e-crime & cybersecurity BENELUX

6th December 2018

Amsterdam,
The Netherlands

Transparency plus transformation: the cybersecurity rubicon

Recorded Future

When You’re Ready for Threat Intelligence, You’re Ready for Recorded Future

www.recordedfuture.com

Welcome to e-Crime & Cybersecurity Benelux 2018

6th December 2018

Novotel Amsterdam City

As business moves increasingly to digital channels across Europe, fraud attempts and other cyber-enabled economic crime are rising sharply. And recent research has shown that as well as increasing volumes, there has been an evolution from short, isolated peaks of fraud attacks to more sustained, high-volume attacks across a number of days or even weeks.

In addition, digital transformation is moving increasingly to mobile, rather than desktop online, channels. In Europe, 58% of all transactions now come from mobile devices and growth is accelerating.

These trends pose a huge challenge for business and for cybersecurity professionals. Businesses need to go digital and to make digital channels as seamless as possible for their customers. But they also need to keep those transactions, and their customers' personal data, secure. Cybersecurity is therefore a strategic business imperative.

It is these topics, and more, that we will be discussing at our 8th annual e-Crime & Cybersecurity Benelux as well as hearing about the latest technologies from some of the key providers. But one of the main aims of our events is to facilitate conversation and dialogue. So please, enjoy your event, and take the opportunity to mingle with colleagues and solution providers. If you have any questions, please do not hesitate to ask any member of the team.

Simon Brady | Editor

@eCrime_Congress #ecrime18

Editor and Publisher:
Simon Brady
e: simon.brady@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 7498
e: simon.brady@akjassociates.com

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

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

Those organisations sponsoring or supporting e-Crime & Cybersecurity Benelux bear no responsibility, either singularly or collectively, for the content of this magazine. Neither can those organisations sponsoring or supporting e-Crime & Cybersecurity Benelux, either singularly or collectively, take responsibility for any use that may be made of the content contained inside the magazine.

Security resilience in the face of evolving attacker tradecraft

Stories from the cyber battlefield.

CrowdStrike reports

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 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/

CrowdStrike® is the leader in Cloud delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The CrowdStrike Falcon platform deploys in minutes to deliver actionable intelligence and real-time protection from Day One. Falcon 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 artificial intelligence/machine learning and indicator-of-attack (IOA)-based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, Falcon instantly correlates over 70 billion security events 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

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

CROWDSTRIKE

Weighing your threat intelligence options

If your organisation is looking to make an investment in threat intelligence, you'll need to evaluate what different vendors deliver, how they align with your objectives, and the advantage they'll bring to your security strategy.

Recorded Future reports

Threat intelligence products and services come in all shapes and sizes. Some provide very specific kinds of intelligence, some consolidate and aggregate threat data, and some give you access to expert analysis.

If your organisation is looking to make an investment in threat intelligence, you'll need to evaluate what different vendors deliver, how they align with your objectives, and the advantage they'll bring to your security strategy.

Below we weigh different considerations to help you make a more informed decision.

Data vs. Insights

There's no doubt that the breadth of available sources that threat data originates from will be an important factor in the success of your threat intelligence programme.

But at the same time, one of the most common issues with threat intelligence is an imbalance between data and insights. Put another way, security teams spend far too long processing alerts that simply aren't relevant to their organisation, network infrastructure, or industry.

When considering which solution will best aid you to reach your objectives, it's vital to consider the balance of data sources versus insights that each solution will deliver. You need a solution that consumes data from a wide range of sources, but you also need one that can contextualise and prioritise relevant alerts, while simultaneously cutting out the noise.

Speed vs. Context

Balancing speed and context is perhaps the most important factor in the production of actionable threat intelligence.

> One of the most common issues with threat intelligence is an imbalance between data and insights. Put another way, security teams spend far too long processing alerts that simply aren't relevant to their organisation, network infrastructure, or industry.

Without context, determining a suitable response to alerts is very difficult. However, context can't always be found instantaneously, and many security events are time sensitive. Taken to extremes, this can result in making the right decision very slowly, or the wrong decision very quickly.

This is why striking a balance is so important. To provide maximum benefit, you need a solution which can balance the speed of new data with the context you'll need to make a quick decision based on actual risk.

Human vs. Machine

For decades now, machines have been 'on the verge of replacing humans' in many areas of activity.

For the most part this simply hasn't happened. Machines have become an invaluable asset in almost every endeavour, but outside of menial tasks, there are very few cases where machines have completely removed the need for human involvement.

There is one simple reason for this: machines are outstandingly good at some tasks (e.g., completing a huge number of calculations very quickly or labelling inputs based on pre-programmed conditions), and extremely bad at others. In particular, machines are totally incapable of critical decision making.

This is why it's so important to identify a solution that strikes the right balance between human and machine involvement.

The sheer volume of available data makes collection and processing functionally impossible for humans to perform alone. Even with alerts aggregated and normalised into one location, as they are by simple threat intelligence platforms, security teams are quickly overwhelmed.

An effective solution is one in which the simple tasks – data aggregation, comparison, labelling, and contextualisation – are completed by machines, leaving humans to do what only they can: make effective, informed decisions.

Reports vs. Integration

Excluding the automation of simple and repetitive tasks, the primary benefit offered by threat intelligence is to inform human decision making.

Decide what you need threat intelligence for and choose the solution that not only best provides what you need to achieve it today, but also adds the potential to become a partner that both equips and enables your security teams as you move forward.

This can happen in one of two ways:

1. Reports are produced and used to inform high-level strategic decisions.
2. Individual, contextualised alerts are used to inform operational decisions.

Striking a balance between these two approaches will depend heavily on your specific objectives.

Threat reports, whether produced internally or by a security vendor, can provide strong insight into broad industry trends, commonly used threat vectors, and emerging TTPs. This type of intelligence is highly valuable when making investment decisions or hammering out policy documents.

On the other hand, more operational objectives such as empowering vulnerability management or incident response benefit far more from having specific and relevant contextualised intelligence in the right place, at the right time. This is where integration comes in.

Many threat intelligence solutions are intended for integration with a variety of security technologies such as vulnerability scanners and SIEMs, either in the form of turnkey integration with established partners or APIs. Depending on your specific needs, you will want to ensure a chosen threat intelligence solution is capable of integrating with your existing systems via one of these approaches.

Striking a balance

It's important to understand that none of the considerations outlined above are 'either–or' situations. Identifying the best solution for your specific needs is a case of determining the outputs you'll need to inform better decision making.

In reality, none of these variables is inherently 'better' than any of the others. Without machines to aggregate and contextualise data, there is very little security teams can do to produce intelligence. And without a reasonable turnaround time, all the context in the world is useless – late decisions are often no better than wrong decisions.

Always keep your use cases front of mind and follow this mantra as you look to identify the right solution for threat intelligence:

Decide what you need threat intelligence for and choose the solution that not only best provides what you need to achieve it today, but also adds the potential to become a partner that both equips and enables your security teams as you move forward. □

To understand phishing, look at crimes of the past

Phishing is a modern problem but its roots go back hundreds of years.

John 'Lex' Robinson reports

You've heard it a million times: "Those who cannot remember the past are condemned to repeat it." While the Victorian philosopher George Santayana never heard of phishing, his aphorism applies to these rampant cyber-attacks.

Phishing is a modern problem, a spawn of digital life, but its roots go back hundreds of years to classic criminal scams. To understand phishing, you'd do well to study history. You'll see that the criminal landscape changes, but human nature does not. Once you grasp this, you can reshape your anti-phishing strategies to focus on your people.

Hacking the human

In cybersecurity, there has been a Cold War escalation of technology-based solutions between the black hats and the white hats. While effective in reducing tech-based vulnerabilities, this approach misses the most powerful processor in existence: the human mind.

The vast majority of cybercrime is straightforward consumer fraud, with much of the remainder focused on identity theft, along with classic scams designed to separate consumers and businesses from their private information and money.

Each of these scams has its foundations in 'hacking the human' and most begin with a phishing email or via online links that connect an unwitting victim to the attacker. To recognise contemporary scams more readily, have a look at some criminal tactics that have been around forever.

The pig in a poke

Have you ever purchased a product online only to find out later it was not as advertised – maybe not even close?

> The vast majority of cybercrime is straightforward consumer fraud, with much of the remainder focused on identity theft, along with classic scams designed to separate consumers and businesses from their private information and money.

If so, you've fallen victim to the classic con known as the 'pig in a poke.' It dates back to the Middle Ages and plays on our sense of scarcity and desire for high-value commodities.

At the time of its origin, quality meat was rare and livestock highly valued. Criminals sold piglets in a poke (poque – French for small bag) to unwary buyers who would later discover they had actually been handed a bag with a cat inside.

We see this same approach *daily* in email coupon scams and online auctions.

Its why consumers need to be leery of phishing emails and links to websites that promise deals too good to be true. Unlike in the Middle Ages, when the bag at least contained an item of some value, today's online fraud victims often receive nothing.

The pig in a poke is the grandfather of a common email phish dubiously titled 'package delivery'. In this case, the targets get an email saying they have an unclaimed package requiring a signature. A helpful link will make this easy, directing victims to a malicious website.

The badger game

Dating back to the 19th century, this is one of the most prolific cons of all time. The 'badger game' is a straightforward form of blackmail that continues to this day. The rapid growth of social media usage, dating websites and presumed anonymity of the internet have seen it branch out into multiple forms.

In its original manifestation, wealthy married businessmen, politicians and other lucrative targets were approached by a woman allegedly seeking romantic companionship. Once she compromised the target, she would extort him for money by threatening to expose photographs or other evidence of the indiscretion.

The tactics have changed, and the consequences of exposure have broadened, but the game has remained the same. In our digital era, this sweetheart scam is often referred to as 'catphishing'. Most often these scams begin on dating websites or via phishing emails from secret admirers.

To paraphrase the old maxim, don't trust emails and verify. On a personal level, you should learn to trust your intuition and use your emotions to trigger verification, not susceptibility. If it's too good to be true, it probably is.

Consider the scope of this digital goldmine for criminals. The criminals certainly have. According to Marketdata Enterprise, Inc., 10% of free online dating accounts are opened by scammers.[1] Maybe worse is the elevated risk of compromise. MSNBC research shows that 11% of people using dating services are married.[2]

And we would be remiss if we didn't point to the growing links between cyber and physical crime. Each year, internet predators commit more than 16,000 abductions, 100 murders and thousands of rapes, according to InternetPredatorStatistics.com.[3]

When the potential consequences are this dangerous, we should drop the notion that cybercrime is strictly a technology issue.

Anti-phishing best practices

The examples we've examined are just a handful of the social engineering cons that have evolved to plague us today. Because compromising the human is the strategy behind 90% of all data breaches and many other cybercrimes, consumers and businesses alike need to hone the skills to recognise, avoid and report these transgressions – as seriously as they approach so-called real-world crimes.

To avoid being victimised by pig in a poke, check the bag *before* you buy. The same is true for the badger game and all online or email-based scams. To paraphrase the old maxim, don't trust emails and verify. On a personal level, you should learn to trust your intuition and use your emotions to trigger verification, not susceptibility. If it's too good to be true, it probably is.

And because the impacts of cybercrime reach beyond the individual, businesses can and should consider the role they play in helping expose the nature of the most common scams and active threats to their clients and users.

In other words, let's develop some social street smarts.

A key strategy: training users to recognise and report phishing. And the best way is to simulate phishing emails, so a company's users can experience these scams in a safe environment, where the only cost of failure is an opportunity to learn. Following are some best practices:

- Phishing simulations should model actual scams and attacks.
- These simulations should utilise a strong emotional driver, such as curiosity, urgency or reward, to help users learn to examine their gut responses to emails – to *verify* them before they respond.
- When scams are difficult to recognise, repetition can and should be used to drive the development of new habits.
- Everyone should be trained to report suspicious emails and remove downstream exposure to other potential victims.
- Security and policing organisations should turn their focus to analysing active threats and response capabilities in real time.

As in the past, avoiding scams, exposures and financial loss starts with emotional control. Organisations – collections of human beings – should focus on securing their people. It's the best way for people today to avoid yesterday's mistakes. □

1, 2 and 3 sourced from https://www.phactual.com/16-scary-statistics-of-online-dating/

John 'Lex' Robinson is Anti-Phishing Security Strategist at Cofense (formerly PhishMe).

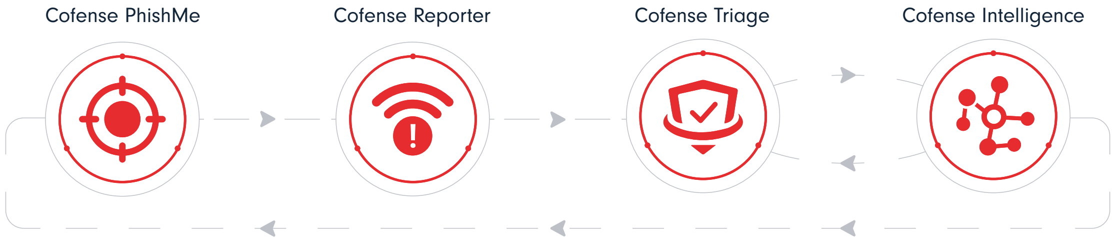
For more information, please visit **www.cofense.com**

COFENSE

PHISHME® is now COFENSE

Visit our stand to learn how Cofense™ combines real-time attack intel sourced from your employees with best-in-class incident response. Stop attacks in progress to stay ahead of breaches.

CONDITION EMPLOYEES
To Recognise and Report Threats



SPEED INCIDENT RESPONSE
Collect, Analyse, and Respond to Verified Active Threats

Voice and the future of personal identification

Despite the more general upward trend of data breaches and sophisticated cross-channel attacks, businesses have mostly remained stagnant when approaching phone channel security.

Pindrop reports

With physical and online information security always growing stronger and harder to crack, fraudsters gravitate toward the weakest link in your security – your contact centre and voice channels. For many years, we have shown that fraudsters increasingly exploit the phone channel; fraud rates continue to increase every year, and this year is no different.

Between 2016 (1 in 937 calls) and 2017 (1 in 638 calls), the overall voice channel fraud rate increased by 47%, continuing on the upward trend from last year's 113% increase. From 2013 through 2017 we have seen the fraud rate climb over 350%, with no signs of slowing down.

The costs of this are significant, both for businesses and consumers. Consumers lose $12bn a year to phone-based ID theft in the US, while for businesses this rises to $14bn. It's also worth noting that these costs represent just the amount affected by fraud activity over the phone; as voice-activated smart devices continue to come online – nearly one in five U.S. adults today have access to a smart speaker – the opportunity to abuse the voice channel for fraudulent purposes is growing rapidly and potentially much larger than it currently is today.

Stagnant voice channel security

Despite both this increase in the rate of attacks and the more general upward trend of data breaches and sophisticated cross-channel attacks, businesses have mostly remained stagnant when approaching phone channel security. Identity verification still largely relies on easily accessible KBA questions such as asking for your mother's maiden name – even though this is now readily available information on the dark web. 'Something you know' questions are no longer secure when more than one person has the same information.

> Even for organisations that have implemented some form of advanced authentication with positive voice bio or one-time passwords, there are fraudsters at the ready to either socially engineer the call back to KBAs or will have tactics on-hand to overcome them.

Yet many organisations use KBA questions out of ease and habit. Even for organisations that have implemented some form of advanced authentication with positive voice bio or one-time passwords, there are fraudsters at the ready to either socially engineer the call back to KBAs or will have tactics on-hand to overcome them:

- *Imitation:* An attacker may try to impersonate the legitimate speaker or disguise themselves to escape a positive identification

- *Replay attack:* A fraudster simply records the target victim's voice such as getting on the phone with them for a few moments or even looking up a video online where they may be speaking. With a replay attack, there is no need for social engineering or imitation, and the quality of the voice can be quite high depending on how the fraudster acquired the voice sample

- *Voice modification software:* This is software that converts a fraudster's voice to match their victim's voice through the use of features such as electronic pitch control.

- *Voice synthesis software:* In an era of 'fake news', voice synthesis is raising ethical concerns over how easy it becomes to imitate a human voice. Lyrebird just needs a few minutes of audio to recreate a voice avatar. Obviously, fraudsters will take advantage of software such as this to create near-accurate versions of a victim's voice.

A new wave of authentication technology

However, technology can also be the solution to this as well as the problem. It is possible to accurately identify individuals using voice data, a capability which can be applied to keeping private information secure and an area in which Pindrop has been developing a product suite since its foundation in 2011. This is done by utilising the full range of data contained within audio files of a human voice. This data is not just a simple replication of a voice; it contains information about the natural behaviour of our voices, as well as metadata, such as the location of the user attempting to gain access. Implementing security that utilises all of this available information,

We are entering an era in which voice is soon to be the de-facto method for engaging with our technology. Within five years, 25% of businesses in the UK will be using voice-activated technology for all of their customer communications.

rather than simply checking the surface layer voice for a match – a method which is easily conned – will help voice become a much more secure biometric channel than it currently is. Pindrop's proprietary technology has been leading the way in this space.

- *Phoneprinting™:* technology that analyses the full audio of a phone call to determine its true characteristics, helping call centres identify malicious behaviour and verify legitimate callers. More than 1,300 audio features are checked, creating a distinct telephony profile that involves geo-location, device type and carrier data.
- *Deep VoiceTM Biometric Engine:* Pindrop's proprietary deep neural network speaker recognition system, it runs throughout the lifecycle of a call, from IVR to agent, identifying and analysing repeat callers. Every caller's voice presents unique acoustic and behavioural features. Pindrop analyses these unique signals, extracted from short utterances of a caller's speech to develop a unique voiceprint for each caller that can be used to authenticate callers more securely and in less time.

The future of voice

However, it is not just the security benefit that such technology provides. Running in the background of every call, such systems offer friction-free voice analysis to authenticate legitimate callers and identify fraudsters. 'Friction-free' is the key word here. We are entering an era in which voice is soon to be the de-facto method for engaging with our technology. Within five years, 25% of businesses in the UK will be using voice-activated technology for all of their customer communications. Amazon's Alexa already has a number of banking skills on its platform and voice is becoming a key part of multi-factor authentication.

Voice will also not be limited to private transactions; Asos has recently announced voice shopping through Google's Assistant, taking advantage of a market sector predicted to be worth £40bn by 2020. Devices such as door locks are beginning to use biometric information instead of keys and car manufacturers are building voice-activated dashboards to create truly hands-free driving experiences. It doesn't take too much of an imagination to picture a future in which most of our interactions with devices are voice-based; checking into a flight or hotel, asking a sat-nav for directions, ordering groceries online.

This means that our full immersion into the voice channel may be just getting started. But this proliferation of voice technologies will continue to put consumers' security and identity at risk. Currently, fraudsters can easily get around existing authentication methods. As businesses adopt the latest voice technologies for the majority of customer interactions, there will be a parallel need for top-notch security. □

Pindrop is the trusted voice anti-fraud and authentication provider of choice for the largest organisations across the globe. Our customers include global Fortune 500 enterprises, who have partnered with us to provide the safest voice ecosystem for consumers. Whether voice engagements occur through the call centre or the next generation of voice assistants, Pindrop is committed to securing every voice interaction.

For more information, please visit
www.pindrop.com
or email info-emea@pindrop.com

pindrop

Healthcare beware: crypto-mining, malware, and IoT attacks

The healthcare industry is increasingly being targeted by advanced cyber-attacks.

Dave Palmer reports

In the past year, the healthcare industry has been increasingly targeted by advanced cyber-attacks. While a marked rise in medical IoT devices has allowed healthcare companies to become much more efficient, this increase has also opened new avenues for threat actors attempting to infiltrate their networks.

Medical staff now carry multiple connected devices with them, including personal devices that lack appropriate security controls. Confidential patient records and life-critical medical systems run an increased risk of being compromised, and the sensitive nature of the information they contain could impact patient safety and hospital reputation. Financially, healthcare companies are also at greater risk: according to a study by the Ponemon Institute, lost or stolen healthcare records can cost up to 136% more than data breached in other industries.

Going for gold

Towards the end of last year, we observed a noticeable spike in the number of crypto-mining infections within the healthcare sector. In December 2017 alone, the number of crypto-malware attempts on healthcare customers' systems was 800% higher than in the six months prior and following.

Whilst healthcare companies have always been the target of malware infections, the sudden increase in crypto-malware was significant. This could be attributed to the price of Bitcoin and similar cryptocurrencies skyrocketing around the same time. As their price has now fallen, so have the crypto-mining attempts.

Breaking through Windows

Although 2018 brought with it a decrease in crypto-mining attempts, the healthcare sector experienced an increase in active malware infections captured by sinkhole domains. The infections were varied, with no bias towards botnets, trojans, or ransomware, but were almost entirely united in that the threat actors widely targeted outdated Windows operating systems.

> The risks of the EternalBlue SMB vulnerability are now well known. However, as learnt in the aftermath of WannaCry, entire NHS trusts are also susceptible to other unpatched Windows 7 vulnerabilities.

The risks of the EternalBlue SMB vulnerability are now well known. However, as learnt in the aftermath of WannaCry, entire NHS trusts are also susceptible to other unpatched Windows 7 vulnerabilities, including those that facilitate remote code execution and privilege escalation – prime pickings for any malware that successfully enters a system.

Hiding in plain sight

A private medical institution recently trialled Darktrace's Enterprise Immune System technology through a Proof of Value. Darktrace immediately discovered that an AXIOS spectrometer, a medical IoT device for characterising materials using x-ray, had been compromised. It had breached hundreds of models, many of a potentially serious nature. The device was continuously making outbound SSH connections to rare external IP addresses, transferring over 1GB of data a week.

Further analysis determined that the compromised medical device was being used to send large volumes of outbound spam mail, resulting in the medical institution's external IP address being blocked by spam filters. Effectively classified as a sender of junk mail, emails from the medical institution risked falling into recipients' trash or not being received at all – anything from appointment updates, to the results of cancer scans. Faith in the institution's ability to handle patient data and uphold its duty of care could have been severely undermined, risking its reputation among prospective patients and service providers.

Likely C2 beaconing was also noted from this device, indicating that it might have been part of a wider botnet, or network of compromised devices being used to propagate malicious spam malware. On further investigation, at least one of the HTTP connections was to a server utilised within cryptocurrency exchange and bitcoin activity, which suggests a crypto-mining malware presence. The institution's security team were advised immediately. The device was then isolated, giving the team precious time to conduct further investigation.

As threat actors are continually employing novel methods to compromise a network, a growing number of healthcare companies are now having to play catch-up in a fast-evolving threat landscape.

What next?

The healthcare sector is a clear target for threat actors, especially considering the wealth of sensitive data such networks safeguard, and the security holes left open in the challenge to continuously maintain and patch highly complex and distributed networks. WannaCry and Petya ransomware were unlikely to have been the last aggressive attacks that successfully exploit such vulnerabilities.

Insider threat is also manifest in healthcare networks. User compliance problems are prevalent, for example, there is a sizable use of Tor as the preferred VPN, widespread use of BitTorrent, and a high volume of illicit uploads to cloud storage services.

Darktrace's technology has the unique ability to detect and respond to in-progress cyber-attacks that would ordinarily bypass traditional security tools. As threat actors are continually employing novel methods to compromise a network, a growing number of healthcare companies are now having to play catch-up in a fast-evolving threat landscape. □

Dave Palmer is Director of Technology at Darktrace.

Darktrace is the world's leading AI company for cyber defence. Created by mathematicians, the Enterprise Immune System uses machine learning and AI algorithms to detect and respond to cyber-threats across diverse digital environments, including cloud and virtualised networks, IoT and industrial control systems.

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

DARKTRACE

Global financial firm reduces risk of third-party breach with BitSight Security Ratings

A leader in commercial banking, this global financial services firm is no stranger to security risk.

BitSight reports

Recognised as an early adopter of risk management and security best practices for their industry, they were confident that their own security risk was being vigilantly managed. However, avoiding breach through a third party was an area of significant concern.

The challenge

Sharing sensitive data with thousands of partners around the world, ranging from small businesses to multi-national institutions, the vendor risk management team had their work cut out for them. The organisation followed industry standards for assessing the security risk of their third-party business relationships, which included annual questionnaires and audits, with more frequent assessments and additional testing for more critical partners. However, this amount of insight was not enough to enable the level of risk-based decision making the organisation made in other areas of their business.

As the Head of Global Vendor Risk Management explained, these assessments presented many weaknesses. Primarily, the responses to these questionnaires were rarely an indicator of actual risk and did nothing to highlight which partners presented the most risk to the organisation. In some cases, he described the responses as being ‘aspirational’, and he lamented the amount of time his team spent crafting better questionnaires in order to try and gather more insight into the security postures of their business partners.

The solution

BitSight Security Ratings for Third-Party Risk Management delivers timely, data-driven analysis of a partner’s security effectiveness. Unlike labour-intensive self assessments and questionnaires, BitSight’s SaaS offering continuously analyses, rates, and monitors companies’ security postures, all from the outside. New ratings are generated on a daily basis, giving organisations continuous visibility into the security of their assets. This empowers organisations to manage risk based on evidence of their partners’ current security postures, instead of subjective responses to point in time questionnaires.

The result

BitSight’s automated, evidence-based solution immediately demonstrated its value to the team. The outside-in approach provided an unprecedented amount of insight, enabling the organisation to focus resources where they were most needed as risks emerged. The ability to continuously monitor the security posture of third-party networks meant that they could quickly assess trends and see which partners presented the most concern based on the organisation’s business objectives.

> An unanticipated benefit, the team was also pleased to see which organisations were performing well and to be able to monitor for positive security trends.

Knowing which partners required deeper investigation allowed the team to spend less time developing and analysing questionnaires and more time working with their partners to improve their security effectiveness.

An unanticipated benefit, the team was also pleased to see which organisations were performing well and to be able to monitor for positive security trends. This changed the tone of conversations they could have with their partners and fostered better business relationships. Most significantly, BitSight Security Ratings for Third-Party Risk Management identified points of risk in partner networks that the questionnaires were not designed to catch, proving its use as an important tool for mitigating third-party security risks. □

BitSight Technologies is a private company based in Cambridge, MA. Founded in 2011, BitSight is backed by Menlo Ventures, Globespan Capital Partners, Flybridge Capital Partners, Commonwealth Capital Ventures, and the National Science Foundation.

For more information contact us at:

BitSight Technologies
125 Cambridge Park Drive
Suite 204
Cambridge, MA 02140
www.bitsighttech.com
sales@bitsighttech.com

BITSIGHT®
The Standard in SECURITY RATINGS

Forthcoming events

e-crime & cybersecurity FRANKFURT 23rd January 2019 Frankfurt	PCI LONDON 24th January 2019 London	SECURING THE LAW FIRM 24th January 2019 London	e-crime & cybersecurity CONGRESS 5th & 6th March 2019 London
e-crime & cybersecurity CONGRESS 19th March 2019 Dubai	e-crime & cybersecurity FRANCE 4th April 2019 Paris	e-crime & cybersecurity GERMANY 18th June 2019 Munich	PCI LONDON 3rd July 2019 London
e-crime & cybersecurity CONGRESS 17th September 2019 Abu Dhabi	SECURING THE LAW FIRM 19th September 2019 London	e-crime & cybersecurity MID-YEAR 17th October 2019 London	SECURING ONLINE GAMING 17th October 2019 London
e-crime & cybersecurity SCOTLAND 12th November 2019 Edinburgh	e-crime & cybersecurity SPAIN 21st November 2019 Madrid	e-crime & cybersecurity NORDICS 27th November 2019 Stockholm	e-crime & cybersecurity BENELUX 3rd December 2019 Amsterdam

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

Sponsors and exhibitors

Cofense | Strategic Sponsor

Cofense™, formerly PhishMe, is the leading provider of human-driven phishing defence solutions worldwide. Our collective defence suite combines best-in class incident response technologies with timely attack intelligence sourced from employees. Cofense enables thousands of global organisations to stop attacks in progress faster and stay ahead of breaches.

For more information, please visit www.cofense.com

CrowdStrike | Strategic Sponsor

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionised endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), and a 24/7 managed hunting service – all delivered via a single lightweight agent. The CrowdStrike Falcon™ platform, certified to replace legacy antivirus, has reinvented how endpoint security is delivered with its industry-leading, cloud native architecture. CrowdStrike Falcon protects customers against advanced cyber-attacks, using sophisticated signatureless artificial intelligence/machine learning and Indicator of Attack (IOA) based threat prevention to stop known and unknown threats in real-time. Core to its innovative approach is the CrowdStrike Threat Graph™, which analyses and correlates over 27 billion events per day from millions of sensors deployed across more than 170 countries, uniquely providing crowdsourced protection for the entire customer community.

Many of the world's largest organisations already put their trust in CrowdStrike, including three of the 10 largest global companies by revenue, five of the 10 largest financial institutions, three of the top 10 health care providers, and three of the top 10 energy companies.

CrowdStrike was founded by George Kurtz, former McAfee CTO and author of the best-selling 'Hacking Exposed' series, with former McAfee VP of Threat Research Dmitri Alperovitch. The company has received numerous accolades, including being named Pioneer of the Year by World Economic Forum and making Forbes list of America's Most Promising Companies. CrowdStrike has secured $156 million in funding from A-list investors including Google Capital, Rackspace, Accel Partners, and Warburg Pincus.

For more information, please visit www.crowdstrike.com

Darktrace | Strategic Sponsor

Darktrace is the world's leading AI company for cyber defence. Created by mathematicians, the Enterprise Immune System uses machine learning and AI algorithms to detect and respond to cyber-threats across diverse digital environments, including cloud and virtualised networks, IoT and industrial control systems. The technology is self-learning and requires no set-up, identifying threats in real time, including zero-days, insiders and stealthy, silent attackers.

Darktrace is headquartered in San Francisco and Cambridge, UK, and has over 30 offices worldwide.

For more information, please visit www.darktrace.com

Duo Security | Strategic Sponsor

Duo Security helps defend organisations against data breaches by making security easy and effective. Duo Beyond, the company's category defining zero-trust security platform, enables organisations to provide trusted access to all of their critical applications, for any user, from anywhere, and with any device.

The company is a trusted partner to more than 10,000 customers globally, including Dresser-Rand, Etsy, Facebook, K-Swiss, Random House, Yelp, Zillow, Paramount Pictures, and more.

Founded in Michigan, Duo has offices in Ann Arbor and Detroit, as well as growing hubs in Austin, Texas; San Mateo, California; and London, UK.

For more information, please visit duo.com

Endace | Strategic Sponsor

Endace's multifunctional Analytics Platform can host 3rd-party network analytics applications while simultaneously recording a 100% accurate network history, providing definitive evidence for investigating cybersecurity threats, quantifying data breaches and analysing network or application performance problems.

Deploying a dedicated Analytics Platform enables agile deployment of analytics functions on-demand and dramatically reduces OPEX and CAPEX costs by consolidating datacentre hardware. Hosted analytics applications can analyse live traffic at full line rate, or use Playback to analyse historical traffic for powerful, back-in-time analysis.

Global customers include banks, hospitals, telcos, broadcasters, retailers, web giants, governments and military.

For more information, please visit www.endace.com

Pindrop | Strategic Sponsor

Pindrop is the trusted voice anti-fraud and authentication provider of choice for the largest organisations across the globe. Our customers include global Fortune 500 enterprises, who have partnered with us to provide the safest voice ecosystem for consumers. Whether voice engagements occur through the call centre or the next generation of voice assistants, Pindrop is committed to securing every voice interaction.

With over $14b in annual fraud loss attributed to the phone channel, and over $8b wasted on ineffective authentication, it's clear that voice is natively insecure. Pindrop® Panorama was developed as a single platform for passive, multi-factor authentication and fraud detection to reestablish confidence in the voice channel. Today, Panorama applies authentication and fraud intelligence to over 650m calls per year. Pindrop's unique architecture allows the platform to analyse customer calls before they reach a call centre, and continues to identify legitimate and fraudulent engagements throughout the entire lifecycle of the call, including the IVR and agent.

Pindrop's authentication solutions, runs in the background of every call, combining patented Phoneprinting^{TM} technology, voice biometrics, and behavioural analytics to determine if a caller has the right device, voice, behaviour, and CLI to access an account.

Pindrop's anti-fraud solution, Pindrop® Protect, analyses thousands of indicators of anomalous behaviour across the fraud event lifecycle – from CLI spoofing and account mining in the IVR to social engineering attacks against agents.

Pindrop's multi-factor solutions use every facet of a call – audio, voice, and metadata – to provide risk scores and unique prints using Deep Voice™ biometrics along with Phoneprinting™ and Toneprinting™ technologies. These technologies, used in concert with machine learning and a consortium of 650 million phone calls per year, allows Pindrop solutions to provide highly accurate and unrivaled results.

For more information, please visit www.pindrop.com

Recorded Future | Strategic Sponsor

Recorded Future delivers the only complete threat intelligence solution powered by patented machine learning to lower risk. We empower organisations to reveal unknown threats before they impact business, and enable teams to respond to alerts 10 times faster. To supercharge the efforts of security teams, our technology automatically collects and analyses intelligence from technical, open, and dark web sources and aggregates customer-proprietary data. Recorded Future delivers more context than threat feeds, updates in real time so intelligence stays relevant, and centralises information ready for human analysis, collaboration, and integration with security technologies. 91% of the Fortune 100 use Recorded Future.

For more information, please visit www.recordedfuture.com

BitSight | Education Seminar Sponsor

BitSight Technologies is transforming how companies manage information security risk with objective, evidence-based security ratings. The company's Security Rating Platform continuously analyses vast amounts of external data on security behaviours in order to help organisations manage third-party risk, benchmark performance, and assess and negotiate cyber-insurance premiums.

For more information, please visit www.bitsighttech.com or follow us on Twitter (@BitSight)

Cloudflare | Education Seminar Sponsor

Cloudflare, Inc. is on a mission to help build a better internet. Today, the company runs one of the world's largest networks that powers more than 10 trillion requests per month, which is nearly 10% of all internet requests worldwide. Cloudflare protects and accelerates any internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all traffic routed through its intelligent global network, which gets smarter with each new site added. As a result, they see significant improvement in performance and a decrease in spam and other attacks.

Cloudflare was recognised by the World Economic Forum as a Technology Pioneer, named the Most Innovative Network & Internet Technology Company for two years running by the Wall Street Journal, and ranked among the world's 50 most innovative companies by Fast Company. Headquartered in San Francisco, CA, Cloudflare has offices in Austin, TX, Champaign, IL, New York, NY, Washington, DC, London, and Singapore.

For more information, please visit www.cloudflare.com or follow us on Twitter (@cloudflare)

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.

For more information, please visit digitalguardian.com

foreseeti | Education Seminar Sponsor

foreseeti has harnessed the power of a computer assisted design (CAD) based approach to analyse the cybersecurity of an IT system. Their state-of-the-art product, securiCAD®, can be used to model an IT system before or after it has been built. From the model, it can automatically develop an attack graph showing all possible attacker paths through the model. Attack paths can be visualised showing each attack step and the defences that a successful attacker would need to defeat. securiCAD can help analysts understand the capabilities required of a successful attacker and to select the best options to defeat them. Managers, directors and regulators with cybersecurity responsibilities can set meaningful numerical targets for the cybersecurity of sensitive data. The targets can be based on the expected time for a hypothetical, skilled attacker to compromise the data.

The history of securiCAD relates back to cybersecurity and system architecture research at KTH, the Swedish Royal Institute of Technology. For many years, prototypes of cybersecurity assessment formalisms and tools were developed under the name of the Cyber Security Modelling Language and the Enterprise Architecture Analysis Tool, along with a wealth of research papers. foreseeti was founded in 2014 to commercialise the research and consists of a dynamic, dedicated team of highly qualified academics, seasoned security experts, experienced business professionals and skilled developers. It has received awards as one of Sweden's most promising tech start-up companies.

For more information, please visit www.foreseeti.com

Ground Labs | Education Seminar Sponsor

Ground Labs is a global leader in sensitive data discovery through the development of our security and auditing software. Our software is used to perform cardholder and sensitive personal data discovery on computer systems worldwide, helping companies prevent security breaches that result in the theft of customers' personal information, credit and debit card numbers.

Ground Labs software is being used by more than 2,500 organisations across 80 countries to find unsecured sensitive data on their systems; securing their data with our products helps them comply with important global information security standards such as the PCI DSS and the General Data Protection Regulation (GDPR).

At Ground Labs, we are committed to continually maintaining high levels of customer satisfaction, we provide solution oriented technical support across multiple time zones.

For a free trial, visit www.groundlabs.com

Our software products include:

Enterprise Recon

Enterprise Recon is the complete solution for the identification, remediation and monitoring of sensitive personal data across your entire network. We find more data types and support more platforms than anyone else. Using in-built scheduling and real-time alert features, keeping your data secure will become just another one of your company's Business-As-Usual practices.

- *Search* all the major locations personal data might be stored including, databases, documents, emails, deleted files, memory, disks, shadow files, cloud storage, servers and more.
- *Find* over 200 personal identifiable data types including 110 relevant to the GDPR. The software identifies stored bank account numbers, SWIFT codes, IBAN. Over 50 types of National ID supported across 28 EU countries.
- *Support* 7 different platforms – Windows, Mac, Linux, Solaris, FreeBSD, HPUX, and IBM AIX. In addition to this, we also support EBCDIC mainframe storage formats.
- *Remediate* We help you take action to secure the information found. Our remediation process includes permanently deleting the data so it's unrecoverable, safely relocating the information to a secure location of your choice or modifying the data so that anything sensitive is removed without impacting the surrounding data.
- *Monitor* through powerful reporting, quickly see where the sensitive data is stored and what departments or teams have access to it.

Card Recon

Card Recon is the leading cardholder data discovery tool for PCI compliance. Card Recon will accurately search servers, workstations, file shares, email, databases, cloud storage and many more locations for cardholder data storage using a simple and easy to use interface.

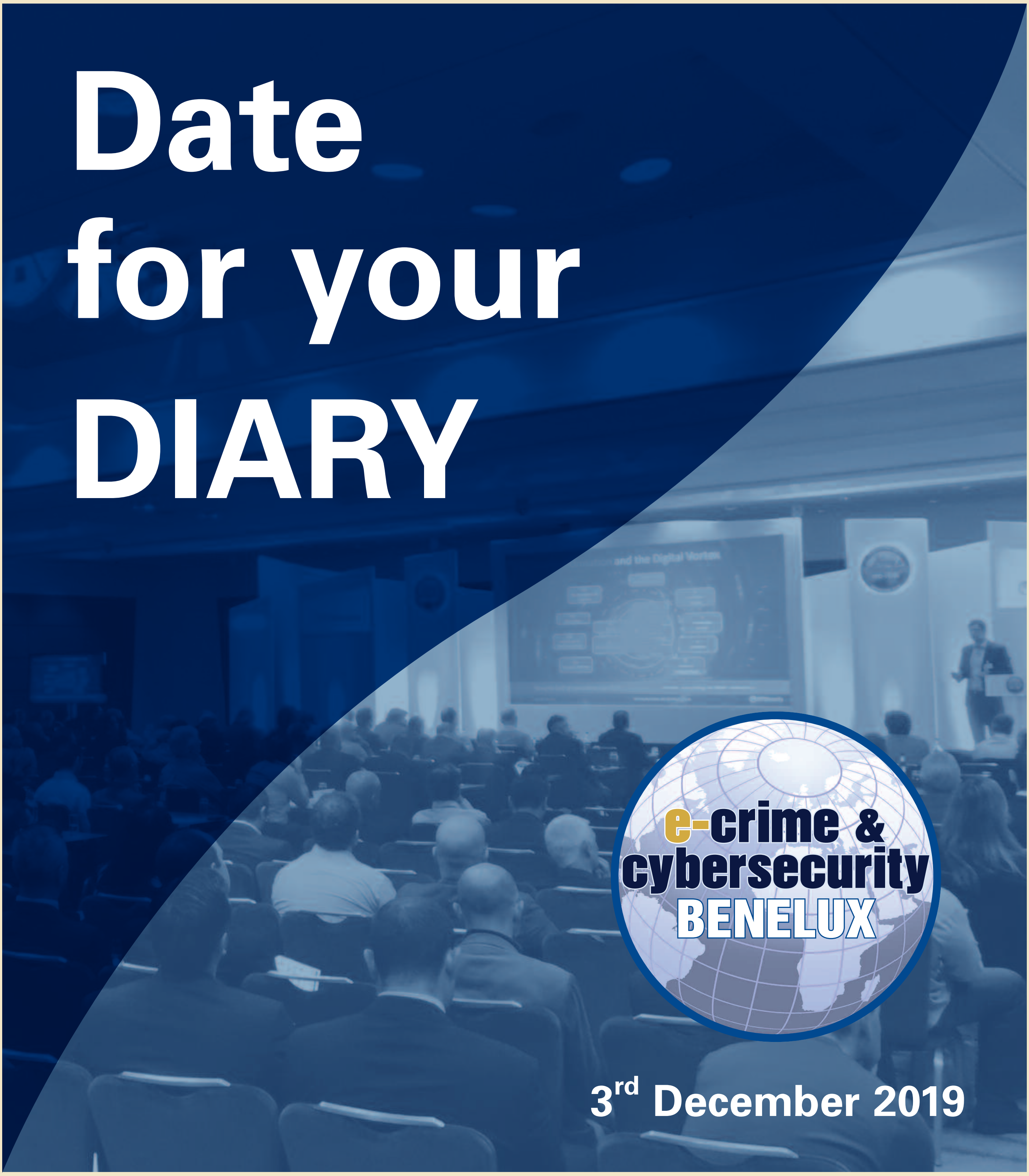
Once a search is complete the solution provides powerful data classification and PCI remediation actions to eliminate any non-compliant storage found.

Used and recommended by over 300 PCI QSAs globally, Card Recon offers an affordable and fast way to reduce PCI compliance risk whilst avoiding the likelihood of a cardholder data breach.

ThreatMetrix | Education Seminar Sponsor

ThreatMetrix®, a LexisNexis Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymised user identities, ThreatMetrix ID™ delivers the intelligence behind 100 million daily authentication and trust decisions, to differentiate legitimate customers from fraudster.

For more information, please visit www.threatmetrix.com



AGENDA

08:00	Breakfast networking and registration
08:50	Conference welcome
09:00	**Cybersecurity: the investor's priority** **Vera Krückel,** Trend Researcher, Trends Investing Equity Team, Robeco • Truths from one of the largest global investors and asset managers • Cybersecurity as a risk indicator for investors • Cybersecurity as an investing opportunity • Combining risk and opportunities
09:20	**Disrupting the disrupters: how are we doing?** **David Janson,** VP Sales, UK & Europe, Cofense • The latest threat and phishing attack data – and what to expect in the future • Compare industry benchmarking susceptibility and resilience to active phishing attacks • Best practices to protect your organisation against phishing
09:40	**The importance of philosophy to establish a vigilant information security culture** **Owais Ahmed,** Chief Information Security Officer, Kyocera Document Solutions, and **Fraz Rasool,** Head of Internal Control EMEA, Kyocera Document Solutions • How Kyocera's philosophy impacts human behaviour • Tone at the top: how everyone's responsibility for information security is given from a top-down approach • Practically measure information security performance on the basis of Kyocera's philosophy
10:00	**Hacking exposed: lessons learnt in responding to the fight against malicious behaviour** **Ronald Pool,** Senior Sales Engineer, CrowdStrike • See what advanced tactics, techniques & procedures nation-state and organised e-crime hackers have been using recently • Learn how you can detect and arm your organisation against these threats • Learn which tools you probably already have unused in your organisation to help you harden your stance against these attacks
10:20	**Education Seminars | Session 1** **See pages 28 and 29 for more details** **Cloudflare** **Security: the serverless future** **Olga Skobeleva,** Solutions Engineer, Cloudflare **ThreatMetrix** **Digital identities, social engineering and mule networks** **Dr. Stephen Topliss,** VP of Products, ThreatMetrix
11:00	Networking and refreshments break
11:30	**Intelligence-based cybersecurity** **Gal Messinger,** Head of Global Security, Philips Lighting • Why do we need cyber-threat intelligence in a commercial entity? • What exactly is cyber-threat intelligence? • Where should we position it in a company? • Who should be running it? • A use case
11:50	**Beyond security: zero trust – making the perimeter less lonely** **Richard Archdeacon,** Advisory CISO, Duo Security • Concept of zero trust or the BeyondCorp model • Why a zero trust model will reduce risk • Key elements in implementing a zero trust approach
12:10	**A new era of cyber-threats: the shift to self learning, self defending networks** **Elisabeth Entjes,** Account Manager, Darktrace • Leveraging AI algorithms to defend against advanced, never-seen-before, cyber-threats • How new immune system technologies enable you to pre-empt emerging threats and reduce incident response time • How to achieve 100% visibility of your entire business including cloud, network and IoT environments • Why automation and autonomous response is enabling security teams to neutralise in-progress attacks, prioritise resources, and tangibly lower risk • Real-world examples of subtle, unknown threats that routinely bypass traditional controls

AGENDA

12:30 **Fast and accurate issue resolution**

Sandrine Kubach, Enterprise Account Manager, Endace, and **Rob Earley,** Senior Pre-Sales Engineer, Endace

- The cost of network and security issues
- Being prepared for a potential breach
- The various approaches to breach detection
- Using the right tools for the job

12:50 **Education Seminars | Session 2** **See pages 28 and 29 for more details**

BitSight	Ground Labs
How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal) **Lennart Pikaart,** Sales Director – Benelux, BitSight	**Standards don't bother me – all I want is your data!** **Matt Jennings-Temple,** Digital Marketing Manager, Ground Labs

13:30 Lunch and networking

14:30 **GDPR and the Internet Of Medical Things**

Ferdinand Uittenbogaard, GDPR Specialist, Ministrie van Defensie, and
Conrad Veerman, Data Protection Officer, Ministrie van Defensie

- The Internet of Things, particularly the Internet of Medical Things, can prove valuable for both employers and employees, yet there are significant risks associated with such devices
- IoT brings challenges for privacy by design and GDPR
- How we can make sure that organisations and employees benefit from such devices, whilst also staying safe and secure?

14:50 **Authentication and security at the speed of conversation**

Vijay Balasubramaniyan, Co-Founder, CEO & CTO, Pindrop

- Building a voice identify platform that authenticates customers
- Protecting you from fraudsters
- Building new customer experiences
- The emergence of the conversational economy

15:10 **Intelligent threat intelligence: how machines are learning the language of the dark web**

Chris Pace, Technology Advocate, Recorded Future

- The impact of the threat intelligence language barrier
- How machines can be taught to read and understand references to cyber-threats from the dark web and other sources
- The places where humans and machines can combine to form superhuman security analysts
- What predictive analytics are, and how the future is forecasting where the next threat is coming from

15:30 **Education Seminars | Session 3** **See pages 28 and 29 for more details**

Digital Guardian	foreseeti
How to run a successful DLP programme **David Mole,** Strategic Technical Manager – EMEA , Digital Guardian	**Threat modelling: the challenge in managing risk of both structural and technical vulnerabilities** **Jacob Henricson,** Senior Risk Management Advisor, foreseeti

16:10 Networking and refreshments break

16:30 **Business security advisory: from 'no' to 'know'**

Benessa Defend, Business Security Advisory Manager EU, Ahold Delhaize

- Providing business-centric, pragmatic security advice
- Determining the 'just right' level of security
- Ensuring that security is considered throughout the project lifecycle
- Increasing automation and adapting to agile

16:50 **A new approach to cybersecurity & risks: control your own destiny**

Muhittin Hasancioglu, Former Chief Information Security Officer, Shell

- Current reality
- What is coming towards us: technology shift, digitalisation drive, new technologies, increased threat landscape
- What is the step change that we need to be on?
- How do we get there?

17:10 Final remarks **17:15** Conference close

PCI LONDON

The 18th PCI London

24th January 2019 | London

“ I did find this event extremely well organised and all speakers and presentations were smooth and seamless. It was a pleasure to be there! I found it very thoughtful to have short seminars in between too. ”

Risk and Compliance Manager,
Wirex Ltd

“ Another great PCI event with excellent speakers from various backgrounds and industries. Thought the panel discussions were particularly thought provoking and came away with lots of food for thought. ”

Lead IT Auditor,
Camelot Group

“ Another worthwhile PCI London with plenty of insights on best practice to maintain compliance with PCI DSS as well as a look ahead to the future of payments, and emerging compliance and security benefits from AI technology. Well done. ”

Head of Information Security,
Travis Perkins

“ As a project manager new to both PCI and GDPR, I found the PCI London seminar extremely useful. The speakers were informative and educational whilst the seminars provided an insight to real-life case studies from security professionals. A thoroughly interesting day. ”

Project Manager,
The Travel Corporation

PCI 2018 sponsors included:

Strategic Sponsors

Pay360 by Capita

gemalto security to be free

SRM Smart Security, Smart Compliance.

Education Seminar Sponsors

ARMOR™

barclaycard

datadivider

Card Easy™ Keypad payment by phone From Syntec

CRYPTOMAThIC

pcipal

TOKENEX

Networking Sponsors

Aeriandi Voice Matters

blackfoot

it governance™

f5®

Infradata

RIVINGTON INFORMATION SECURITY

semafone® securing data · protecting reputations

silver lining communication innovation

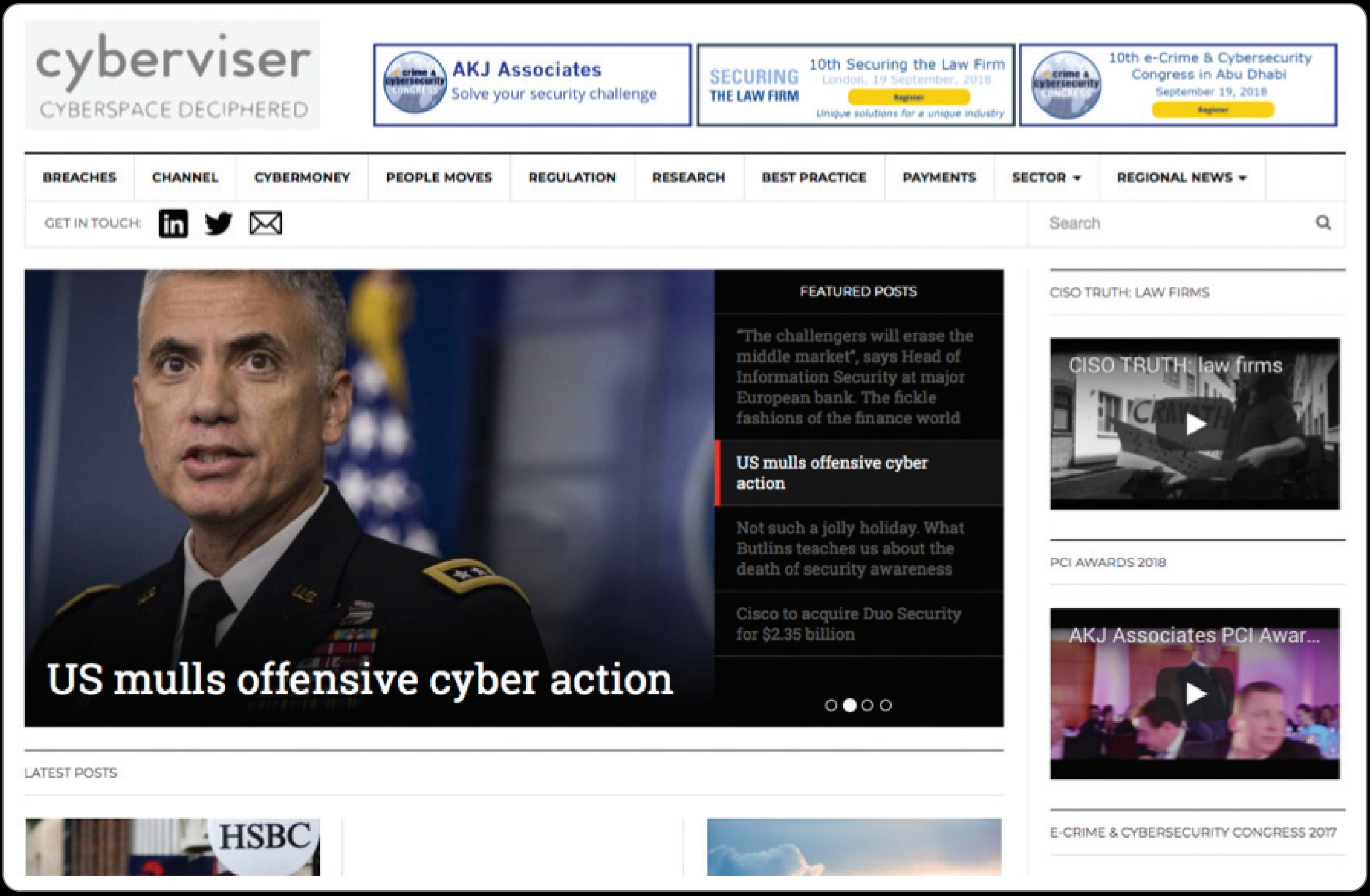
For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

www.cyberviser.com – launching now!

You know AKJ Associates for its 20-year record of market-leading conferences and events in cybersecurity and compliance. Under the e-Crime Congress, Securing the Law Firm and PCI London brands, we have consistently tried to get ahead of the trends shaping your market and careers, instead of rehashing the same old ideas.

We were first to bring CFOs and institutional investors to you, to reveal what business and stakeholders really think about cyber. We were at the forefront of understanding the collision of cybersecurity, operational risk and compliance. And we have not been afraid to confront cybersecurity's many inconvenient truths.

To expand the resources we provide to you, we are launching a website to continue our mission of delivering independent thought leadership, news and views.



"The challengers will erase the middle market", says Head of Information Security at major European bank. The fickle fashions of the finance world

US mulls offensive cyber action

Not such a jolly holiday. What Butlins teaches us about the death of security awareness

Cisco to acquire Duo Security for $2.35 billion

US mulls offensive cyber action

www.cyberviser.com will bring you:

- ✓ **Research and data:** AKJ Associates' proprietary data and conclusions gathered from security professionals around the globe. Our first project, 'Who Secures the UAE' is now live.
- ✓ **News and comment:** the most significant news stories with interpretation and comment from AKJ editors and the market.
- ✓ **Best practice:** what works and what doesn't, direct from leading end-users and security practitioners.
- ✓ **Regulation:** the latest global news on regulation and compliance, cross-sector, cross-region.
- ✓ **People:** who is firing, who is hiring and what are they paying? CISO profiles and interviews.
- ✓ **Vendors:** start-ups, funding, M&A, new solutions and new technologies.

Education seminars

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

Session 1: 10:20–11:00

Cloudflare

SESSION 1
10:20–11:00

Security: the serverless future

Olga Skobeleva, Solutions Engineer, Cloudflare

Does security have to come at a cost to performance and maintenance? Your security is only as strong as the weakest human link and their patience and diligence in following proper protocols. Serverless computing is the future of how complex software systems and their security will be designed and built.

This talk will demonstrate several migration cases that Cloudflare Workers can already help with today. Some modern hosting platforms don't give you enough access to deploy certain security features. Let's say you would like to use security headers like Content Security Policy and Strict Transport Security, manage bot traffic, or do some advanced multi-factor authentication; that can be a struggle and consume many resources in your current infrastructure. With a futuristic serverless platform like Cloudflare Workers, such solutions can be deployed in seconds.

What attendees will learn:

- Security doesn't have to cost you performance or maintenance resources
- Challenges of popular security implementations
- Serverless computing as a security tool, eg. Cloudflare Workers
- Examples: security headers, advanced multi-factor authentication, alerting, etc.

ThreatMetrix

SESSION 1
10:20–11:00

Digital identities, social engineering and mule networks

Dr. Stephen Topliss, VP of Products, ThreatMetrix

The use of digital identities in preventing fraud and enhancing customer experience in the financial industry is becoming more and more prevalent. As fraud shifts to the weakest link – the end customer – what can digital intelligence offer in combating social engineering fraud?

What attendees will learn:

- How digital identities are used today to enhance new customer acquisition on the digital channel and protect digital banking sessions for existing customers
- Specific approaches to identify the risk of social engineering based account takeover
- How a targeted approach to real-time mule account detection can enhance existing fraud prevention strategies

Session 2: 12:50–13:30

BitSight

SESSION 2
12:50–13:30

How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal)

Lennart Pikaart, Sales Director – Benelux, BitSight

Participants will see a live view into the BitSight Portal. We will demonstrate how continuous cyber-risk monitoring works for your company and the affiliates, your suppliers and peers.

What will attendees learn:

- How the cyber-risk rating can be improved in the easiest way; all risk vectors and the results will be demonstrated
- How cyber-risk for your company and the affiliates, the suppliers and peers can be managed based on qualified events and ratings

Ground Labs

SESSION 2
12:50–13:30

Standards don't bother me – all I want is your data!

Matt Jennings-Temple, Digital Marketing Manager, Ground Labs

How a business-as-usual approach to data security and performing sensitive data discovery can aid in achieving PCI and GDPR compliance:

- Insights into how cybercriminals do not comply with global security standards, data theft is their only concern
- Understanding the totality of your data helps in risk assessment for cybercrime
- Data sprawl is one of the key challenges across corporate infrastructure as it presents a huge vulnerability to cybersecurity professionals

Session 3: 15:30–16:10

Digital Guardian

SESSION 3
15:30–16:10

How to run a successful DLP programme

David Mole, Strategic Technical Manager – EMEA , Digital Guardian

Learn about DLP Project Scope and the best DLP process, including:

- Planning and requirements phase
- Deployment phase
- Use case implementation phase
- Transition phase

Learn about DLP best practices

Learn about DLP flexible deployments

Learn how to set up a DLP project with no upfront classification to effectively monitor and ensure data protection. See and understand who, what, where and how data flows through the enterprise out-of-the-box. This visibility and contextual intelligence can be used to confirm sensitive data (structured and/or unstructured) to permanently tag it so that it can be monitored and controlled throughout its complete lifecycle. By providing complete event visibility without predetermined rules, you can quickly assess all the ways uses access, use, and move data so that you can determine where it is most at risk.

foreseeti

SESSION 3
15:30–16:10

Threat modelling: the challenge in managing risk of both structural and technical vulnerabilities

Jacob Henricson, Senior Risk Management Advisor, foreseeti

Companies today are experiencing an ever-increasing connectivity and complexity of infrastructure risk management. The underlying challenge today is that infrastructures are complex and interconnected, let alone the fact that a lot is run in the cloud. With the complexity of architectures increasing, the focus on technical vulnerabilities is not enough. Traditional vulnerability scanning offers insight on technical vulnerabilities but lacks the ability to prioritise what to focus on.

That said, in general, there needs to be a more holistic approach to ensure that risk is managed in a proper way related to IT infrastructures. Using a combination of technical and structural vulnerabilities, being able to map large infrastructures in a scalable way, needs to be combined with a probabilistic approach in threat modelling, which enables organisations to focus on true risk instead of theoretical risk on a technical level.

Taking this further, and being able to focus on true business risk, requires a new approach. At the Royal Institute of Technology, extensive research has been conducted in threat modelling and the probability of a certain set of parameters to be exploited to get access to an infrastructure. Join this seminar to learn the latest of research on threat modelling from both academia and the corporate world.

What attendees will learn:

- Distinction between technical and structural vulnerabilities
- How to address the challenges in scaling traditional risk assessments and threat modelling of complex IT infrastructures with objective fact-based data
- Using research findings to perform threat modelling on large corporate IT infrastructures
- How to use threat modelling in the design process of IT infrastructures □

Speakers and panellists

e-Crime & Cybersecurity Benelux is delighted to welcome delegates, speakers and panellists. The event has attracted a large number of key names and decision-makers across industry.

Owais Ahmed

European Information Security Officer, Kyocera Document Solutions

Owais Ahmed is the European Information Security Officer at Kyocera Document Solutions. Within his role, Owais is responsible for establishing, maintaining, interpreting and communicating organisation-wide information security policies, standards and procedures across the EMEA region. He works with the business to develop an understanding of the business value and processes around each area and aligning the corporate strategy and roadmap.

Prior to his current role, Owais was working as a Senior Information Systems Auditor within KPMG's Information Risk Management Advisor Practice. He has extensive experience with working on assignments related to governance, risk and compliance and was responsible for managing the preparation of audit requisite documentation. He helped to deliver assurance and advisory services to clients in the areas of information technology, enterprise applications, business process control, IT governance, enterprise risk, information security and regulatory compliance.

Owais holds several postgraduate qualifications in cybersecurity from the University of Twente, Delft University of Technology and Technische Universität Darmstadt.

Richard Archdeacon

Advisory CISO, Duo Security

Richard is the Advisory CISO for the EMEA region. He was previously with DXC – HPE – where he was a Chief Technologist in the Security Practice working with clients across all industries and regions.

Prior to that, he worked for Symantec for many years. He has also contributed to security industry organisations such as IAAC and the IISP, and more recently worked with the World Economic Forum on a Cyber Resilience Toolkit for Board members.

Vijay Balasubramaniyan

Co-Founder, CEO & CTO, Pindrop

Vijay Balasubramaniyan is Co-Founder, CEO & CTO of Pindrop. He's held various engineering and research roles with Google, Siemens, IBM Research and Intel. Vijay holds patents in VoIP security and scalability and he frequently speaks on phone fraud threats at technical conferences, including RSA, Black Hat, FS-ISAC, CCS and ICDCS. Vijay earned a PhD in Computer Science from Georgia Institute of Technology. His PhD thesis was on telecommunications security.

Benessa Defend

Business Security Advisory Manager EU, Ahold Delhaize

Benessa Defend joined the Business Security Advisory team at Ahold Delhaize in 2017. Viewing security as a business enabler, Benessa aligns technical requirements to business needs and drives security projects that impact the global organisation. Benessa has more than 10 years of experience ranging from technical applied research to development of high-level cybersecurity strategies for multinational organisations.

Prior to Ahold Delhaize, Benessa did research and consulting in critical infrastructure security, industrial control systems, the smart grid, and implantable medical devices. Benessa has previously held roles at the European Network for Cyber Security, Deloitte, and MITRE. She has a BS and an MS in Computer Science from Austin Peay State University and the University of Massachusetts Amherst.

Rob Earley

Senior Pre-Sales Engineer, Endace

Rob Earley is a Senior Pre-Sales Engineer at Endace. Rob has over 30 years' experience of computer networking, including 10 years within the cybersecurity and threat management environment. Currently his role covers the EMEA region, where he deals with many different types of customers, including retail, financial, trading, legal, pharmaceutical, and service providers.

Elisabeth Entjes

Account Manager, Darktrace

Elisabeth Entjes is an Account Manager at Darktrace. A graduate from the University of Amsterdam, Elisabeth joined Darktrace last year to set up the BeNeLux office in Amsterdam. She has worked with clients across Europe delivering Darktrace's world-leading technology, and helps protect the networks of businesses across all sectors.

Muhittin Hasancioglu

Former Chief Information Security Officer, Royal Dutch Shell

Muhittin Hasancioglu is the Former Vice President of Information Risk Management & CISO at Royal Dutch Shell. Muhittin is US educated; he holds double degrees BSc in Computer Science specialised in Application Development & Design and a BA in Economics. He studied at the Erasmus Rotterdam School of Management where he successfully completed an MBA in 2001. Muhittin joined the Shell group in December 1994 as IT Manager of Shell Turkey, after eight years at Goodyear Turkey. He has 32 years of professional IT, cyber-risk & security leadership experience in roles across multiple IT disciplines and businesses within Shell and externally, with a proven track record of delivering significant business outcomes in challenging environments. He has broad experience in business IT, cyber-risk & security, technology, service delivery/operations, as well as having worked extensively with third-party services providers and joint ventures across the globe. Through this CISO role in Shell, Muhittin developed the cyber-risk & security strategy and delivered an integrated information risk management and cybersecurity agenda; including production control domain and unstructured data (information management) risk management and compliance. Muhittin is a Dutch citizen born in Istanbul, Turkey and has lived in Germany, the UK, the USA and the Netherlands.

Jacob Henricson

Senior Risk Management Advisor, foreseeti

Jacob is a Senior Risk Management Advisor at foreseeti, a Swedish company specialised in threat modelling and strategic information security management. Jacob has 15 years of experience in information security and risk management from both operational and strategic roles. Through his current and previous roles with PwC and global CISO at LM Ericsson, Jacob brings a global view on the concept of simulating attacks against IT infrastructures, and the benefits from a risk management perspective.

David Janson

VP Sales, UK & Europe, Cofense

David has 19 years' experience in software sales and sales leadership roles, of which nearly 10 years have been in the security and cybersecurity industries. During this time, he has helped many organisations to secure their employees and their data. Most recently, at Cofense, he has been showing customers how to protect their employees from human-targeted attacks.

Matt Jennings-Temple

Digital Marketing Manager, Ground Labs

Matt Jennings-Temple moved to Dublin, Ireland from Staffordshire in the UK. He studied Finance and Marketing at the University of Birmingham and proceeded to work for growth-driven organisations in finance, telecoms and utilities. Matt has brought his 20 years of experience to Ground Labs to manage their global marketing presence, helping to educate enterprise businesses around the world for the need to improve their ability to search for sensitive data within their network and comply with the global standards including GDPR, PCI, POPI and HIPAA.

Vera Krückel

Trend Researcher, Trend Investing Equity Team, Robeco

Vera Krückel is a Trend Researcher at the Robeco Trend Investing Equity Team with a focus on digitisation and demographic trends. Before joining Robeco in October 2010, she was employed by Ernst & Young as an Advisor for Financial Performance Improvements and worked in the Investment Banking division of BNP Paribas in London. She holds a master's degree in Finance from the Università Bocconi in Milan, Italy, and has extensively researched the risks and opportunities related to cybersecurity from an investment perspective. She has co-published a whitepaper on the subject (https://www.robeco.com/nl/visie/2018/06/cybersecurity-turning-threats-into-investment-opportunities.html) and will give insights into how investors look at the opportunity around investing in the cybersecurity industry, and also how Robeco looks at the risk of cybersecurity for its portfolio holdings, integrates cybersecurity into its sustainability analysis and engagement activities.

Sandrine Kubach

Enterprise Account Manager, Endace

Sandrine Kubach is the European Sales Manager at Endace. Sandrine has 15 years' experience in IT, including five years within the cybersecurity and threat management environment. Sandrine covers Europe, building on the successful collaboration with partners as well as ensuring great customer experience from existing and potential customers.

Gal Messinger

Head of Global Security, Philips Lighting

Gal Messinger is a visionary leader with over 35 years of security expertise. At STMicroelectronics, he was a CSO for 13 years, dealing with risk management, physical and logistics security, brand protection, product security, business continuity and crisis response, as well as business and competitive intelligence. Now at Philips Lighting, he is a CSO of a centralised security department that includes cyber domain.

David Mole

Strategic Technical Manager – EMEA, Digital Guardian

David Mole has specialised in data protection for 10 years, as a consumer, implementor and Sales Engineer. Before joining the Digital Guardian Sales Engineering team, David was the Technical Lead for the HP Enterprise Data Protection Practice, consulting on global data protection projects of many thousands of users over a range of technologies. David has over 20 years of experience in the IT security arena, from designing and implementing network security architectures to data protection projects that span the globe. David understands the challenges of IT security and deals with customers from a wide spectrum of industries from finance, energy, manufacturing to law and automotive.

Chris Pace

Technology Advocate, Recorded Future

Chris works for Recorded Future to engage and educate audiences on the power of intelligence-driven security, he has most recently worked editing and contributing to *The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence*. Before beginning a career in information security, Chris trained as a Broadcast Journalist and also has worked in IT departments in the public and private sectors.

Lennart Pikaart

Sales Director – Benelux, BitSight

Lennart helps BitSight clients in the Benelux transform their cybersecurity performance and the management of third-party supplier cyber-risk. He has a background in data analytics applications for risk management and facilitated companies in creating innovative solutions to improve their risk posture and prevent fraud. He is passionate about helping keep the balance between continuous learning and ironic humorous self-consciousness. In his personal life, he enjoys family life, reading and outdoor sports like mountaineering; last seen at the summit of the Matterhorn.

Ronald Pool

Senior Sales Engineer, CrowdStrike

Ronald is a frequent speaker at events, giving insights into the movements of attackers or a broader threat landscape. With over a decade of experience in cybersecurity, Ronald has advised customers on their cybersecurity challenges for several vendors as a trusted security advisor. He advises enterprises on a daily basis on their protection and detection strategies, forensics & security operations. In his role, he encounters the acts of organised hackers at a regular basis, adding to his ever growing cybersecurity context, which he enthusiastically shares with his audiences.

Fraz Rasool

Head of Internal Control EMEA, Kyocera Document Solutions

Dr Fraz Rasool is the Head of Internal Control, including governance, risk and compliance, and of export control, at Kyocera Document Solutions. Additionally, he is also in charge of developing merger & acquisition activities and the internal audit department for EMEAR. Fraz has also worked as Chief Export Control Officer and Head of Internal Audit EMEA.

Olga Skobeleva

Solutions Engineer, Cloudflare

Olga Skobeleva helps build the future of the internet as a Solutions Engineer at Cloudflare. She developed her first website at 8 years old, which was about an anime called Sailor Moon. Before getting a computer science degree in Finland she also studied law including cybercrime. Her web development experience and passion for law led her to a career as a Security Network Engineer. During her CS studies, she got the top female score in the Cisco Networking Academy 2014 CCNA NetRiders Skills Competition for Northern Europe. Along with bringing her expertise on web security and performance, she became a technical customer advocate within Cloudflare, ensuring customers' success on the Cloudflare platform.

Stephen Topliss

VP of Products, ThreatMetrix

Dr Stephen Topliss is a thought leader in fraud and digital identity, with nearly 20 years' experience working in software alongside some of the world's largest organisations in advisory and management roles. As the VP of Products for ThreatMetrix, he guides customers on defining strategies for the evolution of market-leading fraud and digital identity solutions.

Ferdinand Uittenbogaard

GDPR Specialist, Ministry van Defensie

Ferdinand Uittenbogaard is the GDPR Specialist at the Ministry of Defence Netherlands.

Prior to this, Ferdinand was the Chief Information Security Officer at the Department of Health. Here, he worked with internal and external stakeholders, compliance, risk and technology teams to improve the cybersecurity posture of the organisation, covering education of employees and partners, technology, capability and response capability. At the Ministry of Defence, Ferdinand is working on a major new project to become GDPR compliant. Ferdinand has also held roles at the National Audit Office, Randstad and Shell. He holds the CISSP and CISM certifications.

Conrad Veerman

Data Protection Officer, Ministry van Defensie

Conrad Veerman is the Data Protection Officer (DPO) for the Royal Netherlands Airforce (RNLAF). Conrad is responsible for implementation and continuous compliancy of the General Data Protection Regulation (GDPR) within the RNLAF. His aim is to strengthen and unify data protection. Conrad has 20 years of experience in information management and life cycle management of operational information systems. He is skilled in innovation management, executive data science and GDPR. □

17th e-Crime & Cybersecurity Congress

e-crime & cybersecurity CONGRESS

5th & 6th March 2019
London, UK

“I’d like to thank you for allowing me to attend. I learnt some good things from the vendors, which were my reasons for attending, i.e. to learn and understand what security products may/may not help our organisation.”

IT Security Manager, BTL Group Ltd

“This was the 2nd year I attended the e-Crime & Cybersecurity Congress and I would not miss it again. It’s a brilliant forum for getting some perspective around your security posture whilst being able to appreciate we all have the same common enemy and goals.”

IT Director, SevenC3

“The Congress overall was excellent, with a wide range of topics being covered. I was particularly impressed with the presentations on the second day and the topics that were covered, from Michael Stawasz at the US Dept of Justice covering hack back – and why we shouldn’t do it – to the view portrayed by fund investors given by David Sneyd, and for the presentation skills (as well as the content) of the presentation by Simon Wiseman.”

Head of IT Audit, Crossrail TFL

“The e-Crime & Cybersecurity Congress is one event that I try not to miss. The topics presented are relevant and of good standard. The event is also excellent for networking with people from different industries/ sectors and gaining knowledge from peers and vendors.”

IT Security & Risk Officer, UBS

2018 Congress sponsors included:

Strategic sponsors

Bitdefender

Centrify THE BREACH STOPS HERE

COFENSE

CROWDSTRIKE

DARKTRACE

DEEP SECURE

IMPERVA

InteliSecure

Menlo Security IT’S SAFE TO CLICK

MICRO FOCUS

NTT Security

SECUREDATA TRUSTED CYBERSECURITY EXPERTS

wombat security technologies

ZoneFox A FORTINET COMPANY

Education Seminar Sponsors

AGARI

ANOMALI

BITSIGHT The Standard in SECURITY RATINGS

CYBERBIT PROTECTING A NEW DIMENSION

DUO

egress

EyeOn ID

foreseeti

GROUP IB

KENNA Security

Malwarebytes

SAI GLOBAL

Skyhigh

TITUS

TREND MICRO

Networking Sponsors

THREATCONNECT.

XQ CYBER

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

A new dawn for data loss prevention

For more than 10 years, Digital Guardian has enabled data-rich organisations to protect their most valuable assets with a SaaS deployment model or an outsourced managed security programme.

Digital Guardian reports

Digital Guardian's mission is to provide ubiquitous data protection to organisations and corporations independent of the threat actor, data type, the system, application, device type or the point of access. Our unique data awareness and transformative endpoint visibility, combined with behavioural threat detection and response, provide a comprehensive security posture. We carry this data-centric security posture across the network and into the cloud thus adapting to today's borderless networks. Our customers use Digital Guardian's Data Protection Platform to secure both structured and unstructured data, everything from executive emails, to chemical formulas, to customer data. For more than 10 years, Digital Guardian has enabled data-rich organisations to protect their most valuable assets with a SaaS deployment model or an outsourced managed security programme (MSP). The company operates in more than 60 countries. Seven of the top 10 global patent holders and seven of the 10 largest global automobile manufacturers are our clients.

Digital Guardian is also the only vendor to provide both data loss prevention and endpoint detection and response via a fully managed services offering. Our team of security experts provides the eyes on the data protection for your organisation. We have deep expertise in threat hunting and incident response to provide the data protection needed for risk reduction and compliance. Our MSP protects organisations immediately and can scale quickly to meet customer needs. Our team manages the entire programme, eliminating the need to staff up or purchase additional hardware for a comprehensive data protection programme that requires a lot of hands-on treatment and management from the customer.

The core business advantage to Digital Guardian is the consolidation of security capabilities into a single data protection platform. Digital Guardian is the only platform that provides:

- Network, endpoint and cloud data loss prevention leveraging the same management console, same endpoint agent and same network sensor. Other solutions require multiple management consoles or servers, more than one endpoint agent and/or network sensor.
- Protection from well-meaning and malicious insiders and outside attackers. Competitive DLP solutions continue to focus on protecting data for the insider or compliance use case only. DG for DLP is the only solution that has extended capability to prevent data loss by outside attackers too – leveraging the same technology. To match this capability, buyers would need to purchase 2–3 different technologies from our competitors.
- Flexible deployment options including SaaS-based delivery or as a managed service.

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

DIGITAL GUARDIAN®

Threat modelling: The challenge in managing risk to both structural and technical vulnerabilities

Traditional vulnerability scanning lacks the ability to see the bigger picture.

foreseeti reports

Companies today are experiencing ever-increasing connectivity, as well as increased complexity of infrastructure risk management. Nowadays, the underlying challenge is that infrastructures are complex and interconnected, not to mention the fact that a lot is operated in the Cloud. With the increasing complexity of architectures, the focus on technical vulnerabilities is not sufficient. Traditional vulnerability scanning offers insight into technical vulnerabilities but lacks the ability to see the bigger picture and to prioritise what to focus on.

In general, there needs to be a more holistic approach to ensure that risk related to IT infrastructures is managed in a proper way. Evaluating a combination of technical and structural vulnerabilities and being able to map large infrastructures in a scalable way needs to be combined with a probabilistic approach to threat modelling. This methodology enables organisations to focus on true risk instead of theoretical risk on a technical level.

Taking this further, and being able to focus on true business risk, requires a new approach. At KTH, the Royal Institute of Technology in Sweden, extensive research has been conducted into threat modelling and the probability of a certain set of vulnerabilities being exploited to get access to an infrastructure. securiCAD has evolved from this extensive research.

securiCAD is a threat modelling and risk management tool that enables you, the user, to get a holistic understanding of your IT infrastructure, incorporating risks from both structural and technical vulnerabilities. The decision support you receive from securiCAD shows where you are the most vulnerable, and the attack path to this area, and presents suggestions on how to strengthen security. The data you receive is also expressed quantitatively, which helps you prioritise actions based on return-on-investment, as well as helping communicate the results to other stakeholders.

By employing a probabilistic calculation engine, securiCAD allows for running attack simulations on any type of IT infrastructure in any development phase (from design-phase to implemented). This enables you to predict weak areas in not-yet-implemented IT infrastructure, or to continuously evaluate an existing one.

> Evaluating a combination of technical and structural vulnerabilities and being able to map large infrastructures in a scalable way needs to be combined with a probabilistic approach to threat modelling.

We at foreseeti are on a mission to move IT security from a state of reactivity, with a focus on technical vulnerabilities, and with decisions being based on subjective opinions, to working proactively with a holistic approach and decisions that are data driven. □

foreseeti has harnessed the power of a computer assisted design (CAD) based approach to analyse the cybersecurity of an IT system. Their state-of-the-art product, securiCAD®, can be used to model an IT system before or after it has been built. From the model, it can automatically develop an attack graph showing all possible attacker paths through the model. Attack paths can be visualised showing each attack step and the defences that a successful attacker would need to defeat. securiCAD can help analysts understand the capabilities required of a successful attacker and to select the best options to defeat them.

Join our education seminar or contact us directly at contact@foreseeti.com

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

DISCOVER **CYBER RISK ASSESSMENT** THROUGH **THREAT MODELING**

securiCAD®

foreseeti enables companies to conduct threat modeling and cyber risk simulations on IT- architectures of today's globally interconnected infrastructures. With our product, securiCAD, our customers are able to assess the robustness and risk exposure of their company's IT architecture. By revealing both technical and structural vulnerabilities of IT-infrastructures, securiCAD enables IT decision makers to access the robustness of the IT-architecture, both from a technical and structural perspective.

AUTOMATED ATTACK SIMULATIONS

HOLISTIC AND QUANTITATIVE RISK ASSESSMENTS

PROACTIVE AND DATA DRIVEN DECISIONS

foreseeti

www.foreseeti.com

Harness the power of global shared intelligence with the ThreatMetrix Digital Identity Network

Distinguish fraudsters from genuine customers in real time, throughout the customer journey.

ThreatMetrix reports

A network that grows more powerful each day. ThreatMetrix gives businesses the ability to genuinely recognise good, returning customers by collating Digital Identity Intelligence from the complex digital DNA of online transactions; whether logins, payment transactions or new account applications. ThreatMetrix ID is the technology that brings this Digital Identity Intelligence to life; helping businesses elevate fraud and authentication decisions from a device to a user level as well as unite offline behaviour with online intelligence.

ThreatMetrix ID helps businesses go beyond just device identification by connecting the dots between the myriad pieces of information a user creates as they transact online and looking at the relationships between these pieces of information at a global level and across channels/touchpoints. ThreatMetrix ID comprises a unique digital identifier, a confidence score and a visualisation graph for each connecting user, which together act as a benchmark for the trustworthiness of current and future transactions.

The three components of the Digital Identity Network Digital Identity Intelligence

The best crowdsourced intelligence from the world's largest digital identity network.

- *Web and mobile device intelligence:* Device identification, detection of device compromises across web and mobile, device health and application integrity
- *True location and behaviour analysis:* Detection of location cloaking or IP spoofing, proxies, VPNs and the TOR browser detection of changes in behaviour patterns, such as unusual transaction volumes

Dynamic Decision Platform

Using Digital Identity Intelligence to make the most accurate and timely decisions.

- *Behavioural analytics (ThreatMetrix Smart Rules):* Advanced behavioural analytics rules that enable better understanding of legitimate user behaviour and more accurately detect genuine fraud
- *Machine learning (ThreatMetrix Smart Learning):* A clear-box approach to machine learning that integrates Digital Identity Intelligence with Smart Rules to produce optimised models with fewer false positives
- *Workflow and orchestration:* Ability to integrate external data sources into the ThreatMetrix decision engine as well as access pre-integrated third-party services for transactions that require additional assurance/exception handling
- *Case management:* Enabling continuous optimisation of authentication and fraud decisions by monitoring, updating and isolating transactions that require additional review, providing a smarter, more integrated way to handle increasingly complex caseloads with shrinking resources

Smart Authentication

Combining frictionless RBA with low-friction SCA for an enhanced customer experience.

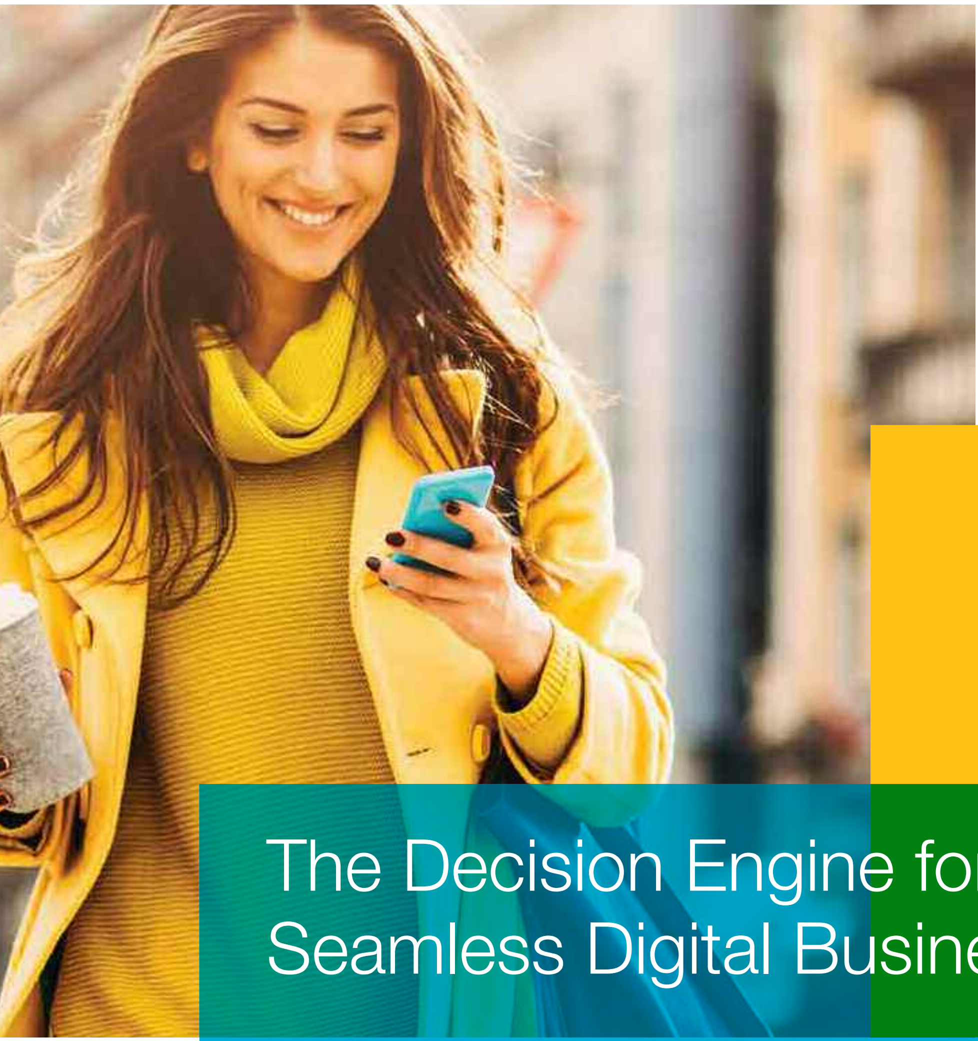
- *Mobile app security:* Detect breaches to the application itself and verify the trustworthiness of the mobile device
- *Device binding:* Leverage the trust of existing devices, using strong device ID and carrier ID, to avoid repetitive authentication
- *Multi-factor authentication (MFA) secure notification:* Push notifications to the user's mobile device for low friction authentication
- *Biometrics:* A comprehensive range of FIDO-compliant, low friction, password-free authentication strategies

The ThreatMetrix advantage

- *An unparalleled network:* The ThreatMetrix Digital Identity Network protects 1.4 billion unique online accounts using intelligence harnessed from 2 billion monthly transactions
- *A comprehensive end-to-end solution:* Universal fraud and authentication decisioning across all use cases and throughout the customer journey
- *Bringing digital identities to life:* ThreatMetrix ID combines a unique identifier, a confidence score and a visualisation graph to genuinely understand a user's unique digital identity across all channels and touchpoints
- *An integrated approach to authentication:* Flexibly incorporate real-time event and session data, third-party signals and global intelligence into a single Smart Authentication framework
- *Advanced behavioural analytics and a clear-box approach to machine learning:* ThreatMetrix Smart Analytics analyses dynamic user behaviour to build more accurate, yet simpler, risk models
- *Privacy by design:* ThreatMetrix is unique in its ability to solve the challenge of providing dynamic risk assessment of identities while maintaining data privacy through the use of anonymisation and encryption
- *Rapid, lightweight deployment:* The ThreatMetrix solution is cloud based, providing simple and straightforward integration with existing systems. □

ThreatMetrix
A LexisNexis® Risk Solutions Company

www.threatmetrix.com



The Decision Engine for Seamless Digital Business

Fighting fraud with digital identity intelligence from billions of transactions and a powerful decision platform.

ThreatMetrix Digital Identity Network®

Harness the power of global shared intelligence from the largest network of its kind.

24b	1.4b	4.5b	.8b	1.5b	185
annual network transactions	unique online identities	unique devices identified	unique email addresses	mobile devices	countries served globally

GDPR needs you to know where your sensitive data is. Do you?

Do you know where all your sensitive data is?

Ground Labs reports

Businesses and organisations across the EU need to become GDPR compliant. The large majority of companies will have to increase their level of security around the PII data they collect and how they store it. But before they can go ahead and do this, they first have to find out where their sensitive data is currently stored and figure out what to do with it.

All businesses want to protect the data they collect but how can you protect something if you don't know where it is?

Ask any IT Manager in the EU today if finding out where their sensitive data is across their network is simple, without a tool to use, and I guarantee you won't like their response! In simple terms finding that data right now is a long and laborious process that takes time! Time is something every business doesn't have a lot of let alone the already under pressure IT department. So discovering that data for all businesses has to be a priority.

Businesses have to know what data is relevant under GDPR, what systems and departments hold the most sensitive data, who's workstation or cloud storage has sensitive data on it that might put the business at a higher state of risk if they were to be breached.

There seems to be some misconception around the Cloud. Most companies have a lack of understanding of what sensitive data is being stored there and that they themselves must take responsibility to secure it. GDPR guidelines clearly state if you are storing sensitive data, irrespective of where, you have to take steps to secure it. This is a great example of needing the correct tool that can discover and remediate sensitive data across your entire network not just certain parts of it.

Deleting all your sensitive data is like cleaning all the dust in your house, it always comes back. So you need continuous monitoring

At Ground Labs, we use an analogy of cleaning your house being similar to cleaning up your sensitive data. You can vacuum and the dirt is gone but you are not going to clean your house once. The dirt will always find its way back into the house. This is similar to sensitive data, once you manage to clean it up, it will always find a way back into your business. So the tool you choose has to be able to continuously look to discover and monitor where your sensitive data is.

GDPR guidelines clearly state if you are storing sensitive data, irrespective of where, you have to take steps to secure it. This is a great example of needing the correct tool that can discover and remediate sensitive data across your entire network not just certain parts of it.

This is where the correct data discovery tool plays a major factor in finding your sensitive data. Such a tool has data security at its core and it allows organisations to constantly track where the sensitive data is. I'm sure some of you will be asking the question, "could we not find our own sensitive data?"

Maybe…but to discover and identify where every last instance of sensitive data is across your entire network has to be the foundation of your compliance for GDPR. The hefty fines of *4% of global turnover or 20 million*, if you get something wrong, should not be taken lightly.

A discovery tool can provide business insights into exactly where the sensitive data is and give options to make some quick wins by remediating the data found. By having a tool in place the process of discovering data becomes an ongoing process.

Summary

Instead of eating into the IT departments already hefty schedule, you need to find a tool that works for your company. As your GDPR compliance project continues past the deadline, having such a tool will become invaluable to help you fight cybercrime and the possibility of a data breach.

For more information, please visit
www.groundlabs.com

GROUND LABS

Sensitive Data Discovery

The most powerful discovery & remediation tool available

Discover, monitor and remediate all your sensitive data across your systems

Don't become the next headline

FIND

REMEDIATE

ASSIGN

MONITOR

JOIN US AT e-CRIME FOR

Standards don't bother me – all I want is your DATA

Matt Jennings-Temple,
Digital Marketing Manager for Ground Labs

See event agenda for time & location

marketing@groundlabs.com | groundlabs.com

GROUND LABS

Why nothing less than complete visibility is enough when the worst happens

The surety of knowing precisely what happened, how, and what was affected – and knowing it quickly – is invaluable.

Endace reports

It has become an all-too-frequent pattern as breaches are reported by the media: the story breaks and another household name is under the microscope. They claim that just a few thousand customer records have been compromised. A week later it's ten thousand and within a month that number has risen into the millions. All the while, Twitter is awash with customers dissatisfied with the level of communication that they have received and the share price is taking a pounding.

The problem these organisations face is actually quite simple to define: it's a lack of facts. And the void this creates is quickly filled by opinions.

The first time this occurs is during the hours that immediately follow the discovery of the breach, before it is made public. The security analysts are pulling together logs from servers, applications, databases and network infrastructure and starting the lengthy process of analysing them. Being human, they will inevitably start with a preconception as to what may have happened and look for evidence to back up their theory.

The problem is the evidence they are working with is itself less than perfect; it is an interpretation of the facts, rather than facts themselves. For example, who decides what the log entries on a firewall will say? It is a product engineer working for the firewall vendor, undoubtedly a very talented person, but one who has to come up with a one-size-fits-all interpretation of the behaviour of a stream of network packets.

So the analyst keeps working until he or she disproves his theory, then tries something else, and so on. This trial and error approach to incident response is far more common than one might hope, but is simply a result of combining human nature with insufficient facts. The real issue though, is that the process takes time. A lot of time.

The problem these organisations face is actually quite simple to define: it's a lack of facts. And the void this creates is quickly filled by opinions.

While the technical work is happening in the background the PR, Legal and Communications teams are also working to prepare to make an announcement within the 72 hours allowed by GDPR. All the relevant materials are drafted, awaiting facts from the analysts to fill in the gaps. But those facts do not come, or at least nothing solid enough to stake the company's reputation on. So the ICO and affected customers are informed as required, but the announcement is so vague and watered down that there is nothing at all to inspire confidence. Again, a lack of facts.

This time the opinions that fill the void are far more dangerous. They are the opinions of the loud and uninformed.

By this process, a technical problem leads to a communications problem, which leads to a business problem. Even in the recent Superdrug case, which at the time of writing appears to be little more than a credential stuffing attack affecting about 400 customers, a lack of hard facts in the way Superdrug communicated the incident has led to a Twitter-storm and subsequent reputational damage that could impact the business for months or years to come.

So, how do we ensure we do not suffer the same consequences if we are breached in the future. Obviously we need to start at the beginning of the process and ensure security analysts have the facts they need to provide really conclusive evidence in a timely manner: so communications can be fact-filled and not leave a void for opinion to take over.

Network Recording is a good way to ensure this. Think of Network Recording as analogous to the CCTV system in an office. If the alarm goes off, it tells you what time it went off and perhaps what zone caused the alarm, but not much else. The first thing we would do in this instance is to rewind the CCTV to the right time, and see a recording of the break-in. We would see how they got in, what they did while in the building, what they took and how they got out. We might even be able to see who they are. We could also rewind to previous nights to see them casing the building. Perhaps even see their car licence plates.

Network Recording provides the same capability for our computer network. We would even choose

With the Network Recording system in place, the analyst can draw fast and accurate conclusions when a problem occurs and can provide the communications team with solid facts and figures.

whereabouts in the network we record in the same way that we would physically position CCTV cameras, focusing on the entrances and on the most valuable things in our building/network.

For the security analyst, the next time a problem is detected, they will have a complete recording of all activity around that event so they can quickly see what happened, how it happened, what data was affected and what other impacts there may be. They would also be able to see any reconnaissance that took place and what other parts of the network the attacker attempted to break into.

Another advantage for the analyst is that Network Recording provides a fast and accurate way to triage events, like telling the difference between a cat burglar and a cat setting off the alarm. This improves productivity and reduces ‘alert fatigue’ produced by the volume of alerts that come from the many security tools on our networks.

With the Network Recording system in place, the analyst can draw fast and accurate conclusions when a problem occurs and can provide the communications team with solid facts and figures about exactly how many customers are affected, who they are and what sort of data has been taken. This will lead to assured communications to customers and the ICO, give customers confidence in our abilities, and diminish the voices of those for whom only opinion matters.

When the worst happens, the surety of knowing precisely what happened, how, and what was affected – and knowing it quickly – is invaluable. □

Endace’s multifunctional Analytics Platform can host 3rd-party network analytics applications while simultaneously recording a 100% accurate network history, providing definitive evidence for investigating cybersecurity threats, quantifying data breaches and analysing network or application performance problems.

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

Duo has the solution

The first article discusses restricting users so that they can only enter into an area that is approved & relevant to their duties. The second focusses on Duo's authentication solution characterised by its simplicity in implementation and operation.

Duo Security reports

Right user, right door

By Richard Archdeacon

The zero-trust concept starts with establishing a level of trust around the identity of the user and what they can access to work within the organisation's environment. Having checked the device and authenticated the user, the next fundamental element is controlling what doors to what applications they can enter, and what is considered out of bounds. This is not a new idea. As Hamlet once said all those years ago:

> *"Let the doors be shut upon him, that he may play the fool nowhere but in's own house."*

This is not to suggest that Chief Information Security Officers (CISOs) should start getting worked up about familial or romantic issues; as it didn't appear to work out too well for poor old Hamlet. But the idea of restricting a user so that they can only enter into an area that is approved and relevant to their duties is a necessary control.

Virtual private networks (VPNs) ensure that the user is connected within the virtual corporate network. But once the credentials are accepted, the user is through the main door into the organisation. This is all well and good in a world where all users are completely honest and, in fact, who they say they are. Unfortunately, compromising credentials is all too common an occurrence. For example, the ease with which phishing has become an attack tool of choice has made relying on controlling the main door with a username and password a limited security control.

The Duo solution starts to address this level of control over users at the entry point. The use of a reverse proxy enables the mapping of users to applications. This means that each application has a door that the user has to open. It is a house on its own with one way in, and that is under lock and key. This provides a triple layer in the defence structure:

- The user is known and authenticated.
- The device is checked and found to be adequate.
- The user is limited to where they can go.

This all needs to be done with minimal impact on the end user. Introducing difficulty into any security control area just breeds avoidance. By integrating with established single sign-on (SSO) capabilities, the users' rights can be identified without the need for any duplication of effort. The ease of adaptive authentication at the device level makes this a non-disruptive activity on the user side, and a natural part of the workflow of logging in to do some work. Meanwhile, the ability to block non-approved devices leverages the awareness of endpoint security. Wrapping this around a browser-based gateway screen provides a simple, secure single point of entry into each of the application doors.

What is appealing about the agile and flexible approach is the ability to bring new applications on board wherever they are found – whether running in the cloud, in a local data centre or a third-party application. No matter where the doors are, they can be open or shut from a central point based on a policy. So as digital transformation drives change in the business and new applications are brought on stream, the Duo solution ensures that security controls enable, rather than block or hinder.

And, of course, because we want to control the doors, it doesn't mean we think that all users are there to play the fool. Just the bad guys. □

Simplicity in a complicated world

By Richard Archdeacon

Authentication is increasingly becoming an issue for the enterprise CISO (Chief Information Security Officer). It is not new. It is well-established as a control. However, the extent to which it is used and its commonality is widening. As a newcomer to the company, one of the factors that attracted me to join was that Duo addresses this with a solution that is characterised by its simplicity in implementation and operation.

About ten years ago, I was speaking on a panel at a conference when the question of encrypting laptops arose. Should it be standard? One of the panel members was quite vociferous about the need to

No matter how great the solution, if it is resource-heavy at the implementation and operational stages, it becomes a negative weight on the CISO's shoulders. A solution that brings in control whilst being easy and resource-light makes everyone's lives a lot easier.

have all endpoints controlled in this way. Now it is standard practice and no one would think of releasing a laptop without encryption into the wild. The same trend is happening with multi-factor authentication (MFA). It is widely used, but will soon become a mandatory part of connecting to networks.

There are a number of drivers for this – the limitations of passwords are now understood. With reams of them available for criminals to buy and try, with technology-matching capabilities increasing and the ever-present issue of users understandably wanting to repeat passwords over the multiple sites with which they interact, the day of the password alone is over.

The broader issue is of identity – *Is the person who they say they are?* – is a constant riddle that requires solving at every login stage.

There are technical solutions around. However, these introduce complexity or user dependence, such as the ability to keep a token and not lose it. This limits the benefit of the control. The last thing a CISO wants is more complexity and increased technology management overhead. I have yet to hear a CISO complain that their team had nothing to do.

This issue was recently recognised by National Cyber Crime Centre (NCSC) when they embarked on an initiative called Secure by Default to push the use of authentication. The NCSC is, of course, the outward face of the UK's Government Communications Headquarters (GCHQ). One of their recommendations is to:

> *"..enforce multi-factor authentication on your externally-reachable authentication endpoints."*

They put out a test and have published some of their case studies. The need for authentication is also recommended by the Information Commissioner's Office. With the ever-present emphasis on General Data Protection Regulation (GDPR), the introduction of the Secure by Design principle as a fundamental requirement is another driver.

Which, of course, gets us to the Duo position. The technology rollout has been proven to be straightforward on many occasions with clients at different levels of complexity and security maturity.

No matter how great the solution, if it is resource-heavy at the implementation and operational stages, it becomes a negative weight on the CISO's shoulders. A solution that brings in control whilst being easy and resource-light makes everyone's lives a lot easier.

A key advantage is the ease of user enrolment. Intuitively, enabling users to engage themselves rather than have to go through a complicated process will result in greater acceptance of the security control. The nature of an easy push notification option to the mobile phone will bring security home to the user and will change the level of awareness. Providing alternative means of authentication such as SMS, a friendly voice down the line, U2F, a code or a hard token provides the correct level of user flexibility. Adaptive authentication, rather than a one means fits all approach.

Additional characteristics can be introduced to build a better picture of the device and the individual. To misquote Goethe, *"Tell me with whom you associate and I will tell you who you are."* That broader picture of a user being more than just a login and a password, but, rather, an association of factors enables us to shed more light on their identity.

So to return to the beginning, if we look at the emphasis on MFA as being best practice and part of Secure by Default, or Secure by Design, we have to assume that it too will be a ubiquitous part of the CISO's technology controls toolkit. It will provide the greater picture and the increased control needed as passwords fade into history. Provided it is simple. □

Richard Archdeacon is the Advisory CISO for the EMEA region at Duo Security.

For more information, please visit
duo.com

Login Request
Duo Security
Duo Access Gateway
Approve
Deny