e-crime & cybersecurity BENELUX VR

8th December 2021
Online

Securing an uncertain transition

Forthcoming events

e-crime & cybersecurity GERMANY 20th January 2022 Frankfurt	pci LONDON 26th January 2022 London	e-crime & cybersecurity CONGRESS 2nd & 3rd March 2022 London	e-crime & cybersecurity CONGRESS 9th March 2022 Dubai
e-crime & cybersecurity FRANCE 22nd March 2022 Paris	e-crime & cybersecurity NORDICS 12th May 2022 Stockholm	e-crime & cybersecurity GERMANY 2nd June 2022 Munich	e-crime & cybersecurity CONGRESS 7th June 2022 Doha
SECURING FINANCIAL SERVICES 6th July 2022 London	e-crime & cybersecurity CONGRESS 21st September 2022 Abu Dhabi	e-crime & cybersecurity SWITZERLAND 28th September 2022 Zurich	e-crime & cybersecurity MID-YEAR 19th October 2022 London
e-crime & cybersecurity NORDICS 1st November 2022 Copenhagen	e-crime & cybersecurity SCOTLAND 9th November 2022 Edinburgh	e-crime & cybersecurity SPAIN 16th November 2022 Madrid	e-crime & cybersecurity BENELUX 8th December 2022 Amsterdam

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

Workplace and business model changes now drive cybersecurity strategies. What are the key priorities?
Security professionals face continued complexities in securing workplaces and business models that will remain in flux for, possibly, years as we come to terms with both the impact of the Covid pandemic and of the overwhelming digitalisation of business models, payment channels and even governments and money itself.

So, what does this mean in practice and what can CISOs do about it?
Business demands for new functionality immediately mean a sudden jump in Cloud and SaaS applications, not necessarily bought with the CISO's say so or even knowledge. New e-Commerce platforms and payment platforms suddenly appear, along with new marketing websites. Mobile apps are bought in from third parties; or perhaps a small department responsible for some small proprietary coding projects suddenly become the app development team – and now reports to the CIO and the business heads. The ideals of SecDevOps take a back seat to getting products up and running as fast as possible.

And all of this is still being done mostly by remote CISOs running remote teams, by SOCs overloaded with alerts and with hack after hack reminding them that the enemy could be their own security stack.

How can CISOs maintain acceptable levels of cybersecurity in this environment? What are the priorities and what is just nice-to-have?
We will be looking at this and much more in this latest e-Crime & Cybersecurity Congress Benelux online. The event is a fantastic opportunity to hear real-life case studies and in-depth technical sessions from peers on how accelerated digitalisation requires a new kind of security. Please take this opportunity to network with your peers in the networking lounge, pose questions to speakers in the auditorium and visit the exhibition hall to mingle with solution providers. We hope you enjoy the event, please do visit our team at the virtual registration desk if you have any questions!

Simon Brady | Editor

@eCrime_Congress **#ecrimecongress**

8th December 2021

Online

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

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

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

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

What threat intelligence tells us about ransomware’s evolution

The threats that are emerging today go well beyond simply taking a company offline and demanding payment to restore operations. Now, it’s all about the data.

By IntSights, A Rapid7 Company

The word ‘ransomware’ strikes fear in the hearts of most business leaders, regardless of the organisation’s size, location, or industry. Yet it wasn’t always this way; in fact, only within the last couple of years have organisations begun protecting themselves against ransomware by making data backups that would allow them to restore operations in the wake of an attack.

As is the case with many data security best practices, however, most organisations are already falling behind in their ransomware-related precautions. The threats that are emerging today go well beyond simply taking a company offline and demanding payment to restore operations. Now, it’s all about the data.

Since the beginning of 2021, and with greater momentum in the past few months, IntSights has noticed ransomware groups operating in a multichannel mode, where they are now auctioning some of the full data leaks, in different sections of their existing websites.

The future of ransomware: Private data for anyone, any use

At first, ransomware group sources were only a means for extortion. Victims who saw their data hanging by a thread, soon to be published, had exclusivity and the first right to buy their way out of the sticky situation. This comfortable setup lasted for only about a year, however, before cybercriminals decided to make their victims’ lives even more complicated.

Since the beginning of 2021, and with greater momentum in the past few months, IntSights has noticed ransomware groups operating in a multichannel mode, where they are now auctioning some of the full data leaks, in different sections of their existing websites. Fast forward months later, IntSights is familiar with several hacking groups offering all of their goods for sale to the highest bidder. This means that when a company is attacked with ransomware, it’s working against the clock to get back on its feet and start running the business; however, the company is also in danger of losing its data to an unknown entity, possibly not even knowing what data was compromised and/or who else now has access to it.

The latest evolution in the ransomware landscape can be attributed to a group that goes by the name BABUK. This group, assumed to be Russian, has

> The real cyber-threat going forward, then, involves more than loss of functionality or physical damage, extending to leakage of data and the numerous ways in which it can be exploited.

recently published a few 'press statements' on its website. In one of the latest, BABUK declares it will no longer 'encrypt networks' but will still 'get to you and take your data,' and afterwards, obviously, notify the attacked party.

BABUK is essentially telling us that network encryption is no longer profitable as merely encryption. In other words, for companies with backup programs in place, this formerly tried-and-true tactic is no longer damaging enough.

This new reality has several implications:

- *Obsolete backups:* You should still maintain high-pace backups, and make sure they're detached from your networks, but these will only allow your business to get back up and running quickly and will not necessarily save you from ransomware-related business damage.
- *Paralysing uncertainty:* Just because your network is still up and running, and endpoints aren't encrypted, doesn't mean you're not already infected with serious data-stealing malware.
- *Breaking ethical barriers:* Some hacking groups avoided attacking critical infrastructure and healthcare institutions, such as hospitals, not willing to inflict a direct threat on human lives. In this new modus operandi, the gloves are off, with cybercriminals actively targeting medical, physical, educational organisations, etc., all while allowing them to maintain operationality. In some cases, the patients whose data was stolen are even being extorted. Victims would 'just' have to pay a hefty ransom or their data will be published/sold to other ransomware groups/private buyers/hostile countries.

In correlation with this new trend, IntSights started identifying a new type of source materialised in the data leaks landscape: data leaks black markets. Though the concept of data leak trade and auction is something we've seen before, this new trend realises a platform that wasn't seen before, with some of the operators claiming to not be cybercriminals at all. These markets are essentially based upon – among other vectors – collaborations between attackers and sellers.

No longer are attackers 'forced' to be the ones offering the data for sale, jeopardising themselves to being exposed and putting time into the trade work. Now, they can extort more victims with this new platform of black markets dedicated solely to data leaks. A ransomware group can hack into an organisation, extract all the information it needs, sell it to a third party operating some black market, and only at this point – and not even necessarily – inform the victim.

The real cyber-threat going forward, then, involves more than loss of functionality or physical damage, extending to leakage of data and the numerous ways in which it can be exploited. According to IntSights predictions, we're about to see more and more versions and appearances of such data theft, leakage, and trade over the coming years, possibly up to a certain point in which companies will no longer hold secrets. Maintaining a leakage-proof infrastructure will cease to be a realistic option. □

This article is excerpted from the IntSights white paper, "The Evolving Ransomware Threat: What Business Leaders Should Know About Data Leakage."

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

INTSIGHTS

A RAPID7 COMPANY

ELIMINATE THE COMPLEXITY OF EXTERNAL THREAT INTELLIGENCE

Instant Value

IntSights can be deployed in as little as 24 hours, giving you the fastest path to protection against external threats.

Industry-Best ROI

Validated by Forrester consulting, IntSights customers enjoy a $2.1 million return on investment while dramatically reducing staff workload.

Force Multiplier

IntSights is like having an enterprise-grade threat intelligence team working for you 24x7x365.

IntSights.com

Lookout®

Work anywhere with integrated endpoint-to-cloud security

With remote work and digital collaboration skyrocketing, data now goes wherever it's needed. To tap into productivity without risking your data, you need to stay in full control while also protecting privacy. At Lookout, we've integrated SASE with endpoint security to protect your data in a way that protects your business and respects theirs.

Discover a privacy respecting security solution that's focused on the data.

Protect People And Data Everywhere With SASE

CASB Enables Smart Zero Trust Access To Apps And Data

Tap Into Mobile Security And Stay In Control

Download your SASE Strategy Guidebook

Find out more at www.lookout.com

Not all CASBs are created equal

How do you choose? Below is a short list of must-have capabilities for a CASB. These are features that you need regardless of whether you're only looking to secure a single app like Microsoft 365 or SAP SuccessFactors, or want protection across multiple SaaS apps.

Lookout reports

Software as a service (SaaS) apps have reshaped the way we stay productive. By having everything easily accessible in the cloud, we are able to get work done from anywhere and on any device.

But, as we know, this flexibility has also introduced security challenges, as your data is also easier to reach for malicious actors. This is why the purchase of a cloud access security broker (CASB) is never that controversial. Most organisations understand that cloud apps require additional protection. They are also aware that legal and regulatory requirements continue to apply even as sensitive data migrates to the cloud.

But how do you choose the right CASB? This is an especially important purchase in this work-from-anywhere environment. Your employees are increasingly using personal devices and networks you don't manage, which means you have little visibility or control over what's going on with your users,their devices and networks.

I've put together a short list of must-have capabilities for a CASB. These are features that you need regardless of whether you're only looking to secure a single app like Microsoft 365 or SAP SuccessFactors, or want protection across multiple SaaS apps.

Must-have capabilities for your CASB

1. Full understanding of your users' behaviour

Some of the most critical threats you will encounter will not likely start with malware deployment. Cyberattackers will avoid using malware and behave like users in order to remain undetected. This is why – whether you are defending against ransomware or insider threats – you need awareness of what's going on with your users and their accounts.

A modern CASB solution should have a deep understanding of how your users behave. With this telemetry data, a CASB will be able to automatically detect anomalous behaviour and stop an attack. An example is someone logging in from a restricted or new location, or a user suddenly downloading bulk files of sensitive data.

Your CASB solution should be able to automatically classify how sensitive your data is on the fly and across your multi-cloud infrastructure.

2. 360-degree data protection

Data access and collaboration have become easier with SaaS apps, but they've also made data security harder. With data now everywhere, maintain control over who is accessing data, where the data is going, the networks it transits and whether it is being copied and saved elsewhere.

This is why you need a data-centric CASB with advanced data protection technologies built in. Your CASB solution should be able to automatically classify how sensitive your data is on the fly and across your multi-cloud infrastructure. It's only with this insight that you can define granular policies that are dynamically applied depending on the sensitivity level of your data and the context by which it's being accessed, such as the user's location and the type of device they are using.

The other critical feature is the ability to enforce these policies no matter how your data is handled. You should be able to change file share settings when a user accidentally sends a document to an unauthorised user. The CASB should also have enterprise digital rights management technology (E-DRM) to encrypt data as it's being downloaded. This way, even when a file is passed around offline, only designated individuals can access it.

3. Posture management to ensure your apps are correctly configured

Just like with any other technology that processes and stores your data, you need to understand the risks involved. Threat actors are always looking for new ways to infiltrate your infrastructure, especially ways to exploit SaaS apps.

Your CASB should have the ability to assess your app's configurations and security events, provide guidance on how to improve your posture and enforce security measures to ensure your risk level remains low.

Cloud security is one piece of a bigger puzzle

At the end of the day, your mission is to secure data and comply with regulations. You can achieve this only by deploying a CASB that has a full

To ensure your Zero Trust architecture provides end-to-end protection, you need integrated controls to mitigate and continuously monitor risk for your on-premise apps and endpoint devices.

understanding of your users and data. With a complete visibility of what's happening, you can retain control over your data without compromising on cloud productivity.

There is a 'bonus' fourth CASB feature I want to mention here: integration with network and endpoint security technologies. CASB is critical in securing your entire cloud environment, but that's only one part of an organisation's attack surface. To ensure your Zero Trust architecture provides end-to-end protection, you need integrated controls to mitigate and continuously monitor risk for your on-premise apps and endpoint devices.

To learn more about a CASB that is built with data protection in mind, download Lookout SASE Strategy Guidebook to learn more about how you can holistically secure your organisation from endpoint to cloud.

For more information, please visit
www.lookout.com

Lookout

Download
Lookout SASE Strategy Guidebook

How today’s supply chain attacks are changing enterprise security

Identifying trust weaknesses and helping mitigate potential future problems.

SentinelOne reports

Exploiting trust

When we think of the word ‘trust’, what thoughts jump into mind? We trust security systems that have earned trust by proving to be reliable and consistent, by demonstrating integrity, value and confidentiality, through a trusted network of recommendations amongst many other data points.

That trust is used to help us manage and mitigate risk and in turn helps other business relationships place their trust in us, and so trust is chained together from business to business, supplier to supplier, vendor to vendor.

Supply chain attacks look to areas of trust that are fragile. Weaknesses in these chains can be used to bypass the implicit trust you have in your own security systems, processes and organisations.

Let’s explore some of the high-profile examples of where these chains have been compromised and look to learn lessons from these incidents, to help identify trust weaknesses and help mitigate potential future problems.

CCleaner March 2017

In March 2017, the hugely popular computer cleaning software called CCleaner was compromised by an attacker to help distribute their malicious code to unsuspecting victims that used CCleaner as a trustworthy tool. It was a devastatingly successful attack, which reportedly led to approximately 1.6 million downloads of the infected copy of CCleaner.

The attackers compromised the maker of CCleaner’s network to inject their software, known as ShadowPad, into the application. The attackers were specifically targeting a smaller group of companies and some 11 of those targeted were successfully compromised by the backdoored CCleaner application.

NotPetya June 2017

The NotPetya attack of summer 2017 involved a ransomware-style attack that encrypted data and, in some cases, also destroyed the MBR (Master Boot Record) of infected computers.

This attack leveraged the Shadowbrokers recently released Eternalblue and EternalRomance exploits, which took advantage of vulnerabilities within the SMBv1 (Server Message Block) protocols for computers running MS Windows. These were the same vulnerabilities that were used in the WannaCry outbreak earlier that year.

A similar theme of leveraging the trust in the supply chain was implemented. The attackers used a legitimate software package update mechanism of a company called M.E.Doc, a financial software package predominantly used by Ukrainian financial institutions, to launch their attack. While it was clear the target of the attack was Ukraine, the attack quickly spread elsewhere.

What became most interesting was that the encrypted computers were not designed to be decrypted; therefore, the purpose of the attack was solely destructive rather than a financially motivated ransomware attack. It is widely accepted that the financial impact of this attack was in the region of $10bn.

SolarWinds December 2020

While there seemed to be a temporary lull in supply chain attacks after those mentioned above, the SolarWinds attack put them firmly back on the map back in December 2020.

SolarWinds is a widely trusted software vendor with some 300,000 customers, but as the story unfolded it became clear that their Orion software had been severely compromised. The attackers managed to incorporate their malware into a legitimate Symantec certificate, which was used to update the SolarWinds software.

After further investigation, SolarWinds reported that there was evidence that the malicious code was placed into their software and updates between March and June 2020. They also reported that they believed it to impact some 18,000 of their customers.

The SolarWinds attack was highly sophisticated. For example, the malware was sandbox aware and only activated after 14 days of dormancy. Given the nature of the targets impacted, such as US government institutions, and the attackers level of sophistication, it was rapidly apparent that the threat actor was APT in nature, and now widely attributed to the Russian Foreign Intelligence Service (SVR).

Kaseya July 2021

Fast forward to summer 2021 and the discovery that Kaseya VSA software, responsible for monitoring and troubleshooting endpoint computers and widely used by Managed Service Providers to help support their customers, had also been compromised. An update to the VSA software included a ransomware component that went on to compromise some 1,500 customers. The attackers leveraged two vulnerabilities, one known since April 2021 and the other since July 2015, in the VSA software.

What is most interesting about this attack is that the motivation seemed to be purely financial as the attackers were initially asking $70m for the recovery of the decrypted data of their victims.

This attack leveraged the REvil group's ransomware. It is also worth noting that the delivery vehicle of the ransomware was only the externally facing Kaseya VSA infrastructure, exploited by known vulnerabilities rather than through an internal breach.

Supply chain attack commonalities

Analysis of these examples shows that adversaries are often either manipulating the code signing procedures via compromised but legitimate digital signing of certificates, hijacking the update distribution network of an ISV solution, or compromising original source code.

The majority of the attackers have a high sophistication level, with the exception of the recent Kaseya attack, which leveraged an external facing service with known vulnerabilities.

Preventing and mitigating supply chain attacks

Attackers always attempt to take the least path of resistance. Today, it's often done by first compromising one of the end targets' upstream suppliers and then abusing the trust relationship that they have to the true target to obtain their goals.

As part of any organisation's risk management programme, supply chain attacks must be factored in, so what are the typical processes for compliance, governance and technology areas that could be bolstered to help mitigate these problems?

1. Develop and implement a vendor risk management programme to evaluate, track, and measure 3rd-party risk.
2. Enforce through contractual requirements vendor cybersecurity assessments, including for the vendors own supply chain risk.
3. Require ISO 27001 certification or CMMI and/or comply with cybersecurity frameworks like NIST or CIS
4. Plan to move to a zero trust network (ZTA) architecture ensuring that all identities and endpoints are no longer trusted by default but instead continuously validated for each access request.
5. Deploy a modern, platform-agnostic XDR platform capable of detecting and remediating sophisticated attacks across your endpoints, cloud and network infrastructure.
6. Enforce multi factor authentication (MFA) to prevent the most typical of authentication brute forcing attacks.
7. Increase your network and endpoint visibility retention rates so that long lasting attacks can be identified. The SolarWinds attackers were present for at least five months before launching their outward-facing attack.
8. Be exceptionally careful as to how and where you configure your endpoint tool exceptions. Being overly permissive here with tools that you supposedly trust could lead to detection gaps.
9. If you are an ISV then ensure best practices for Secure Development Lifecycle (SDL), vulnerability assessment and patch management programmes to address identified issues.

Conclusion

The real challenge with these sophisticated supply chain attacks is that they leverage the implicit trust we place into our 3rd parties and also the implicit trust we place in the tools we use to support our businesses.

The real benefit to the attacker is that if they are successful, they have potentially increased their ability to scale the targets that they can infect, as well as allowing them the benefit of going completely undetected for potentially many weeks or months in length, depending on the goal of the attack.

It is essential that organisations review their cybersecurity requirements, gain visibility into supply chain dependencies, and deploy a modern XDR platform that can identify and contain a breach even if it originates deep within the company's own supply chain.

Want to know more about how SentinelOne can help? Contact us via sentinelone.com/contact.

For more information, please visit
www.sentinelone.com

SentinelOne™

Multicloud security: more clouds, more problems

Today, cloud vendor lock-in fears of the past seem overblown. Instead of choosing one cloud or another, organisations are simply choosing both, or to be more precise, many!

BeyondTrust reports

Most organisations aren't merely in the cloud – they're in many clouds (PaaS, IaaS), and their end users regularly consume dozens, or even hundreds, of different SaaS applications. A McAfee study published in 2019 reported the average organisation used 1,935 cloud services. And that number has almost certainly ballooned further since then.

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

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

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

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

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

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

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

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

For more information, please visit
www.beyondtrust.com

BeyondTrust

BeyondTrust

UNIVERSAL PRIVILEGE MANAGEMENT

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

Privileged Password Management

Endpoint Privilege Management

Secure Remote Access

Cloud Privilege Protection

beyondtrust.com

The only universal security intelligence solution

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

Recorded Future reports

Who we are

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

Security intelligence solutions

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

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

Intelligence-led security

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

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

Innovative security intelligence technologies

Security Intelligence Graph

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

Recorded Future Intelligence Cards™

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

For more information, please visit
www.recordedfuture.com

Recorded Future®

Watch out! Cybercriminals are coming for the financial sector

How more coordinated cyber-attacks and the sudden move to a remote workforce makes it imperative that security professionals expand their view of what needs to be protected.

OneLogin reports

Cybercrime is a business, so we all should be aware that cybercriminals act as other businesses do. Taking the global economic environment and current market conditions into consideration cybercriminals will, of course, continue to focus on their efforts to generate revenue streams. During 2021, we are likely to see cybercriminal individuals and groups partner together to try to maximise their return of investment with their attacks. This means they will be able to coordinate attacks against high-value individuals as well as large enterprise organisations. In particular financial systems.

I envision we will also see an increase in insider threat being used as a support vehicle to execute attacks. Forrester predicts that employees will be responsible for 33% of breaches in 2021. A comprehensive security programme incorporates the measurement and management of accidental behaviour activity to constant risky behaviour and/or activities.

The key message here is no one individual nor industry is exempt from these threats, and it requires constant focus, assessment and review to ensure you and your critical information assets remain safeguarded and protected against attacks.

The business disruption caused by COVID-19 has accelerated the need for digital transformation within the financial sector particularly the smaller financial industry providers. Though many smaller organisations might have planned to replace manual processes with digital processes, time and money often prevented them from moving forward. Because the pandemic forced them out of their offices many had to quickly scramble and accelerate their digital transformation.

The fundamental security requirement for the finance industry is to understand who and what is trying to access finance technology environments and data stored within. The lockdowns and the return to work regulations have required organisations to put hybrid operating models in place that cater for both office and remote working. Organisations that relied on users only being able to access resources from within the office no longer have this level of control.

> It requires constant focus, assessment and review to ensure you and your critical information assets remain safeguarded and protected against attacks.

Systems that were only available from within the internal network are now having to be accessed externally. This change has further highlighted the importance of identity and access management to support businesses through this transformation.

As a result of this need to expand access yet keep data secured, we are seeing an increase in financial providers and general practitioners reaching out to us as industry experts to partner on identity and access management. As an identity and access management (IAM) provider, we are keenly aware that financial data is subject to both regulatory and compliance requirements and work to ensure that our customers understand how utilising an IAM platform can help them fulfill their requirements.

OneLogin is the number one value-leader in identity and access management. Our Trusted Experience Platform$^{\text{TM}}$ provides everything you need to secure your workforce, customers, and partners at a price that works with your budget. Headquartered in San Francisco with EU headquarters in Dublin, OneLogin secures 30+ million identities with over 5,500 customers worldwide, including Airbus, BritishRedCross, and Tesco.

To learn more, please visit **www.onelogin.com**

onelogin

Sponsors and exhibitors

BeyondTrust | Strategic Sponsor

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

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

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

Learn more at www.beyondtrust.com

Darktrace | Strategic Sponsor

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

For more information, please visit www.darktrace.com

IntSights | Strategic Sponsor

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

For more information, please visit intsights.com

KnowBe4 | Strategic Sponsor

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform.

Realising that the human element of security was being seriously neglected, KnowBe4 was created to help organisations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach. This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting.

Tens of thousands of organisations worldwide use KnowBe4's platform to mobilise their end users as a last line of defence and enable them to make smarter security decisions.

For more information, please visit www.knowbe4.com

Lookout | Strategic Sponsor

Lookout is a leading cybersecurity company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C.

For more information please visit www.lookout.com

Recorded Future | Strategic Sponsor

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

Learn more at recordedfuture.com

SentinelOne | Strategic Sponsor

SentinelOne's cybersecurity solution encompasses AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform.

For more information, please visit www.sentinelone.com

Corelight | Education Seminar Sponsor

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders. Based in San Francisco, Corelight is an open-core company founded by the creators of Zeek, the widely-used NSM tool and providing an Open NDR Platform.

For more information, please visit corelight.com

GateWatcher | Education Seminar Sponsor

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders. Based in San Francisco, Corelight is an open-core company founded by the creators of Zeek, the widely-used NSM tool and providing an Open NDR Platform.

For more information, please visit www.gatewatcher.com

Kenna Security | Education Seminar Sponsor

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

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

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

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

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

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

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

OneLogin | Education Seminar Sponsor

OneLogin is the number one value-leader in Identity and Access Management. Our Trusted Experience Platform™ provides everything you need to secure your workforce, customers, and partners at a price that works with your budget.

To learn more, visit www.onelogin.com

OPSWAT | Education Seminar Sponsor

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

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

Synack | Education Seminar Sponsor

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

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

Devo | Networking Sponsor

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

Learn more at www.devo.com

AGENDA

08:00	Login & networking
08:50	Chairman's welcome
09:00	**Securing critical national infrastructure** **Joost Rommelaere,** former Regional CIO EMEA & Americas, PSA International • Do you operate a critical national infrastructure? • What is the regulatory impact at this moment? • How cyber-secure can you make your critical infrastructure? • How to deal with cyber-resilience of critical national infrastructure in a multinational context? • How to interact with your national cybersecurity centre and other stakeholders of your ecosystem?
09:20	**Supply chain attacks are the new high watermark – it's not all trucks and fish tanks** **Thom Langford,** Security Advocate, SentinelOne • See the vectors of attack and what makes supply chain attacks quite so devastating • Understand the scale of the supply chain and why attacks are an inevitability • Learn three simple tricks to help combat supply chain attacks (number two will astound you!)
09:40	**The battle of algorithms: How AI is beating AI at its own game** **Toby Lewis,** Head of Threat Analysis, Darktrace • How cybercriminals are leveraging AI tools to create sophisticated cyber weapons • What an AI-powered spoofing threat may look like, and why humans will not be able to spot them • Why defensive AI technologies are uniquely positioned to fight back
10:00	**Trusted computing and its application in preventing e-crime** **Dr. Ian Oliver,** Technical Staff (Cybersecurity), Nokia Bell Labs • The shift from malware to supply chain attacks in the domain of 'nation state actors' • How effective is TPM 2.0 in addressing these attacks? • Higher level services and integrating technology into IoT, Edge Cloud and communications • Case studies from safety critical domains such as medical and railway systems
10:20	**Education Seminars | Session 1** **See pages 25 and 26 for more details** **OneLogin** **Leveraging IAM for effective and efficient threat mitigation** **Lonnie Benavides,** Head of Infrastructure and Application Security, OneLogin **Synack** **How hackers hack: Attacker methodology & lifecycle** **Jeremiah Roe,** Synack
10:50	Networking Break
11:20	EXECUTIVE PANEL DISCUSSION **Cybersecurity leaders** **Roy Konings,** Head of Security Benelux, Ericsson **Daniela Lourenço,** Business Information Security Officer, CarNext • Is cybersecurity finally going to become a truly C-suite concern? • Is this the moment we move from technology-oriented CISOs to strategic, business-advisory CISOs? • Does this public urgency on the part of government imply a greater role for information security in the change management process around digitalisation?
11:40	**How to increase incident response efficiency with security intelligence** **Mikael Mörk,** Sales Engineer, Recorded Future • Integrate unprecedented, real-time security intelligence into your SIEM or SOAR to enhance your existing workflows (Splunk, QRadar, XSOAR, ServiceNow SIR) • Use the broadest set of external data sources available anywhere to rapidly contextualise alerts and accelerate prioritisation • Utilise real-time risk scores of IPs, domains, hashes, and malware to enable fast threat detection and response
12:00	**The psychology of a social engineering attack** **Jelle Wieringa,** Security Awareness Advocate, EMEA, KnowBe4 • Learn how psychology plays a vital role in social engineering • Understand the techniques cybercriminals use to fool you • Get actionable insight on how to better protect yourself
12:20	**Building cybersecurity immunity to ransomware with PAM** **James Maude,** Lead Cyber Security Researcher, BeyondTrust • Explore ransomware attacks and how you can protect your environment by making it inhospitable to them • Learn 6 things to know about ransomware • Takeaway realistic security practices you can implement to protect against ransomware • Understand the role of PAM (privileged access management) in mitigating the risks of ransomware and other cyber-threats with a powerful, blended defence

AGENDA

12:40 **Education Seminars | Session 2** — **See pages 25 and 26 for more details**

Gatewatcher

Rolling out of an NDR: What benefits to expect

Luis Delabarre, Solution Architect, Gatewatcher

Kenna Security

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

Stephen Roostan, VP, EMEA, Kenna Security

13:10 Lunch & networking

14:00 **Future crimes: Emerging threats from cyber-malicious innovators**

Robin Smith, CISO, Aston Martin

- What can we tell about the future of cybercriminality from current trends, gross criminal revenue and attack by sector? How can this be used to build a profile of the attackers?
- The global cost of crime is increasing: has ransomware changed the rules of the game for CISOs?
- Drone offences. Robot attacks. Artificial intelligence plagues. Science fiction or future threat?
- Moving towards the defences of the future

14:20 **Selling breaches – the transfer of network access on criminal forums**

Paul Prudhomme, Head of Threat Intelligence Advisory, IntSights

- The sale and purchase of unauthorised access to compromised enterprise networks have become significant enablers for criminal cyber-attacks, particularly ransomware infections
- Some criminals specialise in network compromises and sell the access that they have obtained to third parties, rather than exploiting the networks themselves
- By the same token, many criminals that exploit compromised networks, particularly ransomware operators, do not compromise those networks themselves but instead buy their access from other attackers
- These exchanges on underground criminal websites enable specialised criminals with complementary skills and resources to maximise the severity and impact of the underground criminal ecosystem and the criminal kill chain
- This specific variety of criminal market offerings is less well-known than others, such as the sale of compromised bank cards from retail & hospitality breaches

14:40 **Security from endpoint to cloud**

Aaron Cockerill, Chief Strategy Officer, Lookout

- How Secure Access Service Edge (SASE) protect your organisation's data in the cloud
- Why you need integrated endpoint-to-cloud security to safeguard your data while complying with regulations and respecting personal privacy

15:00 **Education Seminars | Session 3** — **See pages 25 and 26 for more details**

Corelight

An alert has fired, now what?

Alex Kirk, Global Principal, Corelight

OPSWAT

Critical infrastructure protection by OPSWAT – Live Demo

George Chereches, Sales Engineer Team Lead for EMEA, OPSWAT

15:30 Networking break

16:00 **PCI SSC Update**

Jeremy King, VP, Regional Head for Europe, PCI Security Standards Council

- PCI DSS V4.0 latest news
- PA DSS migration to Software Security Framework
- Software Security Framework latest news
- Training
- Informational training
- Work from home
- Remote assessments
- PCI at a glance

16:20 **Securing the university**

Garry Scobie, Deputy CISO, University of Edinburgh

- Universities are unique entities. Comprised of disparate faculties, departments and campuses, they operate as a miniature city might. Furthermore, with the wealth of personal data they hold, their capacity to conduct cutting edge research, and their lack of funding when it comes to cyber-defences, they are an attractive target for criminals
- For years institutions in the higher education sector have been being hit: what should information security professionals in universities be doing to improve their defences?
- What can CISOs from different industries learn from the university challenge?

16:40 **How does Benelux cybersecurity stack up?**

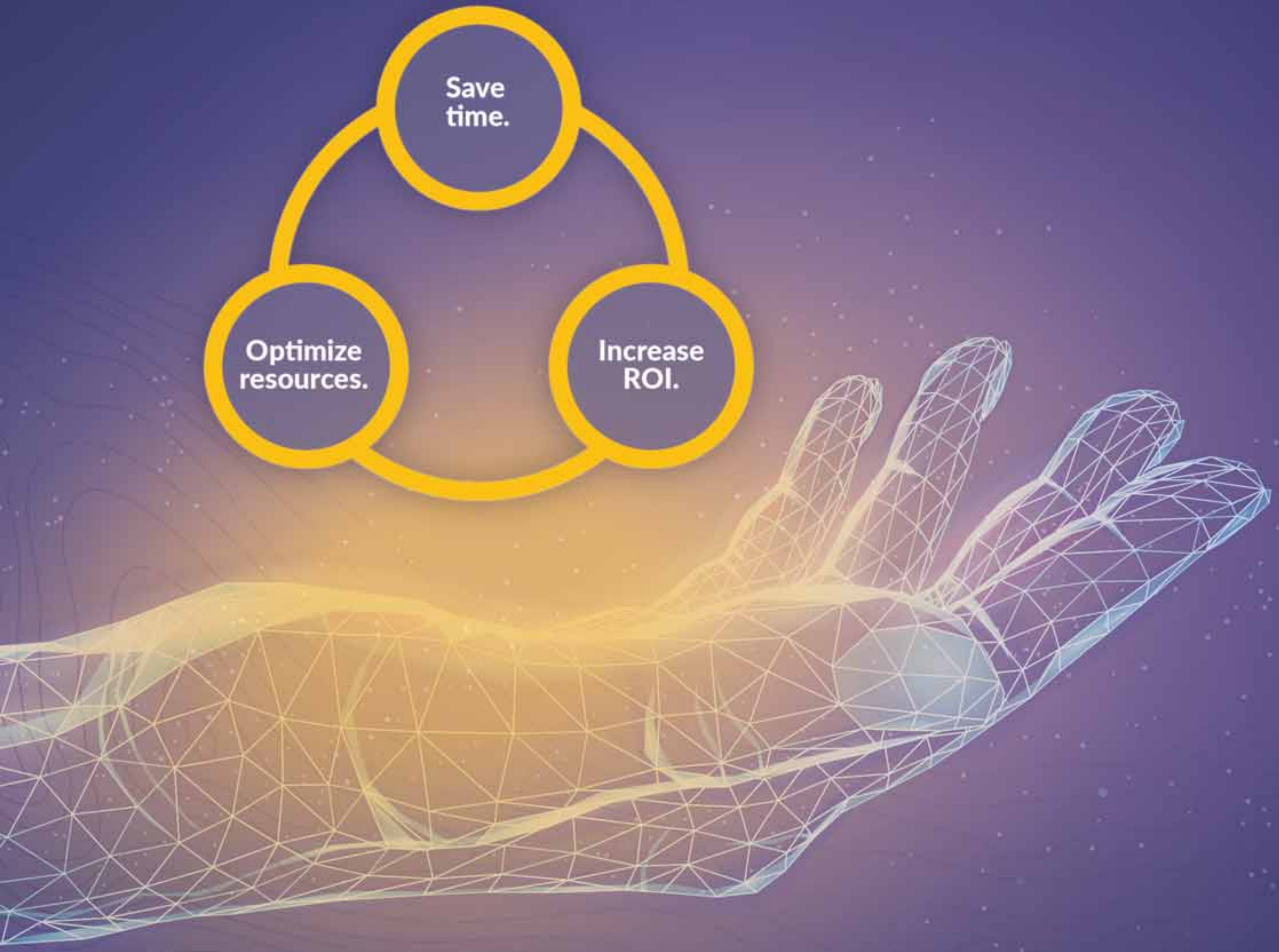
Simon Brady, Managing Editor, AKJ Associates

- Comparing CISO opinions and attitudes across Europe
- What are the most significant changes to CISO roles in the last 12 months?
- Why cybersecurity will be unrecognisable in three years' time

17:00 Chairman's closing and networking break

17:30 Conference close

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



Modern Vulnerability Management

Focus on the threats that matter most.

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

www.kennasecurity.com

CISCO | KENNA Security

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: 10:20–10:50

OneLogin

SESSION 1
10:20–10:50

Leveraging IAM for effective and Efficient Threat Mitigation

Lonnie Benavides, Head of Infrastructure and Application Security, OneLogin

There's no question that the current cybersecurity landscape is constantly shifting and evolving as new threats and security solutions emerge. Increased cyber-attacks and distributed workforces have created new challenges that require innovative solutions.

Faced with the challenge of managing identities and securing access to data and applications from a growing number of endpoints, what are the fundamental controls organisations need to maintain business continuity and secure their remote and hybrid workforce?

Hear from Lonnie Benavides – Head of Infrastructure and Application Security, Onelogin – for a discussion on practical information and advice regarding the utilisation of identity and access management solutions to effectively mitigate modern cyber-threats to your business.

Key takeaways:

- Understanding the key fundamentals of a strong cloud security posture
- Why passwords alone are not enough
- Best practices for building a cybersecurity strategy at scale

Synack

SESSION 1
10:20–10:50

**How hackers hack:
Attacker methodology & lifecycle**

Jeremiah Roe, Synack

In this deep dive discussion, Synack Solutions Architect and Red Team Expert, Jeremiah Roe takes a practical approach to the attacker lifecycle. He walks through each of the 7 steps of the kill chain, from Reconnaissance to Actions on Objectives, providing live demonstrations and tools.

You'll learn:

- How the adversary applies the kill chain: We share the 7-step process of the attacker lifecycle and methodologies with an in-depth demonstration of the kill chain
- New exploits (and how to defend against them)
- How to add rigor to your pentesting: where traditional penetration testing stops and crowdsourced penetration testing probes further

Session 2: 12:40–13:10

Gatewatcher

SESSION 2
12:40–13:10

**Rolling out of an NDR:
What benefits to expect**

Luis Delabarre, Solution Architect, Gatewatcher

Addressing advanced attacks is more and more a challenge, even for the most mature enterprises. It's time for a different approach, mainly based on more useful data and automation.

- What is an NDR
- Advanced detection to address complex attacks (ie: sunburst)
- Investigate with threat intelligence
- Ecosystem integration as an answer

Kenna Security

SESSION 2
12:40–13:10

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

Stephen Roostan, VP, EMEA, Kenna Security

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

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

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

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

Session 3: 15:30–16:00

Corelight

SESSION 3
15:30–16:00

An alert has fired, now what?

Alex Kirk, Global Principal, Corelight

While the security industry spends a lot of time and energy getting more and/or better alerts, comparatively little investment has gone into helping analysts operationalise and contextualise those alerts.

This session will discuss:

- How a solid foundation of network telemetry can enable a high-velocity, high-confidence processing of alerts of all stripes
- How this can also be a host of other critical security applications, from fundamentals like asset management to advanced techniques like proactive threat hunting
- Real-world examples and code will be used throughout the talk, along with practical considerations for operating in an enterprise environment

OPSWAT

SESSION 3
15:30–16:00

Critical infrastructure protection by OPSWAT – Live Demo

George Chereches, Sales Engineer Team Lead for EMEA, OPSWAT

How can file transfers be secured across the entire enterprise, especially between uncontrolled devices? George Chereches, EMEA Sales Engineer Manager at OPSWAT will demo how to secure files transfer into, across, and out of secure environments to avoid malware and/or data breach.

- Breach prevention with multiscanning
- Cybersecurity compliance
- Digital perimeter control with automated device blocking
- Secure file transfer with automated media blocking

Speakers and panellists

Lonnie Benavides

Head of Infrastructure and Application Security, OneLogin

Lonnie Benavides is an accomplished cybersecurity leader with more than 20 years' industry experience, and is currently the Head of Infrastructure and Application Security at OneLogin. Lonnie began his career as a communications encryption specialist in the US Air Force and went on to conclude his military service as a Technical Lead of the first red team in the Air National Guard. As an advanced penetration tester, Lonnie supported companies such as Washington Mutual and JP Morgan Chase, and eventually went on to launch the Boeing red team. Lonnie was responsible for leading global cybersecurity services and operations at DocuSign and McKesson, fostering his expertise in enterprise cyber-threat detection and response. Lonnie is a recognised speaker within the Phoenix education community, numerous industry conferences, and has also contributed to publications and radio shows such as TechRepublic and NPR.

Simon Brady

Managing Editor, AKJ Associates Ltd

Simon is a former Journalist, Editor and Publisher specialising in wholesale financial markets, particularly the technology intensive areas of derivatives, securities trading, cash management and FinTech. He has sat as an Executive Director on the main board of a FTSE-250 listed media company and has spent a lifetime travelling the globe talking to CEOs, CFOs and government ministers about the trends driving business and finance. His experience has led him to look at cybersecurity as a key component of the value chain and to ask whether firms are really taking cyber-threats seriously and why third parties will force them to.

George Chereches

Sales Engineer Team Lead, EMEA, OPSWAT

George Chereches is Sales Engineer Team Lead for EMEA at OPSWAT, an innovative cybersecurity company with the mission of providing the most effective threat prevention technology possible. Prior to joining OPSWAT, he was managing messaging infrastructure for big enterprise customers.

Aaron Cockerill

Chief Strategy Officer, Lookout

As the Chief Strategy Officer, Aaron is responsible for developing, validating and implementing cross-functional strategic product initiatives that align with the Lookout vision of a secure connected world. Prior to Lookout, Aaron was the VP of Mobile Technologies at Citrix, where he and his team were responsible for the development of Citrix's mobile apps and container technology while driving the acquisition of Zenprise. During his time at Citrix, Aaron drove the creation of Citrix's desktop virtualisation product, XenDesktop, which grew into more than $1 billion yearly revenue for Citrix during his five years of leadership.

Luis Delabarre

Solution Architect, Gatewatcher

As Solution Architect at Gatewatcher, Luis Delabarre helps enterprises combat cyber-threats and improve their security posture, implementing cybersecurity security controls in complex environments. More specifically deploying Gatewatcher's NDR Solution in the most mature and complex environments where machine learning combined with other detection technologies are adapted to the ever-evolving threat landscape. Throughout his career he has held various positions in the IT field and, more specifically, in the security domain. In his most recent role, as Global CTO for Cybersecurity at Capgemini, he led project teams for very large projects (Cloud Transformation for Bayer, SOC improvement for AXA and SOC modernisation for SAMA Bank), and as a Cybersecurity Authority at Thales, he was involved in very large projects in the areas of governments, telcos, banks and transportation. Prior to that, he was the EMEA CTO for Trend Micro where his role was to support major accounts in defining complex architectures and deploying critical infrastructures, in particular involving virtualisation, encryption and Cloud. Luis Delabarre is also a member of different security industry working groups and think tanks.

Jeremy King

VP, Regional Head for Europe, PCI Security Standards Council

Mr King leads the Council's efforts in increasing adoption and awareness of the PCI Security Standards internationally. In this role, Mr King works closely with the Council and representatives of its policy-setting executive committee from American Express, Discover, JCB International, Mastercard and Visa, Inc. His chief responsibilities include gathering feedback from the merchant and vendor community, coordinating research and analysis of PCI SSC-managed standards through all international markets, and driving education efforts and Council membership recruitment through active involvement in local and regional events, industry conferences and meetings with key stakeholders. He also serves as a resource for Approved Scanning Vendors (ASVs), Qualified Security Assessors (QSAs), Internal Security Assessors (ISAs), PCI Forensic Investigators (PFIs), and related staff in supporting regional training, certification and testing programmes.

Alex Kirk

Global Principal, Suricata, Corelight

Alex is a veteran open source security technologist, and currently serves as Corelight's Global Principal for Suricata. Previously, he spent 10 years with Sourcefire Research (VRT), where he wrote the team's first malware sandbox and established its global customer outreach and intelligence sharing programme. He has spoken at conferences across the globe on topics from 'Malware Mythbusting' to 'Using Bro/Zeek Data for IR and Threat Hunting', and was a contributing author for 'Practical Intrusion Analysis', and oft-used textbook for university courses on IDS. His security engineering background also includes five years at Cisco and Tenable.

Roy Konings

Head of Security Benelux, Ericsson

Roy Konings is a regional security manager for international telecommunications firm Ericsson. Within his role, he is responsible for the security operations and is involved in ISO27001 compliance, audits, customer support, data privacy, cyber-investigations and governance. Roy has previously worked as Deputy Country Security Officer for T-Systems Netherlands, where he was responsible for compliance checks, risk management, forensic investigations and auditing. Roy is an experienced Head of Security with a history of working in the information technology and services industry as well as government.

Thom Langford

Security Advocate, SentinelOne

Thom is an industry engaged and sought after information security subject matter expert and speaker. As Security Advocate for SentinelOne, Thom is able to further explore his passion of communicating and educating on information security topics to a global audience through storytelling, humour and plain language. He is the founder of (TL)2 Security (tl2security.com), a strategic information security consultancy that focuses on Virtual CISO, strategic business alignment and public speaking/advocacy for hire. As Chief Information Security Officer of Publicis Groupe, Thom was responsible for all aspects of information security risk and compliance as well as managing the Groupe Information Security Programme. Additionally, the role was responsible for business continuity capabilities across the Groupe's global operations. Having successfully built security and IT programmes from the ground up, Thom brings an often opinionated and forward-thinking view of security risk, both in assessments and management, but is able to do so with humour and pragmatism (mostly). An international public speaker and award-winning security blogger, Thom contributes to a number of industry blogs and publications. Thom is also the sole founder of Host Unknown, a loose collective of three infosec luminaries combined to make security education and infotainment films. Thom can be found online at both thomlangford.com and @thomlangford on Twitter.

Toby Lewis

Head of Threat Analysis, Darktrace

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

Daniela Lourenço

Business Information Security Officer, CarNext

Daniela Lourenço is currently the Business Information Security Officer for CarNext. In this role, she bridges the gap between business needs and security requirements, by translating the security roadmap to an organisation-wide project. Daniela holds a master's degree in Communication & Cultural Studies and an executive master's degree in Cybersecurity. With multinational experience in compliance and information security, her ultimate objective is to embed information security in the organisation's model and culture as an inherent feature, understood by everyone throughout a supply chain.

James Maude

Lead Cyber Security Researcher, BeyondTrust

James Maude is the Lead Cyber Security Researcher at BeyondTrust. James has broad experience in security research, conducting in-depth analysis of malware and cyber-threats to identify attack vectors and trends in the evolving security landscape. His background in forensic computing and active involvement in the security research community makes him an expert voice on cybersecurity. He regularly presents at international events and hosts webinars to discuss threats and defence strategies.

Mikael Mörk

Sales Engineer, Recorded Future

Mikael Mörk is a Sales Engineer for the Nordics region at Recorded Future. Responsible for the technical aspects of sales in the Nordic markets, Mikael's role centres around preparing and delivering technical presentations, assisting customers in assessing needs and requirements, and providing sales support. Mikael has extensive experience in software and service development, both in the role of a programmer and a solutions architect.

Dr Ian Oliver

Technical Staff (Cybersecurity), Nokia Bell Labs

Dr Ian Oliver is a distinguished member of technical staff at Bell Labs Finland working on trusted and high-integrity cybersecurity in 5G and future 6G telecommunication systems including areas such as Edge Cloud, IoT and Trusted Computing. Much of the work is involving safety-critical systems such as medical, aerospace and railway systems build upon these technologies. He holds a visiting position at Aalto University Neurobiology Dept working on the application of cybersecurity and trust techniques to future medical applications. Other areas of active research include privacy engineering and various topics related to information theory, measurement of privacy and semantics. Prior to these, he has worked as the privacy architect and officer for Here and Nokia Services; and for 11 years at Nokia Research Centre working with Semantic Web, UML, formal methods and hardware-software co-design. He has also worked at Helsinki University of Technology and Aalto University teaching formal methods and modelling with UML. He is the author of the book 'Privacy Engineering: A data flow and ontological approach' and holds over 200 patents and academics papers and lectures semi-regularly on privacy engineering and cybersecurity.

Paul Prudhomme

Head of Threat Intelligence Advisory, IntSights, a Rapid7 company

Paul Prudhomme is Head of Threat Intelligence Advisory at IntSights. He previously served as a leader of the cyber-threat intelligence subscription service at Deloitte and as an individual contributor to that of iDefense. Paul previously covered cyber issues as a contractor in the US Intelligence Community. Paul specialises in the coverage of state-sponsored cyber-threats, particularly those from Iran. Paul originally served as a linguist and cultural advisor and speaks multiple languages, including Arabic. He has a master's degree in History from Georgetown University. Paul is also a certified scuba diver and an award-winning amateur underwater photographer.

Jeremiah Roe

Synack

Jeremiah Roe is a Red Team operator with nine years of hands-on experience in a range of different contexts. He is experienced in web application, network, and host testing. Prior to working in offensive cyber-operations, he served in the Marine Corps at 29 Palms. Currently, he leads client implementation of Synack solutions so the DoD can combat digital dance moves attackers make.

Joost Rommelaere

former Regional CIO EMEA & Americas, PSA International

Joost Rommelaere has an MSc in Electrical Engineering (University of Ghent, Belgium) and MSc in Control and IT (UMIST, UK) which he complemented with an MBA from Vlerick Business School, one of the leading business schools in Europe. Throughout his career, he has focused on automation and IT within industrial environments and with special focus on supply chain management. He has taken up various roles in programme management (Pioneer Europe, Terumo Europe) and as a Global/Regional CIO (Pioneer Europe, Tessenderlo Chemie, PSA). He offers his wealth of experience in the digital and cybersecurity arena as an advisory service to C-levels and boards.

Stephen Roostan

VP EMEA,
Kenna Security

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

Garry Scobie

Deputy CISO,
The University of Edinburgh

Garry Scobie is the Deputy Chief Information Security Officer for The University of Edinburgh. He is a Certified Information Systems Security Professional and ITIL Expert and is featured in the Global Top 100 Leaders in Information Security published by Corinium Global Intelligence in 2021. He regularly presents on computer security including sessions on ransomware, mobile security and cyber in the movies. Prior to this, he was responsible for Microsoft Windows server infrastructure and an enterprise Active Directory. Having trained as an ethical hacker, he has a particular interest in vulnerability assessment, penetration testing and promoting security awareness.

Robin Smith

CISO,
Aston Martin

Robin is a cybersecurity programme lead in the UK's automotive industry, developing lean approaches to implementing security standards and services. Robin has worked across law enforcement, financial services and the nuclear industry prior to joining Aston Martin in 2021. He is the author of four books and recently won the Gold Award at the New York Sound & Vision Film Festival for his new feature documentary, 'Machina I; Building the Immortal Technologies'.

Jelle Wieringa

Security Awareness Advocate,
EMEA, KnowBe4

Jelle Wieringa has over 20 years of experience in business development, sales, management and marketing. In his current role as Security Awareness Advocate for EMEA for KnowBe4, he helps organisations of all sizes understand why more emphasis is needed on the human factor, and how to manage the ongoing problem of social engineering. His goal is to help organisations and users increase their resilience by making smarter security decisions. Previously, Wieringa was responsible for building an AI-driven platform for security operations at a leading managed security provider. □

Egregor ransomware: Gone but not forgotten

This blog studies the techniques, tools and procedures (TTPs) observed from a real-life Egregor intrusion last autumn, which showcases how self-learning AI detected the attack without relying on signatures.

Justin Fier reports

Ransomware groups are coming and going faster than ever. In June alone, we saw Avaddon release its decryption keys unprompted and disappear from sight, while members of CLOP were arrested in Ukraine. The move follows increasing pressure from the US intelligence community and Ukrainian authorities, who took down Egregor ransomware back in February. Egregor had only been around since September 2020. It survived less than six months.

But these gangs aren't going away – they are simply going underground. Despite 'closures', cases of ransomware continue to rise and new threat actors and independent hackers pop up on the Dark Web every day.

As malware actors lay low and resurface with new variants, keeping up with the stream of signatures and new strains has become untenable. This blog studies the techniques, tools and procedures (TTPs) observed from a real-life Egregor intrusion last autumn, which showcases how self-learning AI detected the attack without relying on signatures.

Egregor: Maze reloaded

Law enforcement authorities have been busy this year. Aside from Egregor and CLOP, actions were taken against Netwalker in Bulgaria and the US, while Europol announced that an international operation had disrupted the core infrastructure of Emotet, one of the most prominent botnets of the past decade.

All parties – from governments down to individual businesses – are taking the threat of ransomware more seriously. In response to this added pressure, cybercriminals often prefer to shut up shop rather than hang around long enough to be arrested.

Darktrace detects malware regardless of the name or strain. It stopped Maze last year, and, as we shall see below, it stopped its successor Egregor, even though the code and C2 endpoints used in the intrusion had never been seen before.

DarkSide famously closed down after the Colonial Pipeline attacks, only nine months after it had been created. An admin from the Ziggy gang announced that it would issue refunds and was looking for a job as a threat hunter.

"Hi. I am Ziggy ransomware administrator. We decided to publish all decryption keys. We are very sad about what we did. As soon as possible, all the keys will be published in this channel."

Take this apology with a pinch of salt. The players which have 'closed down' have not had a change of heart, they've just changed tack. Different names and new infrastructure can help keep the heat off and circumvent US sanctions or federal scrutiny. PayloadBIN (a new ransomware that cropped up last month), WastedLocker, Dridex, Hades, Phoenix, Indrik Spider… all just aliases for one single group: Evil Corp.

The FBI are becoming more aggressive in their methods of infiltration and disruption, so it is likely we will see more of these U-turns and guerrilla-style tactics. Temporary pop-up gangs are an emerging trend in place of large, established enterprises like REvil, whose websites also vanished following the attack against Kaseya. And there is no doubt we will continue to witness these 'exit scams', where groups retire and re-brand, like Maze did last September, when it came back as Egregor.

Darktrace detects malware regardless of the name or strain. It stopped Maze last year, and, as we shall see below, it stopped its successor Egregor, even though the code and C2 endpoints used in the intrusion had never been seen before.

Egregor ransomware attack

Back in November 2020, Egregor was in full bloom, targeting major organisations and exfiltrating data in 'double extortion' attacks. At a logistics company in Europe with around 20,000 active devices, during a Darktrace Proof of Value (POV) trial, Egregor struck.

As a Ransomware-as-a-Service (RaaS) gang, it appears Egregor had partnered with botnet providers to facilitate initial access. In this case, the compromised device carried signs of prior infection. It was seen connecting to an apparent Webex endpoint, before connecting to the Akamai doppelganger,

> Ransomware attacks are occurring at a speed that even five years ago was unimaginable. In this case, the overall dwell time was less than a week, and part of the attack happened out of office hours.

amajai-technologies[.]network. This activity was followed by a number of command and control (C2) and exfiltration-related breaches.

Three days later, Darktrace observed lateral movement over HTTPS. Another device – a server – was seen connecting to the **amajai** host. This server wrote unusual **numeric executables** to shared SMB drives and took new service control. A third host then made a ~50GB upload to a rare IP.

After two days, encryption began. This triggered multiple hosts breaches. On the final day, the attacker made large uploads to various endpoints, all from ostensibly compromised hosts.

Retrospective analysis

If the attack had not been neutralised at this point, it could have resulted in significant financial loss and reputational damage for the company. The two-pronged attack enabled Egregor both to encrypt critical resources and to exfiltrate them, with a view to publicising sensitive data if the victims refused to pay up.

The affiliates who deployed the ransomware in this case were highly skilled. They leveraged a number of sophisticated techniques including the use of a large number of C2 endpoints, with doppelgangers and off-the-shelf tools.

The adoption of HTTPS for lateral movement and reconnaissance reduced lateral noise for scans and enumeration. The complex C2 had numerous endpoints, some of which were doppelgangers of legitimate sites. Furthermore, some malware was downloaded as masqueraded files: the mimetype Octet Streams were downloaded as ‘g.pixel’. These three tactics helped obfuscate the attacker’s movements and trick traditional security tools.

Ransomware attacks are occurring at a speed that even five years ago was unimaginable. In this case, the overall dwell time was less than a week, and part of the attack happened out of office hours. This highlights the need for Autonomous Response, which can keep up with novel threats and does not rely on humans being in the loop to contain cyber-attacks.

Gone today, here tomorrow

Egregor was busted in February, but we may well see it resurface under a different name and with modified code. If and when this happens, signatures will be of no use. Catching never-before-seen ransomware, which employs novel methods of intrusion and extortion, requires a different approach.

The endpoint in the case study above is now associated via open-source intelligence (OSINT) with Cobalt Strike. But at the time of the investigation, the C2 was unlisted. Similarly, the malware was unknown to OSINT and thus evaded signature-based tools.

Despite this, self-learning AI detected every single stage of the in-progress attack. No action was taken as it was only a trial POV so Darktrace had no remote access in the environment. However, after seeing the power of the technology, the organisation decided to implement Darktrace across its digital estate. □

Justin Fier is Director of Cyber Intelligence & Analytics at Darktrace.

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

DARKTRACE

Avoiding storage data leaks and PII regulation noncompliance

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

OPSWAT reports

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

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

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

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

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

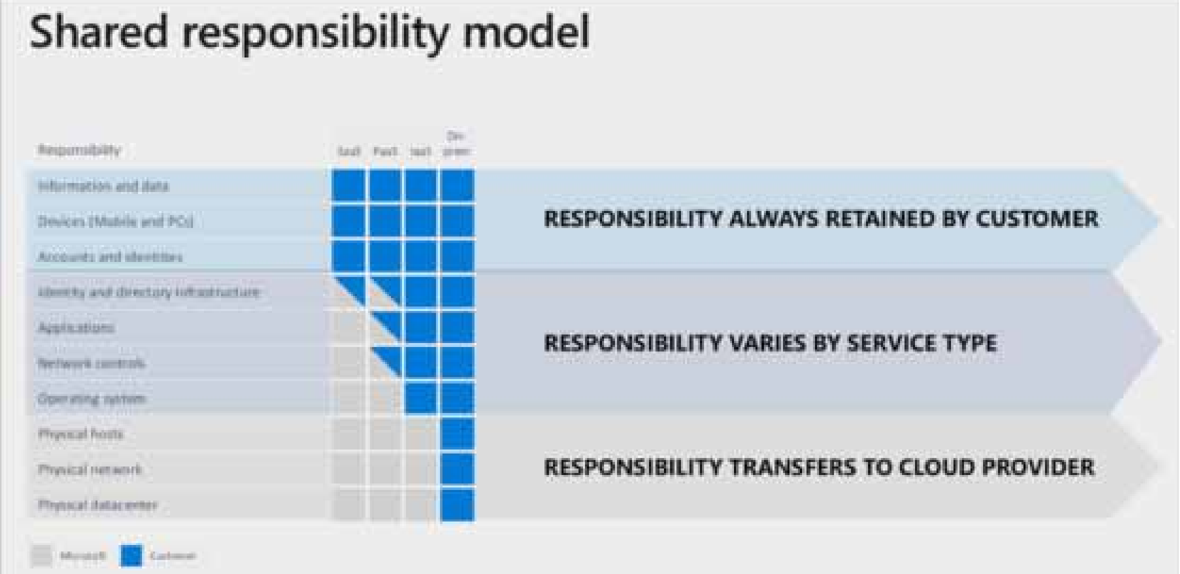
- *Use DLP* (Data Loss Protection) to identify personal data (PII) in files before they are uploaded and stored in the cloud
- *Use CDR* (Content Disarm and Reconstruction) on any file saved to the cloud to verify it does not carry any malicious 'payload' that is aimed to steal information
- *Take remediation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

OPSWAT designed MetaDefender for Secure Storage to cover the security holes for files and data uploaded to the most common cloud storage providers like AWS(S3), OneDrive, SharePoint, Azure, Box, Dropbox, Google drive and more.

The easy to integrate solution helps you secure and protect your mission critical data (whether stored on the cloud or on-premises) before it can be targeted by hackers, and helps you meet regulatory compliance requirements. □

For more information, please visit
www.opswat.com

OPSWAT.



Critical Infrastructure Protection Solutions

Cross-Domain Solutions

Secure Device Access

Network Access Control

File Upload Security

Malware Analysis

Email Security

Storage Security

Developer Tools

OPSWAT.com

The Synack platform expands to confront the cyber-skills gap

Changing organisations' approach to cybersecurity.

Peter Blanks reports

At Synack, we're truly committed to making the world a safer place. We're doing that by helping organisations defend themselves against an onslaught of cyber-attacks. We're doing it by harnessing the tremendous power of the Synack Red Team, our community of the most skilled and trusted ethical hackers in the world, and through the most-advanced security tools available today.

Now, the Synack Platform is expanding to help organisations globally overcome the worldwide cybersecurity talent gap. I am excited to announce the launch of **Synack Campaigns** to provide on-demand access to the SRT, who will be available 24/7 to execute specific and unique cybersecurity tasks whenever you need them – and deliver results within hours. This new approach to executing targeted security operations tasks will fundamentally change organisations' approach to cybersecurity by providing on-demand access to this highly skilled community of security researchers.

During my time at Synack, I've seen first hand how the Synack Operations and Customer Success teams creatively engage with the SRT to address a growing range of clients' security operations tasks, in addition to our traditional vulnerability discovery and penetration testing services. Now, we are making these targeted security activities directly available to every organisation in the form of **Synack Campaigns**, available through the new **Synack Catalog**, also launching today on the Synack Client Platform.

I know from speaking to our clients across multiple industries that security teams are struggling to keep pace with the speed of product development. At the same time, they are trying to scale defences to meet the complexity and magnitude of today's threats. Our customers ascribe challenges with their growing backlog of security tasks such as CVE checks and cloud configuration reviews. On top of all of that, there's the need to implement industry best-practice frameworks such as OWASP & Mitre Att&ck. Essentially, customer security teams are struggling with demanding workloads and have asked us for assistance in a number of areas:

- On-demand access to talented Synack Red Team members who are available 24/7 and capable of completing diverse security operations activities across a growing range of assets.
- A flexible security solution that can be configured to meet their specific needs in one centralised platform with their existing pentesting insights.
- A security solution that delivers results quickly *(hours and days, not weeks or months)* and is aligned with their agile development processes.

Synack Campaigns expands the core capabilities of the **Synack Platform**, including our trusted community of researchers, an extensive set of workflows, payment services, secure access controls and intelligent skills-based task-routing to provide customers with the ability to execute a growing catalog of cybersecurity operations.

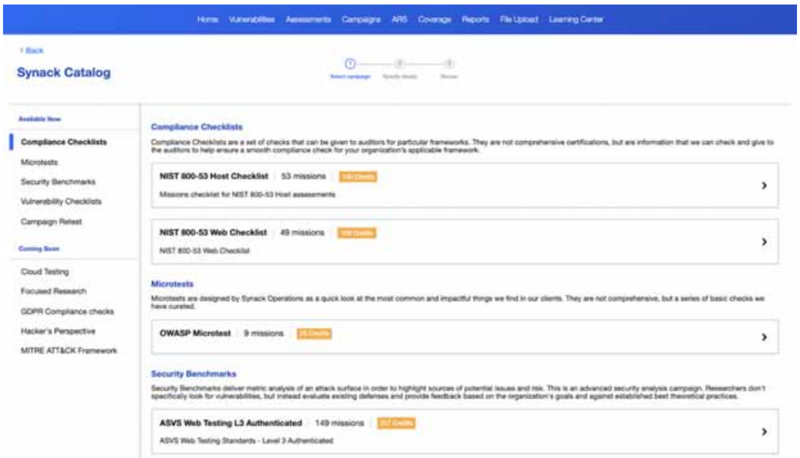
With **Synack Campaigns** our researchers can augment internal security teams by performing targeted security checks such as:

- CVE and OWASP Top 10 vulnerability checks
- Cloud configuration checks
- Compliance testing (NIST, PCI, GDPR, etc.)
- ASVS checks

Synack Campaigns are built to complement our vulnerability management and pentesting services, and help customers achieve long-term security objectives, such as application security, M&A due diligence, and vulnerability management.

We are excited for you to learn more about **Synack Campaigns** and to hear how you and your teams would like to leverage our on-demand community of researchers to address your organisation's growing operational security needs. □

The new **Synack Catalog**, where customers can discover, configure, purchase and launch **Synack Campaigns is available** now on the Synack Client Portal. Please speak with your CSM to have this feature enabled for your organisation.



Synack Catalog

Compliance Checklists

Compliance Checklists are a set of checks that can be given to auditors for particular frameworks. They are not comprehensive certifications, but are information that we can check and give to the auditors to help ensure a smooth compliance check for your organization's applicable framework.

NIST 800-53 Host Checklist | 53 missions | [illegible]
Missions checklist for NIST 800-53 Host assessments

NIST 800-53 Web Checklist | 49 missions | [illegible]
NIST 800-53 Web Checklist

Microtests

Microtests are designed by Synack Operations as a quick look at the most common and impactful things we find in our clients. They are not comprehensive, but a series of basic checks we have curated.

OWASP Microtest | 9 missions | [illegible]

Security Benchmarks

Security Benchmarks deliver metric analysis of an attack surface in order to highlight sources of potential issues and risk. This is an advanced security analysis campaign. Researchers don't specifically look for vulnerabilities, but instead evaluate existing defenses and provide feedback based on the organization's goals and against established best theoretical practices.

ASVS Web Testing L3 Authenticated | 149 missions | [illegible]
ASVS Web Testing Standards - Level 3 Authenticated

Peter Blanks is Chief Product Officer at Synack.

Reach out to us with your thoughts or for more information visit us at **www.synack.com**

GATEWATCHER

AIONIQ

Augmented Detection

100%
assets cartography

100%
NDR

100%
cyber-risks modeling

www.gatewatcher.com

AionIQ to detect the most advanced attacks

Most advanced attacks are leveraging the best technics to compromise, evade and finally leak critical information. Defensive posture must be also ubiquitous.

Luis Delabarre reports

AionIQ to detect complex attacks

NDR experts used to say that the network never lies, compared to endpoint where any solution could be compromised. Nevertheless, to improve the overall level of security of our customers, conventional technics are definitely not enough.

We also know that detection is the most important use case for any NDR implementation, on top of hunting, forensics and response. And we are not minimising other detections or other key features like visibility of all assets, risk-based approach, Mitre ATT&CK classification. But we also acknowledge the reality of machine learning today, as long as the cybersecurity industry explains the technics implemented, instead of just providing a silver bullet.

With AionIQ, machine learning plays a major role in the continuous improvement of our detection technics, to cope with our customers' complex environments. We strongly believe that the future of 'explained and hybrid' machine learning, in addition to other advanced solution like Shellcode detection, in cybersecurity is bright and endless.

Machine learning applied to AionIQ

Since day 1, we believe that the cybersecurity challenges we are all facing are not addressable using a single approach. Even the very promising Unsupervised approach alone, called anomaly detection (identifying outliers or deviation after building the 'normal' baseline) cannot face the most complex attacks, or the most dynamic environments. That is why, by design, we provide to our customers an integrated solution based on advanced signatures-based IDS, real time detection of Shellcodes and malicious PowerShells, anti-malware engines, in addition to a very large AI/machine learning arsenal.

Even if we don't want to oppose the different machine learning 'families', we confess that we are also leveraging unsupervised algorithms (outliers' detection), but we decided to adopt a more disruptive approach:

- Our choice of machine learning algorithms is driven by **use cases**.

A second driving principle is our willingness to avoid Cloud processing for our customers' data. Our machine learning algorithms should fit in our AionIQ software and hardware (when relevant) components, to become the **only fully air-gapped NDR solution** on the market.

There is a large consensus about the learning/training delay required to build an efficient unsupervised model, and we also have the objective to deliver to our customers out of the box detection models. This is why we strongly believe that hybrid models is the most relevant approach in cybersecurity.

The table below will give you a better understanding of the different use cases chosen and their associated type of machine learning models (this list

DGA detection	Supervised	DNS	Protocol analysis and our algorithm are detecting random generated domain names (https://attack.mitre.org/techniques/T1568/002/).
Ransomware detection	Semi-supervised	SMB	The algorithm is detecting anomaly in file operations (read/write) through SMB.
Phishing	Hybrid/supervised	SMTP	In this hybrid approach (with Deep Learning), we are detecting malicious URL in e-mails.
Ransomware detection	Deep learning	Files	We are implementing LSTM neural networks to combine fuzzy hashes with other features to detect similarities and categorise files.
Malicious authentication	Hybrid/supervised	Kerberos	A combination of Graph and Supervised algorithm is detecting malicious attacks in Kerberos protocols. A kind of UEBA approach.
False positive ratio	Semi-supervised	Alerts	False positive ratio reduction with clustering.
Augmented analyst	Supervised	Alerts/triage output	Supervised algorithm to provide guidance or recommendations to analysts.

Verecundus catelli lucide miscere adlaudabilis cathedras, quod suis insectat fiducias, quamquam verecundus suis senesceret catelli. Bellus apparatus bellis fortiter adquireret Aquae Sulis, etiam

is not exhaustive).

We stated above that Graph on top of any other Machine learning algorithm is delivering a superior solution with more efficiency and explicability; thanks to the context added by the Graphs (nodes and relations). More generally, Graph is already a very promising solution for cybersecurity, and **Graph ML** is actually even more interesting from an attack's detection perspective (https://medium.com/oracledevs/graphs-and-machine-learning-for-cybersecurity-7115b9b544b5).

In a nutshell, Graph ML is part of Gatewatcher's technics our data scientists have implemented in AionIQ.

Real time detection augmented by CTI

Many people consider real time detection based on static rules as an outdated approach. We address this fact by fully integrating cyber-threat intelligence in our real time detection engine. Automation and high-quality intelligence are key to providing a very low false positive ratio. We consider that north–south traffic detection is a very good candidate for real time detection with rules generated with new IoCs and IoAs.

Dynamic malware detection

We combine in the same solution 16 different anti-malware solutions with dynamic file analysis to detect malicious files, not only in the north–south traffic but also at the core of any environment.

Zero-day detection

More than often, malicious actors are leveraging vulnerabilities with specifically crafted encoded shellcode (platforms like Empire, Cobalt Strike are simplifying the shellcode generation phase) remotely. Therefore, being able to detect these network payloads is also a major breakthrough in this domain.

Gatewatcher has developed a technology (also combined with AI) to detect malicious shellcodes and PowerShell.

Automatic hunting

Gartner has identified the investigation/hunting use case as important as the three others (detection, intelligence, response), and we acknowledge the criticality of this function in an SOC because it's one of the few catalysts to switch from a defensive to a pro-active posture.

As you may know, threat hunting offers many benefits, including:

- Reduction in breaches and breach attempts
- A smaller attack surface with fewer attack vectors
- Increase in the speed and accuracy of a response
- Measurable improvements in the security of your environment
- Moreover, CTI and automation are also a requirement to augment your analysts' day to day duty

Who we are?

European leader in intrusion and advanced threat detection, Gatewatcher has been protecting critical networks of large companies and public institutions since 2015. Our solutions provide immediate improvement to current cybersecurity challenges and through an adapted response to the growing threat detection needs of organisations.

Our vision is to offer a flexible (cloud, on-premise, hybrid), scalable, innovative, open to new technologies and artificial intelligence approach without disrupting the architecture in place. But also,

Luis Delabarre is Solution Architect – Director at Gatewatcher.
luis.delabarre@gatewatcher.com

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

Ransomware 3.0: The threat layer will become even more critical

The focus must be on initiating the right defensive measures in the right places against the right things in the right amount.

Jelle Wieringa reports

The future trends in the field of computer security and cybercrime occupy the experts every year. The question that always arises is whether the attacks will get worse next year or whether the cybersecurity industry will succeed in preventing cybercrime and thus malware activity as a whole will actually decline.

Year after year, more and more attacks are occurring, and the bitter lesson is that the cybersecurity industry is not yet able to implement robust defence measures to at least slow down the continued rise of cybercrime. For a few years now, criminals have been using ransomware to extort billions of dollars and euros a year, paralyse hospitals, shutting down businesses and blackmailing entire cities.

Developments in 2021

Statistics from the latest European Union Agency for Cybersecurity (ENISA) Threat Landscape Report, based on trends in responses to ransomware incidents, show which ransomware groups have been particularly successful this year. The largest market shares in the first quarter of 2021 are REvil/Sodinokibi (14.2%), Conti V2 (10.2%), Lockbit (7.5%), Clop (7.1%) and Egregor (5.3%). In the second quarter, Sodinokibi (16.5%), Conti V2 (4.4%), Avaddon (5.4%), Mespinoza (4.9%) and Hello Kitty (4.5%) are at the top.

The dominance of Conti and REvil in the ransomware market in 2021 is illustrated by these figures, both from a financial point of view and in terms of the number of incidents. However, no attacks by the original groups REvil/Sodinokibi and Darkside are expected in the coming months, as they have now ceased their activities.

Ransomware 2.0 – Fivefold blackmail

First, a look back. At the end of 2019, the blackmailers began using ransomware to exfiltrate data, which is now commonly known as double blackmail. Ransomware programs and gangs are also active in the following areas beyond traditional encryption:

- Theft of intellectual property/data
- Threat to employees and customers of the victim
- Using stolen data to spear phishing partners and customers
- Public display of victims

The most important thing about these new ransomware activities is that none of the new threats can be mitigated by a good backup. It is believed that the five-fold extortion is now practiced in over 90% of all ransomware incidents. According to the US Treasury Department, the 10 largest ransomware gangs have collected at least $5.2 billion in extortion funds. The total cost, including damage and restoration costs, is estimated to be up to $265 billion by 2031. There have also been successful attacks on critical infrastructure, including national gas pipelines and food consortia. More than half of all businesses have already been attacked by ransomware, and an even higher percentage is expected to be affected this year and next. The percentage of victims who pay the ransom (over 60%) and the average ransomware extortion sum (US$280.000) also continue to rise.

At the beginning of the five-fold blackmail phase, the ransomware 2.0 phase, ransomware gangs realised that the ultimate value they possessed was not the ability to encrypt or even exfiltrate the data of a compromised victim. The real 'Holy Grail' was unrestricted access to the victim's digital resources. In hacker language, this is called 'pwning' of the victim. They break in, get all the passwords, including passwords for administrator accounts, and then have access to everything that the legitimate administrators have access to.

The devastating potential of ransomware 3.0

The ransomware gangs are gradually evolving into multi-faceted attack gangs that are no longer limited to encryption and five-fold extortion, but are expanding their portfolio to include other related or unrelated activities, including:

- Sale of stolen, exfiltrated access data and initial access
- Theft of money from bank and stock accounts
- Personal blackmail of individuals
- Hacking against payment
- Selling lead lists from stolen customer data
- Business email compromise
- Install adware and launch DDoS attacks
- Cryptomining and creation of rentable botnets

Current reports show that cybercriminals usually use attack strategies that are easily scalable and can be used in large numbers against different victims. The novel, three-stage attack strategy, consisting of the former banking Trojan Emotet, the trickbot malware and the Ryuk ransomware, allows attackers to deploy attack strategies en masse that had previously only been known from strategically targeted APT spying attacks. As a first step, the Emotet Trojan spreads via Outlook harvesting by analysing the victim's email traffic and then using it for authentic-looking social engineering attacks on the victim's contacts. In addition, it has downloader functionalities, so that the attackers can install the spy malware Trickbot on the infected systems in the second step. Trickbot allows the attackers to set up extensive espionage activities on the infected systems. The ransomware Ryuk is rolled out to particularly lucrative victims and then the extortion of ransom takes place.

Variety of attack variants

The ransomware gangs have expanded their methods, whereas in the past they mainly carried out the traditional ransomware five-fold blackmail, recently they have also ventured into other areas of work. Brian Krebs recently reported on the Conti ransomware gang selling the first access to the compromised victims. This is the opposite of what was common until recently. Previously, it was the ransomware gangs that bought the first access to new victims to start the ransomware process, and now they are becoming the original sellers of that access.

It is known that some ransomware gangs installed cryptomining bots on victims' computers before they started encrypting the data. The Rakhni Trojan has long delivered both ransomware and cryptomining bots to victims, often for the same gangs. They receive the money they earn from cryptomining and in addition the sum they can extort through the result of the encryption incident. Ransomware gangs like Avaddon and Sun.Crypt are known to simultaneously carry out DDoS attacks and encrypt victims' data to inflict more damage on them, getting them to pay faster.

Some reporting actors are beginning to use DDoS as the first and only method of attack against the victims. An example of this is the very popular REvil ransomware gang, which blackmailed a popular VoIP provider into paying a $4.2 million ransom to stop the DDoS attack that brought the victim's services to a standstill. The ransomware gangs don't even try to encrypt the victim's files. They simply start and end with the DDoS attack.

Ransomware 4.0 – automation

Currently, most ransomware groups first gain access, then install the malware as a backdoor, and notify the scammers' command-and-control (C&C) servers so that the ransomware group or their partners can learn about the new compromised victim. The original malware can collect some passwords and details of the environment, download and install other malware, and then wait for further instructions. Then the hackers initiate the new actions, be it data exfiltration or starting the encryption routines. Ultimately, the future of cybersecurity and hacking will be for the bots that hunt threats to compete against malicious all-rounder bots, adapting on the fly and presumably triumphing in the end.

Effective prevention through security awareness

Preventing a ransomware infection, no matter how automated and sophisticated it is, always works the same way. The focus must be on initiating the right defensive measures in the right places against the right things in the right amount. The problem is never the ransomware itself, but the way the ransomware was able to get into the system in the first place. The two main methods attackers use to penetrate are social engineering and unpatched software. If you can't effectively fend off these threats, you'll usually fall victim to a cyber-attack at some point. Preventing social engineering, with the help of patches, MFA, and good password policies, greatly increases resilience to hackers and malware, including ransomware. The most effective measure to prevent such attacks is a comprehensive security awareness training for employees. Basically, an attempt is made to use simulated phishing mails to test how attentive the employees are.

The number of successful phishing attacks on the company can be greatly reduced by such training and in addition to the technical security options, the employees can thus be established as a human firewall.

Outlook

At the moment, ransomware groups that take the complex path of Blackmail 4.0 are the minority. However, the importance of this minority is growing more and more. In comparison, the simple encryption of company data by infiltrated ransomware programs is harmless. However, the solution to these novel threats continues to be to combat social engineering, use good patches, deploy MFA, and implement an effective password policy. The improvement of existing protective measures and a high level of security awareness of all users form the foundation for being prepared against future ransomware attacks. □

For more information, please visit
www.knowbe4.com

KnowBe4
Human error. Conquered.

20th e-Crime & Cybersecurity Congress

e-crime & cybersecurity CONGRESS

2nd & 3rd March 2022 Online

“While this e-Crime was different, it was more valuable than ever, bringing my home-desk straight to the key topics, issues, speakers and solutions, to consider e-crime risks and controls in the New Normal! ”

Snr IT Risk Manager IT Infra Assurance, Diligenta Limited

“I found the event highly relevant for the issues faced across the industry. The ranges of topics and multiple viewpoints being discussed helped to confirm existing strategies, inform others underway and prompt further discussion. Overall a good two days investment; congratulations to the AKJ team. ”

Principal Advisors, Mastercard

“e-Crime & Cybersecurity Congress 2021 is one of the best cyber conferences on the UK circuit. This year was a first being carried out remotely and very different to the normal 2-day event in person in London due to Covid-19. I found this remote approach worked very well and there was a great selection of speakers available and some excellent educational seminars. I also found the panel discussions very informative with a great selection of representative experts from their respective fields to provide a good and balanced view. I also found the resources very useful and thought it was a great touch that you could pause a session if required and that it was also available for 20 mins or so after it started in case you needed to attend to another matter prior to attending. Very good overall as ever, fingers crossed the mid-year review will be back in person again covid depending! ”

Information Security Officer, North Group

“Great job done by all involved. The virtual conference operated flawlessly given the variables of presentations given. I also enjoyed still having the ability to join with likeminded people, learn the challenges people are facing, or what is going right as well as of course the nod to the products out there. ”

Security Consultancy Specialist Cyber Threat Management, BT

“The e-Crime & Cybersecurity Congress is a must for people within many areas of industry, as the speakers excellent, the content very relevant, the presentations fantastic, and the event excellent. I left feeling more informed and ready for new challenges. ”

Senior Manager Operational Risk (IT Risk)/ Data Protection Officer, UBL

2021 Congress sponsors included:

Strategic sponsors

BeyondTrust
censornet.
COFENSE
DARKTRACE
egress
illumio
INTSIGHTS Democratizing Threat Intelligence™
okta
OneTrust GRC INTEGRATED RISK MANAGEMENT
Recorded Future®
SentinelOne™
sixgill

Education Seminar Sponsors

BARRIER
bitglass
CyGlass by NOMINET
INTEL471
KENNA Security
KEYSIGHT TECHNOLOGIES
LogRhythm®
ManageEngine
Menlo Security
onelogin
OPSWAT.
RANGEFORCE
Synack.
tenable
tripwire®

Networking Sponsors

ThreatConnect®

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

Thank you to all our sponsors

Strategic Sponsors

BeyondTrust

DARKTRACE

INTSIGHTS
A RAPID7 COMPANY

KnowBe4
Human error. Conquered.

Lookout

Recorded Future®

SentinelOne™

Education Seminar Sponsors

corelight

GATEWATCHER

CISCO
KENNA
Security

onelogin

OPSWAT.

Synack.

Networking Sponsors

DEVO