always present; they are somewhat uncontrollable, but we can react accordingly if we acknowledge the impact they can have both on our business and our cybersecurity strategy.

A lot of spending today is misplaced, with strategies being driven by fear and the perception of threats. Security and compliance vendors often capitalise on this fear, and sell the products they have, rather than the solutions customers need.

Geopolitical forces

The first of the three forces is **geopolitics**, which can equate to military, political, economic, social or legal factors on a national or international level. Geopolitical forces are the result of the vast energy and resources that governments inject into an environment when they have the political will to do so. Collectively, geopolitical forces have more impact on the state of the threat than any other factor.

The recent splintering (or balkanisation) of the internet is a prime example of geopolitical forces at work. This is perhaps epitomised by recent developments between Huawei and many nations across the globe, as corporations begin to scale back implementations and usage of the Chinese company's technology, for fear of surveillance and insecurity.

As we cannot control or prevent geopolitical forces, our only choice here is to observe them and orient ourselves accordingly.

Structural factors

The second force is **structural factors** – the enablers and constraints woven into our local environments. They can have a significant impact on the shape the threat takes, and our ability to respond to it.

These structural factors include, but are not limited to:

- *Innovation by criminals* – new ways of monetising existing attack methods, such as crypto-mining and ransomware, which change the nature of the threat at a rapid rate.
- *Cyber-insurance* – whilst in its infancy, cyber-insurance promises to remove much of the uncertainty and angst from breaches and hacks and, as a result, is shaping our strategies, policies and technology choices. Insurance providers are having a further impact on the threat landscape when they make the decision to pay ransom on behalf of their insured clients, rather than accept the much higher cost of responding and recovering from a compromise. In doing so, they in fact fuel the cybercrime economy and even create price inflation that draws more black hat players to the space.
- *Regulation* – in conjunction with insurance, government regulations are playing a dominant role in shaping our landscape. Collectively, these

Orange Cyberdefense reports

As threats continue to evolve, it's important for businesses to recognise that attack is inevitable. But an understanding of the real risks posed, and strategic engagement with the cyber-enemy is essential, affordable and achievable with the right insight, expert knowledge and tools.

regulations are certain to impact corporate spending, strategy and behaviour in a significant way. GDPR promises to shape the future of information security in Europe. The emerging Californian Data Protection legislation will likely have a similar impact in the United States.

Structural factors can significantly shape the current state of the threat. From a defensive point of view, structural factors are beyond our power to control, but we can often influence them.

The evolution of technology

The third and final force is the **evolution of technology** – as the technology at our disposal changes, so does the threat and our response to it.

However, new technologies (think cloud technology, artificial intelligence and more) rarely replace old ones – they simply add to them. Therefore, over time, a business becomes burdened with a deep pool of security 'debt' that never goes away. New and evolving technologies will probably not reduce the risk, but only add new potential threats.

The good news is, technology is something we can exert control over. We can choose which technologies to adopt within the business, and how and when we deploy others to address cyber-threats, thereby reducing the size of our attack surface and limiting risk by finding vulnerabilities. Since these efforts are completely under our control, it makes perfect sense for us to use recognised best practices to do so.

Building a threat map

By addressing the factors that influence today's threat landscape, we can then start to build a holistic threat map of the '*genuine*' threats that emerge and can impact businesses – whether that's supply chain attacks, OT attacks and abuse, ransomware or otherwise. As a business, we also collect and analyse data (as a function of our role as an operator) to track, validate and tune our assumptions of this threat map on a continuous basis.

As we're only able to control one of the three key factors – the evolution of technology – it stands to reason that this should be our immediate short-term focus, setting guidelines and best practice on how we can smartly deploy technology, people and processes to counter threats. That said, we also need to accept and anticipate that this alone will not be enough to achieve the level of resilience we require, considering the other factors at play.

Tipping the scales

In contemplating the state of the threat today, it's clear that businesses of all sizes and sectors are going to find themselves in a constant, dynamic state of conflict with cybercriminals, who are aided by large, systemic forces over which we have little to no control. These factors collectively outweigh all the resources that we as defenders have at our disposal.

We therefore need to prepare to engage our adversaries in an active manner, behind the traditional perimeters of our environments. This includes the deployment of mature and effective detection and response capabilities to minimise attackers' element of surprise and significantly increase their cost state as well as drive their efforts back and limit the real damage they can cause to the business bottom line.

Cybersecurity is complex and we cannot hope to predict what tomorrow will bring. As threats continue to evolve, it's important for businesses to recognise that attack is inevitable. But an understanding of the real risks posed, and strategic engagement with the cyber-enemy is essential, affordable and achievable with the right insight, expert knowledge and tools. □

Changing from network access to application access should be part of any digital transformation

The workplace is changing, which is leading many companies down the path of digital transformation.

Employees are no longer anchored to their desks or beholden to the corporate data centre. The digital employee of today demands flexible access to data and applications regardless of where those resources are stored, which device the employee is using or where the employee might be working.

Users accessing corporate resources as part of their day-to-day working lives aren't concerned with how they are being connected. They just want access to what they need, when they need it. With the proliferation of enterprise apps and a growing number of mobile and remote working policies, organisations need to change their approach when it comes to network security. Gone are the days of allowing employees unfettered access to the network, as these employees are no longer secluded behind the corporate firewall. Organisations must enable secure application access without necessarily granting access to the corporate network each time, as this inevitably introduces risk.

However, any change must first be preceded by the acceptance of a new approach. This is becoming easier by the day, as even the most stubborn deniers can no longer ignore the benefits of a cloud transformation. This is evidenced by the latest survey data from Atomik Research. According to the State of Digital Transformation–EMEA 2019 report, digital transformation efforts are gaining ground among EMEA businesses, with a majority now conscious of its benefits. More than 70% of decision-makers in the UK, Germany, France and the Netherlands within enterprises of more than 3,000 employees are already in the implementation phase of their digital transformation projects or are already benefitting from a digital transformation initiative.

The digital employee of today demands flexible access to data and applications regardless of where those resources are stored, which device the employee is using or where the employee might be working.

Only 7% of the companies surveyed have not yet started, with many having already completed their transformation projects. Encouragingly, the survey also found that many of these digital transformation initiatives are being driven from the highest levels within the organisation.

While cloud transformation is undoubtedly a priority for most businesses, in reality, some companies remain at least partially locked into their legacy infrastructures. Even those businesses with a portion of their staff working remotely or on the move often retain a large amount of their on-premises resources. The cultural shift to a cloud-first infrastructure approach – along with moving applications to the cloud – seems to be too large a first step for many.

Yet, the mere relocation of applications to the cloud is far from a complete and secure cloud transformation. If applications are kept in the cloud and the internet becomes the new corporate network, how must secure access to these same applications be designed? Companies often neglect this network transformation step while in the planning stages. They remain loyal to their traditional structures and instead backhaul users over their legacy network. This detour not only affects speed, but also the security of the entire network.

Organisations must factor in the effect that application transformation has on their network performance and bandwidth consumption, as well as the latency added by hub-and-spoke architectures from the outset. Moving applications to the cloud needs to be considered alongside new network infrastructure and security requirements. However, the State of Digital Transformation–EMEA 2019 report found that only 9% of enterprises consider application, network and security transformation equally important when planning their journey to the cloud.

This holistic view is vital in any digital transformation project, as it plays a key role in the overall user experience. And, especially with today's digital workforce, user experience is of paramount importance. This means speed, reliability, security,

Zscaler reports

Companies should consider integrating zero trust network access as part of their secure cloud transformation from the outset to ensure the workplace of the future – as traditional network access is quickly becoming a thing of the past.

and usability are key factors to consider when embarking on a cloud transformation journey, irrespective of the size of the company in question.

As part of that experience, the user no longer wants to differentiate between applications that are kept in the cloud or on the network. Seamless access to applications is critical, whether they are held in private or public clouds, in Azure and AWS, or in the corporate data centre. Employees also expect business applications to provide the same smooth user experience they get from the consumer apps on their smartphones. This is the start of the transition to a limitless working environment. Whether the desk is in the office or home office, or whether the employee is a road warrior and accesses his applications and data from the hotel or airport, the path to that data must be secure and fast.

To ensure an undisturbed experience for the user, secure cloud transformation should also be accompanied by another change – from network access and to access at the application level. After all, if the application has already left the company network, why should the employee still be connected to the network and not immediately access the app on the most direct connection? Opening up the entire network to remote users only creates a security risk for the company. When companies undergo a cloud transformation for efficiency reasons, they must incorporate modern approaches to secure access at the same time.

The concept of zero trust is one approach. In this model, users are securely connected only to the applications for which they are authorised with ongoing verification of their access rights.

Companies should consider integrating zero trust network access as part of their secure cloud transformation from the outset to ensure the workplace of the future – as traditional network access is quickly becoming a thing of the past. □

zscaler™

Secure your cloud transformation

Zscaler is securing thousands of leading organizations as they move to the cloud, providing:

- Fast user experience
- Identical protection for every user, everywhere
- The full security stack, no compromises
- Local internet breakouts
- Unmatched security, no appliances

For more information, visit zscaler.com

CROWDSTRIKE

BUILT TO STOP BREACHES

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

FIND OUT MORE AT
CROWDSTRIKE.COM/SEEDEMO

Security resilience in the face of evolving attacker tradecraft

Stories from the cyber battlefield.

The impact left in the wake of a successful intrusion can be massive when customer data or other confidential information is stolen, exposed, changed or deleted. It's an inescapable certainty that where valuable digital assets exist, threat actors follow. From the global WannaCry ransomware attack to the destructive stealth propagation techniques of NotPetya malware, threat actors are continuously adopting new means to achieve their objectives.

To keep pace, security stakeholders from CISOs and SOC managers to incident responders must evolve their security strategies and ensure resilience in the face of new attacks. Below is real-world case study featured in the CrowdStrike *Cyber Intrusion Services Casebook, 2017.* This much anticipated publication offers detailed accounts of some of the cases the CrowdStrike Services incident response (IR) team has investigated over the past year, and provides expert, real-world analysis and practical guidance that can further your organisation's progress toward that goal.

Drawn from real-life engagements, the Casebook provides valuable insights into the evolving tactics, techniques, and procedures (TTPs) used by today's most sophisticated adversaries. It also describes the strategies the CrowdStrike Services team used to quickly investigate, identify and effectively remove dangerous threats from victims' networks.

One key trend the CrowdStrike team observed is that the lines between nation-state sponsored attack groups and e-crime threat actors continue to blur. As part of this trend, the increase in criminal hackers using fileless attacks and 'living off the land' techniques has been especially pronounced. This uptick in fileless attacks is also documented and independently verified in a recent report from Ponemon Research.[1] Fileless attacks include exploiting processes that are native to the Windows operating system such as PowerShell and Windows Management Instrumentation (WMI). 'Living off the land' describes how adversaries move within the victim's environment once they gain access, often employing anti-forensics tools to erase signs of their presence and increase dwell time.[2] Evidence of this trend is also reflected in the prevalence of brute-force attacks on RDP (remote desktop protocol) servers, which was also observed by the CrowdStrike Services team during their 2017 client engagements.

Situational analysis

A commercial services organisation contacted CrowdStrike Services after being hit by the SamSam ransomware variant, which is commonly associated with xDedic, a Russian-operated darknet forum. The e-crime operators of xDedic have been implicated in a number of nation-state attacks against public sector organisations (you can read more about them at: https://www.crowdstrike.com/blog/education-darknet-hackers-profit-data/).[3]

xDedic operates a market for the selling and buying of crimeware and compromised credentials used for accessing RDP servers. After xDedic sells access to these compromised RDP servers, they are then used in attacks against government agencies and other commercial targets.

Although the organisation had already paid the ransom when they contacted CrowdStrike, they sought help to prevent the ransomware from spreading to other systems and to determine the original point of entry by the attackers.

The CrowdStrike Services team first verified the exact ransomware variant used in the attack. Notably, the variant involved automatically encrypts files on the victim's network – a common ransomware tactic – however, it doesn't give the attacker the ability to access, acquire or exfiltrate data from the network.

The team observed that the adversary used Sticky Keys to launch brute-force attacks and gain RDP login credentials so they could move about the victim's environment freely. Sticky Keys is a Windows Ease of Access feature that enables keyboard shortcuts. Once compromised, it can provide an adversary system-level access without needing to authenticate and provided the attackers with an effective persistence mechanism.

Other fileless or 'living off the land' TTPs tied to xDedic that the investigators found included compromised privileged accounts and network login brute-force attacks, both of which reflect the varied toolsets a sophisticated threat actor leverages in order to penetrate a target environment.

Incident investigation and analysis

After conducting forensic analysis by deploying CrowdStrike Falcon® endpoint monitoring, the team

CrowdStrike reports

was able to identify the root cause of the intrusion that led to the deployment of the SamSam ransomware within the victim's network. Because they were able to identify the persistence mechanism used by the ransomware, the team could immediately stop its propagation and prevent it from encrypting any additional files. During this process, the team provided comprehensive analysis of a number of areas including:

- Forensic artifacts commonly seen in IR investigations
- Known malicious indicators in each image collected, including file names and MD5 hashes of malicious software
- System registry hives
- Artifacts indicating process execution of malicious and benign software

The analysts also included the manual review of the forensic data looking for other indicators not included above. CrowdStrike determined that an attacker accessed systems within the client environment to create user accounts and to deploy and execute ransomware and batch scripts. Investigators also determined that the attacker's goal was to secure more RDP server logins to sell to other cybercriminal threat actors.

Results and key recommendations

CrowdStrike Services was able to rid the client's environment of the damaging SamSam ransomware completely and help the organisation close the security gaps that had allowed the attack to occur. The team concluded their investigation by providing the client with tailored recommendations to help them strengthen their defences against future attacks. These recommendations included the following:

- *Enforce Network Level Authentication (NLA) for RDP sessions:* Any server that is public-facing on the internet and accessible via RDP should be configured to require NLA for RDP sessions. This forces a user to successfully authenticate prior to receiving the Windows logon screen.
- *Implement two-factor authentication (2FA) to prevent unauthorised access:* 2FA requires users to provide a one-time generated token on a separate device after entering login credentials.
- *Consider CrowdStrike Falcon endpoint protection:* The CrowdStrike Services team begins every investigation by deploying the CrowdStrike Falcon platform to provide endpoint visibility and real-time Indicators of Attack (IOA). You can test drive Falcon[4] or try a no-obligation trial[5] and see first-hand what your current security may be missing.

You can learn more details about this specific case and others investigated by the CrowdStrike Services team by downloading the CrowdStrike Services Cyber Intrusion Casebook 2017[6] which also covers:

- The emerging trends observed in attack behaviours, including the tactics threat actors use to gain entry and maintain a foothold in targeted environments
- Key takeaways – based on the CrowdStrike Services team's extensive experience in the field – that can help both executive stakeholders and security professionals respond more effectively to future attacks
- Recommendations your organisation can implement proactively to improve your ability to prevent, detect and respond to attacks □

1 http://www.zdnet.com/article/fileless-attacks-surge-in-2017-and-security-solutions-are-not-stopping-them/
2 https://www.crowdstrike.com/blog/why-dwell-time-continues-to-plague-organizations/
3 https://www.crowdstrike.com/blog/education-darknet-hackers-profit-data/
4 https://www.crowdstrike.com/resources/demos/test-drive/
5 https://www.crowdstrike.com/resources/free-trials/try-falcon-prevent/
6 https://www.crowdstrike.com/resources/reports/cyber-intrusion-services-casebook/

Four tips for a smarter approach to password policy

There's no one-size-fits-all approach to optimising password policy, the following measures and best practices are worth considering.

Josh Lefkowitz reports

In many cases, passwords are the primary line of defence protecting user accounts from being hijacked in an account takeover (ATO) attack. With the right policies and parameters in place to ensure strong, unique passwords, this defence can be quite effective. That being said, as we all know, passwords are highly susceptible to human fallibility.

According to a 2019 survey by Google[1], a staggering 65% of participants report using the same password across multiple accounts. And all too often, there is an overlap between personal and work-related account passwords. With the rise of credential stuffing, adversaries can take a set of username/password combinations obtained by attacking one target and use them to compromise employee or customer accounts with other organisations. Easier yet, threat actors can even carry out credential stuffing using the low-hanging fruit of publicly disclosed dumps available on the open web.

Such activity can pose a business risk on several fronts – from the financial and reputational costs of fraud against customer accounts to the potentially massive impact of adversaries gaining privileged network access though ATO against an employee account.

As the technology and tools to leverage stolen credentials advance, a more thoughtful approach to your organisation's password policy is a highly effective way to reduce risk by better protecting your customers, network assets, and employees. While there's no one-size-fits-all approach to optimising password policy, the following measures and best practices are worth considering:

While long accepted as a best practice, cybersecurity leaders are increasingly coming around to the realisation that automatically forcing password resets at a specified time interval – such as every 90 days – does not reduce the likelihood of accounts being compromised.

1. Monitor for compromised credentials

Dumps containing compromised passwords, usernames, and other credentials are easy pickings for threat actors, and employee or customer accounts using these credentials are ripe for the taking. By monitoring public dumps and leaks privately shared and sold only within illicit online communities, defenders can assess the exposure of accounts they're tasked with safeguarding and take proactive action against ATO.

While establishing the data collections and technology required to automatically monitor, process, and act upon compromised credentials data is extremely talent and resource intensive, organisations can gain these capabilities through a trusted partner. In doing so, defenders can augment traditional password policy best practices with the ability to take action based on indicators observed within the cybercrime underground.

2. Use a password manager

While in many circles it's become conventional wisdom, it bears repeating: password managers are an easy, efficient way for users to maintain unique passwords for each account. That being said, a word of caution is in order: not all password managers are created equal, and using a password manager that is unsecure or unreliable can lead to all of a user's passwords being lost or compromised at once.

3. Know when to reset passwords

While long accepted as a best practice, cybersecurity leaders are increasingly coming around to the realisation that automatically forcing password resets at a specified time interval – such as every 90 days – does not reduce the likelihood of accounts being compromised. On the contrary, forcing users to frequently come up with new passwords can encourage them to reuse a password they're already using for another account or simply make a slight modification to an existing password. The most effective policy is to only reset passwords known to have been exposed in breaches, which can be accomplished by monitoring for compromised credentials and simultaneously make users comfortable with using complex passwords or phrases.

While these best practices are not a comprehensive roadmap to strong password hygiene, they're a great starting point for organisations that have taken a laissez-faire or reactive stance when it comes to ensuring the security of user credentials.

4. Enforce complexity and uniqueness standards

Case-sensitive combinations of letters mixed with special characters are exponentially more difficult for automated brute-forcing tools to mathematically guess than simple combinations of words and numbers – and the longer the password the better. And while it's unlikely that users will be able to memorise lengthier, more random credentials, adopting the aforementioned best practice of using a password manager makes it easy to implement and enforce strict standards for complexity and uniqueness.

While these best practices are not a comprehensive roadmap to strong password hygiene, they're a great starting point for organisations that have taken a laissez-faire or reactive stance when it comes to ensuring the security of user credentials. In particular, as the technology and tools to leverage stolen credentials advance, defenders should seek out innovative new ways to proactively flag exposed passwords leveraging insights gleaned from illicit communities and open-web dumps. □

[1] https://services.google.com/fh/files/blogs/google_security_infographic.pdf

Josh Lefkowitz is CEO & Co-founder at Flashpoint.

Flashpoint delivers converged intelligence and risk solutions to private and public sector organisations worldwide. As the global leader in Business Risk Intelligence (BRI), Flashpoint provides meaningful intelligence to assist organisations in combating threats and adversaries.

For more information, please visit **www.flashpoint-intel.com**

FLASHPOINT

Best practices for mitigating the insider threat in the cloud

What exactly are the main risks associated with business users?

Ilia Sotnikov reports

Gartner says that by 2022, at least 95% of cloud security failures will be the customer's fault. Indeed, even though cloud vendors like Microsoft now offer additional security services (e.g., the Microsoft 365 Security Center), to ensure protection of their data and services, companies need their own controls as well.

Why? Many different types of cloud users put corporate data at risk, including IT teams, managers and contractors. But the 2019 Netwrix Cloud Data Security Report found that the biggest threat in the cloud comes from regular business users. In fact, 43% of organisations say their business users are responsible for cloud security incidents, which is 10% higher than a year ago. Therefore, to reduce the risk of incidents, organisations need to implement additional controls. What exactly are the main risks associated with business users, and how can organisations mitigate those risks?

What makes organisations vulnerable?

One of the main benefits of the cloud is that it enables business users to access data more easily, at any time and from nearly any location. Unfortunately, though, not all business users understand their data security responsibilities, and many organisations don't provide cybersecurity training to help improve security awareness. As a result, users are likely to make mistakes that could result in security incidents. In fact, the 2019 Netwrix survey found that the most frequent cause of security incidents in the cloud was accidental mistakes – 45% of respondents had incidents due to errors, up 28% from a year ago.

Deep visibility into user behaviour is a great practice that can help organisations mitigate the risk of data breaches caused by the human factor. However, 36% of organisations in the 2019 Netwrix survey couldn't identify who was responsible for security incidents – a dramatic increase from just 6% in 2018. This shows that the level of insight into user activities around data in these organisations leaves much to be desired.

Another way to reduce the insider risk is to use a data discovery and classification (DDC) tool to help you understand how much data you have, who has access to it and which information is most critical and requires protection. Unfortunately, the Netwrix survey revealed that many organisations neglect this critical practice: among organisations where business users were involved in security incidents, 86% failed to classify all data they store in the cloud.

How do organisations plan to mitigate the risk?

To protect data in the cloud, organisations need to implement measures to keep employee activity under control. Some organisations are already planning steps: They are willing to invest in the education of current IT staff (37%), provide sufficient budget (36%) and require periodic status reports (31%). Still, nearly a quarter (23%) of IT teams say their management does nothing to support cloud security initiatives, which leaves them ill prepared for the growing security risks in the cloud.

Recommendations

Based on my 15 years of experience working with organisations to combat the insider threat, the following three best practices are the most effective:

- *Train your employees.* Never underestimate the value of human factor in cybersecurity. Regular awareness trainings and tests help ensure that your employees are familiar with basic security practices and won't accidentally put your data and entire infrastructure at risk.
- *Get actionable insight into your cloud.* Since both user mistakes and cyber-attacks are inevitable, you need to regularly audit your cloud environment to see who did what, when and where. But being able to review what happened in the past is only half of the battle; you also need to be able to detect and respond to abnormal behaviour before it results in a security incident. Moreover, having actionable visibility into your systems and data will enable you to investigate incidents properly to prevent similar issues in the future.
- *Classify your data.* Data classification technology can take you a long way – you will be able to understand what data exactly you have and increase your awareness of its value and sensitivity to implement adequate controls and secure this data properly. This will be a great instrument for mitigating the risk of inadvertent data leakage due to mistakes by business users. □

Ilia Sotnikov is VP of Product Management at Netwrix.

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

netwrix

FIND US.
WE'LL FIND AND SECURE YOUR DATA.

Take this quick quiz to see if you're in **control** of your **IT infrastructure** and **sensitive data**

Quick Quiz

- Do you know who is violating security policies or acting strangely?
- Can you prove your compliance with regulatory standards?
- Are you able to minimise the risk of cybersecurity incidents?
- Can you respond to threats in time to prevent data breaches?
- Do you know which information is sensitive and where it resides?
- Can you say who has access to your sensitive data and if it's at risk?
- Is there any improper or abnormal activity around that data?
- Can you tell who has done what across your IT environment?

If you answered **NO** to more than a couple of these questions, **your data is at risk**.

VISIT US TO LEARN
HOW TO GET THE CONTROL YOU NEED.

OneTrust Targeted Data Discovery: Not your average data discovery tool

November 25, 2019 – CCPA.

OneTrust reports

Privacy is a global phenomenon. With the rise of global privacy laws like the CCPA and GDPR, businesses across the world are now required to comply with large volumes of consumer and data subject rights requests. Responding to these requests is a time-consuming process full of manual tasks, and processes can change depending on the type of request – making it a challenge to respond to the regulatory requirements for Consumer Rights Requests and the need to detect exactly where consumer data exists, in order to access, port, delete it, or comply with CCPA opt-outs.

As data models become more complex and consumers continue to exercise their consumer privacy rights, traditional data discovery tools are no longer scalable for businesses of all sizes.

These manual processes are time-consuming and prone to error, yet traditional data discovery tools aren't built to meet the specific needs of processing and responding to consumer requests, giving you more data than you need and, in some cases, incorrect or incomplete data. As data models become more complex and consumers continue to exercise their consumer privacy rights, traditional data discovery tools are no longer scalable for businesses of all sizes.

So then how do you filter through all of your systems to find only what you need?

Targeted Data Discovery (TDD) is purpose-built to remove the complexities of manual processing, automating each manual step used to process consumer rights and opt-out of sale requests and replicates it automatically with the right exception rules to flag outliers. Targeted Data Discovery leverages automated workflows that easily scale with your data, working across your existing internal systems in parallel to find the exact consumer data you're looking for, no matter how the data is stored – whether it's structured, unstructured, on-prem, in the cloud, or in redacted emails.

Targeted Data Discovery can automate the most basic tasks like searching a database, to the more complex like processing combination workflows with multiple identities and cross-referencing data across multiple systems – working across one system or thousands, giving you only the data you need, when you need it. This allows the organisation to act on the data in order to port it from system to system, both internally and externally, to provide it to a consumer as part of a consumer rights request, to process a CCPA opt-out of sale request, or when needed, delete it.

It's not your average data discovery tool.

It's OneTrust Targeted Data Discovery, the revolutionary new way to automate the fulfillment of consumer rights requests. □

To learn more about OneTrust Targeted Data Discovery sign up for our Targeted Data Discovery Master Class webinars or request a demo today!

OneTrust is the #1 most widely used privacy, security and trust platform used by more than 5,000 companies to comply with the CCPA, GDPR, ISO27001 and hundreds of the world's privacy and security laws. OneTrust's primary offerings include OneTrust Privacy Management Software, OneTrust PreferenceChoice™ consent and preference management software, OneTrust Vendorpedia™ third-party risk management software and vendor risk exchange and OneTrust GRC integrated risk management software.

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

World's #1 Most Widely Used Privacy Management Software

FOR PRIVACY, SECURITY & THIRD-PARTY COMPLIANCE

Fast Track Your Compliance with CCPA, GDPR, LGPD, ISO & Hundreds of Global Privacy Laws & Security Frameworks

Technology to Power Your Privacy, Security & Third-Party Risk Programs			
Privacy Program Management	**Marketing & Privacy User Experience**	**Third-Party Risk Management**	**Incident & Breach Response**
Maturity Planning Compliance Reporting Scorecard	**Cookie Compliance** Website Scanning & Consent	**Vendor Assessments** Security & Privacy Risk	**Incident & Breach Response** Assessments, Notifications & Reporting
Program Benchmarking Comparisons Against Peers	**Mobile App Compliance** App Scanning & Consent	**Vendorpedia Risk Exchange** Security & Privacy Risks	**Incident Intake** Centralized Register
Assessment Automation PIAs, DPIAs, PbD & Info Sec	**Preference Management** End User Preference Center	**Vendorpedia Monitoring** Privacy & Security Threats	**Risk Assessments** Risk & Harms Analysis
Data Mapping Inventory & Records of Processing	**Data Subject & Consumer Requests** Intake to Fulfillment Automation	**Vendor Chasing Services** Managed Chasing Services	**Notification & Reporting** Obligation Tracking
Targeted Data Discovery™ Access, Deletion & Portability	**Policies & Notices** Centrally Host, Track & Update	**Vendor Data Flows** Reporting & Recordkeeping Automation	**Real-Time Activity Feed** Breaches & Enforcements

Join our webinar!

Risk Exchanges: The Secret to Supply Chain Risk Management

Tuesday 17 March | 6PM GMT

Jaymin Desai
CIPP/E, CIPM, Third-Party Risk Management Offering Manager

Visit OneTrust.com to Register!

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

ATLANTA | BANGALORE | HONG KONG | LONDON | MELBOURNE
MUNICH | NEW YORK | SAN FRANCISCO | SÃO PAULO

OneTrust is the #1 most widely used privacy, security and trust technology platform used by more than 5,000 companies to comply with the CCPA, GDPR, ISO27001 and hundreds of the world's privacy and security laws. OneTrust's primary software offerings include OneTrust Privacy Management , OneTrust PreferenceChoice™ consent and preference management, OneTrust Vendorpedia™ third-party risk management and OneTrust GRC integrated risk management. To learn more, visit OneTrust.com or connect on LinkedIn, Twitter and Facebook.

Understanding all security technology – hard; workload segmentation – not hard

Segment your environment and prevent the propagation of attacks.

Illumio reports

Some things in life are just hard; brain surgery, Valentine's Day and watching England play rugby. There are also several hard things in the life of a security professional including the 'more is more' approach to security. Over the years, as new threats have appeared, new products have been developed to solve the problem. This has led to a sprawl of security products with some organisations having up to 100 different technologies. Getting control of all of this is hard and so a selection of frameworks and initiatives have been created to provide some order to the challenge.

The most widely adopted high-level strategy is zero trust. This was created by Forrester to provide a framework that includes both technology and people. The idea is to simplify the approach to security by taking a more strategic view. One of the cornerstones of this is segmentation. If you can segment your environment, then you can prevent the propagation of attacks by preventing lateral movements and controlling which processes can communicate.

In a highly regulated environment like banking where you face a raft of regulations in each country like BAFIN, LPM, the NIST directive, PCI and from SWIFT, all of these require the segmentation of data within the compute environment. At this point the network managers all draw a heavy breath as they know how complex this project can be.

In the mid-2000s, opinion said that the development of virtual networking spelt the end of high-function ethernet switches with customers buying low cost white boxes for their networks. This did not really materialise as the implementation of SDN networks started to become more and more complex. Using SDN for segmentation has become one of those things that has proved to be hard.

There are two popular options when segmenting a network:

1. *Running an SDN on Ethernet switches:* In this scenario an SDN controller is used to create virtual networks on the switch network using TAGs to identify the groups that each service or workload belong to. Rules are then defined around how resources within each group will communicate with each other. The challenges with this scenario include the cost of upgrading to the latest version of switches, the complexity of tagging services if you want to achieve the level of granularity that you wish.
2. *Running an SDN using virtual switches in the hypervisor:* This scenario is very similar except that instead of needing to upgrade the existing switches virtual switches are used. The challenge of complex configuration of each of the micro-services and workloads is still the same.

In a highly regulated environment like banking where you face a raft of regulations in each country like BAFIN, LPM, the NIST directive, PCI and from SWIFT, all of these require the segmentation of data within the compute environment. At this point the network managers all draw a heavy breath as they know how complex this project can be.

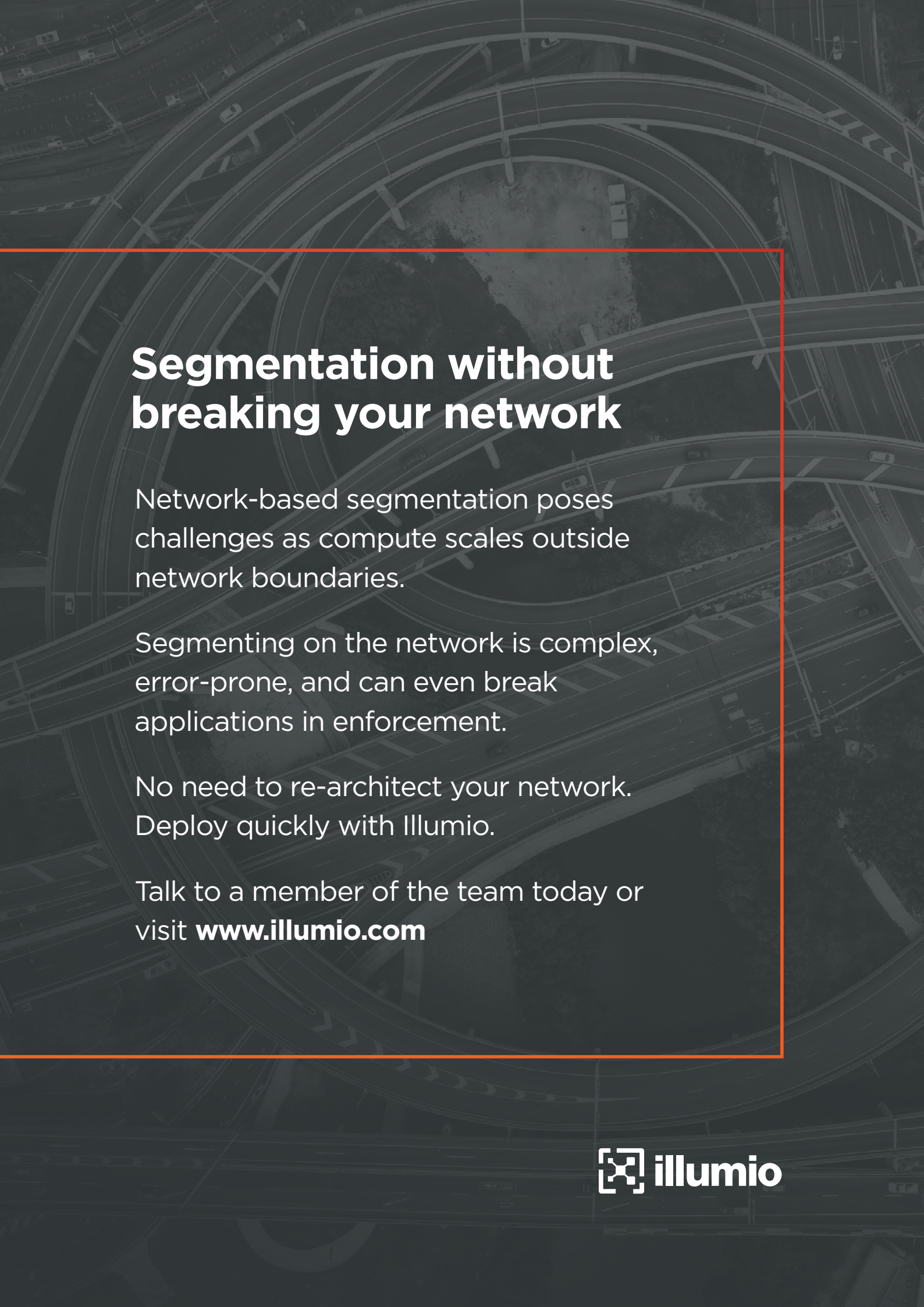
Imagine we could make segmentation not hard. So as an alternative:

1. Map the flows of traffic for each application.
2. Map the vulnerabilities for each application.
3. Automatically generate the policies to segment the traffic at a very fine level.
4. Segment the traffic on the host.

No network upgrades, no complex SDN configuration, complete flexibility across platforms.

In the same way that no-one remembers the late 1990s attempts to use SDN style technology to switch IP on ethernet networks, the same will be true of many complex virtualisation technologies of today.

In years to come, there will only be host-based segmentation. □



Segmentation without breaking your network

Network-based segmentation poses challenges as compute scales outside network boundaries.

Segmenting on the network is complex, error-prone, and can even break applications in enforcement.

No need to re-architect your network. Deploy quickly with Illumio.

Talk to a member of the team today or visit **www.illumio.com**

illumio

Checkmate.

Shifting Power to the Defender with Cyber Deception

Deception has been used for millennia to outmaneuver one's adversary. Attivo Networks brings advanced deception technology to cybersecurity with high-interaction decoys and lures that confuse attackers into believing what is fake is real, causing them to make mistakes and reveal their presence.

High-fidelity alerts are backed by engagement-based adversary intelligence for accelerating investigation and response to threats. Change the asymmetry of attacks and call checkmate on your opponent with Attivo Networks threat deception. To learn more, visit attivonetworks.com

Attivo NETWORKS®

Deception solution overview

Organisations are now shifting their security strategies from a reactive defence to one of an active defence.

Cyber-attacks are occurring at an unrelenting pace as sophisticated attackers continue to find ways to penetrate perimeter defences. With each breach, security professionals are faced with mounting pressure to quickly detect and stop threats, before damage is done. In addition to compliance expectations, new breach notification laws are being proposed with the promise of significant fines and potential jail time if notification expectations are not met. Organisations of all sizes and across all industries are seeking innovation to mature their security models, close detection gaps, better understand their adversaries, and be prepared to adhere to breach tracking and disclosure requirements. Organisations are now shifting their security strategies from a reactive defence to one of an active defence, which is not solely based on reacting to attacks but instead a balanced investment in the early detection and rapid response to threats.

Deception technology

Deception technology provides the innovation required to non-disruptively evolve to an active defence security posture. By deploying a fabric of deception-based detection throughout the network stack, companies are able to achieve efficient detection for every threat vector and the life-cycle of an attack. Utilising high-interaction decoys and lures, deception deceives attackers into revealing themselves, thereby alerting on and identifying detection gaps on threats that have evaded other security controls.

With early visibility into threats and actionable alerts for incident handling, deception solutions are rapidly becoming the solution of choice for proactively uncovering and responding to external, internal, and supplier threat actors. Organisations of all security maturity levels are aggressively adopting deception technologies in order to mitigate risks related to employee credential theft, data exfiltration, ransomware, crypto-mining, and attacks with the intent to disrupt services or impact public safety. The accuracy and ease of use of threat deception has been a major driver in its adoption and wide-spread deployment.

In 2018, analysts recognised deception for its efficiency in detecting advanced threats and Gartner, Inc. recommended deception for the third year in a row as a top strategic security priority. A variety of recent surveys have also recorded the market's intent to add deception technology to their security controls given its efficacy and efficiency in deterring attackers.

The Attivo Networks solution

The ThreatDefend™ Deception and Response Platform is designed to turn the entire network into a trap, forcing the attacker to be right 100% of the time or risk being discovered. The solution combines network and endpoint high-interaction deception lures and decoys designed to provide early visibility into in-network threats, efficient continuous threat management, and accelerated incident response.

Recognised as the industry's most comprehensive solution, the ThreatDefend Platform provides an overall deception fabric for cloud, network, endpoint, application, and data/database deceptions and is highly effective in detecting threats from virtually all vectors such as advanced persistent threats, stolen credential, Man-in-the-Middle, Active Directory, ransomware, and more. These deceptions can deploy within all types of networks including endpoints, user networks, server, data centre, ROBO, cloud, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications.

The ThreatDefend Deception Platform is a modular solution comprised of Attivo BOTsink ® engagement servers, decoys, and deceptions, ThreatStrike® endpoint service, ThreatPath® for attack path visibility, ThreatDirect deception forwarding for remote and segmented networks, the Informer for adversary intelligence, ThreatOps™ incident response orchestration playbooks, and the Attivo Central Manager (ACM), for creating an active defence against cyber-threats.

Deception for detection and attack path visibility

The ThreatDefend Deception and Response Platform provides unparalleled visibility into threats inside the network and attacker lateral movements and tactics. The platform detects advanced threats propagating throughout the network by laying strategic decoys and lures to deceive, detect, and defend against attacks as they scan network clients, servers, and services for targets and seek to harvest credentials.

Lures and decoys work together to attract and detect attackers in real-time, raising evidence-based alerts while actively engaging with them so that their lateral movement and actions can be safely analysed. For attacker believability, the decoy systems mirror match

Attivo Networks reports

production assets by running real operating systems, full services, and applications, along with the ability to customise the environment by importing the organisation's golden images and applications. As a result, the platform creates a 'hall of mirrors' environment that is baited with lures and traps designed to redirect attackers away from company assets. Machine learning is used to prepare and deploy deceptions, keeping the network and endpoint deceptions fresh and for making ongoing maintenance easy.

To increase deception authenticity and for visibility into attempts to compromise, the solution incorporates with Active Directory. By inserting deception into areas that attackers target for reconnaissance, the deployment appears as part of the production environment in multiple layers.

Endpoint deceptions and mapped shares provide easy and highly effective redirection of attacks seeking to harvest credentials or execute a ransomware attack. Additionally, high interaction deception can be instrumental in slowing and occupying the attention of a ransomware attack providing the time advantage to stop the attack before it can cause extensive damage.

With the rapid migration to the cloud, it is critical for the deception fabric to scale seamlessly into the cloud. The ThreatDefend platform offers extensive support for AWS, Azure, Google, and Oracle cloud environments inclusive of decoys and lures for containers, serverless, and cloud shared-security models. The ThreatDefend Platform capabilities include support for Lambda functions, access keys, reconnaissance, credential harvesting, as a means to verify the efficacy of security controls along with CloudWatch/SIEM monitoring for finding attempted use of deception credentials.

For proactive threat prevention and attack surface reduction, the ThreatPath solution provides visibility into attack paths that an attacker could traverse through misconfigured systems, credential exposure, or misuse. A topographical illustration and attack path associations provide a straight-forward view of how attacks can move laterally to reach their target. When paired with the BOTsink solution threat intelligence and attack time-lapsed replay, defenders achieve unprecedented levels of threat visibility and the information required to build pre-emptive defence against its adversaries.

Deception for active defence and accelerated incident response

In addition to the early detection of attackers inside the network, the ThreatDefend Platform's actionable alerts, automated analysis, and native integrations for incident handling work collectively to dramatically improve a responder's time-to-remediation. When an attacker engages with a deception decoy, credentials, application, or data the engagement server will record and alert on the activity while simultaneously responding to the attacker. The activity is consolidated in the Informer dashboard, which assembles forensics, correlates events, and raises evidence-based alerts on malicious activity.

Alerts only occur on confirmed attacker interactions with deceptions and unlike other detection methods, is not dependent on signatures or behavioural analysis to detect an attack. The alerts are substantiated with attack analysis that can be used to automate the blocking of an attacker, to isolate an infected system, and to hunt for other compromises so that a company can completely eradicate the threat from the network. The elimination of false positives and the high-fidelity alerts save valuable hours for InfoSec teams.

Information is presented in the Informer dashboard, which delivers a comprehensive view of incident and forensic information gathered during an attack. Forensic reports include identification of infected systems and C&C addresses and are created with full IOC, PCAP, and STIX formats to allow easy information sharing and attack recording. By correlating all relevant information and forensics from an event into a single interface, the Informer dashboard gives analysts and incident response teams a streamlined view of an attack to effectively contain and remediate the incident. This accelerates intelligence-driven response, enhances network visibility, and creates a predictive defence to improve their security posture.

Deception is an offensive counterintelligence function designed to disrupt the attacker's ability to collect accurate information. It also provides defensive counterintelligence functions as it diverts attacks from production assets, and collective counterintelligence information on attacker TTPs, IOCs, and insight into attacker objectives. Additionally, DecoyDocs delivers data loss tracking, allowing organisations to track stolen documents inside or outside the network.

Organisations can also use the ThreatOps solution to automate incident handling and create repeatable incident response playbooks. This threat orchestration can be fully customised to match their environment and policies so that organisations can make faster and better-informed incident response choices. □

RE:Thinking email security

Criminals are increasingly turning to more subtle forms of attacks.

Mariana Pereira reports

When thinking about email security, a familiar story usually comes to mind: an attacker sends a malicious payload hidden in a link or attachment, and an unsuspecting recipient clicks and inadvertently downloads malware onto their device. But in reality, this kind of attack represents just the tip of the iceberg when it comes to the broader spectrum of threats that target organisations via the inbox.

Criminals are increasingly turning to more subtle forms of attacks which involve sending 'clean emails' containing only text, and coaxing a recipient into replying, revealing sensitive information or performing an offline transaction. These methods easily bypass legacy security tools that rely on checking links and attachments against blacklists and signatures. Moreover, they generally involve registering new 'look-a-like' email addresses, which not only trick the recipient but also bypass traditional defences set on identifying blacklisted domains.

A quick RE:ply

Solicitation attempts are impossible to stop without a comprehensive understanding of 'normal' across digital traffic from both email and the wider digital business. With every email analysed in the wider context of the sender, the recipient, and the entire organisation, seemingly harmless emails that bypass traditional security tools can be identified in seconds given a vast range of metrics, including suspicious similarities to known users, abnormal associations, and even anomalies in email content and subject line.

Darktrace recently discovered such an attack whereby a new Gmail domain was created in the name of the company's CEO. From this address, an email was sent to a member of the payroll department requesting that the employee update the CEO's direct deposit information. Since the email successfully mimicked the CEO's typical writing style, it could have easily succeeded if Darktrace's AI hadn't been analysing the organisation's mail flow in connection with the rest of the business.

Solicitation attempts are impossible to stop without a comprehensive understanding of 'normal' across digital traffic from both email and the wider digital business.

A bleak outlook

Cybercriminals are also turning to supply chains – comprised of vendors, partners and contractors – in their attacks to infiltrate an organisation or establish offline communication. Having taken over a supplier's account, attackers seek to reply to previous email exchanges in order to accomplish their goals. And with cases of credential compromise increasing 260% since 2016, this threat vector is only set to increase in the coming decade.

A customer trialling Darktrace Antigena Email recently caught an instance of this, whereby an attacker had taken over the account of a trusted consultancy firm. Darktrace recognised that the sender was well known to the company, and a number of internal users had in fact corresponded directly with them earlier that same day.

Less than two hours after a routine email exchange, the account was taken over by an attacker who sent emails to 39 users, each containing a phishing link. There was variation in the subject lines and links, suggesting highly targeted emails from a well-prepared attacker.

Darktrace identified the full range of anomalies that are typically associated with account takeovers, including the unusual IP address, the inconsistency of the link based on its learned 'pattern of life', the unusual group of recipients, and in some emails, the topic anomaly.

FW: Thinking

In this instance, the attacker had taken the time to read the previous correspondence to contextualise their impersonation attempt. Going forward, artificial intelligence will increasingly be adopted to learn prior communication patterns between two senders to make for more legitimate-looking emails, which can be sent at machine-speed and scale. One of the most notorious pieces of contemporary malware – the Emotet trojan – is a prime example of a prototype-AI attack. Emotet's main distribution mechanism is through email, usually via invoice scams.

'Forward thinking' attackers could easily use AI to supercharge attacks. With artificial intelligence analysing the context of every email thread and replicating the language used, these email attacks could become highly tailored to individuals. This would mean that an AI-powered Emotet trojan could create entirely customised, more believable emails

By leveraging AI to learn 'normal' behaviour across email traffic and the entire digital estate, Antigena Email is able to protect email users not only from traditional phishing attacks, but from every threatening email seeking to cause harm.

and, crucially, send these out at scale, allowing cybercriminals to increase the yield of their operations enormously.

This possibility gives rise to a new chapter in email security, and one in which a holistic 'immune system' platform is necessary. Legacy security tools that are confined to the email gateway or inbox are no longer sufficient to stop this vast range of sophisticated attacks. By leveraging AI to learn 'normal' behaviour across email traffic and the entire digital estate, Antigena Email is able to protect email users not only from traditional phishing attacks, but from every threatening email seeking to cause harm. □

Mariana Pereira is Director of Email Security Products at Darktrace.

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

DARKTRACE

Go beyond the firewall for securing your critical assets on the hybrid cloud

The age of the hybrid cloud has created a need for a different approach when it comes to firewalls.

Guardicore reports

Containers, cloud deployments, serverless infrastructure... all of these are the modern data centre environments that enterprises are utilising every day. Legacy firewalls simply don't protect these environments effectively.

For some, virtual cloud firewalls seemed like they might be the answer to protecting the modern hybrid data centre, but the truth is, these are also insufficient for today's e-crime landscape. There is no application layer security, no process level visibility or control, and no ability to segment at user level. When looking for a solution that meets these challenges, there are a few key elements that forward-thinking enterprises need to keep in mind:

- *Latency:* When traffic is passed through virtual firewalls, this can cause great latency, directly impacting the pace of business.
- *Visibility:* For everything from meeting compliance regulations, to reducing complexity in the hybrid data centre – you simply can't secure what you can't see.
- *Ease of deployment:* Many firewalls require network changes and downtime. Most enterprises can't afford the toll that takes on operations.
- *Complexity:* Without visibility, identifying issues becomes extremely cumbersome, and complex rule sets in the thousands need to be maintained, opening the door to misconfigurations. As traditional firewalls do not extend to containerised or serverless environments, multiple firewall solutions need to be used to cover your whole environment.
- *Maintenance:* With multiple firewalls, and each configuration taking days or even weeks, the maintenance costs start stacking up. Coordination between teams gets increasingly complex, making every change a huge decision.
- *Cost:* Despite firewalls being a limited solution that doesn't meet today's needs, all of these issues lead to a very high cost for implementation and maintenance.

Meeting these requirements with a single solution for infrastructure agnostic segmentation

Any traditional solution, from VLANs to Virtual Firewalls will not protect and control in an infrastructure-agnostic way. In contrast, Guardicore Centra covers every environment, including on-premises, legacy systems, virtual, both public and private cloud, and containers.

Deployment takes hours rather than days, and days instead of months – utilising just one architect rather than multiple teams and requiring zero network or architecture changes. As a software-defined solution, we are part of the ecosystem, and so easily integrated with DevOps tools such as Ansible, Chef, Puppet and more.

The simplest way to do micro-segmentation

Recognising that segmentation projects are always going to be innately complex, Guardicore has built its platform from the ground up to meet the exact limitations of traditional security solutions such as firewalls. Where firewalls are limited, Guardicore Centra has the widest and deepest coverage available. Where firewalls lack visibility, we start with a highly visible UI that allows you to visualise your data centre in exactly the language you use to discuss it, utilising a map as the first step in building out policies. Firewalls are rigid and inflexible, but Centra enables you to set one policy, and have it follow the workload when your assets migrate, whether that's between clouds, or from on-premises to cloud. Security becomes an enabler for innovation rather than a hurdle to overcome.

Once we've met the limitations of firewalls head on, we then offer the smartest, fastest tool to meet your segmentation roadmap. Centra understands application dependencies with deep context, using historical data and process-level information to build both blacklist and whitelist rules. You can even include user identity access policies to provide an added layer to your security hygiene.

We know that the firewall is not good enough for your enterprise data centre. Frankly, it isn't even close. That's why we've built a best-of-breed distributed software firewall that eliminates chokepoints, and provides equal protection to all traffic. It works at the same pace of agility and speed of today's DevOps teams. Whatever your segmentation pain points are, we pride ourselves on delivering exactly what the customer is looking for, across dozens of deployment scenarios on the hybrid cloud. Schedule a demo, and let's discuss how we can help. □

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

Guardicore

Guardicore

SECURING YOUR CRITICAL ASSETS ON THE HYBRID CLOUD

The age of the hybrid cloud has created a need for a different approach when it comes to firewalls. Any traditional solution, from VLANs to Virtual Firewalls will not protect and control in an infrastructure-agnostic way.

Guardicore Centra simplifies segmentation providing the widest and deepest coverage available, including on-premise, legacy systems, virtual, both public and private cloud and containers.

✓ Reduce Complexity ✓ Reduce Risk ✓ Innovate Faster

For more information visit
www.guardicore.com

Evaluating external threat intelligence sources

With the expanding attack surface and growing sophistication of threats, just reacting to an incident is not enough.

Kaspersky reports

Increasingly complex environments provide multiple opportunities for attackers. Each industry and each organisation has its own unique data to protect, and uses its own set of applications, technologies, etc. All this introduces an enormous number of variables into possible methods of executing an attack, with new methods emerging daily.

A new approach is needed

With enterprises increasingly falling victim to advanced and targeted attacks, it's clear that a successful defence requires new methods. To protect themselves, businesses need to take a proactive approach, constantly adapting their security controls to the ever-changing threat environment. The only way to keep up with these changes is to build an effective threat intelligence programme.

Threat intelligence has already become a key component of security operations established by companies of varying sizes across all industries and geographies. Provided in human-readable and machine-readable formats, threat intelligence can support security teams with meaningful information throughout the incident management cycle and inform strategic decision-making.

However, the growing demand for external threat intelligence has given rise to an abundance of threat intelligence vendors, each offering a host of different services. An extensive and competitive market with innumerable, complex options can make choosing the right solution for your organisation highly confusing and extremely frustrating.

Threat intelligence that isn't tailored to the specifics of your business can exacerbate the situation. In many companies today, security analysts spend more than half their time sorting out false positives instead of proactive threat hunting and response, leading to a significant increase in detection times. Feeding your security operations with irrelevant or inaccurate intelligence will drive the number of false alerts even higher and have a serious, negative impact on your response capabilities – and the overall security of your company.

Think like an attacker

To build an effective threat intelligence programme, companies, including those with established Security Operations Centres, must think like an attacker, identifying and protecting the most likely targets.

Deriving real value from a threat intelligence programme requires a very clear understanding of what the key assets are, and what data sets and business processes are critical to accomplishing the organisation's objectives. Identifying these 'crown jewels' allows companies to establish data collection points around them to further map the collected data with externally available threat information.

Issues to consider when evaluating external threat intelligence

There are still no common criteria for evaluating various external threat intelligence offerings, but here are some things to bear in mind when doing so:

- Look for intelligence with global reach. Attacks have no borders – an attack targeting a company in Latin America can be initiated from Europe and vice versa.
- If you are looking for more strategic content to inform your long-term security planning then look for a threat intelligence provider with a proven track record of continuously uncovering and investigating complex threats in your region or industry.
- Context makes intelligence from data. Threat indicators without context are of no value – you should look for providers that help you to answer the important 'why does this matter?' questions.
- Look for delivery methods, integration mechanisms and formats that support smooth integration of threat intelligence into your existing security operations. □

Proven intelligence. Guided defense.

With leading protection technologies, unique threat intelligence and recognized expertise Kaspersky powers your SOC at every level for greater efficiency in fighting increasingly sophisticated threats.

kaspersky BRING ON THE FUTURE

www. kaspersky.com

Going beyond simple vulnerability scores to maximise efficiency and effectiveness

Even the best scoring algorithm is really just that – a score.

Jeff Aboud reports

An increasingly popular feature of modern vulnerability risk management platforms is to include a 'score' for each vulnerability listed in the system. The purpose of the vulnerability score, of course, is to provide security teams with some understanding of relative urgency so that they can prioritise the remediation efforts of some vulnerabilities over others. But do these scores really help, or do they simply lull security professionals into a false sense of intelligence, believing that they have the context necessary to determine which vulnerabilities pose the most risk to the organisation?

To be useful, the vulnerability score has to be based on real-world, real-time risk assessments, as well as additional security information from throughout the enterprise's environment, to provide the context necessary to be truly relevant.

Even when the vulnerability score takes all of this into account, it's essential to realise that it only provides a very small portion of what's required to make appropriate decisions on which vulnerabilities pose the greatest risk, and therefore should be remediated first. That's because even the best scoring algorithm, considering all relevant context and based in data science, is really just that – a score. While it certainly provides an indication of relative importance, the vulnerability score can't single out any specific vulnerability to tell you what to fix *first*. Instead, it can really just help narrow down the consideration set to help you focus.

Consider this: If you have 2,000,000 vulnerabilities and a vulnerability scoring system of zero to 100, you obviously can't have a unique score for each of them. In all likelihood, you'll have well over 100,000 vulnerabilities that are assigned a score of 100. In a tool where that's the sole guidance that's provided, you'd be directed to simply 'fix all the 100s', which obviously won't help you much. While it certainly seems less intimidating than millions, how long would it take your team to remediate 100,000? And where do you start? That is, if you can only get to 20 of them this week, which are the most critical 20 that will reduce the most risk? A vulnerability score alone can't answer this important question.

Don't get me wrong, there's definitely value in having a risk-based vulnerability score. But there's exponentially more value when you pair that score with remediation intelligence that leverages data science to automate the analysis of all data to determine which vulnerabilities pose the greatest risk to the organisation, and whose remediation will have the maximum impact on risk score reduction.

By taking into account the number of instances of each vulnerability in your environment, the potential severity, and the assets that are threatened as a result of each vulnerability, remediation intelligence can granularly prioritise your remediation efforts based on what will have the greatest impact on your overall risk score for the least amount of effort. So rather than simply narrowing things down to the 'top 100,000' vulnerabilities, as in the example above, remediation intelligence can tell you which *specific* vulnerability to fix *first* for any asset or group of assets. This benefits your teams by maximising their efficiency and effectiveness while reducing the greatest amount of risk to the organisation.

So when you are evaluating a vulnerability scoring system, ask:

1. What are they basing that score on?
2. Does it employ full context by leveraging real-world, real-time risk assessments and additional security information from throughout your environment?
3. And, more importantly, is the score the primary value-add, or is the score just the first step in a larger set of intelligence that directs you on how best to use your limited security and IT resources?

These are critical considerations, because the answers can mean the difference between having to sift through 100,000 vulnerabilities today, or just focus on the one that has the greatest impact.

For further reading please refer to the Cyentia report series, Prioritization to Prediction, commissioned by Kenna Security, Volume 4: Measuring What Matters in Remediation available to download at www.kennasecurity.com □

Jeff Aboud is Director of Product Marketing at Kenna Security.

KENNA Security

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

Forthcoming events

e-crime & cybersecurity CONGRESS 10th March 2020 Dubai	e-crime & cybersecurity FRANCE 1st April 2020 Paris	e-crime & cybersecurity GERMANY 5th May 2020 Munich	SECURING FINANCIAL SERVICES 8th July 2020 London
e-crime & cybersecurity CONGRESS 16th September 2020 Abu Dhabi	SECURING THE LAW FIRM 22nd September 2020 London	e-crime & cybersecurity NORDICS 23rd September 2020 Stockholm	
e-crime & cybersecurity MID-YEAR 15th October 2020 London	SECURING ONLINE GAMING 15th October 2020 London	e-crime & cybersecurity SCOTLAND 3rd November 2020 Edinburgh	
e-crime & cybersecurity CONGRESS 10th November 2020 Kuwait	e-crime & cybersecurity SPAIN 17thth November 2020 Madrid	e-crime & cybersecurity BENELUX 1st December 2020 London	

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

Sponsors and exhibitors

Attivo Networks | Strategic Sponsor

Attivo Networks®, the leader in deception technology, provides accurate in-network threat detection, analysis, and accelerated response to advanced, credential, insider, and ransomware attacks. The ThreatDefend™ Deception and Response Platform provides continuous visibility and efficient threat management for user networks, data centres, cloud, branch, IoT, ICS-SCADA, and POS environments. Camouflage dynamic deception sets high-interaction traps to misdirect and lure attackers into revealing themselves. The solution's advanced attack analysis and lateral movement tracking automate investigation, deliver evidence-based alerts, and in-depth forensic reports. Incident response is simplified with ThreatOps™ playbooks and third-party integrations for automated attack blocking, quarantine, and threat hunting.

For more information, please visit www.attivonetworks.com

CrowdStrike | Strategic Sponsor

CrowdStrike is the leader in cloud-delivered endpoint protection. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver actionable intelligence and real-time protection from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber-attack types, using sophisticated signatureless AI and Indicator-of-Attack (IOA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates over 100 billion security events a day from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

CrowdStrike was positioned the highest in ability to execute and furthest in completeness of vision in the 2018 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP).

You can gain full access to CrowdStrike Falcon Prevent™ by starting your free trial here.

For more information, please visit www.crowdstrike.com

Darktrace | Strategic Sponsor

Darktrace is the world's leading cyber AI company and the creator of Autonomous Response technology. Its self-learning AI is modelled on the human immune system and used by over 3,000 organisations to protect against threats to the cloud, email, IoT, networks and industrial systems.

The company has over 1,000 employees and headquarters in San Francisco and Cambridge, UK. Every 3 seconds, Darktrace AI fights back against a cyber-threat, preventing it from causing damage.

For more information, please visit www.darktrace.com

ExtraHop | Strategic Sponsor

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Our breakthrough approach analyses all network interactions and applies cloud-scale machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises including Home Depot, Credit Suisse, Caesars Entertainment, and Liberty Global to rise above the noise of alerts, organisational silos, and runaway technology. Whether you're investigating threats, ensuring the availability of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.

Learn more at www.extrahop.com

Flashpoint | Strategic Sponsor

Flashpoint delivers converged intelligence and risk solutions to private and public sector organisations worldwide. As the global leader in Business Risk Intelligence (BRI), Flashpoint provides meaningful intelligence to assist organisations in combating threats and adversaries. Through sophisticated technology, advanced data collections, and human-powered analysis, Flashpoint is the only intelligence firm that can help multiple teams across an organisation bolster cybersecurity, confront fraud, detect insider threats, enhance corporate and physical security, improve executive protection, address third-party risk, and support due diligence efforts.

For more information, please visit www.flashpoint-intel.com

Illumio | Strategic Sponsor

Illumio enables organisations to realise a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data centre or cloud. Founded in 2013, the world's largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite trust Illumio to reduce cyber-risk.

For more information, please visit www.illumio.com/what-we-do and:
Engage with us on Twitter
Follow us on LinkedIn
Like us on Facebook
Read our blog
Subscribe to our YouTube Channel

IntSights | Strategic Sponsor

IntSights is revolutionising cybersecurity operations with the industry's only all-in-one external threat protection platform designed to neutralise cyber-attacks outside the wire. Our unique cyber-reconnaissance capabilities enable continuous monitoring of an enterprise's external digital profile across the clear, deep, and dark web to identify emerging threats and orchestrate proactive response. Tailored threat intelligence that seamlessly integrates with security infrastructure for dynamic defence has made IntSights one of the fastest-growing cybersecurity companies in the world. IntSights has offices in Amsterdam, Boston, Dallas, New York, Singapore, Tel Aviv, and Tokyo.

For more information, please visit intsights.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

Netwrix | Strategic Sponsor

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organisations worldwide rely on Netwrix solutions to secure sensitive data, realise the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers. Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the US.

For more information, please visit www.netwrix.com

OneTrust | Strategic Sponsor

OneTrust is the #1 most widely used privacy, security and trust platform used by more than 5,000 companies to comply with the CCPA, GDPR, ISO27001 and hundreds of the world's privacy and security laws. OneTrust's primary offerings include OneTrust Privacy Management Software, OneTrust PreferenceChoice™ consent and preference management software, OneTrust Vendorpedia™ third-party risk management software and vendor risk exchange and OneTrust GRC integrated risk management software.

OneTrust is co-headquartered in Atlanta and in London, and has additional offices in Bangalore, San Francisco, Melbourne, New York, São Paulo, Munich, Hong Kong and Bangkok. Our fast-growing team surpasses 1,500 employees worldwide.

To learn more, visit OneTrust.com

Orange Cyberdefense | Strategic Sponsor

In early 2019, SecureData, the largest independent managed security service provider in the UK, was acquired by the Orange Group to become part of Orange Cyberdefense, the Group's expert cybersecurity business unit. Today, Orange Cyberdefense is Europe's go to market, threat detection and threat intelligence services provider.

For more information, please visit www.orangecyberdefense.com

Telesoft | Strategic Sponsor

Telesoft provide services and cutting edge technology used by global and national networks to protect their digital assets and maximise data equity at Tbps. We offer capability extending across converged and hybrid networks from 5G telco core and IOT to fixed line to virtual, edge and fog networks. Telesoft support imperatives of cybersecurity, compliance and network engineering.

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

TrapX Security | Strategic Sponsor

TrapX Security is a leader in the delivery of advanced threat cybersecurity defence. Our deception-based solutions rapidly detect, analyse and defend against new zero-day and APT attacks in real-time. DeceptionGrid provides automated, highly accurate insight into malware and malicious activity unseen by other types of cyber-defence. We enable a pro-active security posture, fundamentally changing the economics of cyber-defence by shifting the cost to the attacker. The TrapX Security customer base includes global 2000 commercial and government customers around the world in sectors including defence, healthcare, finance, energy, consumer products and other key industries.

Learn more at www.trapx.com

Zscaler | Strategic Sponsor

Zscaler enables the world's leading organisations to securely transform their networks and applications for a mobile and cloud-first world. Applications have moved from the data centre to the cloud and users are connecting to their workloads from everywhere, but security has remained anchored to the data centre. Zscaler is redefining security by moving it out of the data centre and into the cloud.

The Zscaler Cloud Security Platform uses software-defined business policies, not appliances, to securely connect the right user to the right application, regardless of device, location, or network. Zscaler offers two service suites. Zscaler Internet Access™ scans every byte of traffic to ensure that nothing bad comes in and nothing good leaks out. Zscaler Private Access™ offers authorised users secure and fast access to internal applications hosted in the data centre or public clouds – without a VPN.

Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, the Zscaler multi-tenant, distributed security cloud protects thousands of customers from cyber-attacks and data loss, enabling customers to embrace the agility, speed, and cost containment of the cloud – securely.

For more information, please visit www.zscaler.com

Accellion | Education Seminar Sponsor

The Accellion enterprise content firewall prevents data breaches and compliance violations from third-party cyber-risk. CIOs and CISOs rely on the Accellion platform for complete visibility, compliance and control over the communication of IP, PII, PHI, and other sensitive content across all third-party communication channels, including email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows. When users click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world.

With on-premise, private cloud, hybrid and FedRAMP deployment options, the Accellion platform provides the security and governance CISOs need to protect their organisations, mitigate risk, and adhere to rigorous compliance regulations such as NIST 800-171, HIPAA, SOX, GDPR, GLBA, FISMA, and others. Accellion solutions have protected more than 25 million end users at more than 3,000 global corporations and government agencies, including NYC Health + Hospitals; KPMG; Kaiser Permanente; Latham & Watkins; National Park Service; Umpqua Bank; Tyler Technologies; and the National Institute for Standards and Technology (NIST).

For more information, please visit www.accellion.com

activereach | Education Seminar Sponsor

activereach® is a leading technology integrator providing bespoke IT solutions and professional services to customers in the areas of security and connectivity. Our independent consultative approach helps organisations maximise business value from their technology investments, providing a platform for businesses to grow, reinvent and transform.

Working in partnership with many of the world's leading technology vendors and software providers, we offer the most innovative hosted, on-premise and cloud-based services. Our consultancy, technology and services have transformed hundreds of businesses across the UK, Europe & Middle East – ranging from FTSE 500 enterprises to corporates and SMEs. Operating across our activeNETWORKS™ and activeDEFENCE™ technology divisions, activereach is headquartered near London, UK.

activereach is partnering with Swimlane, leaders in security orchestration automation and response (SOAR), at the e-Crime & Cybersecurity Congress 2020.

For more information, please visit www.activereach.net

Check Point | Education Seminar Sponsor

Check Point Software Technologies Ltd. is a leading provider of cybersecurity solutions to corporate enterprises and governments globally. Its solutions protect customers from 5th-generation cyber-attacks with an industry leading catch rate of malware, ransomware and other targeted attacks. Check Point offers a multilevel security architecture with its new Gen V advanced threat prevention that protects all networks, cloud and mobile operations of a business against all known attacks combined with the industry's most comprehensive and intuitive single point of control management system. Check Point protects over 100,000 organisations of all sizes.

For more information, please visit www.checkpoint.com

Cybereason | Education Seminar Sponsor

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Founded by elite intelligence professionals born and bred in offence-first hunting, Cybereason gives enterprises the upper hand over cyber-adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioural patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.

For more information, please visit www.cybereason.com

Digital Guardian | Education Seminar Sponsor

Digital Guardian provides the industry's only data protection platform that is purpose built to stop data theft from both insiders and external adversaries. The Digital Guardian Data Protection Platform performs across the corporate network, traditional endpoints and cloud applications and is buttressed by the DG Cloud, a big data security analytics backend, purpose built to see and block all threats to sensitive information. For more than 15 years, it has enabled data-rich organisations to protect their most valuable assets with a choice of on premises, SaaS or managed service deployment. Digital Guardian's unique data awareness combined with behavioural threat detection and response, enables you to protect data without slowing the pace of your business.

To learn more, please visit digitalguardian.com

Digital Shadows | Education Seminar Sponsor

Digital Shadows minimises digital risk by identifying unwanted exposure and protecting against external threats. Organisations can suffer regulatory fines, loss of intellectual property, and reputational damage when digital risk is left unmanaged. Digital Shadows SearchLight™ helps you minimise these risks by detecting data loss, securing your online brand, and reducing your attack surface.

For more information, please visit www.digitalshadows.com

Forescout Technologies | Education Seminar Sponsor

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environment and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, 100% real-time discovery and classification, as well as continuous posture assessment. More than 3,300 customers in over 80 countries rely on Forescout's infrastructure-agnostic solution to reduce the risk of business disruption from security incidents or breaches, ensure and demonstrate security compliance and increase security operations productivity.

Learn how at www.forescout.com

Guardicore | Education Seminar Sponsor

Guardicore is an innovator in data centre and cloud security that protects your organisation's critical assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security – for any application, in any IT environment. Guardicore was founded in 2013 with the goal of reinventing security to place greater emphasis on security beyond the traditional network perimeter. Guardicore has been entrusted to protect the data centres of enterprises across North America, South America, and EMEA in financial, healthcare and retail industries, including global, blue-chip brands.

For more information, please visit www.guardicore.com

Intel 471 | Education Seminar Sponsor

Intel 471 is the premier provider of intelligence global cybercrime and the cyber underground (including the deep & dark web). We provide adversary and malware intelligence for leading security, fraud and intelligence teams.

Our adversary intelligence is focused on infiltrating and maintaining access to closed sources where threat actors collaborate, communicate and plan cyber-attacks.

Our malware intelligence leverages our adversary intelligence and underground capabilities to provide timely data and context on malware and adversary infrastructure, including in-depth tracking and malware analysis reporting of nearly 30 malware families.

Our team is comprised of intelligence operators and native speakers located across the globe, where cybercriminals operate. Our intelligence operators have extensive experience operating in the intelligence services, military, law enforcement and commercial threat intelligence companies.

At Intel 471, we help to protect your organisation, your products, your assets, your people and your customers.

For more information, please visit intel471.com

Kaspersky | Education Seminar Sponsor

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialised security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help over 270,000 corporate clients protect what matters most to them.

For more information, please visit www.kaspersky.com

Kenna Security | Education Seminar Sponsor

Kenna Security is a leader in predictive cyber-risk. The Kenna Security Platform was built to enable security and IT operations to collaborate and proactively manage and remediate cyber-risks.

The average enterprise has over 60 thousand assets and 24 million vulnerabilities. But not all assets and vulnerabilities are of equal importance. Kenna uses its advanced Cyber Risk Context Technology™ with exploit intelligence capabilities to identify which vulnerabilities present the highest risk, allowing enterprises to focus on what matters most.

Kenna's predictive cyber-risk functionality enables security to stay a step ahead of cyber-attackers by:

- Predicting future exploits with high accuracy.
- Empowering security teams to remediate high-risk vulnerabilities long before they become a threat.
- Focusing teams on the riskiest vulnerabilities using established IT workflows.

No other cyber-risk analysis platform achieves results more accurately or increases IT efficiency as dramatically. With Kenna's data science and breakthrough predictive modelling technologies, a humanly impossible task turns into an easily managed one.

About Kenna's Cyber Risk Context Technology
Kenna Security's Cyber Risk Context Technology™ is the only technology that looks beyond the organisational level to identify which of the multitude of vulnerabilities are most likely to pose a threat. Kenna obtains its findings by collecting data in the wild, investigating hacker forums, exploit-kit directories, and real-time exploitations. Through advanced data science and predictive modelling, Kenna prioritises the vulnerabilities that pose the greatest risk now -- as well as in the near future.

About Kenna Security
Kenna counts among its customers many Fortune 100 companies and serves nearly every major vertical.

For more information, please visit www.kennasecurity.com and follow Kenna on Facebook, Twitter, and LinkedIn

Netacea | Education Seminar 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

OneTrust Vendorpedia | Education Seminar Sponsor

OneTrust Vendorpedia™ is the largest and most widely used technology platform to operationalise third-party risk, security, and privacy management. More than 5,000 customers of all sizes use OneTrust, which is powered by 75 awarded patents, to offer the most depth and breadth of any third-party risk, security, and privacy solution in the market. OneTrust Vendorpedia is purpose-built software designed to help organisations manage vendor relationships with confidence and integrates seamlessly with the entire OneTrust platform, including – OneTrust Privacy, OneTrust GRC, OneTrust DataGuidance™, and OneTrust PreferenceChoice™.

To learn more, visit vendorpedia.com or connect on LinkedIn, Twitter and Facebook

Proofpoint | Education Seminar Sponsor

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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 to mitigate their most critical security and compliance risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com/uk

RangeForce | Education Seminar Sponsor

RangeForce delivers the industry's only integrated cybersecurity simulation and skills analysis platform that combines a virtual cyber range with hands-on advanced cybersecurity training. Cyber and IT professionals from all industry verticals use RangeForce to qualify their new-hires, train up DevOps, IT, and Security Staff, and run CyberSiege simulations to evaluate team skills. Only RangeForce can accurately show users where expertise gaps exist, fill those gaps with highly effective simulation-based training, and accurately report on the entire process.

To learn more about RangeForce, please visit www.rangeforce.com

Red Sift | Education Seminar Sponsor

Red Sift is a data-driven cybersecurity business that uses machine learning to help organisations of all sizes and sectors address day-to-day security challenges. It offers a dashboard of tools that analyse and synthesise data from core business processes – such as email – to help users to better manage their online security.

Red Sift's mission is to democratise the technology essential for cybersecurity and as such has a diverse range of customers including TransferWise, Telefonica, Action for Children, Sadlers Wells and Northmill, not to mention a number of top UK law firms.

Red Sift is a London-based software-as-a-service startup, founded in 2015 by serial entrepreneurs Rahul Powar and Randal Pinto.

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

RiskIQ | Education Seminar Sponsor

RiskIQ is the global leader in attack surface management, providing the most comprehensive discovery, intelligence, and mitigation of threats associated with an organisation's digital presence. With more than 75% of attacks originating outside the firewall, RiskIQ allows enterprises to gain unified insight and control over web, social, and mobile exposures. Trusted by thousands of security analysts, security teams, and CISOs, RiskIQ's platform combines advanced internet data reconnaissance and analytics to expedite investigations, understand digital attack surfaces, assess risk, and take action. Its software protects businesses, brands, and customers.

Based in San Francisco with a European HQ in London, the company is backed by Summit Partners, Battery Ventures, Georgian Partners, and MassMutual Ventures.

For more information, please visit www.riskiq.com

Swimlane | Education Seminar Sponsor

Swimlane is at the forefront of the security orchestration, automation and response (SOAR) solution market. By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, Swimlane maximises the incident response capabilities of over-burdened and understaffed security operations.

Swimlane was founded to deliver scalable, innovative and flexible security solutions to organisations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane is at the forefront of the growing market for security automation and orchestration solutions that automate and organise security processes in repeatable ways to get the most out of available resources and accelerate incident response. The Swimlane solution offers a broad array of features aimed at helping organisations address both simple and complex security activities, from prioritising alerts to remediating threats and improving performance across the entire operation.

Swimlane is headquartered in Denver, Colorado, with operations throughout North America and Europe.

For more information, please visit www.swimlane.com

Synack | Education Seminar Sponsor

Synack offers a new and more disruptive security testing platform for finding and helping resolve serious vulnerabilities in mission critical applications and infrastructure that otherwise go undetected. It arms clients with large teams of international top class security researchers who provide a more diverse, adversarial perspective to clients' IT assets; often discovering vulnerabilities within hours.

Combined with the deployment of self-learning, intelligence-based reconnaissance technology and a transparent AI-enabled platform with a real-time customer portal, Synack provides a more advanced and effective way for security testing. This next generation testing platform overcomes the shortcomings of traditional pen testing and vulnerability scanning and better simulates increasingly sophisticated cyber-attacks and TTPs.

Synack's confidential client base is comprised of some of the largest F500/G500 enterprise organisations across banking and financial services, retail, healthcare, consumer goods, manufacturing, and technology, as well as the US Government (DoD/Hack the Pentagon, IRS). Synack was founded in 2013 by former NSA security experts Jay Kaplan, CEO, and Dr. Mark Kuhr, CTO.

The Synack solution comes in a continuous security testing subscription to assure protection of mission critical assets. For assets that demand point-in-time testing there is a 14-day security test.

For more information, please visit www.synack.com

Tripwire | Education Seminar Sponsor

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organisations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organisations discover, minimise and monitor their attack surfaces.

Learn more at www.tripwire.com, get security news, trends and insights at www.tripwire.com/blog, or connect with us on LinkedIn, Twitter and Facebook

Wandera | Education Seminar Sponsor

Wandera, a cloud security company, protects modern enterprises beyond the traditional perimeter. When remote users access applications from their smartphones or laptops, anywhere in the world, Wandera's unified security cloud provides real-time threat protection, content filtering and zero-trust network access. Wandera regularly shares the latest findings from its industry-leading threat intelligence, which applies machine learning across 425 million sensors worldwide. Founded in 2012 by a team of cloud security veterans, and recognised as a leader by analyst firms including Gartner and IDC, the company is headquartered in San Francisco and London.

To learn more, please visit www.wandera.com, or follow on LinkedIn and Twitter

Agari | Networking Sponsor

Agari is transforming the legacy Secure Email Gateway with its next-generation Secure Email Cloud powered by predictive AI. Leveraging data science and real-time intelligence from trillions of emails, the Agari Identity Graph detects, defends, and deters costly advanced email attacks including business email compromise, spear phishing, and account takeover. Winner of the 2018 Best Email Security Solution by SC Magazine, Agari restores trust to the inbox for government agencies, businesses, and consumers worldwide.

For more information, please visit www.agari.com

ReversingLabs | Networking Sponsor

ReversingLabs File Intelligence Service is the industry's largest and most comprehensive source for up-to-date classification and rich context on files. ReversingLabs harvests over 8 million files daily and processes them with unique File Decomposition and Static Analysis technologies for unpacking and data extraction. This analysis exposes extensive data from all extracted objects and makes it available to customers for searching, hunting, and analysis.

For more information, please visit www.reversinglabs.com

ThreatConnect | Networking Sponsor

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralise your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place.

To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, please visit www.ThreatConnect.com

Cortida | Branding Sponsor

Cortida Limited is an expert UK-headquartered cybersecurity risk mitigation consultancy that helps organisations of all sizes identify, analyse and mitigate cyber-risks and incidents.

We protect clients from reputational damage, financial penalties and operational disruption associated with data incident. Critical to our approach is a desire to ensure security spend is wisely invested.

Key to Cortida's values are the words 'Appropriate Security'. Cortida's driving values ensure security decisions are informed from an elevated understanding of data and its associated regulatory or contractual obligations plus our client's operational objectives and appetite for risk.

Cortida services sit across 6 domains, Consulting, Penetration testing, Detection & response, Security awareness & training, Compliance audits and Virtual support.

- *Consulting services* help organisations identify and remediate information and cybersecurity risk, introduce security best practice and meet and maintain compliance obligations such as ISO 27001, Cyber Essentials, PCI DSS and GDPR.
- *Testing services* help organisations identify potentially exploitable vulnerabilities and then help you understand the root cause, severity and actions required to mitigate the risks.
- *Detection & response services* help organisations monitor network traffic for threats and then respond to incidents in a planned and managed way.
- *Security awareness & training services* include face to face workshops and computer-based training options – these help business leaders and employees understand the security landscape and key issues relevant to their roles and embed a security aware culture.
- *Compliance audit services* prepare an organisation for formal security assessment and then validate the presence of security controls.
- *Virtual support services* provide expert led on or off-site support services that help organisations progress projects and govern security and privacy without the expense of large internal teams.

For more information, please visit cortida.com
Enquiries about Cortida services can be made at info@cortida.com or by calling + 44 (0) 20 7164 6693

Pulse Secure | Branding Sponsor

Put simply, we are the company that is 100% focused on delivering secure access solutions for people, devices, things and services. For years, enterprises of every size and industry have been trusting our integrated virtual private network, access control, virtual application delivery controllers, and mobile security solutions to enable secure access seamlessly in their organisations.

Every single day, our global team are innovating our products to ensure that you can dramatically boost your workers' productivity, make a smooth and secure transition to the cloud and ensure that your networks are protected without a burden on IT. We call it Secure Access for the next generation.

For more information, please visit www.pulsesecure.net

08:00 Registration and breakfast networking

08:50 Chairman's welcome

09:00 **The innovation juggernaut: making security leaders partners in success**

Akhil Lalwani, Head of Digital Platforms, Prudential
- Being a part of the innovation journey: How can today's CISO ensure they are active partners in the journey?
- Innovation and customer needs are constantly changing – can our approach to security remain static?
- Takeaways: the actionable five step framework

09:20 **Defence in diversification: improving cybersecurity through smart consolidation**

Jamie Moles, Senior Security Engineer, ExtraHop
- How a data-first approach to security architectures can illuminate natural consolidation points
- How collaboration with other parts of the IT organisation can improve security posture and reduce tool sprawl
- How this collaborative approach also creates an opportunity to leverage other parts of the organisation to improve security posture through smarter processes and practices

09:40 **Preparing for the next cyber-attack – from the attacker's perspective**

Etay Maor, Chief Security Officer, IntSights
- Cybersecurity solutions often utilise the latest 'AI, machine learning driven, blockchain based, next gen, highly granular, zero trust, future proof technology... as a service'. However, looking at the common themes in the major breaches it looks like cyber-adversaries have a different approach to their attacks
- How our adversaries conduct threat intel gathering and attack preparation, explored through case studies detailing how security breaches are (easily) performed
- How current attack mapping frameworks can be used to prepare for the next attack

10:00 **Collaborative criminal combat. How collaboration between law enforcement and industry is critical to protect us from evolving cyber-threats**

Debbie Grant, Senior Policy Lead, Fraud Strategy & Criminal Disruption, Visa, and
Detective Sergeant **Ben Hobbs** – DCPCU, Dedicated Card & Payment Crime Unit, Metropolitan Police
- Fraud as a catalyst for other forms of high-level crime. The relationship between fraud, AML and cybersecurity, and how the digitalisation of business is making the challenges and risks experienced by all three increasingly interlinked
- Public and private collaboration and how working together can have an impact on disrupting criminal activities
- Real-life case studies and insights into the evolution of social engineering

10:20 **Education Seminars | Session 1** **See pages 54 to 63 for more details**

Accellion	**Third-party communication for confidentiality, compliance and control** **Harry Zorn,** Vice President Sales, EMEA, Accellion
CrowdStrike	**e-Crime and the frontline: lessons learnt in responding to the most advanced cyber-attacks** **Mark Ward,** Senior Solutions Architect, CrowdStrike
Kenna Security	**Risk-based, time-critical vulnerability management: four steps for success** **Stephen Roostan,** VP EMEA, Kenna Security, and **Simon Black,** Pre-Sales Systems Engineer, Kenna Security
Netacea	**Bad Bots 101: how to carry out an ATO attack** **Mark Greenwood,** Chief Technical Architect, Netacea, and **Tom Platt,** Senior Account Manager, Netacea
RiskIQ	**Using internet reconnaissance data to defend against targeted attacks** **Vijay Punja,** Technical Account Manager, RiskIQ
TrapX Security	**Building an effective deception strategy** **Nathan Gilks,** Regional Solutions Architect, TrapX Security
Tripwire	**The future is hybrid: key considerations for cloud and DevOps** **Dean Ferrando,** Lead Systems Engineer, Tripwire
Wandera	**Redefining the edge: making the most of your security investments in a zero-trust world** **Adam Boynton,** Sales Manager, Wandera

11:00 Networking and refreshments

11:30 **The hyper-connected CISO: inconvenient truths and lessons on staying afloat**

Becky Pinkard, CISO, Aldermore Bank
- How digitalisation, of both the financial services and also of the general business landscape, has impacted the information security remit, and how you can secure a hyper-connected world
- The CISO's role in this ever-evolving landscape
- The mandatory changes and evolution required around security awareness across the workforce

11:50 **The hidden adversary. Advanced detection of attackers on the network using deception**

Nick Palmer, Technical Director, Attivo Networks
- Understand how attackers can breach even the most well fortified networks
- Discover how quickly attackers can move towards monetisable targets in an organisation
- Learn how deployment of advanced detection techniques can uncover hidden attackers
- See how integration with existing tooling and SOC workflows can contain threats and minimise risk

12:10 **ISO27001 & the GDPR: identifying overlap and streamlining efforts**

Joseph Byrne, Privacy Solutions Engineer – CIPP/E, CIPM, OneTrust
- Map the most common security operations standard, ISO 27001 to the world's most influential piece of privacy legislation, the GDPR
- Identify how much work toward GDPR compliance that security teams have likely already done
- Outline six main areas of common ground that should help every organisation align their security and privacy operations
- Develop a framework to reduce the risk of a damaging incident while increasing productivity and customer trust
- Understand the importance of building a cohesive compliance strategy across privacy and security teams
- Learn about the stakeholders, teams, tools and processes that should come together for a comprehensive privacy and security strategy
- Take away a roadmap and action plan for bridging privacy and security in your organisation

12:30 **Faking it: combatting email impersonation with AI**

Mariana Pereira, Director of Email Security Products, Darktrace
- 'Impersonation attacks' are on the rise, as AI is increasingly being used to automatically generate spear-phishing emails, or 'digital fakes'
- Humans can no longer distinguish real from fake on their own, so businesses are increasingly turning to AI to distinguish friend from foe and fight back
- Learn how 'immune system' technology can stop cyber-threats before any damage is done

12:50	**Education Seminars | Session 2**	**See pages 54 to 63 for more details**
	Attivo Networks	**Operationalising deception. How to conceive, execute and integrate advanced threat detection into your organisation** **Nick Palmer,** Technical Director, Attivo Networks
	Digital Guardian	**Visibility is key to a successful data protection programme** **Matt Logan,** Vice President of Field Engineering – EMEA, Digital Guardian
	Guardicore	**Beyond the (fire)wall** **Avishag Daniely,** Director of Product Management, Guardicore
	Kaspersky	**To blockchain or not to blockchain** **Maxim Denizhenko,** Lead Business Development, Enterprise Blockchain Security, Kaspersky
	Menlo Security	**Internet isolation: a key requirement for the modern security architecture** **Brett Raybould,** EMEA Solutions Architect, Menlo Security
	Proofpoint	**Building a people-centric security strategy** **Roy Murdoch,** SE Manager UKISA, Proofpoint
	Red Sift	**Lessons from the dark side?** **Rois Ni Thuama,** Head of Cybersecurity Governance & Legal Partnerships, Red Sift
	Zscaler	**How you can achieve a zero trust network access** **Danny Phillips,** Senior Manager of Systems Engineering, Zscaler
13:30	Lunch and networking	
14:30	**Critical intel on threat intel. Fraud threat intelligence and the business benefits and ROI**	
	Terje Aleksander Fjeldvaer, Head of Financial Cyber Crime Center, DNB • Insight into how criminals use technology and the increased complexity of cases • How organised criminal groups cynically defraud and exploit peoples weaknesses for financial gain • The connection between fraud and terrorism • How we work on fraud threat intel and the business benefits and ROI	
14:50	**The latest state of the threat: attack is inevitable, compromise is probable, engagement is essential**	
	Mark Smith, Pre-Sales Manager, Orange Cyberdefense • Security strategies are many times driven on fear and compliance issues, with spending on perceived rather than genuine threats • Understanding the real threat in a world that is highly complex and changing all the time is not a simple task • In this session, discover Orange Cyberdefense's research on how threat is evolving and where you should be spending energy and focusing on	
15:10	**A first, practical step to a zero trust strategy**	
	Trevor Dearing, Technical Director, EMEA, Illumio • Computing environments are becoming so diverse and security so sophisticated that trying to keep them synchronised is now a huge issue • Many agencies and governments have adopted zero trust as the easiest way for organisations to adopt a culture of safe and secure operation • There is a perception that zero trust can be complex and expensive. In this session, we will look at how the basics can be achieved, with very little impact on existing infrastructure, to take the first steps toward a zero trust environment.	
15:30	**Education Seminars | Session 3**	**See pages 54 to 63 for more details**
	Digital Shadows	**Information warfare – what is it and how does it affect me?** **Stewart K. Bertram,** Director of Intelligence, Digital Shadows
	Intel 471	**Extra! Extra! Read all about it! The evolving sophistication of how threat actors are using current news events to spread malware** **Maurits Lucas,** Director of Intelligence Solutions, Intel 471, and **Max Mansson,** Director, UK & Europe, Silobreaker
	OneTrust	**Transitioning GDPR from a compliance checklist to 'business as usual'** **Joseph Byrne,** Privacy Solutions Engineer, CIPP/E, CIPM, OneTrust
	Swimlane	**SOAR in the age of DX** **Toby Van de Grift,** UK Regional Director, Swimlane
	Synack	**Using hackers to beat hackers: innovation at Just Eat** **Justin Shaw-Gray,** Account Director, Synack Inc., and **Kevin Fielder,** CISO, Just Eat
16:10	Networking and refreshments	
16:30	**EXECUTIVE PANEL DISCUSSION** **Breaking down barriers, solving the cyber conundrum**	
	Chaired by: Alphus Hinds, CISO, Standard Bank **Zsuzsanna Berenyi,** Cyber Security Culture and Engagement Specialist, Refinitiv **Deborah Haworth,** CISO, Penguin Random House **Adam Gwinnet,** Head of Enterprise Architecture & Cyber Security, Metropolitan Police Service **Nicola Lishak,** Head of Information Assurance, Royal Mail	
16:50	**Extending data security to the cloud**	
	Dave Matthews, Systems Engineer, Netwrix • What specific challenges are there for securing data in the cloud? • How can a single data security strategy be applied to the entire hybrid IT environment? • What steps can help you protect your data across your on-premises and cloud-based systems?	
17:10	**'Will' vs. 'Skill': are we using the wrong tactics to recruit for our information security team?**	
	Goher Mohammad, Head of Information Security, L&Q Group • There is a cybersecurity skills shortage that is still not shrinking, as hiring managers and leaders we need to tackle the gap between demand and supply of cybersecurity professionals • Traditional methods of hiring need challenging, how to adopt an agile and flexible approach • Get yourself noticed! What are cybersecurity hiring managers looking for in a new recruit? • Positive results: lessons learnt from L&Q Group on building and retaining talent within your security team	
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 **Ransomware: an evolving threat**

Mike Hulett, Head of Operations, National Cyber Crime Unit (NCCU)
- What are the most prevalent forms of ransomware, and common attack methodologies
- How has the threat and the market evolved over the last couple of years
- A case study – what might happen to you, and how law enforcement may assist
- How can you avoid this? Best practice for security & resilience

09:20 **Untangling the spider's web: e-crime exposed**

Mark Ward, Senior Solutions Architect, CrowdStrike
- Understanding the threat landscape, who the adversaries are and how we can spot them
- Examining the latest attack techniques adopted and deployed by e-crime actors
- How we use the intelligence we gather about the adversary to prevent, protect and respond against the cyber-threat of tomorrow

09:40 **Deception in action: how deception helped one of the largest global brands transform its cyber-resilience programme**

Tony Kinkead, Regional Director – EMEA, TrapX Security
- Why do defenders have to be right 100% of the time? How do you turn the odds in your favour?
- Improving detection of the external intruder, zero-day malware and the insider threat
- Reducing alert fatigue, false positives and dead ends for critical resources
- Incorporating detection for IoT, OT and legacy systems across the enterprise

10:00 **Managing fraud in an unregulated market**

Michael Aydeniz, Head of Fraud and Credit Risk, Planet
- Navigating the myriad challenges faced by an organisation when they operate in a largely unregulated market
- Managing cross-jurisdictional fraud issues
- First-hand case study taken by Planet in devising a one-size-fits-all approach to fraud monitoring and mitigation

10:20 **Education Seminars | Session 4** **See pages 54 to 63 for more details**

Cybereason	**A live cyber-attack simulation** **Anthony Wainman,** Senior Sales Engineer, Cybereason
Forescout Technologies	**Device visibility and control: transforming enterprise-wide network segmentation** **Richard Orange,** Regional Director UKI, Forescout Technologies
Illumio	**Decoupling security segmentation from network infrastructure** **Trevor Dearing,** Technical Director, EMEA, Illumio, and **Adam Brady,** Director Systems Engineering EMEA, Illumio
Netwrix	**Back to the future: a data breach prevention plan** **Dave Matthews,** Systems Engineer, Netwrix
OneTrust	**Overcoming today's most common security & privacy challenges** **Alan MacGillivray,** Account Executive, OneTrust
RangeForce	**The RangeForce 'Cyber Gym': building cybersecurity muscle memory through simulated training for enterprise tech teams** **Gordon Lawson,** CRO, President, RangeForce

11:00 Networking and refreshments

11:30 **EXECUTIVE PANEL DISCUSSION** **Threat intelligence in the real world**

Jules Pagna Disso, Group Head of Cyber Risk Intelligence, BNP Paribas
Simon Cross, Security Architect, Lloyds
Dan Burns, Information Security Manager, NEXT
Martin Rudd, Chief Technology Officer, Telesoft Technologies

11:50 **Achieve security without compromise**

Jonathan Lee, Sr. Product Manager, Menlo Security
- Why legacy appliance-based security is not going to cut it in the age of cloud
- Why a detection based, 'almost safe' approach has its limitations
- Why we should challenge Gartner's adaptive security architecture with a new technology
- Learn how isolation makes it possible to approach security and networking in an entirely new way

12:10 **The intelligence lifecycle, dissemination, and why compromised credentials are paramount**

Kevin Tongs, Director Customer Success (EMEA), Flashpoint Intel
- A summary of the intelligence lifecycle
- The rules of dissemination within the cycle
- How these rules have influenced Flashpoint's product development
- Why compromised credential monitoring is key to timely, actionable intelligence

12:30 **Making a cloud-first strategy a reality**

Danny Phillips, Senior Manager of Systems Engineering, Zscaler
- Legacy IT debt, unfinished upgrades and compliance are all quoted as reasons to delay cloud adoption
- So if you were able to start your business again from scratch, and plan the next five-year IT strategy, what would it consist of?
- With technology shifts such as the move to cloud, are current security policies still valid?
- Join our session to discover how you can implement a cloud-first strategy amidst legacy architectures

12:50 **Education Seminars | Session 5** **See pages 54 to 63 for more details**

Check Point	**Cyber warfare 2019/2020** **Lotem Finkelsteen,** Head of Threat Intelligence, Check Point
Darktrace	**Offensive AI vs. Defensive AI: battle of the algorithms** **Nathan Beresforde,** Account Director, Darktrace
ExtraHop	**Winning strategies to scale and upskill your security team** **Jamie Moles,** Senior Security Engineer, ExtraHop
IntSights	**Shutting down attacks with dark web intelligence** **Michael Owen,** Head of Systems Engineering UK&I, IntSights
Kaspersky	**Hunting the hunters** **Jose Alemán,** Global Pre-sales Expert, Kaspersky
RiskIQ	**Defending your organisation against JavaScript injection attacks** **Terry Bishop,** VP, Technical Services, RiskIQ

13:30	Lunch and networking
14:30	**The big blue button – a law enforcement lens on cybercrime response**
	Adam Gwinnett, Head of Strategy, Enterprise Architecture & Cyber Security, Metropolitan Police • A call to arms: bringing cyber from passive FUD to active engagement • Reporting and greater disclosure from industry. Why have we got to the point where c. 99% of fraud cases across financial services go unreported? • Actionable lessons from law enforcement on 'when to push the big blue button'
14:50	**How do you prioritise cybersecurity resources and budget? Metrics and ROI for a cyber-secure culture**
	Federico Iaschi, Head of Information Security, Seqirus • Training and awareness: how do you prove ROI, budget and metrics for a cyber-secure culture? • Key 'action item' breakouts to help an information security awareness programme mature and thrive • The particular risks and consequences of the bio-pharma industry. Supply chain risk, and the physical, 'real world' consequences of a breach
15:10	**The F word: making fraud and forensics a key business priority in the digital world**
	Robert Brooker, Co-Head of Fraud and Forensics, PKF Littlejohn • Actionable insights into current fraud, bribery and corruption risks and the impact of digitalisation • The relationship between corporate fraud, governance and cyber, and why collaboration between the three is vital for the business • How do you get buy in from the C-suite, and how can you implement change in the behaviours and culture of a business?
15:30	Networking and refreshments
15:50	**Cybercrime and the movies. Why cyber needs a makeover**
	Garry Scobie, Deputy CISO, The University of Edinburgh • Cybersecurity is viewed as a complex game of cat and mouse, played out against men in darkened rooms wearing sunglasses and hoods. The movies perpetuate this myth • Does this portrayal of cybercrime hinder the recruitment of diverse security minded individuals to tackle the problem? • Behind the scenes: how the movies compare with the reality of cybercrime. How can we use this disconnect to become security savvy in our on-line lives? • Cybersecurity needs a makeover so let's walk-through some classic movies and see how they fare against the real threats we face today
16:10	**Actionable cyber-awareness. Time for real change**
	Sam Watling, Information Security Governance and Compliance Lead, TUI • How to inspire your colleagues to make real change in the way they secure themselves personally and therefore protect your business • Why TUI embarked on their award-winning colleague awareness and behavioural change programme across a multi-cultural, multi-language, geographically distributed workforce • How a common theme and purpose has driven tangible behavioural change across the business • How to adopt security best practice and behaviours at home and at work, protecting colleagues, families and reducing risk to the company as a whole
16:30	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: 3rd March | 10:20–11:00

Accellion

SESSION 1
3rd March
10:20–11:00

Third-party communication for confidentiality, compliance and control

Harry Zorn, Vice President Sales, EMEA, Accellion

In this presentation delegates will learn different techniques and ideas how to reduce third-party risk.

What delegates will learn:

- The evolution from network to application to content firewall
- How to increase the level of security by making life easier
- Whether or not a newspaper is a good weapon of choice in a knife-fight
- How to decrease third-party risk
- How to consolidate security technologies, reduce risk and save money

CrowdStrike

SESSION 1
3rd March
10:20–11:00

e-Crime and the frontline: lessons learnt in responding to the most advanced cyber-attacks

Mark Ward, Senior Solutions Architect, CrowdStrike

Defending against modern adversaries requires the ability to detect and understand threats quickly and to respond decisively. CrowdStrike's experts fight and win these battles every day, and have one of the industry's most comprehensive pictures of today's top cyber-threats. Allow us to lead you through a deep dive into global observations and trends, and real-world intrusion case studies, delivering deep insights on modern adversaries, and their tactics, techniques, and procedures (TTPs).

- Lessons learnt in the course of conducting in-depth digital forensics, IR and remediation with real-world strategic insight into the current threat landscape
- How advanced attacks succeed in evading modern defences
- How applied threat intel can deliver advantage in protecting your enterprise

Kenna Security

SESSION 1
3rd March
10:20–11:00

Risk-based, time-critical vulnerability management: four steps for success

Stephen Roostan, VP EMEA, Kenna Security, and **Simon Black,** Pre-Sales Systems Engineer, Kenna Security

Join Steve and Simon to find out how leveraging data science through the lens of cyber-risk can quickly deliver multiple value streams across an organisation. This session will show how to empower security, DevOps, and management with a self-service portal that both improves cybersecurity, and delivers measurable efficiency gains to both IT security and development teams.

- Assessing the scale of the problem
- Benchmarking against industry metrics
- Establishing how success should be measured
- Deploying a self-service portal to enable ITOps/DevOps to be part of the remediation task force

Netacea

SESSION 1
3rd March
10:20–11:00

Bad Bots 101: how to carry out an ATO attack

Mark Greenwood, Chief Technical Architect, Netacea, and **Tom Platt,** Senior Account Manager, Netacea

Bots account for more than 50% of all online traffic and are responsible for a range of good, bad and nuisance activity. Consumers and businesses alike are exposed to bot risks, with the attackers able to carry out a range of illicit and often fraudulent activity.

- To highlight the significant, detrimental impact of bots targeting global enterprises, Netacea will simulate a real-time account takeover attack. The attack will demonstrate the ease with which a

threat actor can orchestrate an account takeover that bypasses traditional security measures
- Throughout the attack, we will discuss the impact on various departments throughout an organisation – from security and operations to marketing managers – with reference to bot management best practices

RiskIQ

SESSION 1
3rd March
10:20–11:00

Using internet reconnaissance data to defend against targeted attacks

Vijay Punja, Technical Account Manager, RiskIQ

Network security monitoring solutions regularly highlight indicators associated to assets residing on the internet. Threat intelligence reports regularly detail threat actors and their tactics along with details of some of their assets. However, in both cases these indications are hosted on infrastructure that is connected to other adversary owned infrastructure. The challenge for most security teams is how to quickly assess what they are dealing with so they can take appropriate action. It's not enough to take defensive action against one or a group of URLs or IP addresses when that is only a small part of what could hurt you. You need to know what else those assets are connected to – in other words, the entire bad neighbourhood.

Because hackers can't avoid interacting with core components of the internet, they leave a trail of breadcrumbs over time; registered domains and certificates, servers and supporting infrastructure, fake websites and fishing pages, and campaign assets such as emails, social posts and SMSs that direct victims to their malicious assets. Fortunately, there are organisations like RiskIQ that monitor and map changes to the infrastructure of the internet over time to create global internet datasets that threat hunters can use to connect the dots to map out adversary infrastructure.

In this session we'll cover:

- What are internet datasets and how are they created?
- What are the different types of internet datasets available and their specific strengths?
- What is infrastructure chaining and how can multiple internet datasets support this technique?
- How can your security researchers freely access internet datasets?

TrapX Security

SESSION 1
3rd March
10:20–11:00

Building an effective deception strategy

Nathan Gilks, Regional Solutions Architect, TrapX Security

The TrapX platform allows you to deploy your company's deception strategy by using several layers of capability. Mask your entire network infrastructure by using a 'deception full stack' model. And emulate real network assets at scale without the need to deploy complex and costly systems or overburdening your critical resources.

During our session, you will:

- Understand why organisations are adopting a deception strategy
- Walk-through the 'deception full stack' model
- See a live demonstration of TrapX
- Watch how easily deception traps can be deployed with little to no impact on resources
- Realise how a scalable deception strategy can be implemented
- Finally, delve into the rich ecosystem of security integrations demonstrating the value of TrapX working with your existing security defences to alert, respond and remediate

Tripwire

SESSION 1
3rd March
10:20–11:00

The future is hybrid: key considerations for cloud and DevOps

Dean Ferrando, Lead Systems Engineer, Tripwire

The elasticity and short lifespan of servers, paired with the up-and-coming wave of containerisation, introduces unique challenges to securing cloud infrastructure. In this session, we explore the key considerations and best practices for expanding security operations to the cloud and DevOps, including:

- Understanding the responsibilities and controls of a hybrid environment
- How to properly manage configuration and vulnerability risks
- How to build trust across multiple cloud solution providers
- And learn from the case study of a major financial institution that successfully secured its hybrid enterprise

Wandera

SESSION 1
3rd March
10:20–11:00

Redefining the edge: making the most of your security investments a zero-trust world

Adam Boynton, Sales Manager, Wandera

Your employees work remotely. Your data is in the cloud. You've invested in solutions to help make users productive but with hackers targeting your endpoints, how do you keep your data – and your users – safe? It's time to redefine the enterprise perimeter.

Join this session to discover:

- Why legacy security architectures don't pay off
- The evolving threats targeting your employees
- Why user behaviour has changed and how to adapt
- How to maximise your existing security investments
- Three tips to avoid being the next Jeff Bezos (don't get hacked)

Session 2: 3rd March | 12:50–13:30

Attivo Networks

SESSION 2
3rd March
12:50–13:30

Operationalising deception. How to conceive, execute and integrate advanced threat detection into your organisation

Nick Palmer, Technical Director, Attivo Networks

When the decision has been taken to deploy deception to augment the organisation's security posture, several key questions are raised, which must be addressed to properly leverage value from this critical detection capability. By planning how to deploy deception, matched to organisational risk appetite, integrated into pre-existing SOC workflows and designed to support incident response, security teams can make extremely effective use of deception to understand how and where attackers have managed to breach the network. Additionally, their motives and methods can be more effectively understood to properly plan for future events and take the power from the attackers and place it in the hands of the SOC teams.

- Understand deception maturity – crawl, walk run
- Understand how to deploy deceptive assets and fake data
- Understand the critical integrations and how to gain 360 degree visibility of attackers on the network
- Engage the business in building effective deception campaigns and gain stakeholder commitment to deception

Digital Guardian

SESSION 2
3rd March
12:50–13:30

Visibility is key to a successful data protection programme

Matt Logan, Vice President of Field Engineering – EMEA, Digital Guardian

Data protection programmes should never fail if you use the right tools! Gone are the days of guessing what you need to protect, deploying policies in an hope and pray fashion.

Digital Guardian uses advanced visibility to provide you with a detailed view of exactly how data flows and is being used in your organisation.

Additionally, why combining data protection and endpoint detection and response combined is the future of data protection.

In this session you will learn:

- How to start a successful data protection programme
- Avoiding the pit falls
- Using advanced data protection technologies to show you how data is being used
- DLP and EDR, why combine

Guardicore

SESSION 2
3rd March
12:50–13:30

Beyond the (fire)wall

Avishag Daniely, Director of Product Management, Guardicore

The age of the hybrid cloud has created a need for a different approach when it comes to firewalls. For some, virtual cloud firewalls seemed like they might be the answer to protecting the modern hybrid data centre, but the truth is, these are also insufficient for today's e-crime landscape.

This presentation will cover the main points firms need to take into consideration when choosing the right solution when securing its data centres, including:

- Latency
- Ease of deployment
- Maintenance and more

Kaspersky

SESSION 2
3rd March
12:50–13:30

To blockchain or not to blockchain

Maxim Denizhenko, Lead Business Development, Enterprise Blockchain Security, Kaspersky

Practical cybersecurity reasonings of blockchain-based solutions.

- Key features of blockchain technology
- Cybersecurity threats in blockchain solutions and how to mitigate them
- Does DLT always mean trust?
- Case studies

Menlo Security

SESSION 2
3rd March
12:50–13:30

Internet isolation: a key requirement for the modern security architecture

Brett Raybould, EMEA Solutions Architect, Menlo Security

Organisations should not need to accept the short comings of solutions that cannot solve the problems of inbound threats via web and email. Isolation provides a secure execution environment where content can be executed away from the user and in a way that makes it impossible for the attacker to reach their target, thereby mitigating all risk from infection. Isolation also does not suffer from false positive or negatives. In the session, participants will learn how this is possible and how it solves many specific use cases. There will also be a live demo of Menlo Security's Cloud Proxy Platform, the first of its kind with an Isolation Core™.

What will attendees learn:

- Why isolation can achieve secure cloud transformation
- How to eliminate all risk of infection from browser based threats
- How to protect the user from credential theft via phishing attacks

Proofpoint

SESSION 2
3rd March
12:50–13:30

Building a people-centric security strategy

Roy Murdoch, SE Manager UKISA, Proofpoint

Cybercriminals target employees with access to the information they need through highly sophisticated and personalised attacks.

We will explore how cybercriminals use two of the most powerful information tools – LinkedIn and Google – to perform reconnaissance on potential targets. These social engineering techniques mean that attackers often know more about your employees than you do.

The only security strategy that will successfully combat today's advanced attacks is one that focuses on protecting your people.

This session explores how to build a strategy that:

- Reveals who is targeted and how
- Combats attacks before they reach your users
- Mitigates damage from the attacks that inevitably will reach your people
- Protects the data they create

Red Sift

SESSION 2
3rd March
12:50–13:30

Lessons from the dark side?

Rois Ni Thuama, Head of Cybersecurity Governance & Legal Partnerships, Red Sift

Fraud & prevention: Lessons in trust and identity

During this session, Red Sift's Head of Cyber Governance, Dr Rois Ni Thuama will:

- Explore a series of high-profile frauds that hit the headlines and look at what happened in each case
- Unpick the common denominators that bind these apparently diverse frauds
- Identify what organisations can learn from these fraudsters to shape and inform the steps they take to protect their firm's identity and reputation

Zscaler

SESSION 2
3rd March
12:50–13:30

How you can achieve a zero trust network access

Danny Phillips, Senior Manager of Systems Engineering, Zscaler

Network-centric security wasn't built to secure the agile world of the cloud, which is why Gartner recommends embracing zero trust network access (ZTNA) technologies. ZTNA, also known as SDP, enables secure access to private apps across hybrid and multi-cloud environments enabling secure cloud adoption.

Learn how ZTNA can help you obtain a zero trust access model whilst simplifying the management of not only your users, your controls, but also your access to applications.

- How you can transform your network from open access to a secure, policy-driven framework
- How to gain visibility of application access in a multi-cloud environment
- Keeping your users secure, no matter where they are or how they are connected
- Hide internal services from potentially malicious internet users

Session 3: 3rd March | 15:30–16:10

Digital Shadows

SESSION 3
3rd March
15:30–16:10

Information warfare – what is it and how does it affect me?

Stewart K. Bertram, Director of Intelligence, Digital Shadows

Information warfare is an umbrella term for an amorphous collection of activities that fall under the banner of terminology such as 'phycological warfare', 'fake news', 'disinformation', 'misinformation', and any number of other increasingly complex terms. With recent events such as the United States election in 2016 and the recent developments around Brexit, information warfare is undoubtably an important issue. But where to start with this subject, and is it even a cybersecurity issue?

This talk seeks to address this issue and dissect information warfare as a concept by offering a range of taxonomies to analyse the subject, backed up by several real-world cyberspace case studies.

Topics examined include how threat actors realise information warfare campaigns both at a conceptual level and a practical level, making use of tactics such as data theft and mobilisation via social media platforms.

The paper is both an introduction to the subject as well as a detailed primer for further work within research into the subject.

Key takeaways:

- What information warfare is and how it differs from propaganda and other forms of influence operations
- How cyberspace effects the practise of information warfare on a macro level
- How this abstract concept has the potential to develop into a genuine threat in the future
- The positive and negative aspects of information warfare from the adversary perspective

Intel 471

SESSION 3
3rd March
15:30–16:10

Extra! Extra! Read all about it! The evolving sophistication of how threat actors are using current news events to spread malware

Maurits Lucas, Director of Intelligence Solutions, Intel 471, and **Max Masson,** Director, UK & Europe, Silobreaker

Increasingly, threat actors are aligning their activities to high-profile global events, such as CoronaVirus, natural disasters, etc, to prey upon the fear and uncertainty stemming from mass media coverage of these events. This leads people to lower their state of alertness and do things that they wouldn't typically do, such as clicking links or attachments in emails they don't recognise. Though phishing is nothing new, the level of sophistication in threat actors' methods continually adapts and advances.

In this presentation, we will discuss:

- Insight into campaigns targeting the public's fear and uncertainty regarding CoronaVirus
- The methods threat actors are using to mask their activities and bypass individuals' own security awareness
- The recent evolving state changes of prolific malware families that provide insight into how actors are changing their targeting and delivery
- The identification of new connections among various actors and malware families that have not been seen before, which can help indicate new methods and campaigns that may soon emerge

OneTrust

SESSION 3
3rd March
15:30–16:10

Transitioning GDPR from a compliance checklist to 'business as usual'

Joseph Byrne, Privacy Solutions Engineer, CIPP/E, CIPM, OneTrust

While privacy pros across the globe overhauled business processes leading up to the GDPR's effective date, 25th May 2018 was just the beginning. Compliance is an ongoing exercise and privacy must be integrated into every aspect of the business. In this session, we'll share strategies for shifting your GDPR programme from a compliance checklist item into 'business as usual' within your company. From privacy champions across the business to privacy by design, we'll outline a step-by-step approach to making privacy a reflex (and not a nuisance) to business operations and build privacy as a culture within your company.

- Understand how to shift GDPR compliance efforts from a one-off activity into business as usual
- Take home a step-by-step approach to ongoing GDPR compliance within your company
- Realise how ongoing GDPR efforts can set your company up for success with other global privacy laws

Swimlane

SESSION 3
3rd March
15:30–16:10

SOAR in the age of DX

Toby Van de Grift, UK Regional Director, Swimlane

Digital transformation impacts every part of a business: product creation, customer service, finance, time to market, time to value – everything is faster, more responsive and more 'granular'.

So how does security exist in this new world, and what does this mean for Security Orchestration, Automation and Response (SOAR)?

When correctly deployed, SOAR is truly transformative. It starts by simply augmenting humans in a linear workflow – getting more out of existing tech and your investment in staff. It can quickly evolve into a much higher value security tool.

Swimlane has been automating and transforming SOCs since 2014 and we would like to share our knowledge and experience with you.

My presentation will discuss:

- What is the value of SOAR, and how do you harness it?
- How does SOAR drive DX?
- Why should you use SOAR and what factors should you consider?

Synack

SESSION 3
3rd March
15:30–16:10

Using hackers to beat hackers: innovation at Just Eat

Justin Shaw-Gray, Account Director, Synack Inc., and
Kevin Fielder, CISO, Just Eat

There are big dilemmas in today's complex cybersecurity world. Year on year increases in cyber-attacks, an increase in the sophistication of these attacks, a widening cybersecurity talent gap – not to mention IT security budgets that haven't kept up with growing demands. And these are just some of the security issues companies face today. In this session, Synack's Justin Shaw-Gray will host an open conversation with Kevin Fielder, CISO, Just Eat. Justin and Kevin will discuss an innovative crowdsourced security model deployed at Just Eat and how Just Eat has ultimately made their platform a safer place for their customers.

Attendees will learn how Just Eat:

- Is using an army of ethical hackers to harden corporate assets
- Has transformed and simplified security operations
- Reduced the costs of legacy testing programs
- And is now quickly deploying safer applications

Session 4: 4th March | 10:20–11:00

Cybereason

SESSION 4
4th March
10:20–11:00

A live cyber-attack simulation

Anthony Wainman, Senior Sales Engineer, Cybereason

In today's world, preventing a cyber-attack is difficult and penetration is inevitable. We – the defenders need to find other ways of protecting our organisations. In this session, you will gain insight in the motivations of attackers and see how world class defenders are using their skills and tools in the most efficient and smartest way.

In this session, you will:

- Witness the attacker's infiltration
- See the malicious operation as it moves across the entire environment
- Understand how you can gain the upper hand and learn why current security trends are failing

Forescout Technologies

SESSION 4
4th March
10:20–11:00

Device visibility and control: transforming enterprise-wide network segmentation

Richard Orange, Regional Director UKI, Forescout Technologies

While network segmentation is not new, it is probably the best defence against the growing number of security threats and the best way to enable zero-trust policies. The real question is why are organisations so slow in adopting it?

In this session we will address the need to:

- Have full context of all connected devices and applications across the entire enterprise from campus to datacentre to cloud and OT environments
- Know and visualise traffic flows: map traffic flows to logical taxonomy of users, applications, services and devices
- Design and simulate segmentation policies to learn impact before enforcement
- Monitor segmentation hygiene real time and be able to respond to policy violations

Illumio

SESSION 4
4th March
10:20–11:00

Decoupling security segmentation from network infrastructure

Trevor Dearing, Technical Director, EMEA, Illumio, and
Adam Brady, Director Systems Engineering EMEA, Illumio

Segmentation is the cornerstone of security and with many technologies it is hard to achieve. If you are trying to achieve this by handcrafting VLANs or using SDN you will already know how hard it can be. If segmentation is shackled to your physical or virtual network then you lose the ability to segment by role, application, environment or location which makes expanding to the cloud or containers very hard. If you

can decouple segmentation from the network then things become not hard. You will have the capability to provide strong security independent of platform or network. In this session learn more about simple segmentation.

Bullet points:

- Network segmentation was designed to allow data traffic to move fast, not secure your servers and applications
- Security segmentation prevents lateral network traffic and protects your applications
- Application architects do not know how their systems are deployed in the network, and so cannot implement countermeasures against cybercriminals.
- Data centres often lack the necessary security mitigation systems, putting your high-value applications at great risk

Netwrix

SESSION 4
4th March
10:20–11:00

Back to the future: a data breach prevention plan

Dave Matthews, Systems Engineer, Netwrix

When was the last time you saw a headline about an organisation falling victim to a costly cyber-attack? Yesterday? The day before? Have no doubt – your company is also a target.

In this session, you'll learn how to minimise the risk of a data breach, and how to survive your day if the worst does come to pass. Don't simply dream for a time machine when it's too late; come find out the secret to preventing breaches. If our calculations are correct, we should meet you at this educational seminar!

This session will outline the following:

- Your worst day: How to deal with a breach
- Your best defence: How to minimise the risk of a breach
- The secret to preventing breaches

OneTrust

SESSION 4
4th March
10:20–11:00

Overcoming today's most common security & privacy challenges

Alan MacGillivray, Account Executive, OneTrust

Managing third-party vendor risk before, during and after onboarding is a continuous effort under global privacy laws and security regulations. While outsourcing operations to vendors can alleviate business challenges, managing the associated risk with manual tools like spreadsheets is complex and time consuming. To streamline this process, organisations must put procedures in place to secure sufficient vendor guarantees and effectively work together during an audit, incident – or much more.

In this session, we'll breakdown a practical approach for automating third-party vendor risk management and explore helpful tips and real-world practical advice to automate third-party privacy and security risk programmes.

- Review the drivers and challenges organisations face when managing third-party vendor risk
- Identify priorities before, during and after vendor procurement
- Takeaway a six-step approach for automating the third-party vendor risk lifecycle
- Hear real case studies from privacy experts on how to practically tackle the third-party vendor risk

RangeForce

SESSION 4
4th March
10:20–11:00

The RangeForce 'Cyber Gym': building cybersecurity muscle memory through simulated training for enterprise tech teams

Gordon Lawson, CRO, President, RangeForce

Continuous professional development is crucial to keeping technically focussed teams ahead of the game. CISOs, VPs and Team Leads must also be able to establish baselines of skill levels within those teams, in order to identify any possible

coverage gaps that could represent a threat to the organisation.

With the RangeForce on-demand, 100% cloud-hosted cybersecurity skills training platform, customers can:

- Acquire technical security skills online. Affordable and always accessible from any browser
- Learn essential real-world skills. From security operations to forensics to secure DevOps, training modules cover a breadth of mission-critical topics
- Learn how to defend against advanced attacks, quickly recognise and fix vulnerabilities
- Get actionable insights about performance and skill levels of team members and cross train cybersecurity talent already in your organisation.
- Identify potential new talent (or rule out unsuitable candidates)
- Benchmark performance against industry frameworks including MITRE, NIST, & OWASP

Session 5: 4th March | 12:50–13:30

Check Point

SESSION 5
4th March
12:50–13:30

Cyber warfare 2019/2020

Lotem Finkelsteen, Head of Threat Intelligence, Check Point

2019 presented a complex threat landscape where nation states, cybercrime organisations, and private contractors accelerated the cyber-arms race, elevating each other's capabilities at an alarming pace.

In our session, we will try to cover the trends that characterised 2019 and may design the threat landscape of 2020, supported with real-world cases and data.

- See how the threat intelligence team unravels cybercrimes
- Real cases step by step footage – from the first hunch to the hacker identity
- Learn how you can identify the first signs of a breach

Darktrace

SESSION 5
4th March
12:50–13:30

Offensive AI vs. Defensive AI: battle of the algorithms

Nathan Beresforde, Account Director, Darktrace

Among rapidly evolving technological advancements, the emergence of AI-enhanced malware is making cyber-attacks exponentially more dangerous and harder to identify. In the near future, we will begin to see supercharged, AI-powered cyber-attacks leveraged at scale. To protect against offensive AI attacks, organisations are turning to defensive cyber AI, which can identify and neutralise emerging malicious activity, no matter when, or where, it strikes.

In this session, learn about:

- Paradigm shifts in the cyber-landscape
- Advancements in offensive AI attack techniques
- The Immune System Approach to cybersecurity and defensive, autonomous response capabilities
- Real-world examples of emerging threats that were stopped with Cyber AI

ExtraHop

SESSION 5
4th March
12:50–13:30

Winning strategies to scale and upskill your security team

Jamie Moles, Senior Security Engineer, ExtraHop

Businesses these days often face two main challenges: they have too much technology and they don't have the people to manage it. This requires new ways to make their security layers more effective and to scale their human and technology resources in the face of a growing threat landscape. In this session, we will discuss the challenges and opportunities facing security and IT teams when it comes to scaling their cybersecurity talent, and how they can train and 'upskill' staff members to address the problems of the enterprise.

Key discussion points will include:

- How to efficiently train and retain high-calibre cybersecurity professionals

- The part machine learning can play to alleviate alert fatigue and focus on what really matters
- Strategies for increasing collaboration between Security and Network Operations teams.

IntSights

SESSION 5
4th March
12:50–13:30

Shutting down attacks with dark web intelligence

Michael Owen, Head of Systems Engineering UK&I, IntSights

Threats originate from many different sources, some more obfuscated than others. In today's connected world, protecting your business is a full-time job and time is your most valuable asset. The dark web is one area from which many threats can originate, and monitoring these sources for intelligence related to your business can give you a vital heads-up on potential threats.

In this education session, we will explore some of those dark web sites and see where those threats could originate from and how you can use that intelligence to better protect yourself and your business.

Learning points:

- Expand your awareness of some of the dark web sites
- Understand how data is bought and sold
- Identify how this data can be used to decrease your risk threshold and increase your security

Kaspersky

SESSION 5
4th March
12:50–13:30

Hunting the hunters

Jose Alemán, Global Pre-sales Expert, Kaspersky

Learn how leading global experts go from threat identification to actor attribution with the newest and most sophisticated tools.

In this session, we will provide real-life examples on how to track and identify attacks, providing insights about who is the actor behind the threat, adding threat attribution to threat intelligence as the last link in the chain.

- How to use threat intelligence to identify the most advanced threats in the world
- Step by step guide on how to perform an investigation based on real malware samples of very well-known attacks
- Exclusive premier of how our experts identify the actors behind the threats

RiskIQ

SESSION 5
4th March
12:50–13:30

Defending your organisation against JavaScript injection attacks

Terry Bishop, VP, Technical Services, RiskIQ

Browser-based attacks – web skimming, cryptocurrency miners, fingerprinters, and waterholing (including exploitation) encounters – are responsible for some of the most high-profile breaches in recent history, such as the hacks of British Airways and Ticketmaster. Given the frequency by which RiskIQ researchers now encounter these attacks, we believe that they should be taken as seriously as threat mainstays such as phishing and ransomware.

Browser-based attacks have one thing in common: malicious injects. These can be notoriously difficult to detect as their actions take place in the user's browser. The result is weeks or months of compromise on average.

In this session, we'll break down the most common and interesting injection techniques RiskIQ researchers have observed in our telemetry. We'll also look at ways organisations can defend themselves against this growing class of attack.

- JavaScript injection attacks – what are they?
- A brief history
- The current landscape – attackers acting with impunity
- Steps to defend against JavaScript injection attacks
- How RiskIQ can help □

12th e-Crime & Cybersecurity Mid-Year SUMMIT

"The e-Crime Congress covers a variety of topics relevant to cybersecurity and risk management presented in well-controlled short sessions to keep the interests of the delegates piqued throughout the day. The education sessions and the opportunity to interact with the vendors and other delegates enables the attendees to supplement the knowledge gained in the main presentation. Hence e-Crime Congress is now on my list of favourite events to attend."

IT Security & Risk Officer, UBS

2019 sponsors included:

Strategic Sponsors

Attivo Networks
CROWDSTRIKE
mimecast
OneTrust GRC Integrated Risk Management
SECURE DATA Part of Orange Cyberdefense
SWIMLANE
virsec
zscaler

Education Seminar Sponsors

Accellion
AGARI
Blue Cube Intelligent Protection
Cymulate Breach & Attack Simulation
DIGITAL GUARDIAN
DEMISTO A Palo Alto Networks Company
illumio
NETACEA
netwrix
NOMINET
RED SIFT
RISKIQ
TREND MICRO
tripwire

Networking Sponsors

Cloud Control
illusive
ThreatConnect

Branding Sponsor

Cyber Security Project Works INFOSECABILITY

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

Speakers and panellists

Jose Alemán

Global Presales Expert, Kaspersky

Jose began his career as a Security Auditor and Pen Tester in 2000. He was Deputy Director at the Spanish National Cybercrime Centre of Excellence at Universidad Autonoma de Madrid and a master's degree teacher on cybersecurity at several universities and business schools in Spain. Prior to joining Kaspersky, he was Security Operations Centre and Antifraud Service Manager and has developed expert functions within law enforcement and defence sectors.

Michael Aydeniz

Head of Fraud and Credit Risk, Planet

Michael Aydeniz is Head of Fraud and Credit Risk at Planet, a position he has held since June 2017. He joined Planet during the start-up phase of their merchant acquiring activities, tasked with building a risk management function. Michael now acts as the senior risk stakeholder for the global business, which operates in 60 countries on five continents. Michael's role encompasses, fraud, credit and general risk management, with a focus on developing policies, processes and tools to protect Planet and its merchants. Before joining Planet, Michael held a number of senior positions in fraud prevention and transaction monitoring over his 15-year career, in companies such as First Data and Worldpay.

Zsuzsanna Berenyi

Cyber Security Culture and Engagement Specialist, Refinitiv

Zsuzsanna Berenyi, who is currently consulting in financial services, is a well established Cybersecurity Engagement and Culture Specialist, with nearly 10 years of experience. She specialises in creating strategies and setting up security culture change programmes that transform the way organisations and their staff think and act towards data. Zsuzsanna has been working in large, complex organisations, and is the former Head of Security Skills and Culture for Centrica. She is passionate about data security, changing behaviours and embed the desired habits and mind-set that businesses seeking to turn their employees into their strongest defence.

Nathan Beresforde

Account Director, Darktrace

Stewart K. Bertram

Director of Intelligence, Digital Shadows

Stewart K. Bertram is the Director of Intelligence at Digital Shadows and has been working in the field of technical intelligence and cybersecurity for the past 15 years. His expertise is concentrated in the field of cyber-threat intelligence, with experience in building intelligence teams and developing cyber-intelligence capabilities.

Terry Bishop

VP Technical Services, EMEA, RiskIQ

Terry has over 20 years of experience in IT security and networking, working with both private and public sector organisations to deploy and manage security solutions, in both technical and leadership roles. His experience ranges from the endpoint to enterprise-wide monitoring for security and compliance. Terry is currently VP of Worldwide Technical Services at RiskIQ, delivering a unique approach to security, providing an outside-in view of its customers external attack surface.

Simon Black

Pre-Sales Systems Engineer EMEA, Kenna Security

Simon's role as Systems Engineer and Technical Lead includes supporting end user engagements for enterprise accounts as well as channel and MSSP partners. Prior to Kenna, Simon was an Enterprise Pre-Sales Technical Account Manager with Qualys for two and a half years. He has worked as a Technical Security Lead/Specialist since 1998 within partners,

distributors and vendors such as Azlan, (part of TechData), Symantec and Citrix.

Adam Boynton

Sales Manager, Wandera

Adam has been helping customers better understand their exposure to threats for five years at Wandera. Over this time, he has seen mobile threats evolve from dodgy emails asking for financial information, to sophisticated, multi-layered malware that takes over control of the entire device. Cybercriminals with access to sensitive corporate information could cripple an organisation, and Adam has been instrumental in providing market-leading technology to protect businesses around the world.

Adam Brady

Director, Systems Engineering EMEA, Illumio

Adam is Director of Systems Engineering for EMEA at Illumio. He is an experienced cybersecurity professional with over a decade of on-the-ground exposure to CERT work, emergency response, systems engineering, and security consultancy, working with some of the largest organisations within EMEA. His focus has included combating industry-targeted malware in the ICS/SCADA space, and pre-sales consultancy in multiple areas of cybersecurity.

Robert Brooker

Co-Head of Fraud and Forensics, PKF Littlejohn

Robert Brooker is a confident, self-motivated and proactive fraud specialist with extensive financial crime experience, and strong strategic managerial capabilities, gained over the last 25 years. He is an exceptional communicator with a proven track record of building successful, long-lasting working relationships with internal and external stakeholders. Robert is currently the Head of Fraud and Forensics at PKF Littlejohn, a position he has held since January 2019, where he is responsible for delivering fraud risk management, identifying, assessing and managing the fraud risks with organisations in relation to the supply chain and the insider threat.

Additionally, he is responsible for the investigation of crime, including, online fraud, security breaches, cybercrime, IP, leading to parallel sanctions, criminal, disciplinary and recovery actions being taken in accordance with relevant legislation. Robert was previously Head of Fraud at Transport for London (TfL) and possesses extensive financial crime experience and exceptional communication and interpersonal skills.

Dan Burns

Information Security Manager, Next

Dan is currently the Information Security Manager at Next, a position he has held since 2016. In this role, he is involved in the development, delivery and oversight of Next's information security programme. This includes providing expert advice in all areas of information security, defining and delivering the information security strategy, and managing business risk in order to protect information system assets from intentional or inadvertent modification, disclosure or destruction. Dan has worked at Next since 2007, and during this time has built up extensive experience through a number of technical and management roles in IT. He is driven, highly motivated and passionate about his role, and making information security a critical part of the business.

Joseph Byrne

Privacy Solutions Engineer, CIPP/E, CIPM, OneTrust

Joseph Byrne serves as a Privacy Solutions Engineer at OneTrust – the #1 most widely used privacy, security and third-party risk technology platform. In his role, Joe advises companies large and small on EU GDPR, California Consumer Privacy Act (CCPA), Brazil LGPD, and hundreds of the world's privacy laws, focused on formulating efficient and effective responses to data protection requirements as well as building and scaling privacy programmes. Joe is a Certified Information Privacy Professional (CIPP/E, CIPM).

Simon Cross

Security Architect, Lloyds

After completing a Technology degree at Lincoln University, Simon hit the job market in the year 2000, the first internet boom had begun. He spent the next 10 years building backbone networks; security was always part of what we did but never at the forefront. Today, having completed an MSc in Cyber at Lancaster University and well on his way towards becoming a SABSA master, security is ingrained in everything Simon does. Large scale transformation has been his particular focus for the last five years, preparing enterprises for the future. Simon has held a

number of senior positions in security and architecture across various sectors. He currently manages enterprise security architecture at Lloyds, a role he has held since May 2018.

Avishag Daniely

Director of Product Management, Guardicore

Avishag is a Director of Product Management at Guardicore focusing on product usability & customer experience, with over nine years of experience in cybersecurity, both in offence and defence.

Avishag previously held cybersecurity analyst and research positions at Varonis and CyberArk. Prior to this experience, Avishag has worked in the computer networking industry with a strong information technology background holding a bachelor's degree focused on Computer Science and Middle Eastern Studies from Ben-Gurion University of the Negev.

Trevor Dearing

Technical Director, EMEA, 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.

Maxim Denizhenko

Lead Business Development, Enterprise Blockchain Security, Kaspersky

Maxim Denizhenko is the Lead Business Development Manager for the Kaspersky Enterprise Blockchain Security team. A business developer with 20 years' global experience, he has been working in information security and the blockchain space since 2014. Before joining Kaspersky in August 2019, he held the position of Product Manager for a crypto analytic solution, with deep engagement in sales activities. Driven by the motto 'IT should benefit business', Maxim has managed partnerships with IT vendors and integrators of business automation solutions in enterprises around the world. With a technical background, Maxim can talk technical to engineers and business to businesses, balancing interests and capabilities for the benefit of all parties.

Dean Ferrando

Lead Systems Engineer, Tripwire

Dean has over 20 years of experience in systems engineering within the software industry. As the Lead System Engineer for Tripwire EMEA, Dean is an expert with Tripwire solutions and works closely with account teams and partners to demonstrate how Tripwire solutions map to security, change management, vulnerability management processes & ITIL best practices within the IT service management frameworks.

Kevin Fielder

CISO, Just Eat

Kevin Fielder is the CISO of Just Eat. In this role, he is responsible for global security across all areas of this dynamic FTSE100 company. Kevin has transformed security by building capability from the ground up, raised the profile of security to ensure it is a key consideration for all areas of the business, created security strategy tailored to the needs of the global business, with a strong focus on monitoring, understanding, detection and response. This has enabled him to provide security while remaining agile and minimising the need for excessive process and governance, and built a high-performing team across multiple sites to deliver the strategy.

Kevin's key priorities include: ensuring security and risk are represented at board level, and understood across all areas of the business, developing and delivering clear vision / mission / strategy gaining full executive support for group wide programmes, creating board level reporting on security maturity and risk posture along with industry comparisons and planned end state, automating and integrating security into DevOps processes. All while working to remain relatively technical to be able to engage with technical as well as non technical teams!

Lotem Finkelsteen

Head of Threat Intelligence, Check Point Software Technologies

Lotem Finkelsteen is the Head of Threat Intelligence at Check Point. He is a Communication Systems Engineer, who joined Check Point Research after his military service as Major Officer at Intelligence Forces of Israel.

From cybercrime to nation-state attacks, his work is focused on pinpointing the most advanced threats and uncovering their supporting ecosystem.

Terje Aleksander Fjeldvaer

Head of Financial Cyber Crime Center, DNB

Terje Aleksander Fjeldvaer is a former Police Superintendent from the Norwegian Police where he was a Specialist within investigation of economic crime. He started working in the largest financial institution in the Nordic countries, DNB, in August 2015 as a Fraud Investigator. Since September 2016, he has had the global professional responsibility for handling of fraud cases against DNB Group and the group's customers and is now leading DNBs Financial Cyber Crime Center (FC3). DNB is a global bank and the threat picture FC3 must handle is complex. To be able to prevent economic crime, the team uses a combination of advanced technology and human intelligence.

Nathan Gilks

Regional Sales Engineer UK&I & Northern Europe, TrapX Security

Nathan is the Regional Solutions Architect at TrapX Security, responsible for solutioning their UK, Ireland and Northern Europe business, which includes enterprise accounts across finance, retail, manufacturing, telecoms and oil and gas. He has 24 years' experience in IT with the last 18 specifically in high-growth cybersecurity organisations.

Previous companies include HP Enterprise Security Services, EDS and Vistorm. His experience includes data protection, application security and cyber-transformation solutions including security services.

Debbie Grant

Senior Policy Lead, Policy and Law Enforcement, Ecosystem Risk, Visa

Debbie has been a Senior Policy Lead in the Fraud Strategy and Criminal Disruption department at Visa, since April 2015. In her role, she controls all types of crime in the Visa payment system through the development of internal and external crime prevention strategies to providing training and giving presentations throughout the Visa Europe region. She has successfully supported and coordinated complex international and multi jurisdiction investigations, initiated online fraud prevention and disruption activities and built an extensive network within the public and private sectors to ensure they disrupt criminal activities within the Visa payment system.

Mark Greenwood

Chief Technical Architect, Netacea

Mark is the Chief Technical Architect at Netacea. Mark initiated the creation of a dedicated data science team, that works in tandem with the product development team, to provide our customers with an innovative solution to the growing threat of automated bot traffic.

With a PhD in Natural Language Processing, he has presented internationally on his published research and regularly speaks at cybersecurity events.

Adam Gwinnett

Head of Strategy, Enterprise Architecture & Cyber Security (SEACS), Metropolitan Police Service

Adam Gwinnett is the Head of Strategy, Enterprise Architecture & Cyber Security (SEACS) at the Metropolitan Police Service, where he has been integral in the enterprise and security strategy of the institution since 2017. An experienced Enterprise Architect and Cybersecurity Lead with 15+ years in criminal justice focusing on strategic IT-enabled business change, Adam is focused on driving improved user experience through modern security controls, specialising in identity.

Before the Metropolitan Police, Adam headed digital architecture and cybersecurity at HM Courts and Tribunals, where he helped build an internal digital capability, including technical architecture, DevOps and development.

Deborah Haworth

CISO, Penguin Random House

Deborah has 20 years' experience as an information security professional across multiple industries and has been at the sharp end of changing attitudes to this discipline. With a gift for telling it how it is, Deborah celebrates the highs, revels in lessons learned and is not afraid to face the pain points. Deborah is an ISACA Certified Information Security Manager, Fellow of the British Computer Society and Chartered IT Professional specialising in security GRC (governance, risk and compliance) with extensive experience in crisis management and complex problem solving.

She is known for improving operational effectiveness through motivational leadership.

Alphus Hinds

CISO,
Standard Bank International

Alphus Hinds has over 15 years' experience and is recognised as a leading authority in undertaking lead roles in assessing, reviewing and managing security and public safety risk, including for major sporting events, rail transport and border security. He has proven his expertise through a number of high-profile projects and events including United Nations associate expert advisor on security & public safety during major events, and integral involvement as Head of Security for the Glasgow 2014 Commonwealth Games and London 2012 Olympics.

Detective Sergeant Ben Hobbs

DCPCU, Dedicated Card & Payment Crime Unit, Metropolitan Police

An experienced detective, Detective Sergeant Ben Hobbs leads a team in both proactive/reactive investigations and intelligence development to tackle organised criminals groups

Mike Hulett

Head of Operations,
National Cyber Crime Unit (NCCU)

Mike is the Head of Operations for the National Cyber Crime Unit (NCCU), part of the National Crime Agency, responsible for leading the UK's law enforcement response to cybercrime. The NCCU has around 250 officers based at four sites, with a range of investigation, intelligence, technical, digital forensics, data analysis and financial investigation skills. Mike is responsible for leading the highest level and most complex investigations into cybercrime in the UK, utilising support from across UK & international law enforcement agencies, other UK Government departments and a range of industry partners. NCCU Operations also coordinate and support cybercrime investigations undertaken by police Regional Organised Crime Units (ROCUs) and local police forces across the UK.

The majority of Mike's career has been spent leading serious organised crime investigations across a variety of sectors including drugs, firearms, money laundering, corruption, kidnap, organised immigration crime and now cybercrime. Mike holds a master's degree in Criminology from the University of Cambridge, and lives in the home counties with his wife and two young children.

Federico Iaschi

Head of Information Security,
Seqirus

Federico leads the Information Security team for Seqirus. He is responsible for planning and executing the information security strategy, aiming at assuring information security integrity across all disciplines. In his current position, he considerably promoted a security learning culture creating the first company-wide information security awareness campaign with outstanding results.

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

Tony Kinkead

Regional Director – EMEA,
TrapX Security

Tony is the Regional Director at TrapX Security, responsible for the UK, Ireland and Northern Europe business, which includes enterprise accounts across finance, retail, manufacturing, telecoms and oil & gas. He has over 20 years' experience in cybersecurity organisations, including CyberArk, HP Enterprise Security Services, EDS and Vistorm.

Akhil Lalwani

Group Head of Data Platforms – Group Digital, Prudential PLC

Akhil is Group Head of Data Platforms at Prudential, a role he has held since November 2018. In this role, he is integral to the firm's digital innovation strategy and brings a wealth of expertise from his background in cyber-risk management. Before his current role, Akhil held the position of Head of Data Platform and Innovation – Group Information Risk & Security at Prudential. Prior to Prudential, Akhil held a number of senior positions in product management, innovation, transformation and design at Barclays leading solutions focussed on delivering exceptional customer experience and revenue growth.

Gordon Lawson CRO

President,
RangeForce

Gordon has 18 years of experience in the security sector with a focus on SaaS optimisation and global enterprise business development from global companies such as ReversingLabs, Cofense

(formerly PhishMe) and Pictometry. As a Naval Officer, Gordon conducted operational deployments to the Arabian Gulf and Horn of Africa as well as assignments with the Defense Intelligence Agency, U.S. Marine Corps, and Special Operations Command. He is a graduate of the U.S. Naval Academy and holds an MBA from George Washington University.

Jonathan Lee

Senior Product Manager, Menlo Security

Jonathan Lee is Menlo Security's Senior Product Manager. He is experienced in leading the ideation, technical development, launch and adoption of innovative security products. He has served as a trusted advisor to numerous enterprise clients in the area of information security and compliance. As an industry leader in the cybersecurity space, Jonathan is well-versed in data protection, threat analysis, networking, internet isolation technologies, and cloud-delivered security.

Nicola Lishak

Head of Information Assurance, Royal Mail Group

Nicola is the Head of Information Assurance at Royal Mail Group, driving and embedding change and behaviours in how the business manages information security risk and data compliance, as part of Royal Mail's GDPR journey. With a background in corporate and information security and more recently privacy regulations in the UK and EU, Nicola has a unique story and perspective on the different approaches to achieving information security compliance within large and complex business and IT environments. Fundamentally, Nicola talks about the need to breakdown silos, translate technical or legal speak into business language, provide commercially focussed compliance advice and empower accountable owners to make risk informed decisions about their data. Nicola started her career in the Big 4 working with major clients across all industries; she's delivered large scale international security assurance projects and supported organisations to develop security risk management frameworks and pragmatic data compliance strategies; Nicola also has experience in developing effective ways to stimulate security culture, through training and awareness on the first line.

Matt Logan

Vice President of Field Engineering – EMEA, Digital Guardian

Matt Logan specialised in the data protection space in 2007 and he is currently Digital Guardian's Vice President of Field Engineering – EMEA. Matt worked at Symantec, McAfee and CSC building, managing and selling enterprise scale data protection programmes and technologies. For his five years at Digital Guardian, Matt has been instrumental in leading growth and maturity in technical sales within EMEA. Matt has over 16 years' experience in IT security, covering multiple disciplines in various roles from professional services to programme management and more recently, sales engineering. Matt understands the challenges of IT security and deals with customers from a wide spectrum of industries from finance, energy, manufacturing to law etc.

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.

Alan MacGillivray

Third-Party Risk Specialist, OneTrust

Alan MacGillivray serves as a Third-Party Risk Consultant for OneTrust VendorpediaTM – a purpose-built software designed to operationalise third-party risk management. In his role, MacGillivray advises companies throughout their third-party risk management implementations to help meet requirements relating to relevant standards, frameworks, and laws (e.g. ISO, NIST, SIG, GDPR and CCPA). MacGillivray works with clients to centralise their third-party information across business units, assess risks and performance, and monitor threats throughout the entire third-party relationship, from onboarding to offboarding.

Etay Maor

Chief Security Officer, IntSights

Etay is IntSights Chief Security Officer, an industry recognised cybersecurity researcher and key note speaker. Previously, Etay was an Executive Security Advisor at IBM where he created and led breach response training and security research. Prior to that, Etay was the Head of RSA Security's Cyber Threats Research Labs where he managed malware research and intelligence teams and was part of cutting edge

security research. Etay is an adjunct professor at Boston College and holds a BA in Computer Science and an MA in Counter Terrorism and Cyber Terrorism Etay contributed to the ICT (International Institute for Counterterrorism) in cybersecurity, fraud and dark web topics and is a frequent featured speaker at major industry conferences. He is often tapped by major news outlets for his astute commentary on and insights into the cybersecurity news of the day.

Max Mansson

Director, UK & Europe, Silobreaker

As a Silobreaker Client Director, Max works closely with security teams in both private and public sector organisations. His in-depth understanding of complex security and intelligence requirements across multiple industries, combined with his expertise in how technology can be used for extracting relevant and timely insights from large data-sets, enable him to help customers find value or mitigate risk across numerous use-cases.

Dave Matthews

Systems Engineer, Netwrix

Dave Matthews is a Systems Engineer at Netwrix who specialises in security, governance and compliance and has a proven track record of delivering high-value, data-centric projects. He has deployed and integrated security solutions in a variety of industries, including financial, legal and manufacturing, and in a variety of locations, from central London to rural New Zealand.

Goher Mohammad

Head of Information Security, L&Q Group

Making his mark as one of the youngest IT leaders in Omnicom Group back in 2004, Goher has a huge passion for technology with a drive not just to do things well but to do things better. Having had to deal with more comprehensive but secure and controlled structures in Citibank and Merrill Corporation to more agile environments within Omnicomgroup and Photobox Group Security, the next step for him is how to combine the best of both.

Now at L&Q, his goal is to bring information and cybersecurity to the next level to meet the demands and ambitions of the organisation. A keen diver, traveller keen to explore the world, Goher also loves play retro video games and not so secretly is a complete tech geek. Deep down, his inquisitive nature is always looking to understand the inner workings of everything that's around and in turn, how can it be made better.

Jamie Moles

Senior Security Engineer, ExtraHop

Jamie has worked in the computer industry for over 30 years, focused primarily on security and infrastructure technologies. In the early 1990s, Jamie was one of the UK's leading experts on computer viruses – authoring his own virus scanner for MS-DOS before joining Symantec as Technical Support Lead for the new Peter Norton range of products, including the new Norton AntiVirus product. Nowadays, Jamie is helping customers understand and mitigate the risk contemporary threats pose to their business.

Roy Murdoch

SE Manager UKISA, Proofpoint

With over 20 years in the IT industry, Roy Murdoch started his IT career at Sophos, initially holding positions within support, to then develop and build their initial Technical Pre-Sales team in the UK. Murdoch has also held Senior SE/SE Management roles at Ciphertrust and Proofpoint. During his time at Proofpoint, Murdoch has helped setup various regions within the Nordics and the Middle East. Currently he holds the position of SE Manager UKISA, focused on the field enterprise markets.

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 Cyber Security 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.

Richard Orange

Regional Director UKI, Forescout Technologies

Richard is a Regional Director at Forescout, responsible for their UK business, which includes many global accounts across finance, manufacturing, retail, oil & gas, utilities & government departments. He has 22 years in IT with the last 15 specifically in

high-growth cybersecurity organisations. Previous companies include HP Enterprise Security Services and F5 Networks. His experience includes cyber-transformation, outsourcing and managed security services.

Michael Owen

Head of Systems Engineering UK&I, IntSights

Michael Owen heads up Pre-Sales Engineering for IntSights in the UK & Ireland. He has been in the information systems technology and security arena for over 30 years. His career bridges manufacturer, strategic partners, and end-users and so he brings a useful perspective that covers all parts of the chain. For the last four years, Owen has been heavily involved with big data vendors around data analytics, smart buildings, and more recently cyber-threat intelligence. Owen is currently leading the charge in the UK & Ireland to educate and introduce organisations to increasing their visibility on the many dark web threats that pose a serious risk to them. During his career, Owen has held positions at BT, Siemens, Aruba & Hewlett Packard Enterprise and has been involved in numerous large scale projects.

Jules Pagna Disso

Group Head of Cyber Risk Intelligence, BNP Paribas

Dr Jules Pagna Disso achieved his PhD in 2010, then went onto achieve his Certified Ethical Hacker qualification. In 2012, Jules headed up the Cyber Security Research Labs EADS (Airbus) Innovation Works UK. After 2013, Jules moved to QA ltd working as a Cybersecurity Technical Consultant with particular focus on consultancy, training on malware and ICS. In his most recent position, Jules managed the Research and Innovation department at Netitude, developing and executing the research programme, being at the forefront of malware research and threat intelligence development, whilst managing a team of Senior Cyber Threat Analysts. Jules is currently Head of Cyber Risk Intelligence at BNP Paribas, where he is an integral part of the risk function and manages all aspects of threat intelligence, and cyber-risk analysis.

Nick Palmer

Technical Director, Attivo Networks

Nick has been in and around the IT security industry for over 25 years. He has worked for Microsoft, IBM, HP and Compuware, as well as a number of smaller security start-ups. With a passion for assisting customers in protecting their intellectual property, customer data and commercial strategy, Nick believes that only a multi-partite security strategy will ever succeed. By empowering all stakeholder groups in the organisation to contribute to the security dialogue, and by working with user communities, the security-conscious enterprise can better align risk and expenditure and more effectively protect itself. In his role with Attivo Networks, Nick is working with security teams to introduce Deception to their core IT security strategy. In this way, the economics of cyber-warfare can be shifted and placed back on the attacker – where they belong!

Mariana Pereira

Director of Email Security Products, Darktrace

Danny Phillips

Senior Manager of Systems Engineering, Zscaler

Danny Phillips is the Senior Manager of Systems Engineering at Zscaler UK. Danny has spent the majority of his career working with businesses to design and implement their IT infrastructure, with specific focus on networking components. With over 20 years' experience in the field, Danny has seen technologies come and go in the marketplace. In his current role at Zscaler, he has witnessed the continued rise of cloud computing, and its growing importance in today's IT landscape.

Becky Pinkard

CISO, Aldermore Bank

Becky Pinkard, CISO, Aldermore Bank, is a renowned practitioner and commentator on the information security sector who has been working in information technology and security since 1996. A security transformation expert, Becky has built and managed global information security teams, designed risk and compliance strategies, led security audits and assessments, and developed security awareness training in small and large environments. She began her current role with Aldermore in May 2019. She was a SANS Certified Instructor for over a decade and served as a GIAC Certified Intrusion Analyst advisory board member and on the Strategic Advisory Council for the Center of Internet Security. She co-authored 'Nmap in the Enterprise' and 'Intrusion Prevention and Active Response, Deploying Network and Host IPS'. Becky has shared her expertise in numerous publications,

both written and in live interviews all over the world, including: The Wall Street Journal, Forbes, ChannelPost, The Telegraph, The New York Times, BBC News, Channel 4 News, and more.

Thomas Platt

Senior Account Manager,
Netacea

Tom works with leading e-commerce, fintech, gaming and media organisations, to help them understand and quantify the impact of bots. Tom is currently working closely with Netacea's largest customers to ensure they stay ahead of the latest bot challenges, whilst collaborating with Netacea's product and threat teams to research emerging bot trends across industries.

Vijay Punja

Technical Account Manager,
RiskIQ

Vijay Punja currently serves as Technical Account Manager for RiskIQ in EMEA. His role involves working closely with customers to improve their cybersecurity posture and maximise the value they receive from the RiskIQ solution set.

Before joining RiskIQ, Vijay worked within IT operations across different industry verticals including finance and defence. He has been involved in various digital transformation programmes, as well as security transformation programmes from an engineering and architectural perspective and has been certified across different infrastructure platforms from vendors including Microsoft and VMWARE. He holds a postgraduate diploma in Information Security and Forensics.

Brett Raybould

Solutions Architect,
Menlo Security

Brett Raybould is passionate about security and providing solutions to organisations looking to protect their most critical assets. Having worked for over 15 years for various tier 1 vendors who specialise in detection of inbound threats across web and email as well as data loss prevention, Brett joined Menlo Security in 2016 and discovered how isolation provides a new approach to actually solving the problems that detection-based systems continue to struggle with. Menlo Security facilitates this with their innovative and unique technology that's being adopted with great success across large and small organisations.

Stephen Roostan

VP EMEA,
Kenna Security

Steve 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. Steve has a passion for driving equality, alongside enabling flexibility at work for modern living. 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.

Martin Rudd

Chief Technology Officer,
Telesoft Technologies

Martin is the Chief Technology Officer for Telesoft – a cutting edge technology company specialising in the cybersecurity, compliance and network engineering space. After seven years with Telesoft, Martin has been instrumental in the strategy and execution of our cyber product range and services model. His specialities include threat intelligence on global networks, data equity, digital estate security, supercomputing and future technologies.

Martin has worked in various sectors including telecommunications, retail, government, financial and energy playing a key part in helping large organisations build a robust security posture in a complex and complicated evolving threat landscape.

Garry Scobie

Deputy CISO,
The University of Edinburgh

Garry Scobie is the Deputy Chief Information Security Officer for The University of Edinburgh. He is a Certified Information Systems Security Professional and ITIL Expert. He regularly presents on computer security including sessions on ransomware, mobile security and cyber in the movies. Prior to this, he was responsible for Microsoft Windows server infrastructure and Active Directory. He has a particular interest in vulnerability assessment and penetration testing and promoting security awareness.

Justin Shaw-Gray

Account Director,
Synack Inc.

Justin Shaw-Gray is the UK&I Sales Director for Synack, the hacker powered security platform. Justin has been in the IT industry for over 20 years and has worked for several startups including Blue Coat, Zscaler and Netskope. In 2018, shortly after joining Synack, Justin was recognised as runner-up in the Security Serious Best Cyber Security Sales Leader category. This award recognised the sales person who best cuts through industry jargon and delivers what their customers need. Justin is an avid runner. He lives in London with his wife and three kids.

Mark Smith

Pre-Sales Manager,
Orange Cyberdefense

Since 2001, security has played a significant part in Mark Smith's life in some way. Whether it was protecting high-ranking officials in Iraq during service as a Royal Marines Commando or protecting hosting companies by building secure data centres as a Cisco Security Engineer or his role today at Orange Cyberdefense. Currently, he continues to explore the field of security as the Pre-Sales Manager protecting clients by understanding their security issues and advising them on the best course of action to take as cybersecurity consultant.

Kevin Tongs

Director Customer Success (EMEA),
Flashpoint

Following a career in military intelligence with the British Army, predominantly in the SIGINT field and latterly in training policy and information assurance/cybersecurity, Kevin Tongs was employed as the Information Security Manager for a multinational company. In this role, he was responsible for all aspects of cybersecurity strategy and design, implementation and improvement. He also transitioned the company from ISO27001:2005 to ISO27001:2013.

In 2015, he joined iSIGHT Partners as a Technical Account Manager, prior to their acquisition by FireEye. At iSIGHT/FireEye he was responsible for all pre-sales activities for the EMEA region, helping customers define use cases for FireEye's actionable cyber-threat intelligence, speaking at conferences, assisting with training, and informing product development. He joined Optiv Security Ltd in February 2019, where he was a Senior Solutions Architect, serving as a client advocate to help businesses, governments and educational institutions plan, build and run successful security programmes through the right combination of cybersecurity products, services and solutions. In December 2019, he joined Flashpoint as their Director, Customer Success for EMEA.

Flashpoint delivers Business Risk Intelligence (BRI) to empower business units and functions across organisations with a decision advantage over potential threats and adversaries. The company's sophisticated technology and human-powered analysis enable enterprises and public sector organisations globally to bolster cybersecurity, confront fraud, detect insider threats, enhance physical security, assess M&A opportunities, and address vendor risk and supply chain integrity. For more information, visit www.flashpoint-intel.com or follow us on Twitter at @FlashpointIntel.

Toby Van de Grift

UK Regional Director,
Swimlane

Toby has worked in IT security for just over 10 years, and started working in the SOAR space in 2016 (before it was even called SOAR!). Toby has helped SOCs evolve and improve from a variety of industries – FS, Telco, manufacturing, media, MSSP and more. He also has experience with threat intelligence, EDR, network security, incident response, vulnerability management and SIEM.

He is constantly questioning and looking outside of his immediate area to expand his world view and bring new ideas to his customers. Customers say his key skill is his integrity and authenticity – he will only bring technologies and ideas to customers that he genuinely believes will improve security, add value, reduce risk, or a combination thereof.

Anthony Wainman

Senior Sales Engineer,
Cybereason

Mark Ward

Senior Solutions Architect,
CrowdStrike

Mark Ward is a Senior Sales Engineer with nearly 10 years' experience in the cybersecurity industry. Mark works closely with customers to solve the most challenging cybersecurity problems, helping to stop breaches and achieve positive business outcomes with security solutions.

Sam Watling

Information Security Governance and Compliance Lead, TUI

Sam Watling is the Governance and Compliance Lead within the Information Security practice at TUI, a position he has held since April 2018. In this position, he is responsible for driving governance best practice and managing security compliance programmes for the UK & Ireland business. Sam has been at TUI since 2012, holding a number of roles across IT strategy, technology risk and supplier management.

Prior to TUI, Sam spent the formative years of his career working on both the customer and supplier-side within retail IT for Marks & Spencer, Sainsbury's and John Lewis, giving him a valuable perspective across the industry on both customer and service provider business challenges.

Sam is passionate about helping individuals across the organisation understand 'the why', enabling a pragmatic, risk-based approach to deliver the information security programme that integrates into the culture of the business.

Harry Zorn

Vice President Sales, EMEA, Accellion

Harry Zorn joined Accellion in April 2017 and brings more than 20 years of experience in the enterprise IT security software industry. He focuses on risk management, security monitoring and secure collaboration, as well as innovative security solutions and the IT security channel across Europe. Before Accellion, Harry was Head of the IT Security Business Unit & Competence Center at Konica Minolta IT Solutions, where he developed the portfolio and strategic partnerships to improve the market position of the whole organisation. He joined Konica Minolta in 2013 through the acquisition of headtechnology, the company he founded in 2000. Prior to his role as Founder and Managing Director of headtechnology, Harry founded two other companies in the e-commerce and printing business markets. Harry is a Certified Economics and Business Administrator as well as an IT Business Engineer (Academy for Data Processing, Böblingen) and is based in Accellion's European Headquarters office located in Stuttgart, Germany. □

The inaugural

Securing Financial Services

SECURING FINANCIAL SERVICES

Secure the industry, protect the customer

How the convergence of fraud, KYC/AML, security and privacy makes cyber a manageable operational risk

Cybersecurity is a top investment priority for financial services (FS) firms globally, with the big banks spending up to a billion dollars a year on the problem.

FS firms are prime targets in cyberspace for the same reason that they have always been targets – the money. Smart criminals have long since abandoned guns and dynamite as their tools of choice and now see direct cyber-attacks on financial infrastructure and digital fraud on banks' retail, high-net-worth and wholesale customers as an attractive money maker.

Key themes

- Is open banking open season for cyber-attackers?
- Integrating fraud, KYC/AML and cybersecurity
- Cybersecurity as risk management in the 3LOD model
- Securing banking technology
- Governance and regulation
- Protecting employees in financial services

Confirmed sponsors include:

illumio

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

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

Preparing for cyber-warfare – why you need a simulation tool and what to look for

The cyber-landscape continues to be a challenging place.

Martin Rudd reports

Background: Cyber-warfare is raging, public and private organisations are on the back foot

The cyber-landscape continues to be a challenging place for public and private organisations alike. Both are often on the back foot when it comes to fending off intelligent, determined and motivated attackers focussed on inflicting cyber-warfare and cybercrime attacks on their targets. Such has been the concern of the impact on a global footing, the World Economic Forum's Global Risk Landscape report has previously rated cyber-attacks to be one of the highest risks in terms of impact and likelihood, only closely behind natural disasters and extreme weather events.

In an equally telling way, NATO formally recognises cyber as a domain of operations in which it must defend as effectively as it does in the air, on land, in space and at sea. Cyber-attacks and warfare are a real threat and the attackers are numerous, ranging from inexperienced hacktivists and script kiddies through to highly capable cybercriminals and nation-state groups.

State sponsored cyber-warfare is often targeted at nations and their essential services. Deeply disruptive activities are used to conduct a range of nefarious activities such as: constrain reform, affect democracy, weaken government networks and reduce the capability of critical national infrastructure such as energy, defence, finance, transportation and communication. State backed cyber-attacks are at times also directed at commercial organisations where they are used to disrupt trade and ultimately impact the economies of their enemies and targets.

There is little doubt that cyber-warfare is raging, and it's not just nation on nation. For every attack that is targeted at a nation, there are many more that are deliberately aimed at commercial organisations and for motivations such as investigative journalism, competitive advantage, revenge and financial gain.

In some instances, commercial organisations are caught in the cross hairs of nation-state cyber-aggression. An example that springs to mind is an attack that temporarily crippled the network of one of the world's largest law firms, DLA Piper, whose global network was heavily impacted when it became the collateral damage of a hostile nation conducting cyber-attacks thought to be designed to destabilise the economy of the Ukraine.

There is little doubt that cyber-warfare is raging, and it's not just nation on nation. For every attack that is targeted at a nation, there are many more that are deliberately aimed at commercial organisations and for motivations such as investigative journalism, competitive advantage, revenge and financial gain. Some estimates place the annual value of cybercrime to be $1.5tn a year, making it broadly equivalent to the GDP of Russia.

The challenge: It is difficult to anticipate and eliminate weaknesses

Regardless of whether a cyber-incident is the outcome of an individual and surgical precision attack, or the collateral damage of a bulk attack, state-owned and private organisations will benefit from the ability to limit the likelihood of an attack, anticipate its impact and then eliminate weaknesses in the cyber-infrastructure and team. However, simulating realistic attacks is a real challenge for many organisations, and the bigger the target, the more difficult it is to predict, mimic and replay adversarial attacks.

Today, penetration testing is widely mandated by regulation, industry bodies and supplier contracts. It is undertaken as best practice by responsible organisations who seek to routinely (usually annually or upon significant change) identify exploitable vulnerabilities in their systems. However, penetration testing falls short of helping to recognise attacks as they occur or discover insidious low-level attacks that quietly conduct a range of nefarious activities from hidden locations within a network. This is the job of tools such as Telesoft's Flowprobe 400 and Data Analytics Capability (TDAC) platform, which blends near real-time network monitoring at scale with analytics and threat intelligence.

The creation of incident playbooks, the training of incident teams and rehearsal of response activities

It also brings the ability to test, test and test again and, borrowing the words of Dr Bernhards Blumbergs, a former Technical Director of NATO's cyber-operations exercise Crossed Swords Fail, fail again, fail better.

are great strategies for minimising the impact of an attack, however these are often untested until the heat of an incident. When they are rehearsed in advance, they are often played out in boardrooms as theoretical exercises and base their starting positions on an estimate of how the technology has been impacted by an attack rather than a known state one.

The solution: Realistic attack simulation tools

To truly understand an organisation's ability to withstand a cyber-attack, systems proving should include a known state derived from the use of a simulated but ***realistic*** attack. This is the role of cyber-warfare attack simulation tools that can be easily deployed, used by penetration testers, digital forensic professionals and situational awareness experts across Red, Blue and Purple teams to plan, prepare, execute, identify and prove their organisation's ability to detect malicious activity at each stage of an attack's escalation. This approach can be likened to that used by NATO who bring together experts from multiple nations as a method of preventing, detecting and responding to an adversary. The difference of course, is the ability to create realistic threats with a flexible and powerful tool without the need and expense of large-scale collaborations. It also brings the ability to test, test and test again and, borrowing the words of Dr Bernhards Blumbergs, a former Technical Director of NATO's cyber-operations exercise Crossed Swords – Fail, fail again, fail better.

But what are realistic attacks?

They are those that:

- Emulate the behaviours of real-life attackers
- Coordinate multiple concurrent attacks to create confusion
- Include a variety of attacks from password spraying and large-scale DDoS to AI poisoning
- Use the latest threat intelligence and honeypot data to ensure known and emerging threats are included
- Can be delivered at speeds that reflect the capability and resources of an attacker

Beyond the creation of realistic attacks, a common problem with the use of some testing tools is traffic replay stagnation, which can create an environment where the effectiveness of the monitoring process is diminished because of the predictability of the generated traffic source and destination IP addresses. Simulation tools introduce an element of alert fatigue through the randomisation of source and destination IP addresses bring increased attack realism.

The 400G Triton from Telesoft incorporates the above features and utilises a comprehensive understanding of frontline threat intelligence from around the globe to replicate myriad adversarial attack methods at unprecedented speeds. □

Martin Rudd is Chief Technology Officer at Telesoft.

About Telesoft

Telesoft is an independent global provider of government infrastructure, cybersecurity and telecoms mobile products and services. Our range of cybersecurity solutions include highly scalable network visibility tools for incident response, traffic capture and threat detection in real-time and at scale. Solutions also include attack simulation tools that create and play out multiple concurrent and realistic attack scenarios and incorporate known and emerging threats. These tools improve identification of cyber attacks and help mitigate them. Telesoft develops, manufactures and supports best-in-class cybersecurity, attack simulation and data intelligence solutions that give customers unprecedented network visibility and defence capability.

For further information about Telesoft's monitoring and cyber-warfare simulation tools or to arrange a demonstration, call +44(0)1258 480880 or email: sales@telesoft-technologies.com

www.telesoft-technologies.com

TELESOFT

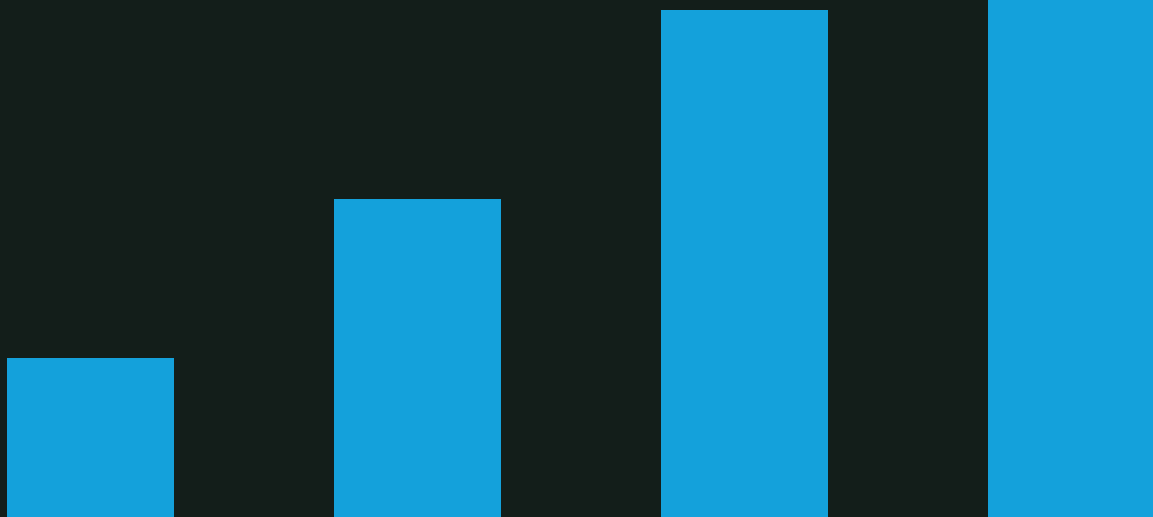
400G CYBER WARFARE SIMULATION

Strengthen your NetSecOps with nation-scale attack simulation.

Prove your infrastructure, teams and suppliers with 400Gbps of threat and traffic simulation. Available with world class professional services, training and as a portable lab appliance.

400G Triton CWS generates multiple threats and complex attack campaigns simultaneously. Take cyber warfare simulation to the next level and prepare your organization for tomorrow.

Learn more at:
www.telesoft-technologies.com



Lessons from Facebook litigation – the boundaries of human capability

Facebook civil litigation, underway in Ireland, should act as a cautionary tale for firms that create stressful environments for employees.

Red Sift reports

For those unfamiliar with the facts: Facebook employs about 15,000 moderators globally, often through third parties. Their job is to review content that has been reported by users for violating Facebook's community standards. The footage sometimes contains images that are graphic and violent. These images might even evidence criminal wrongdoing, ranging from acts of animal cruelty to serious sexual assaults on children and even murders.

Facebook requires moderators to curate these images. The psychological impact of watching unspeakable horrors is well-known, leading to mental health issues, including post-traumatic stress disorder (PTSD).

I asked Red Sift's tech team to give me their insights. Speaking to the machine learning and interactive visualisation expert, I ask him why is it that Facebook doesn't rely on AI to determine whether images are violent or criminal in nature? Dr. Phong Nguyen explains:

> *'Facebook's AI Research is led by one of the godfathers in deep learning,*
> *I'd be surprised if they're not working on it but there is still a long way to go'.*

The view from the rest of the team is that AI is not as sophisticated as people think. Consider Google's reCaptcha, the clever software that helps train machines. As we digitise more books, the machines find words that it doesn't recognise, so humans train the machine by spelling the word. Similarly identifying traffic lights in those images will help machines to learn, which is going to be important if we're to get driverless cars!

Given that machines still have trouble with written words and recognising traffic lights, it isn't a stretch to conclude that recognising scenes of violence is still beyond AI.

While AI can't assist with identifying complex images just yet, that doesn't undermine the moderators' complaints. Processes exist to protect staff to make sure they are not burdened by viewing horrific images at a steady pace. The result of burn-out can be avoided by implementing procedures well understood by the police. No police force requires staff to view horrific or potentially horrific images 8 hours a day, 5 days a week. Facebook aren't the first movers here so why are they not following best practice? It's clear that the lack of technical sophistication is no defence. Firms cannot ask humans to do that which they cannot reasonably do safely.

What if a technical solution did exist and it was reasonable and proportionate to deploy it?

If this was the case, the courts would surely enquire as to why a firm had not deployed it.

Will training suffice?

Training has its uses, it can assist with understanding traditional crimes such as the many forms of tailgating through physical barriers, or *romance fraud*, *419 scam* (aka. *Nigerian Prince scam*). But no amount of training will prepare staff to be able to deal with crimes in the machine, such as spoofing/business email compromise. There's simply too many emails, too much data, it's too complex and they have other work to complete. If we expect human resources to do computational work, we can expect:

1. decreased productivity
2. increased stress levels
3. employment tribunals

There's no question that this lawsuit will be followed. Asking staff to do something that a human cannot reasonably do e.g. determine whether a spoofed email is authentic, will lead to stressed out staff and successful phishing attacks. Firms should avoid turning staff into filters and firewalls. That's what tech is for and it ought to be deployed as a sensible cyber-governance solution. All the more so when it's affordable, tech costing about the same price as one coffee per fortnight for your staff. □

RED SIFT

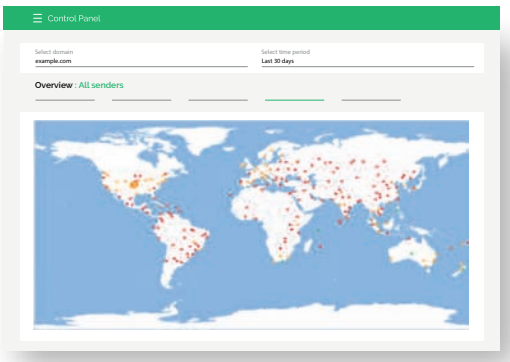
It's **400x more expensive** to stop a cyber attack than it is to start one.

We exist to **change** that.

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

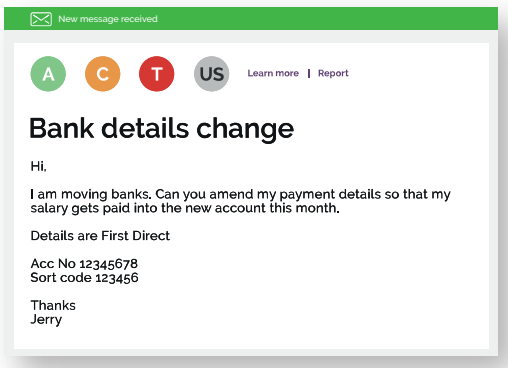
ONDMARC

Protect your domain from email impersonation



ONINBOX

Intelligent email threat detection



Trusted by: Telefónica, NUMED HEALTHCARE, TransferWise, Action for Children, Linklaters

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

The 7 habits of highly effective vulnerability management

How do you know your vulnerability management programme is effective?

Tim Erlin reports

On the surface, vulnerability management (VM) is nearly ubiquitous. If you ask someone whether their organisation has VM, the majority will reply in the affirmative. But how do you know your vulnerability management programme is effective?

To answer that question, let's look at seven habits of highly effective VM programmes.

1. Executive buy-in

If a VM initiative has the right level of executive sponsorship, then you should be able to articulate how the success or failure of the initiative impacts those executives. It might be that there's a specific compensation impact but when a programme can succeed or fail without affecting someone, then that person definitely does not have buy-in.

2. Asset discovery

Any limit you place on the scope of vulnerability management is a limitation on the risk to which you have visibility. That's why asset discovery has to be a core component of any vulnerability management programme. You can't remove risk you don't know about. Likewise, if asset discovery isn't continuous or performed with frequency, it's likely to become stale and inaccurate.

3. Scan frequency

You might think that the mantra here is 'scan continuously,' but that's a red herring. The reality is that you're conducting scans for two reasons: first, to drive remediation activity and second, to identify meaningful changes in your risk profile (e.g. find new, high-risk vulnerabilities). Your scan frequency should be, first and foremost, rational. That means it should be tied to those two objectives. If you remediate on a monthly cadence, then scanning daily isn't going to improve your outcomes. If, however, you have inadequate change management, then you might mitigate some of that risk with more frequent scanning to achieve the second objective.

4. Incorporating business context

Vulnerability risk isn't absolute, and if you're basing your remediation priorities on some notion of absolute risk, then you're likely leaving risk on the table. Highly effective vulnerability management incorporates the business context of the discovered vulnerabilities, and the systems on which they exist, into the prioritisation mechanisms used to drive remediation activity. This means that assets of higher value and higher risk to the business get addressed first.

5. Exceptions are the exception

You can't manage risk you don't know about, and creating exceptions from scanning creates pockets of unknown risk. There may well be devices in an environment that can't be scanned, but they should be few and far between. Organisations that actively measure the total surface area they're missing are generally high-performing when it comes to VM.

6. Managing to metrics

Panic is not a strategy, but it's a big part of the information security industry. There is a lot of fear, uncertainty and doubt to be had out there. Effective vulnerability management programmes aren't built on fear, they're built on metrics. There are plenty of metrics to choose from and more than enough advice on which are the best. I'm always in favour of using the metrics that drive the right behaviour in your organisation.

7. Remediation workflow

The point of all this activity to find and measure vulnerability risk isn't a pretty report. The point is to make better risk mitigation decisions. Effective vulnerability management has to result in effective remediation actions. No vulnerability assessment tool does this automatically for a variety of valid and invalid reasons. That means that effective VM programmes integrate with the remediation workflows that drive action within an organisation.

If you find yourself in a position of ownership for a vulnerability management programme, these seven habits should help you get the most out of your efforts to manage and reduce vulnerability risk. □

Learn more in this video: 7 Habits of Effective VM

Tim Erlin is VP Product Management at Tripwire.

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

Five trends that will dominate the mobile security agenda in 2020

As mobile becomes more powerful, security risks stack up.

Wandera reports

As we head into the new year, security professionals everywhere are piecing together clues from 2019 that might offer some insight into what 2020 will bring by way of threats and cyber-attacks. As mobile becomes more powerful and more ingrained in business, the security risks stack up in step. Here are the risks and evolving threats that we believe will dominate the mobile agenda in 2020.

1. Ransomware will remain merely a distraction for mobile

While ransomware continues to dominate the headlines, it's proving to be nothing more than a distraction when it comes to mobile. Compared to other mobile threats, ransomware ranks at the bottom, accounting for close to zero percent of total incidents experienced. It's time for end-users to shift their focus away from the noise to the threats that truly matter. Our data shows that trojan, adware, and spyware were the most frequently encountered types of malware in 2019. As long as businesses remain distracted by protecting against ransomware, they'll continue to leave themselves exposed to the more pervasive types of malware in 2020.

2. Phishing sophistication will skyrocket

Instead of the mass-produced threats of previous years that relied on 'spray and pray' tactics, we're seeing more sophistication on the attacker's side as spear phishing campaigns continue to move beyond corporate email. Advanced phishing schemes have already appeared in app stores, demonstrating more sophisticated functionality and successfully evading detection. With 81% of mobile phishing attacks already taking place outside of email, 2020 will see attackers making the move toward targeting users via messaging apps and social media; where they are vulnerable to fake profiles and notifications that are convincing enough to make them hand over sensitive data.

3. Context will become king when it comes to authentication

As the drive toward a passwordless future continues, access will be determined by context – where you are logging in, what time, and from what device. This shift in authentication will change the need for passwords. While the methods of authentication will likely continue to move toward a superior biometrics-based approach, the most important authentication factor will become the context in which users are looking to gain access. Soon, opening different apps will not only rely on facial recognition or your fingerprint but where you are, the network you're connected to, the country you're working from. In 2020, context will be king in the world of authentication.

4. The price of personal privacy will peak

In the past, end-users unknowingly forfeited their private information in return for 'free' services, but as privacy becomes both a legal and financial imperative, users are going to have to pay for services that were once free and set aside funds in their budget to pay for privacy itself. Additionally, the idea that businesses could offer an alternative to the monetisation of their personal data with a paid option is no longer abstract. In 2020, privacy will come as a privilege to those with the means to pay for it.

5. Bad apps will continue to slip through the cracks, but official app stores will improve their malware vetting capabilities

It's been proven that the app stores are a step behind when it comes to catching bad apps due to the increased sophistication of threats and it's becoming increasingly clear that Google and Apple can no longer scale and improvements are needed. There are simply too many apps, too many developers and too many attack methods for the app stores to keep up. This isn't to say that the app stores are necessarily negligent, as they've taken action when 'bad' apps are brought to their attention. The issue remains that as the sophistication of malware, adware and phishing continues to advance, the stores struggle to keep up. The good news is that looking ahead to 2020, it's likely the official app stores will improve their malware vetting capabilities to continue to be a more secure option vs sideloading or third-party stores.

The 2019 Verizon Mobile Security Index reported that 33% of organisations admitted to having suffered a compromise involving a mobile device. This number is only likely to increase as users are granted access to increasingly sensitive data from their personal devices. Heading into 2020, security professionals will need to redefine organisational priorities when it comes to mobile and learn to evolve with the changing landscape to keep their information secure across platforms, regardless of the device. □

wandera

Redefining the enterprise edge

Wandera's Unified Security Cloud provides real-time protection when your remote users access applications, websites and the cloud from their smart-phones or laptops, anywhere in the world

- Block threats in real-time
- Detect vulnerabilities, identify zero-day exploits and rogue Wi-FI hotspots
- Limit liability by filtering inappropriate content
- Reduce bill shock with intelligent data policies
- Provide your remote users a secured network route to the cloud

wandera.com

Malicious JavaScript injections are redefining the threat landscape

JavaScript injection attacks should be taken just as seriously by businesses as threat mainstays like phishing and ransomware.

RiskIQ reports

The rise of browser threats

In recent years internet browsers have proved an invaluable attack vector for criminals. Back in 2016 we started seeing malicious JavaScript code being inserted on corporate websites to capture financial transaction data and exfiltrate it directly from the user's browser session. The modified code was buried amongst hundreds or thousands of other scripts making detection extremely difficult. As a result, the compromises remained live for weeks to months on average, with large numbers of users affected in the meantime. The threat actors involved were given the name Magecart by RiskIQ as their initial attacks targeted the shopping carts of the Magento e-commerce server.

Fast forward to today and the situation has become far worse. There are over a dozen cybercriminal groups under the Magecart umbrella that are carrying out evolving attacks at an unprecedented rate and with frightening success. Responsible for the high-profile UK breaches of British Airways, Sotheby's, Cancer Research UK and Vision Express UK in which its operatives intercepted hundreds of thousands of consumer credit card records, Magecart has become an acknowledged risk for all organisations who act as an online merchant, as well for organisations who collect sensitive personal information. Their browser-based attacks have moved beyond web skimming to include cryptocurrency mining, fingerprinting and waterholing. Given the frequency by which RiskIQ researchers now encounter JavaScript injection attacks, they should be taken just as seriously by businesses as threat mainstays like phishing and ransomware.

Tackling browser threats

A key feature of RiskIQ's integrated digital threat platform is our worldwide network of web crawlers that continuously crawl the internet, collecting not just rendered pages but also the entire sequence of requests and responses that make up a web page – headers, dependent requests, certificates, and more. These crawls give our customers insight into what's happening on a web server at any given point in time, and how that server would interact with a real user.

Earlier this year we added a new module to our portfolio called JavaScript Threats, specifically designed to address the JavaScript injection threat.

There are over a dozen cybercriminal groups under the Magecart umbrella that are carrying out evolving attacks at an unprecedented rate and with frightening success.

The module discovers an organisations' JavaScript and third-party JavaScript through proprietary dataprocessing of virtual user web crawling, internet scanning, and collected data sets. The module automatically indexes, classifies, and assesses JavaScript resources to build complete, dynamic inventories. It monitors web applications, JavaScript, and third-party JavaScript continually for changes that can trigger events for investigation by security, IT, and web asset owners. Once an organisation establishes a policy for change monitoring, based on the priority of web assets and probability of malicious JavaScript, events may be configured to automatically trigger for certain changes. Highly customisable classifiers and policies enable triaging and action on prioritised events. With change monitoring, security teams can immediately see a prioritised list of JavaScript changes and associated locations.

JavaScript Threats also detects malicious and suspicious JavaScript using blacklists and a predictive detection engine, both powered by the insights of RiskIQ's threat research group. Malicious JavaScript is detected through blacklists of known malicious domains. When a known malicious domain appears within JavaScript code or resource URL, a blacklist incident is generated. Suspicious JavaScript is detected through a predictive detection engine that inspects code based on threat detection rules and correlates with proprietary data sets.

Through these capabilities, RiskIQ helps organisations protect critical web applications against JavaScript attacks, safeguarding customer trust, and reducing the likelihood of hefty GDPR fines. □

For more information, please visit
www.riskiq.com

RISKIQ®

World Leader in Attack Surface Management

Today's diverse cyber threats circumvent traditional security tools and place an enormous burden on information security organizations.

RiskIQ provides unified visibility, insight, and control for exploits, attacks, and adversaries across web, social, and mobile channels. With RiskIQ, organizations can reduce their digital attack surface and automate external threat detection to protect against targeted attacks.

To find out how RiskIQ can help protect your organization, please contact **sales@riskiq.net** or visit us at **www.riskiq.com**.

RISKIQ®

Simulation-based training is reshaping the way CISOs operationalise cybersecurity

Lack of standardised cybersecurity training is a significant contributor to the ever-increasing number of cyber-incidents.

RangeForce reports

Everyone is familiar with the three pillars of IT: people, process, and technology, but most cybersecurity investments go to just one area – technology. With so many vendors pushing technology and a lack of standards to build an effective training programme, it is no surprise. The lack of standardised cybersecurity training is a significant contributor to the ever-increasing number of cyber-incidents. Much like airline pilots spend countless simulator hours training to deal with inflight emergencies, CISOs must find ways to prepare their teams for a cyber-attack through realistic training in a safe environment. They must also provide accurate assessments that demonstrate that the company is truly ready to defend against a cyber-attack. It is not enough to have certified staff (CISSP, GSEC, etc.). Instead, CISOs need to understand that the entire security team is continually improving their skills and can work together to detect and contain an actual cyber-attack.

Use case 1: A CISO needs to understand and report cyber-effectiveness

The question everyone wants to know, "can the security team detect, respond to and contain a real cyber-attack?" The answer to this question, after weeks of frustration and expense, is usually no. By refocusing efforts and resources on continuous simulation-based training and assessments, and by capturing all these activities in unified reporting, security managers can understand the status quo, build on strengths and remediate weaknesses. CISOs can share an accurate assessment of a team's skills and a path to improvement with executives, board members and compliance teams, building confidence across an organisation.

Use case 2: A CISO is dealing with staffing shortages

Hiring experienced cybersecurity professionals is difficult and expensive. A robust model for countering staffing shortages is to build a flexible team through cross-training. Following a military developed model, each member of a team is trained to do the jobs of others. CISOs need tools that can identify their proficient cyber-pros and cross-train them into other security specialties. The goal is to optimise the roles covered by each team member at each stage in the attack process, so no one is 'sitting on their hands' at any time during an incident. CISOs also need strategies to manage staffing shortages, and one way is to identify IT staff who have the skills and talent to move into a cybersecurity role. IT roles are often easier to fill than cybersecurity roles.

Use case 3: A CISO needs to improving hiring processes

When hiring new cybersecurity staff, and with existing skills shortages, candidates are likely to be fresh out of school or through a cyber training certificate programme. The candidates may not have the operational skills needed to effectively fill the role or the aptitude to be trained in the role. For this reason, hiring managers can no longer rely on a candidate's CVs or training certificates when qualifying them. Hiring managers need objective tools that uncover the actual skills of candidates through on-demand testing, with the results captured and benchmarks created, so that the best candidate can be objectively identified.

Conclusion

CISOs at forward-thinking companies are shifting investment from technology to people and focussing on:

- Role-based advanced cyber-defence training
- On-demand, interactive, hands-on lessons
- Simulated attack scenario training
- Individual & team skills assessments and reporting

Many of these companies including Barclays, Microsoft and Pipedrive chose RangeForce as their cyber-skills training platform. A cloud-based, on-demand, SaaS environment, the RangeForce platform recreates real-life targeted cyber-attacks and teaches users and teams how to identify and defend against them, whilst providing executives with comprehensive reporting to accurately measure skill levels. □

For more information, please visit
www.rangeforce.com

RANGEFORCE

RANGEFORCE

CYBERSKILLS TRAINING PLATFORM

Build and measure the operational skills of your cybersecurity team

With RangeForce your team is prepared to detect and respond to the latest cyber threats and system vulnerabilities with speed.

A cloud-based, on-demand, SaaS environment means no complex setup or hardware requirements.

- Training Modules created by security experts for security experts
- Supports popular programming languages Java, PHP, Node.JS, Python, .NET, AZURE, AWS (Q2)
- MITRE ATT&CK, OWASP, & NIST framework aligned Training Modules
- A reporting dashboard to track team's strengths and weaknesses

www.rangeforce.com

Visibility key to a successful data protection programme

One of the longest running adages in cybersecurity still rings true to this day: You can't protect what you can't see.

Digital Guardian reports

While the idiom may sound like common sense, it underscores just how far we've come in IT.

When rolling out a data protection programme, gone are the days of guessing what you need to protect, deploying one-size-fits-all policies in a hope and pray fashion. Having robust data protection, one of the cornerstones of an effective security programme, isn't possible without visibility.

After all, it's not until an organisation can visualise how data moves throughout the enterprise and into the cloud that it can truly understand what's happening to it, where it's going, and who it's being accessed by.

This can be especially important when it comes to mitigating mistakes made by insiders – either intentional or unintentional – that can ultimately have a grave effect on your company's data.

Consider some of the most sensitive data in an organisation: source code, chemical formulas, schematics, and AutoCAD files. While much of this data tends to be parceled out on a need to know basis, ensuring only those privileged enough have access, mistakes do happen; that's when information can fall into the wrong hands.

As we've seen time and time again, an employee or executive's promise that he or she won't mishandle data is only worth so much.

Over the past year, we've seen countless headlines about former executives, in an act of retaliation, taking company information, usually valuable trade secrets, by emailing it to themselves or transferring it to a portable USB storage device.

Even with data classification and the appropriate access controls in place, employees can still pose a great risk to sensitive data.

While some employees steal data in an act of defiance, in some scenarios there isn't malicious intent at all. Negligent employees, often times careless with clicking and copying files, can compromise data as easily as an insider. In fact, in a study carried out by the Ponemon Institute last fall, 77% of managers admitted to accidentally sending an email containing sensitive information to the wrong person. A separate report, from January, found that employees mistakenly send 130 emails a week to the wrong recipient, leaving any sensitive data within at risk.

This is to say nothing about the sheer volume of data produced by enterprises these days. No matter the industry, with so many data centres, servers, and private cloud environments to oversee, it can prove exceedingly difficult for a data rich organisation to gain insight around the security of its data, let alone keep track of it all.

Without a way to see this data and detect when and where it's moving in real time, a company can be rendered useless when it comes to stopping data theft.

An effective security solution today should provide the visibility necessary to identify sensitive data wherever it resides – on the network, on a user's machine, or in the cloud.

With compliance regulations like the General Data Protection Regulation (GDPR) and in America, the California Consumer Privacy Act (CCPA) mandating even stricter data protection, it's even more important for organisations to ensure it has visibility.

By being able to see and understand your data, admins can get a better idea understanding where risk lies while having peace of mind that their organisation is satisfying regulatory compliance as well.

Data protection in 2020 isn't just a way to keep track of an organisation's data. It's a legal necessity, one that can help safeguard your most prized assets. It's the difference between surviving competition and sustaining profitability. □

For more information, please visit
digitalguardian.com

DIGITAL GUARDIAN®

DIGITAL GUARDIAN®

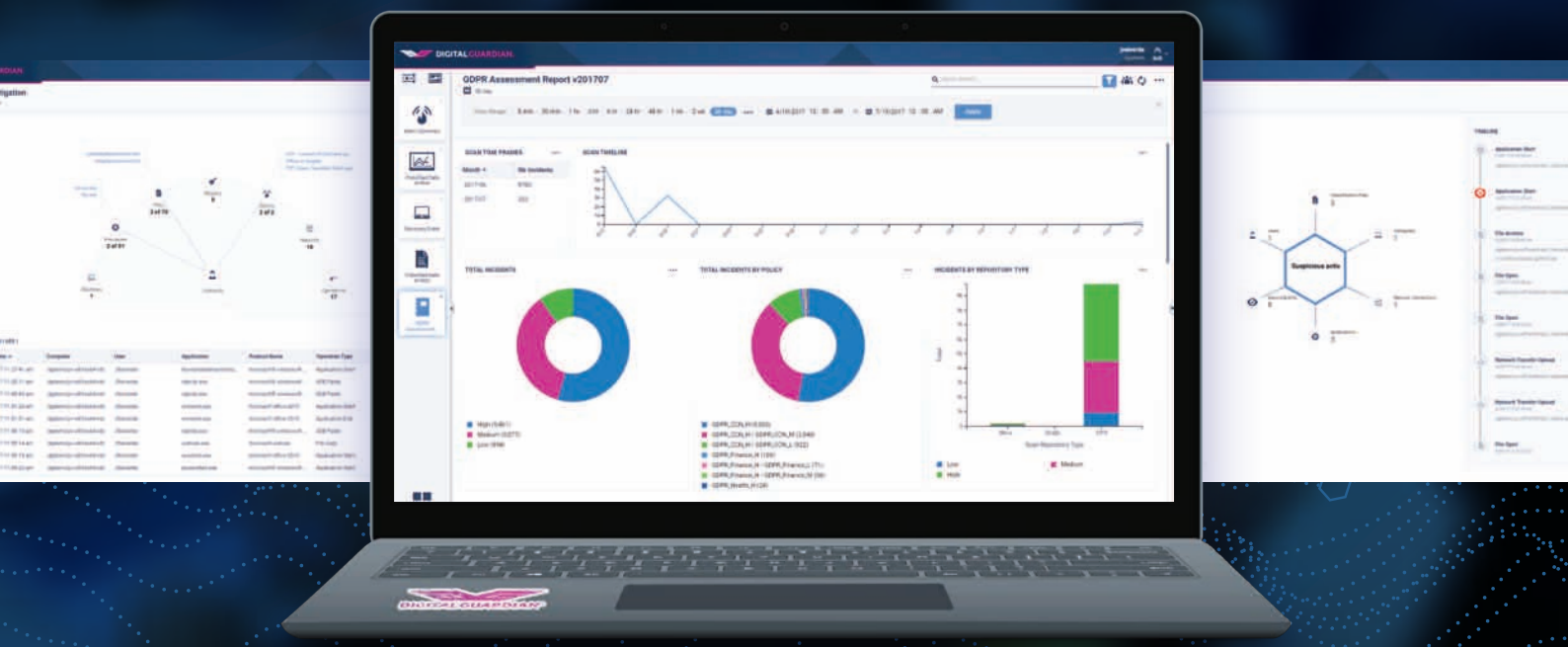
No-Compromise Data Protection

Cloud Delivered

powered by aws

Cross Platform

Flexible Controls



Available on aws marketplace

Gartner®
Enterprise DLP Magic Quadrant Leader

aws partner network
Select Technology Partner

FORRESTER®
Forrester Wave™ EDR Leader

Visit us at digitalguardian.com

Why network segmentation is essential to creating a secure enterprise environment

Network segmentation is not new, but why are organisations so slow in adopting it?

Richard Orange reports

Network access control (NAC) has been foundational to cybersecurity efforts since networks were first deployed. However, it all changed when the internet of things (IoT) revolution began. The mass expansion and increase in the volume of IoT and OT devices posed new questions to network security, as IT and OT devices moved away from the traditional Windows and Linux management structure. NAC technology had to adapt to maintain the high level of security. By becoming an agentless, security protocol it was able to be applied to all devices across any environment. With this, NAC reached the next level of network security.

Since this change, the increased interconnectivity across the campus, data centre, cloud and OT environments, drove a further growth in complexity in today's networks and associated security risks.

Threat actors are targeting large organisations with complex networks, such as manufacturers, with increasing frequency – from 45% of businesses in 2018 to 61% in 2019 having experienced an attack. [Hiscox]. The ease at which offenders pivot laterally across the network results in greater disruption of and damage to both property and reputation. During the WannaCry ransomware attack, shipping company Maersk had to resort to halting its entire operations and reinstall 4,000 servers, 45,000 PCs and 2,500 applications to ensure the network was clear of the ransomware. This caused severe disruption across the business and could have been prevented had its network architecture limited movement once access was gained.

Despite network segmentation not being a new concept, adoption across the enterprise has been slow and when undertaken, often tedious. This is, in part, the result of the limitations of the used technologies being implemented in environments outside of the data centre or address blind spots such as IoT and OT connected devices.

To effectively combat this growing combination of threats and enable zero-trust policies – network segmentation must go through an evolution to become a truly impactful approach for CISOs and IT directors in 2020 and beyond.

The first stage of this is having the full context of connected devices and applications that can be segmented across the entire enterprise from campus to data centre to cloud and OT environments. Visibility is the basic fundamental requirement to be able to begin segmentation. CISOs currently face the challenge of segmenting the network with only partial context and visibility.

Typically, organisations layer network segmentation on top of an existing network. The result of which is being unable to apply network segmentation effectively and across the entire enterprise.

Advanced network segmentation requires traffic context. Having insight into what devices are communicating between each other and what counts as legitimate or illegitimate traffic is paramount for CISOs today.

Make no mistake, without both levels of contextual information the policies are redundant. For network segmentation to be effective in today's enterprise the enforcement of policies must be adaptable and automated, with considerations of device and traffic context that stay up-to-date with the ever-changing network. Forescout is transforming enterprise-wide network segmentation with eyeSegment. This will help organisations accelerate network segmentation projects, matching the demand from businesses to secure critical applications, mitigate increased exposure due to IoT devices and limit the lateral movement and blast radius of threads across flat networks.

CISOs are faced with the challenges of a growing number of threats while meeting more and more compliance directives. The new era of network segmentation has been designed to allow businesses to automate the identification and isolation of threats, without impacting operations. For many, data breaches are thought of as a case of 'it won't happen to me'…until it inevitably does. By limiting risk, maximising control and enabling full visibility across a network, enterprises can more effectively prepare and manage the next wave of cyber-threats. □

Richard Orange is Regional Director UKI at Forescout.

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

FORESCOUT

Security at First Sight™

The First Unified IT-OT Security Platform

Across Your Extended Enterprise

Campus

IoT

Data Center

Cloud

OT

forescout.com

ClearDATA maintains a clean bill of (third-party risk) health with OneTrust Vendorpedia

A customer success story.

OneTrust Vendorpedia reports

ClearDATA is the market leader for healthcare cloud computing and information security services for providers, life sciences, payers and healthcare technology organisations. By enabling their customers to automate, protect, and securely manage healthcare applications, data, and IT infrastructure in the cloud, ClearDATA empowers the industry to focus on making healthcare better by improving healthcare delivery.

As a technology company interacting with sensitive healthcare data, ClearDATA understands the importance working with trustworthy and compliant third parties that hold with their customers' information. "ClearDATA was founded to help with patient care," said Jonathan Slaughter, Director of Compliance, Security and Privacy at ClearDATA. "To accomplish this and move forward as a business we needed to better understand what data our third-parties and vendors are collecting and the level of risk they pose for our customers."

A platform to assess, mitigate, and monitor third-party risks at scale

ClearDATA approached their third-party and vendor risk management initiatives with the objective of protecting customer privacy, while mitigating third-party risks and meeting security and compliance requirements. They needed to streamline existing manual processes by adding automation workflows to manage compliance and reduce risks during the evaluation, onboarding, and monitoring of their vendors.

With critical data housed across three major public cloud providers, ClearDATA needed a centralised software platform that could serve as a single solution to streamline and scale their once spreadsheet-centric third-party risk management programme.

After extensive evaluation, ClearDATA selected OneTrust Vendorpedia™ to automate their third-party risk management operations.

"OneTrust is the one company out there that's taking a holistic approach to understanding third-party, security, and privacy risk from a technology standpoint," said Slaughter. "Their Vendorpedia solution has allowed us to be more agile and scale rapidly to optimise our business processes and simplify our assessment, mitigation, and monitoring of third-party risks," said Slaughter.

OneTrust Vendorpedia is a centralised platform for global third-party risk, security and privacy professionals. Changes to third-party vendor risks are inevitable, making static one-off assessments unreliable over time. The platform offers ongoing monitoring with privacy and security scanning, ongoing assessment updates via the exchange, and scheduled reassessments to maintain a watchful eye on third parties. When significant changes are detected, OneTrust Vendorpedia sends the organisation relevant alerts.

"With OneTrust Vendorpedia we're able to manage the third-party risk management lifecycle and understand risks on an ongoing cadence instead of having to manually reevaluate vendors when renewals or audits are coming up," he added.

Today, ClearDATA can automate their entire third-party risk management lifecycle from onboarding, triaging and assessing risks, managing vendor contracts, demonstrating compliance with recordkeeping, performing ongoing vendor audits, and fully offboarding vendors. "Because of OneTrust, I'm not constantly following up with vendors and I have all the information I need in a timely manner to feel confident about our compliance and risk management processes," said Slaughter.

What's more, Slaughter and his team found little need to spend time on a custom configuration. "We were able to use the solution right out of the box to meet our needs, something that is very unique and really showcases the flexibility of the tool."

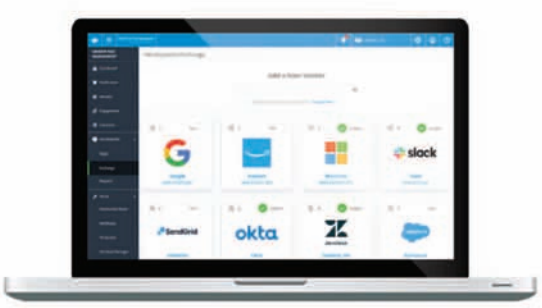
As ClearDATA looks to the rest of 2019 and beyond, they are excited to enhance their use of the OneTrust. With a strong customer base in the Asia Pacific region, and many privacy laws and security frameworks being developed and implemented very quickly worldwide, ClearDATA is planning to dig deeper into OneTrust Vendorpedia and other products to ensure they are confidently protecting customer data on a global scale. □

Intelligence and Automation to Scale Your Third-Party Risk Program

ASSESSMENTS & DUE DILIGENCE

Clarity at Every Stage of the Vendor Engagement Lifecycle, from Onboarding to Offboarding

- Onboarding Automation, Faster Assessments, Dozens of Templates
- Flexible Reports, Visual Dashboards, 360° Third-Party Visibility
- Mitigation Workflows, Centralized Vendor Risks, Out-of-the-Box Controls



GLOBAL RISK EXCHANGE

Thousands of Detailed Vendor Profiles and Pre-Completed Risk Assessments, Updated Daily

- Risk & Performance Monitoring, Alerts and Evergreen Vendor Data
- Supplier Profiles, Product-Level Granularity, In-Depth Risk Research
- Pre-Completed Assessments (SIG Lite, CSA CAIQ, etc.), Compliance Certs

VENDOR CHASING SERVICES

On-Demand Agents Act as Your Personal Questionnaire Collections Agency, at No Extra Cost

- Assessments as a Service, Questionnaire Completion
- Industry-Standard Templates, Faster Vendor Responses
- Multilingual Team, Available 24/7, Expert Assessment Support

POWERED BY ONETRUST DATAGUIDANCE

In-Depth Third-Party Risk & Regulatory Intelligence from 40 In-House Researchers and a Network of 500 Global Lawyers

OneTrust DataGuidance™ intelligence powers Vendorpedia, embedding valuable research directly into the platform to help your organization implement third-party frameworks, standards, and controls to comply with the laws that matter most. DataGuidance intelligence is aggregated from authoritative sources, updated on a daily basis, and continually reviewed to alert your team when critical regulatory changes arise.

OneTrust
Vendorpedia™
THIRD-PARTY RISK SOFTWARE

How educating employees can halt a successful cyber-attack

A strong cybersecurity posture is multifaceted.

Adenike Cosgrove reports

As threats evolve, companies must keep adding to their arsenal to ensure their defences are up to the task. However, there is one line of defence that is often overlooked: people.

The cybersecurity knowledge and understanding of employees is just as important as any policy or control that is put in place. The end user is often the first point of attack. In fact, recent Proofpoint research shows that more than 99% of cyber-attacks require human interaction to be successful. The more they understand about how their behaviour can affect the security of the business, the stronger an organisation's cybersecurity posture.

Unfortunately, as uncovered in Proofpoint's most recent *Beyond the Phish* report, a sufficient level of cybersecurity knowledge is not always present. The report analysed data from almost 130 million questions, answered by employees across 16 industries on a range of topics including phishing, data protection, ransomware and social media safety. Across all topics and industries, 22% of questions were answered incorrectly, suggesting around one in five end users has gaps in their cybersecurity knowledge[1].

The persistent threat of phishing

Phishing remains an ever-present threat to businesses of all sizes across all industries. In fact, Proofpoint's 2020 State of the Phish report, found that 55% of global organisations dealt with at least one successful phishing attack in 2019.

Interestingly, the level of understanding demonstrated in the *Beyond the Phish* study doesn't correlate with the same respondents' ability to spot a phishing attack. The average simulated phishing attack failure rate of the respondents was 9%, compared to an average percentage of phishing questions answered incorrectly of 25%.[2]

This tells us that while simulated email phishing attacks are a powerful way to assess end user weaknesses, they do not tell the full story.

Such tactics alone don't give a complete picture of how well users understand the wide-ranging threat of phishing. Nor does it provide insight into the level of understanding of other key areas that can contribute to an attack such as password hygiene and data protection.

Creating a security-conscious culture

Spotting gaps in user knowledge is one thing. Closing them is another. There is no quick fix. To increase user understanding of complex topics and bring about a change in behaviour, the only effective plan of action is comprehensive, ongoing training, that keeps pace with the cyber-threats organisations are facing. This training should include regular assessments, education, reinforcement activities, and measurement of understanding. The human factor needs to be a key pillar of a company's cybersecurity defences.

To shore up the line of defence that is usually overlooked – people – organisations should consider taking the following actions:

- Deliver comprehensive and continuous cybersecurity training to all employees, at all levels. This means not only training and refreshing end users on how to spot a phishing attack, but what to do when they occur and also eradicating any behaviour that can impact the security of your business.
- Ensure employees are educated in cybersecurity best practices, for example practicing good password hygiene. Not all security incidents stem from an outside attack and teaching employees on how to keep sensitive data secure is vital.
- Treat traditional phishing attacks with the importance they deserve. Ensure that your users know how to spot them and what to do if and when they occur.
- Educating employees on the 'why' as well as the 'what'. Not just what a threat looks like but how it works, the motivation behind it and the ways that their behaviour can increase its success rate.

When awareness and understanding increases, behaviour changes. And that might just be the difference between a successful attempt and a successful attack. □

[1] https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-2019-beyond-the-phish-report.pdf

[2] https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-2019-beyond-the-phish-report.pdf

Adenike Cosgrove, Cybersecurity strategy, International at Proofpoint


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.
Visit the Proofpoint stand for your chance to win some Bose headphones.
proofpoint
Protection starts with people.
proofpoint/uk

Strengthen security and governance with metadata

If you want to protect the sensitive data you share with third parties, you need to know everything you can about that data.

Accellion reports

What data is being shared? Who's sharing it? With whom are they sharing it? How are they sharing it? Ultimately, to protect your data and data workflows, you need deep insight into your data and data workflows. Encrypted data packets and IP addresses only tell part of the story. You'll need to dig deeper. With metadata, you have all the information you need to protect the PII, PHI, and IP you share with trusted third parties.

Third-party workflow threats have a common theme: a user is the actor, and a file is the agent. Complete protection requires a defence that spans the full breadth of the associated threat surface: the collective paths of all files entering and exiting your organisation. A comprehensive defence entails securing, monitoring, and managing all third-party workflows, including secure email, SFTP, and secure file sharing, among others.

With great metadata comes great opportunity

Once you've effectively shrunk the threat surface by limiting the number of entry points, namely the third-party communication applications used to transmit files into your organisation, you can more efficiently analyse every incoming file to detect, isolate, and neutralise all inbound threats.

While inspecting encrypted data packets and IP addresses is a good start to protecting data-in-transit, it's insufficient. By contrast, file transfer metadata lets you see who's sending the file, who's receiving it, where it's coming from, and much more. This information is only available at the user-application-file level, so this defensive strategy is critical for protecting data in risky third-party workflows.

By contrast, file transfer metadata lets you see who's sending the file, who's receiving it, where it's coming from, and much more.

At a minimum, every incoming file should be scanned by anti-virus software prior to being uploaded to an enterprise repository. More suspicious files may require rerouting for advanced threat protection (ATP) analysis. To avoid slowing user productivity, apply stratified inspection to all inbound file traffic. By marking suspicious files for detailed inspection and queuing them based on workflow metadata, higher priority workflows receive higher priority processing.

Source: Accellion enterprise content firewall

Use metadata to employ tight governance over third-party workflows

To protect data in motion as it leaves your organisation, you must establish and enforce strict data privacy rules, including granular policy controls. Policy controls let you prevent costly data leaks and meet internal and external data privacy requirements, like GDPR compliance and HIPAA compliance. Granular policy controls must incorporate sharing metadata like sender, receiver, origin, destination, and time of transfer to be truly effective.

By using metadata to analyse your inbound and outbound communications, you enhance your data security and governance and defend your third-party workflows.

Based on the content a file contains, data leak prevention (DLP) technology can be deployed to deny unauthorised requests. This process can be accelerated by implementing a data classification standard that allows DLP scans to be performed offline and requests for sensitive content to be processed in real-time. This type of context-aware, content-aware security can only be applied to workflows, namely users, applications, and files. As a result, you must screen for PII, PHI, and other sensitive content at the user-application-file level. You must also be able to log file metadata and your DLP results so you can analyse them in the event of any failures. You can then use your CISO dashboard to see file activity in context, drill down with comprehensive reports, and export logs to your SIEM solution. □

Accellion

Prevent Breaches and Compliance Violations with Secure 3rd Party Communications

ENTERPRISE CONTENT FIREWALL

Total Visibility

Get visibility and compliance of IP, PII, PHI, and all sensitive content shared with third parties.

Communication Simplicity

Click the Accellion button to share from email, web, mobile, office and enterprise apps.

Zero-Trust Security

Protect your cyber supply chain against leaks and threats from third party communications.

Deployment Flexibility

Access content everywhere, automate business processes, and deploy on premise or cloud.

Phone: +49 711 252861 0 | E-mail: *EMEA-Sales@accellion.com* | *https://www.accellion.com/*

Why the time is right for SOAR

It is clear that SOAR is gaining a foothold in the security industry and within SOCs of every size.

activereach reports

Industry-wide, analysts are overwhelmed, overworked and in desperate need of tools designed to help them keep pace with today's expanding threat landscape and growing cybersecurity skills shortage. Even more, if it were even possible for a SOC to hire all of the personnel required, it would still need automation and orchestration capabilities to investigate the thousands of alerts received each day.

Why SOAR?

There was a time when industry thought leaders weren't sure whether SOAR was truly 'a thing' or not. But with insights from recent reports, such as the Gartner 2019 Market Guide for Security Orchestration, Automation and Response Solutions or How Using SOAR Tools Makes Life Easier from Enterprise Management Associates (EMA), it is clear that SOAR is gaining a foothold in the security industry and within SOCs of every size. The reason for this is, in short, SOAR enables SOC teams to achieve more with less – an attractive proposition to the CISO and analyst alike. SOAR eliminates the tedious, repetitive and manual tasks typically associated with incident response processes that are known to lead to analyst burnout and alert fatigue.

What about SIEM?

Most organisations use some type of security information and event management (SIEM) system, and it is unlikely that will change. While data gathered from SIEMs are incredibly valuable to the SOC, analysts struggle to keep up with the seemingly endless alerts generated by these tools. The predominately manual investigation processes associated with SIEM tools creates significant fatigue, which leads to errors and organisation vulnerability. SOAR provides respite from the amount of human interaction required by these tools, and in so doing, enables improved alert investigation, faster decision making and overall more effective incident response processes.

SOARing above the problems

SOAR empowers analysts by helping them view and understand large sets of data at a glance, rather than requiring them to toggle between different windows, tools and even machines to investigate a single alert. Instead of relying on traditional strings of text or numeric information, data visualisation with a SOAR solution enables analysts to reach conclusions and take action instantly.

By automating tedious, repetitive tasks and orchestrating disparate tools and processes, a SOAR platform dramatically improves analyst performance, which also decreases the mean time to detect (MTTD) and respond (MTTR) for the organisation.

What's more, many incident response actions can be done without any human intervention when a SOAR solution is implemented. The orchestration component of SOAR enables the SOC to connect disparate resources and bring the data into the case record to enrich the alert. Rather than analysts spending time learning the intricacies of countless unique systems (which are likely to change over time and require workarounds depending on the SOC's ecosystem), they can use the single case record view of the SOAR platform to access and observe all of the data. This bolsters individual analyst performance, which boosts the overall efficacy of the entire SOC.

SOAR without limits

By automating tedious, repetitive tasks and orchestrating disparate tools and processes, a SOAR platform dramatically improves analyst performance, which also decreases the mean time to detect (MTTD) and respond (MTTR) for the organisation. As the SOAR enabled SOC explores the full capabilities of its solution, analysts will likely find additional benefits to enhance their overall functionality and efficacy for the organisation as a whole. A truly robust SOAR solution provides the organisation with almost unlimited options for connecting, automating and orchestrating its operations. □

Contact activereach, leading UK security integrator, to see how the new and amazing ways tools such as the SOAR solution from Swimlane can be used to improve the operational effectiveness of the SOC.

For more information, please visit **activereach.net**

activereach®

SOAR without limits

Think you can't have it all? With Swimlane's security orchestration, automation and response (SOAR) solution, you can. Don't put limits on what your security team can do and automate nearly any use case based on what, how and when you need it.

Orchestrate. Automate. Respond.

SWIMLANE

1-844-SWIMLANE | swimlane.com

Credential stuffing: Who is responsible?

If a customer account is accessed using the correct login credentials, how can you accurately identify the legitimacy of the user vs. an automated traffic attack?

Netacea reports

Credential stuffing attacks account for billions of login requests every year, as the automated bot technique continues to become one of the most prevalent cyber-threats.

Data dumps consisting of millions of unique combinations of usernames and passwords, are readily available at scale and for little to no cost. Although a portion of the data in a given dump is likely to be stale, poor password hygiene and password reuse means that even old data can be valuable to attackers, looking for Personally Identifiable Information (PII) for malicious gain.

With this multitude of PII to hand, automated web injections are used to carry out multiple login attempts at a time against the targeted online accounts in brute force stuffing attacks. Once an attacker has one password for a user, the greater the opportunity to find another account belonging to the same user and exploit this also.

Credential stuffing in action

Dunkin' Donuts

Dunkin' was initially targeted by a series of brute force attacks over a five-day period in 2015. The attack was believed to have compromised around 20,000 customer profiles containing registered Dunkin' Donuts (DD) loyalty cards; which contain loyalty points as well as cash.

The bot operators carried out the attack using account names and passwords leaked following historical data breaches to gain entry to the DD accounts. Once successfully accessed, the attackers sold the victims' DD accounts on the dark web or used them to make purchases, reportedly stealing tens of thousands of dollars from victims.

Following a second mass attack in 2018, which affected 300,000 Dunkin' customers, a lawsuit was filed against the chain by New York Attorney General Letitia James, accusing the business of violating the state's data breach notification statute and failing to implement precautionary measures following the first attack in 2015.

Disney+

Mere hours after Disney launched its streaming platform Disney+, users began reporting that they had been locked out of their accounts by hackers using stolen credentials. This number soon escalated into the thousands.

In this instance, the Disney+ platform hadn't experienced a breach, but its users were victims of a mass credential stuffing attack.

Credentials were then validated using bots to continually stuff usernames and passwords, identify correct combinations and sell the accounts on the dark web for a fraction of the subscription price.

Andy Still, CTO at Netacea said: *"Despite the fault lying at someone else's door, compromised usernames and passwords quickly become your problem when your customers feel the effects, and the reasons are threefold: financial loss, impact on user trust and reputational damage."*

To tackle bot threats, we must identify our weaknesses

Automated bots are used to identify and exploit legitimate business functionality, such as login forms, which expands attack vectors away from those defended by traditional application security. For many systems, business logic is the weak point and the range of infrastructure, products, data and services available to exploit those weaknesses mean that these attack vectors are becoming a target.

Andy Still stated: *"It is not your problem but it is your responsibility to have a sophisticated bot defence solution in place. It is vital that your bot management technology provides comprehensive protection against bot activity that targets weaknesses in your business logic across your website and API-based systems."* □

NETACEA

Up to 1/3 of your web traffic is malicious

Protect your websites, mobile apps and APIs
from automated threats

RAPID

Quickly detect, respond
and mitigate attacks

ACCURATE

Understand intent and
prioritise genuine users

TRANSPARENT

Empower your teams with
actionable threat intelligence

Secure your business today, call us on **03309 950 040**

@netacea_ai company/netacea/ www.netacea.com hello@netacea.com

Crowdsourced security testing

Since day 1, we have had a simple goal: provide a scalable security solution that can help modern organisations minimise security risk.

Synack reports

Traditional pen tests are like blacklisting an IP to block spam: insufficient and obsolete. Traditional pen tests are checklist-driven and compliance-based, failing to mimic the creativity of the adversary. Typically, these pen tests are conducted by small, static testing teams that simply can't scale to the size of modern attack surfaces and diversity of attackers. With a talent gap expected to total 3.5m open cybersecurity positions within the next few years (Cybersecurity Ventures), a rapid release cadence, and noisy alert systems, it's no wonder that security teams are looking for a more effective, efficient answer for finding and fixing vulnerabilities. That's why global enterprises, start-ups, and government agencies are turning to crowdsourced security testing.

This modern approach to testing offers scale, effectiveness, and efficiency that was previously unavailable. However, not all crowdsourced security testing companies are created equal. Crowdsourced security testing solutions vary based on the quality and trustworthiness of the talent, the control available to the customer, the sophistication of the management and analytics technology, the speed and simplicity of deployment, and the level of support service provided for vulnerability discovery, triage, reporting, and remediation, all of which drives differences in ROI.

Synack is the crowdsourced security testing platform of choice for the F500/G2000, mid-market, and government agencies due to our unique platform, purpose-built with trust, control, and visibility at its core. As with traditional pen tests, Synack harnesses the best of human and artificial intelligence – but not just a group of any humans and a generic marketplace matching algorithm. Synack pairs this powerful combination of human talent and technology with data and visibility to provide a scale, ease and thoroughness on a continuous, 365-day basis. Here's the recipe for our platform's success:

1. *Human intelligence – Synack Red Team:* The world's best ethical hackers, vetted for skill and trust and incentivised based on what they find, rather than how many boxes they check
2. *Artificial intelligence – Synack Platform:* Synack's AI-enabled platform is strengthened by learnings from the Synack Red Team and helps accelerate their time to find vulnerabilities.
3. *Data & visibility – LaunchPoint:* A secure gateway for all testing activity that offers risk mitigation for both customers and researchers, customer control and real-time analytics
4. *Concierge service – Synack Operations:* A force multiplier that does what your teams should not have to, including rapid deployments, 24/7 program management, noise removal through triage and patch verification, continuous performance tracking and community management

All four components of our platform work together to provide a simple, easy, effective solution with real-time analytics and on-demand, detailed reports. A painless way of understanding your security risk from a true hacker's perspective.

A Synack pen test means:

- *Higher value:* 4x higher ROI than traditional methods via efficiencies gained from automation, noise reduction, and more actionable insights
- *Greater efficiency:* Synack's smart platform reduces 99.8% of the noise allowing researchers to focus their efforts on the most critical and exploitable vulnerabilities
- *Better results:* 200% more resistance to malicious attack by leveraging a continuous cadence of human + machine augmented testing and ensuring continuous coverage across dynamic apps

So what does that amount to? A realistic understanding of security risk and actionable results. □

Synack offers a new and more disruptive security testing platform for finding and helping resolve serious vulnerabilities in mission critical applications and infrastructure that otherwise go undetected.

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

Synack

Secure Your Everything: using a consolidated architecture to streamline your cybersecurity

As you adopt new digital technologies, new cyber-threats are not far behind.

Check Point reports

Today, a digital transformation is becoming a core piece of your organisation's business model. However, the complex technologies used to digitise your operations are the same ones that can be exploited. Your cybersecurity must be comprehensive and with the mindset to be effective, you need to Secure Your Everything. Migrating to a consolidated security architecture is a way to streamline your security end to end.

Digital transformation means ever more technology

As you adopt new digital technologies, new cyber-threats are not far behind. As a result, many organisations have turned to point solutions to deal with new threats, creating a bewildering patchwork of security from multiple vendors. Unfortunately, these assorted solutions can impede security, rather than boost it. For example, threat intelligence is integral to cybersecurity, but in a mish-mash of point solutions, it can be less effective. The lack of integrated administration and management is an undeniable nightmare. Add multi-cloud computing, SaaS, and mobility to your environment, and it's clear, you must Secure Your Everything because it all matters.

Consolidated architecture benefits

Here are a few ways, among many, where a consolidated architecture can help protect your organisation against sophisticated cyber-attacks:

- *One-click sourcing.* Sourcing a point solution to protect a new technology or to add new security capabilities is time-consuming and it requires tedious researching and testing of multiple products. In contrast, adding new security protections and other functionalities such as forensics or compliance reporting with a modular consolidated security architecture can be as straightforward as clicking a button in the architecture's single interface.
- *Single interface for deployments.* A consolidated security architecture displays security for all on-site and off-site networking environments through the same single interface. This not only fosters fast deployments, but it simplifies staff training when using a single interface.
- *Streamlined administration and management.* Point solutions' standalone interfaces complicate security administration and management. Monitoring and responding to alerts, for example, is more difficult with multiple, diverse interfaces. Changing security settings through several interfaces is a common source of mistakes that leads to security breaches. A consolidated security architecture lets staff administer and manage cybersecurity with a single user interface for all workloads whether they are processed onsite or offsite.
- *Smooth compliance updates.* When staff must independently configure and monitor several point solutions, this can increase the likelihood of a successful attack and regulatory compliance audits. Considering the inevitability of rapid technology growth and the enacting of industry regulations and laws covering security and privacy, you'll not only need to protect the integrity of your data, but for compliance, you must be diligent with your cyber-technology updates. A consolidated model also allows for unified reporting.

A case in point

"We researched the market and found Check Point to be the best overall solution. It convinced us it had the most effective unified approach to cybersecurity."

Marcus Morig, Head of Information Technology, Motortech

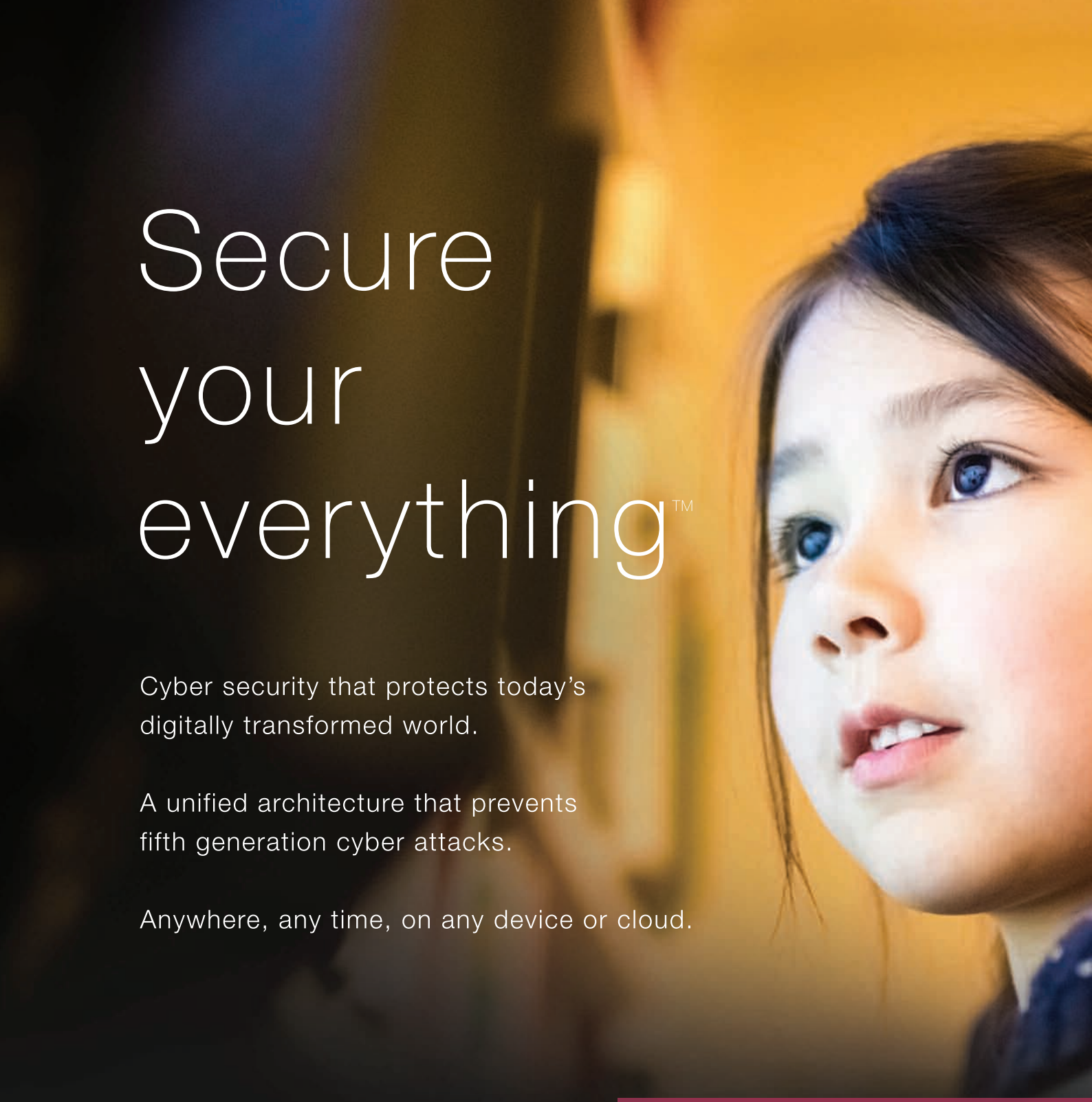
Read how this engineering firm met threat prevention and security management requirements with Check Point Infinity. Visit www.checkpoint.com/customer-stories/motortech/ for details.

Conclusion

It's well documented that human errors in security configurations and in other general practices can lead to security breaches. A Secure Your Everything consolidated cybersecurity architecture plugs the technical security gaps that point solutions leave exposed and gives security professionals more time to excel by streamlining security practices end-to-end. □

To learn more how the Check Point Infinity security architecture helps consolidate your cybersecurity and solve your critical issues, visit us at **www.checkpoint.com/architecture/infinity/** or contact your local Check Point representative.

Check Point SOFTWARE TECHNOLOGIES LTD.



Secure your everything™

Cyber security that protects today's digitally transformed world.

A unified architecture that prevents fifth generation cyber attacks.

Anywhere, any time, on any device or cloud.

Check Point®
SOFTWARE TECHNOLOGIES

checkpoint.com

Introducing Intel 471's Cybercrime Underground General Intelligence Requirements (CU-GIR)

A common framework to address common intelligence challenges.

Intel 471 reports

In a recent blog, we outlined three key benefits of a requirements-driven intelligence programme. We also looked at three challenges that are preventing many programmes from moving from concept to practice.

Benefits	Challenges
Maximise human, data and technology resources	Numerous opaque objectives across many stakeholders
Measured success criteria, aligned to priorities	'Whack-a-mole' approach is reactive and lacks direction
Demonstrated intelligence ROI & value to the organisation	Intel teams, stakeholders and vendors are misaligned

Intel 471's Cybercrime Underground General Intelligence Requirements (or simply 'GIRs') is a compilation of frequently asked questions or topics based on common observables in the cybercrime underground. Roughly 180 GIRs are organised under a nested tree structure under the following six categories:

GIR1: Malware	**GIR2:** Vulnerabilities & Exploits
GIR3: Malicious Infrastructure	**GIR4:** Fraud & Identity Theft
GIR5: Adversary TTPs & Activities	**GIR6:** Threats Impacting Industry or Region

- *GIRs are organisation-agnostic:* The GIR framework allows for consistent and ongoing coverage of commonly-observed and generalised threats to industry, sector, supply chain and geographic areas of interest
- *GIRs are mapped to intelligence consumers and use cases:* Each GIR maps to typical stakeholders and use cases where cyber-threat intelligence (CTI) teams need to produce intelligence. Essentially, GIRs are ready-made intelligence requirements that can be used to guide discussions with your stakeholders.
- *GIRs are not merely tags:* As an analyst, these are the questions one would seek to address in their report or deliverable to satisfy a particular stakeholder use case. When content is marked or tagged with a GIR, it means that it fills a gap in knowledge.
- *GIRs allow for a range in specificity:* GIRs are situated in a nested tree structure to allow for a range in specificity and flexibility in its utility. For example, by addressing a specific child GIR entry, an analyst inherently satisfies the corresponding parent entry.

At Intel 471, CU-GIRs underpin everything we do. GIRs are used as our primary baseline tool to collect, classify and report frequently observed information found in the underground.

- *Prioritised and focused collection:* Our clients use our GIR Handbook to select and rank subsets of GIRs that are aligned to their stakeholders and use cases. These become their Priority Intelligence Requirements (PIRs). Intel 471 weighs and scores all PIRs and uses the resulting list to prioritise and steer our existing collection and production efforts. Using this approach, we also gain insight into priority requirements across industry verticals.
- *Structured intelligence content and automated routing:* Each Intel 471 deliverable is tagged with the applicable GIR or GIRs, which automatically highlights these to clients who have matching PIRs.
- *Measured intelligence production:* Synchronising client PIRs to GIRs gives us a reliable method to measure the value of our intel production against our client needs over time. And, in turn, it gives our clients the ability to objectively measure their support and value to their own internal stakeholders.

At Intel 471, we have seen over 1½ years of real-world success by proving the concept of CU-GIRs both internally and with our customers. □

To read the full blog on this topic and others, please visit https://blog.intel471.com/

For more information, please visit **intel471.com**

INTEL471

Third-party risk: four ways to manage your security ecosystem

The increased number of suppliers can create a huge headache for security teams.

Digital Shadows reports

The digital economy has multiplied the number of suppliers that organisations work and interact with. Using a supplier can bring several benefits, including (but not limited to):

- Accelerating your revenue
- Enhancing customer loyalty
- Providing much needed and more flexible expertise and resources

Although suppliers benefit the balance sheet, the increased number of suppliers can create a huge headache for security teams: the truth is that third parties alter – and increase – the potential attack surface of an individual or organisation.

How?

These days, relationships between an organisation and a third party are mutually beneficial in that the organisation grants the third party access to its digital systems in return for its services. But depending on the level of integration between the two parties, such access could allow the third party to hold some of the organisation's most sensitive data.

Threat actors are drawn to supply chains by the nature of this sensitive data. With a successful compromise, that data can be monetised on criminal forums, be used for fraud, or offer a strategic advantage to those seeking intellectual property.

Supply-chain attacks are widely reported to be growing in popularity. In fact, according to a study conducted by Ponemon Institute in 2018 for US organisations, 61% of breaches were caused by one of their vendors or third parties. That's 5% higher compared to the previous years of study.

Although suppliers benefit the balance sheet, the increased number of suppliers can create a huge headache for security teams: the truth is that third parties alter – and increase – the potential attack surface of an individual or organisation.

The challenge for security professionals is ensuring that suppliers aren't exposing their systems or data. A challenge made even more difficult if the organisation uses lots of suppliers. It is thought that suppliers can range from tens to thousands, in some cases hundreds of thousands.

Bolster your security with continuous monitoring

But security professionals need not face this challenge alone. There are plenty of measures in place to help reduce the likelihood of a third party exposing this sensitive data, including privacy impact assessments, background assessments, and vendor risk scoring.

However, a reassuring point-in-time risk score of a vendor can give you a false sense of security: **effective third-party risk monitoring must be continual**. What's more, if you're not assuming that your third party is exposing you, and taking measures to mitigate it, you are burying your head in the sand. Last year, we recorded a webinar with ADP where they provided some of the best practices, including the use of security audits, insider threat programmes and segmentation of network access.

Monitoring third-party risk with Digital Shadows

With third parties continuing to expose organisations, here's how you can safeguard your data with our service, Digital Shadows SearchLight™.

1. *Detecting third-party data exposure instantly with SearchLight:*
   Our instant data detection module, allows organisations to detect inadvertent documents exposed by third parties, across a broad number of data sources. Monitoring for data exposure is critical. As you may recall, earlier this year in May 2019, the Photon Research team published a report, *Too Much Information: The Sequel*, which identified more than 212,000 files exposed by a third party for a small IT consulting company in the United Kingdom. In this case, passwords were exposed in plaintext, and two instances in which the password lists included the passcode to an individual's cell phone.

   This is just one example… there have been many other instances of contractors and third parties

Don't assume your data is safe because you've completed a vendor risk questionnaire, or the third party has a promising risk score. Data finds a way online, and you should find a way to detect it when it does.

exposing sensitive data via misconfigured devices and file sharing services. Our research report findings shared that there were 700,000 instances of payroll information, 65,000 tax return documents, 700 penetration tests, and 5,800 documents on security audits.

2. *Monitor credentials associated with third-party applications:*
Digital Shadows' former research highlighted that criminals are constantly on the hunt for your business emails (*Business Email Compromise: When You Don't Need to Phish*). If credentials are obtained, say from a breach, this could result in account takeover. Using SearchLight, organisations can continuously monitor for credentials in breaches to prevent compromise even further. We've currently collected more than 14 billion credentials – a number that continues to grow.

3. *Keep track of incidents affecting suppliers:*
Access a wealth of timely updates on incidents that may affect your suppliers, simply by accessing our intelligence library. Using Office365, Intel, or WordPress? Just filter by that tag and you'll be alerted to incidents involving those technologies.

4. *Tailor your monitoring via Shadow Search:*
Using the 'Saved search' function in Shadow Search, you can easily monitor for mentions of third parties across our public intelligence library (as described above), but also any mentions across blog posts, dark web sources, and more.

Protect your data, whoever exposes it

Don't assume your data is safe because you've completed a vendor risk questionnaire, or the third party has a promising risk score. Data finds a way online, and you should find a way to detect it when it does. □

To learn more about data leakage detection, check out our resources at **resources.digitalshadows.com/data-leakage-detection**.

digital shadows_

Generating actionable intelligence

Intelligence isn't much good if you can't act on it.

IntSights reports

The goal of cyber-threat intelligence is to provide advance warning and detection of cyber-attacks so you can take proactive protection measures. That second part, the part about taking action, is key. Intelligence isn't much good if you can't act on it. Therefore, strong, actionable intelligence is the foundation of DRP (Digital Risk Protection).

No one needs to tell you that the internet is an astonishingly big place, with an ever-expanding collection of data and information. The total number of websites out there is right around 2 billion. And that's just the part of the internet that people *want* you to see.

Beyond that lies the *dark web,* a much more secretive part of the internet that allows users to access websites anonymously. Plenty of legitimate activity takes place there, but it's also the home of the cybercriminal underworld. Their part of the dark web hosts all kinds of nefarious activities, hidden more or less in plain sight, if you know where to look. Meanwhile, social media has become a popular attack vector for cybercriminals, paste sites are openly accessible to any browser, and app stores allow cybercriminals to target users on their mobile devices.

Surveys of the people who use cyber-threat intelligence tools have found that many are overwhelmed by the information they get. For those who are using traditional or first-generation, tools, there's just so much data to process, normalise, and determine whether it's relevant to their operations and brand. These users are hit with what they feel are excessive and generic alerts. There's just a lot of noise, and it's hard to make sense of that noise.

Newer, more advanced tools understand the multidimensional nature of threats and use your digital footprint to provide context and relevancy. That gives organisations a much better ability to understand if and how a specific threat impacts them, which means they can act much more promptly to mitigate the threat.

Sources and types of intelligence

Intelligence comes in many different forms and from a variety of sources. Each of the possibilities has value in uncovering the motives driving cybercriminals, as well as their tactics and tools.

Here are some of the types of intelligence on the menu:

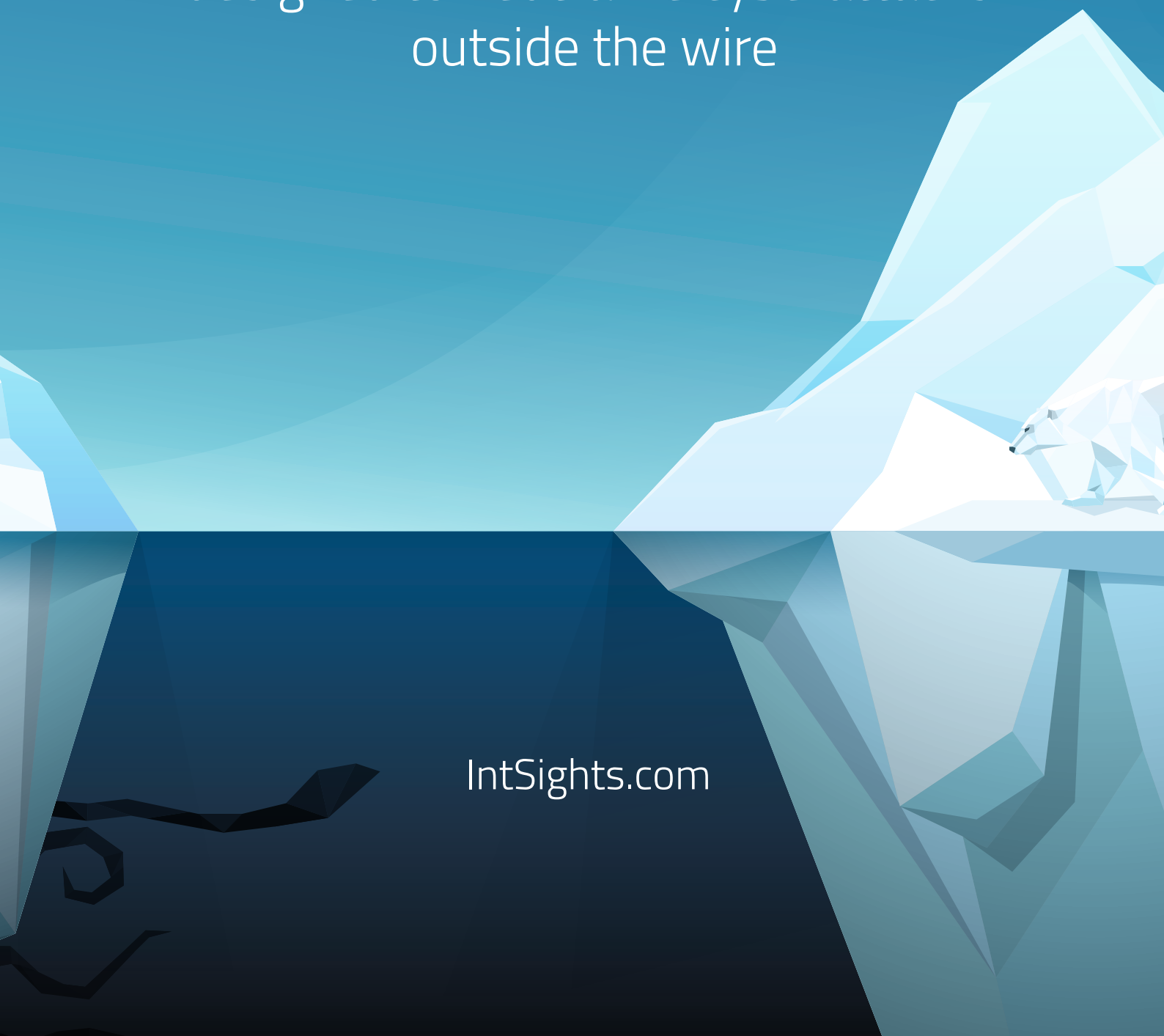
- *Open source intelligence:* Known as OSINT for short, this is the kind of intelligence you can derive from publicly available or open sources. Web pages are open sources, as are many online forums and intelligence feeds. They're out there for any user, including you.
- *Signals intelligence:* This refers to collecting intelligence by way of signals from communications and electronic sources. You'll see it referenced as SIGINT, and some people call it machine intelligence. Cell phones and computers are the most common sources of SIGINT.
- *Social media intelligence:* You may view intelligence gathering via social media channels and networking sites to be a subset of open source intelligence. A lot of organisations see SOCMINT as its own unique kind of intelligence, because social media play such a big role in the major threats of customer phishing and brand impersonation.
- *Human intelligence:* Also known as HUMINT, this is what it sounds like – intelligence gathered by contacting and engaging with actual people, rather than automatic monitoring or digging through feeds and technical processes. Human intelligence gathering takes just the right knowledge and skills to gather intelligence this way without raising suspicion.
- *Dark web intelligence:* This is what you gather when you monitor the various dark web sources, such as black markets, private chat rooms, dark web forums, and other anonymous and villainous places.

As you can see, some of these types of intelligence overlap. Social media intelligence is related to open source intelligence, and a fair amount of human intelligence gathering takes place in dark web places. Despite the overlaps, there may be differences in the intent of the research. □

INTSIGHTS

Defend Forward™

The only all-in-one
external threat protection suite
designed to neutralize cyberattacks
outside the wire



IntSights.com

TRAPX SECURITY

DECEIVE CYBER ATTACKERS AT EVERY STEP

An advanced cyber-deception platform able to defeat sophisticated attacks with no changes to the network.

Learn more at

www.trapx.com