e-crime & cybersecurity BENELUX

7th December 2023
Amsterdam, The Netherlands

@eCrime_Congress
#ecrimecongress

#ecrimecongress

From NIS2 to AI:
The cybersecurity juggling act

Forthcoming events

PCI LONDON 24th January 2024 London	SECURING THE LAW FIRM 25th January 2024 London	SECURING FINANCIAL SERVICES 25th January 2024 London	e-crime & cybersecurity NORDICS 30th January 2024 Helsinki
e-crime & cybersecurity GERMANY 30th January 2024 Frankfurt	e-crime & cybersecurity CONGRESS 28th & 29th February 2024 London	e-crime & cybersecurity CONGRESS 6th March 2024 Dubai	e-crime & cybersecurity NORDICS 25th April 2024 Stockholm
e-crime & cybersecurity AUSTRIA May 2024 Vienna	e-crime & cybersecurity FRANCE 30th May 2024 Paris	e-crime & cybersecurity GERMANY June 2024 Munich	SECURING THE LAW FIRM July 2024 London
SECURING FINANCIAL SERVICES July 2024 London	SECURING THE PUBLIC SECTOR July 2024 London	e-crime & cybersecurity CONGRESS September 2024 Abu Dhabi	e-crime & cybersecurity SWITZERLAND September 2024 Zurich

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

Generative AI is hogging the headlines and some European governments (like Finland's) have even factored the AI threat into new budgets for cybersecurity.

And it is true that AI is already being used to develop new hacks – such as cloning voice authentication or using Deepfakes. In addition, the availability of programs like chatGPT give employees new ways to be insecure. And AI promises to supercharge the threat development cycle.

But organisations have much more to think about than AI.

New regulations, NIS2 in particular in Europe but others elsewhere, are expanding the universe of businesses that fall under the most rigorous regime. They are creating ever more significant penalties for firms and their executives for security and disclosure failings. And they create new obligations that CISOs and other compliance and assurance professionals must act on.

At the same time, CISOs must still get on with foundational cyber-hygiene. They must continue the fight against phishing and third-party attacks. And they must continue to improve security culture and awareness through training and other means.

In this event, we will be looking at these different sides of the cybersecurity challenge. Our end-user speakers will discuss their current use of AI in security and in the business, and their hopes and fears around future developments.

They will also give their most up-to-date insights into the more everyday issues they face in terms of threats, solutions, budgets, staffing and the evolution of the cybersecurity function at their organisations.

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

Simon Brady | Chairman

@eCrime_Congress **#ecrimecongress**

7th December 2023

Novotel Amsterdam City

3 **Ransomware 3.0: The threat layer will become even more critical**
The ransomware gangs are gradually evolving into multi-faceted attack gangs that are no longer limited to encryption and five-fold extortion.
KnowBe4

5 **4 key insights from the 2023 Gartner® Market Guide for Microsegmentation**
Here are the top insights that we believe stood out from the report.
Illumio

9 **What is NDR (network detection and response)?**
Learn what NDR is, why the traffic crossing your network is foundational to your cyber-defence strategy, and how the network evidence from Corelight's Open NDR Platform helps data-first defenders disrupt ever-changing attacks.
Corelight

11 **We don't have a malware problem, we have an adversary problem**
Cyber-adversaries are finding new ways to broaden their reach and optimise attacks.
CrowdStrike

15 **XDR: Reducing complexity and cost while improving incident response and remediation**
Three key insights from CISOs to help you prioritise as you look to adopt XDR.
SentinelOne

17 **NDR and NIS 2 – How to transform an obligation in an opportunity**
Meet the NIS 2 compliance requirements serenely with Gatewatcher.
Gatewatcher

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
e: simon.brady@akjassociates.com

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

20 Sponsors and exhibitors
Who they are and what they do.

24 Agenda
What is happening and when.

26 Education seminars
Throughout the day a series of education seminars will take place as part of the main agenda.

29 Speakers and panellists
Names and biographies.

33 How TomTom automatically navigated human cyber-risk
A Hoxhunt case study.
Hoxhunt

37 From speed to consistency: The power of automation for your SOC
This article will provide insights from a conversation with experts from Recorded Future, Splunk, Ernst & Young, and NOV on automation best practices and tips on how to get started.
Recorded Future

39 Quick wins: 3 ways to act on security operations metrics
This blog provides three actionable steps for security teams to achieve desired metric outcomes, without significant time or resource investment.
ReliaQuest

42 Protect the new attack surface: How organisations can break the attack chain
Cybercriminals continue to target humans, rather than infrastructure and their attacks remain inherently 'people-centric'.
Proofpoint

45 5 tips for cybersecurity success and ransomware resilience
Five tips every organisation should consider when protecting itself against cyber-threats
S-RM

Ransomware 3.0: The threat layer will become even more critical

The ransomware gangs are gradually evolving into multi-faceted attack gangs that are no longer limited to encryption and five-fold extortion.

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 fivefold 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 (280.000 US dollars) also continue to rise.

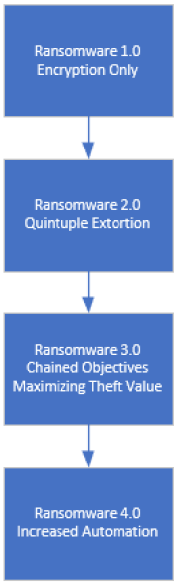
At the beginning of the five-fold blackmail phase, the ransomware 2.0 phase, ransomware gangs realised that the ultimate value they possessed was not the ability to encrypt or even exfiltrate the data of a compromised victim. The real 'Holy Grail' was unrestricted access to the victim's digital resources. 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
- Crypto-mining 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 crypto mining bots on victims' computers before they started encrypting the data. The Rakhni Trojan has long delivered both ransomware and crypto-mining bots to victims, often for the same gangs. They receive the money they earn from crypto-mining 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. □

Jelle Wieringa is Security Awareness Advocate at KnowBe4.

For more information, please visit **www.knowbe4.com**

KnowBe4
Human error. Conquered.

4 key insights from the 2023 Gartner® Market Guide for Microsegmentation

Here are the top insights that we believe stood out from the report.

Raghu Nandakumara reports

Growing hybrid environments, building Zero Trust initiatives, and increasing risk of lateral movement – if these sound like your organisation's cybersecurity concerns, you're not alone.

And you're likely finding that the traditional detection and prevention tools you've been using aren't enough to secure against today's complex threat landscape. Ransomware and breaches are inevitable, and it's vital that your organisation has a way to stop and contain the spread of breaches.

The first-ever Gartner® Market Guide for Microsegmentation recommends implementing microsegmentation, also called Zero Trust Segmentation (ZTS), to secure hybrid environments, stop lateral movement, and build Zero Trust. Illumio has been named as a Representative Vendor for microsegmentation in the report.

Read the full Market Guide here.

4 takeaways from the Gartner Market Guide

Here are the top insights that we believe stood out from the report:

1. **By 2026, 60% of enterprises working toward zero trust architecture will use more than one deployment form of microsegmentation, which is up from less than 5% in 2023**

In the report, Gartner explains that traditional perimeter-based security can enforce policies between network sites but can't segment traffic between workloads. Network firewalls simply can't keep up with the scale and pace of today's infrastructure.

That's why cybersecurity leaders are turning to ZTS, says Gartner. They're looking for ways to enable security policies at the workload level to enforce Zero Trust principles, stop lateral movement, and limit the blast radius of breaches.

In fact, according to Gartner, "By 2026, 60% of enterprises working toward Zero Trust architecture will use more than one deployment form of microsegmentation, which is up from less than 5% in 2023."

This reflects a growing realisation that it simply doesn't make sense to use yesterday's security to protect today's and tomorrow's complex environments from breaches.

> Ransomware and breaches are everyone's concern – making ZTS an essential, high-value technology.

2. **Gartner sees interest across all verticals and geographies**

It's no longer acceptable to assume that certain organisations can be excluded from cybersecurity concerns based on their size, industry, or location. Over the last few years, we have seen organisations from every industry targeted by ransomware gangs as they seek to cause maximum disruptions.

Ransomware and breaches are everyone's concern – making ZTS an essential, high-value technology.

The new guide says that "Gartner sees interest across all verticals and geographies. Midsize organisations are evaluating microsegmentation solutions, which is a relatively new development."

It's important for organisations to look for vendors that offer scalable, flexible ZTS implementation that can grow and adapt with their organisation. ZTS vendors should also be able to prove their return on investment (ROI) while offering ways for organisations to see and secure their vulnerabilities.

3. **Perimeter-based security technologies, which are deployed at the edge of on-premises and hosted ('in the cloud') data centres, enforce policies between sites but cannot segment traffic between workloads or processes**

The last few years saw a wave of digital transformation as organisations worked overnight, in many instances, to manage remote work and migration to the cloud. This has introduced a more complex environment and, most importantly, an increase in fragmented perimeters.

Gartner sees cybersecurity leaders turning to Zero Trust security strategies to deal with these risks. This has led organisations to "Implement fine-grained zoning and microsegmentation technologies as a practical way of enforcing Zero Trust principles for public, private, and hybrid cloud infrastructures," says Gartner.

By building granular security policies at the workload level, security teams can protect the risks associated with today's fragmented network perimeters without needing to rely on inconsistent IP addresses.

By building granular security policies at the workload level, security teams can protect the risks associated with today's fragmented network perimeters without needing to rely on inconsistent IP addresses.

4. **Test the tools' capability extensively**
Gartner recommends that cybersecurity leaders prioritise testing the capabilities of ZTS solutions before committing to a vendor.

This includes ensuring the solution can:

- Create rules based on application – identity, tags, labels, and characteristics
- Collect contextual data from various cloud sources, asset inventory, CMDBs, etc.
- Scale seamlessly when implementing these features

We believe, not all ZTS vendors offer all these features, especially in a way that can scale seamlessly, easily integrate with other security tools and platforms, and provide quick, provable ROI.

How Illumio delivers ZTS core capabilities

We believe the core capabilities of ZTS as outlined by Gartner in the report align not only with Illumio's founding purpose but also with the problems we're solving for our customers and the approach we recommend in taking to adopt ZTS in a way that scales and delivers real value.

Find out how we believe Illumio aligns with these core capabilities:

- *Flow mapping, which is the ability to gather and show North/South and East/West traffic flows and use them in the policy definition (it can present this data in a visual manner):* Illumio's application dependency mapping allows organisations to gain easy-to-understand visibility into traffic across all workloads, including containers, IoT, and virtual machines, in a single console. This allows security teams to pinpoint network risks and create security policies that block unnecessary connections between ports.
- *Workload isolation, which is isolation from other workloads based on security policy:* Illumio enables microsegmentation between workloads and uses context (i.e., tags or labels) to define policy between those workloads.
- *Policy enforcement, including the definition of rules based on different factors:* With Illumio, teams can specify security policy without relying on IP addresses, ensuring that policy is flexible and adaptable to network changes.
- *The ability to deploy in the virtualised and infrastructure-as-a-service environments:* Illumio delivers one comprehensive ZTS solution for all on-premises, cloud, and hybrid environments, enabling visibility and policy deployment at scale.

Longer-term, Gartner expects ZTS vendors to offer additional capabilities, including extending ZTS to endpoint devices. Illumio Endpoint already meets this need by dynamically limiting what ports are open and what IP addresses the endpoint can communicate with to stop ransomware and breaches from spreading.

Read the full Market Guide here.

Contact Illumio today for a free consultation and demo. □

Gartner, Market Guide for Microsegmentation, Adam Hils, Rajpreet Kaur, Jeremy D'Hoinne, June 2023

Raghu Nandakumara is Senior Director, Industry Solutions Marketing at Illumio.

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

illumio

Gartner® has named Illumio as a Representative Vendor in its "2023 Market Guide for Microsegmentation."

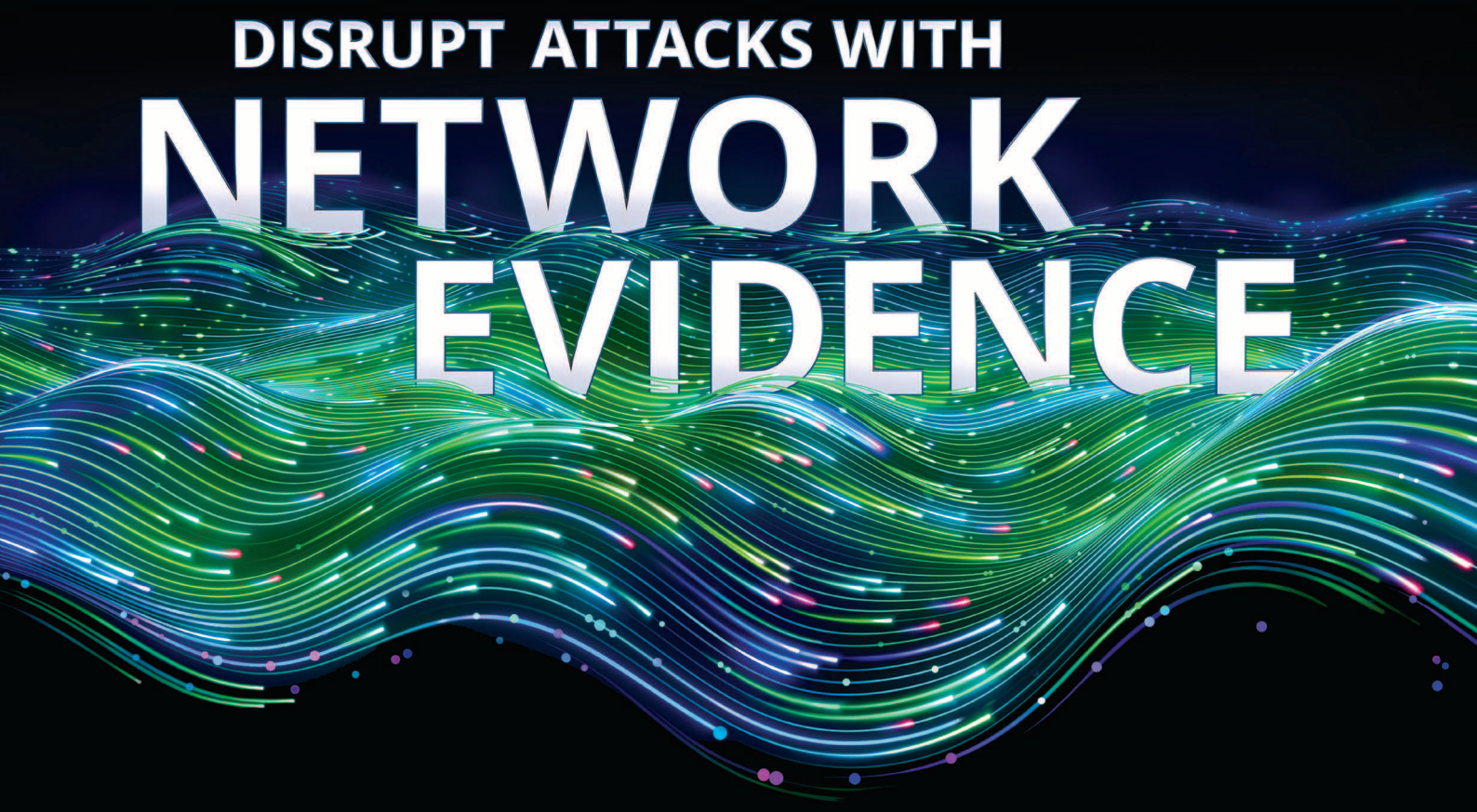
Scan to get the guide so you can better understand the microsegmentation market, choose the right solution —and protect your organization from the spread of breaches and ransomware.

READ THE STUDY

corelight

COMPLETE VISIBILITY | NEXT-LEVEL ANALYTICS | FASTER INVESTIGATION | EXPERT HUNTING

Corelight combines the power of open source and proprietary technologies to deliver a complete **Open Network Detection & Response (NDR) Platform** that includes intrusion detection (IDS), network security monitoring, and Smart PCAP solutions.



Schedule a demo at **corelight.com**

What is NDR (network detection and response)?

Learn what NDR is, why the traffic crossing your network is foundational to your cyber-defence strategy, and how the network evidence from Corelight's Open NDR Platform helps data-first defenders disrupt ever-changing attacks.

What is network detection and response (NDR)?

Network detection and response (NDR) is a cybersecurity technology that continuously monitors network traffic from physical and cloud-based environments to enable security teams to detect adversary activity, respond to incidents, and shore up their security posture.

Why is NDR so important?

Many organisations go days, weeks, months, and even years without realising that they have been infiltrated because, despite their best efforts to create a solid defence system, their security team does not have complete visibility into their network. According to IBM's 'The Cost of a Data Breach' report, in 2022 the average time to identify and contain a breach was 277 days. With time frames like these, an adversary can do some serious damage to an organisation.

The fact is that you cannot defend what you cannot see. To stop a breach, you need to be able to see an adversary's tracks. Often all it takes is a single clue that something looks awry on the network to pull the thread that unravels adversarial activity. According to author and security expert Richard Bejtlich, "The defender only needs to detect one of the indicators of the intruder's presence in order to initiate incident response within the enterprise." This is where network visibility is vital. Adversaries are human and make mistakes, which are then imprinted within network records – just like a burglar who leaves behind a single fingerprint.

That's the fundamental idea of network detection and response (NDR): To find an intruder, you need to be collecting evidence all the time, and one of the best sources for that evidence is the traffic in your network, whether that's in a cloud, a data centre, or a Kubernetes cluster or similar.

Most security operations centres (SOC) security stacks include an endpoint detection and response (EDR) solution to provide depth of coverage, and a security information and event management (SIEM) to aggregate and analyse information. However, while SIEMs and EDR solutions are fundamental to the modern SOC strategy, they are not enough to provide the breadth of coverage – specifically insights into the network itself – that security teams need to proactively defend their organisation.

The fact is that you cannot defend what you cannot see. To stop a breach, you need to be able to see an adversary's tracks.

Network data contains immutable clues about people, devices, applications, and assets that are critical to successful incident response and threat hunting. Attackers use a wide variety of techniques to try to hide their tracks, but ultimately they can't avoid pushing packets across the wire, leaving behind an unchangeable record of their activity. This network record is gold to security teams.

A common misconception among security professionals is that breaches can be stopped by simply 'keeping the bad actors out'. And yet cyber-attacks continue to be successful despite decades of work and billions of dollars spent on security solutions that are intended to stop attackers in their tracks. This is because adversaries are constantly creating new and more sophisticated techniques, tools, and malware that firewalls and intrusion detection/intrusion prevention systems (and other solutions) have never seen before.

Ultimately, 'keeping the bad actors out' leads to a detection-centric and reactive approach, which is not a great strategy in cyber-defence because:

- Too many attacks generate too many alerts, swamping security teams.
- Too many alerts mean lots of false alarms, incidents that aren't run to ground completely, or attacks that are missed.
- Blue teams (defenders) often don't have the data they need to analyse security incidents quickly and accurately.
- Attackers are adept at hiding in plain sight, using 'normal' applications, traffic, and tools to move around networks.
- After breaching an organisation, attackers often lay low for weeks or months, before they act, making their detection even more challenging.

Adversaries are creative, determined, highly motivated, and often well-funded. Whether they are a part of industrial espionage, a nation-state operation,

Corelight reports

Corelight's Open Network Detection and Response (NDR) Platform, which is trusted by some of the biggest names in the industry including CrowdStrike, Microsoft, and Splunk, is the only solution that takes an evidence-based approach to cybersecurity.

are a disgruntled employee, or are just a hacker looking for a challenge, they all pose serious problems for blue teams who are charged with defending their organisations.

What are the benefits of NDR?

According to research from Enterprise Strategy Group (ESG), almost half of organisations use network detection and response (NDR) solutions as a first line of defence for threat detection and response. Why? As the old security saying goes, "the network doesn't lie". Networks create an unavoidable extension of the enterprise attack surface, but when properly monitored they also provide a great source of evidence for investigation when you're attacked. Network data is ground truth.

Here is an overview of why NDR is an essential part of any security tech stack:

- *Expanded network visibility:* One of the most difficult challenges that organisations face is having inconsistent and incomplete visibility across different security layers. NDR eliminates blindspots by illuminating all network activity to and from any asset on monitored segments, providing ground truth for threat detection, incident response, breach disclosure, asset management, and network operations.
- *Improved detection coverage:* The sophistication of threats has increased (and so has the volume of threats), which makes it difficult to distinguish attacks from legitimate traffic. NDR helps security teams quickly detect attacks and MITRE ATT&CK TTPs missed by legacy network security tools and EDR, while providing the context required to understand false positives, drive effective network engineering, and improve accuracy.
- *Accelerated incident response:* Organisations tend to use too many siloed data sources to drive threat detection and response workflows. NDR provides a single source of network truth that gives analysts the comprehensive network evidence they need to more effectively investigate, resolve incidents, and reduce mean time to resolution (MTTR).
- *Reduced operational costs:* Due to economic headwinds and the sheer number of disparate security tools in their stack, many organisations are moving toward a more tightly integrated security operations and analytics platform architecture (SOAPA). NDR consolidates standalone technologies and amplifies SOC automation investments by following the design pattern of elite defenders.

A recent ESG report called 'The Evolving Role of NDR' found that:

- Almost half of organisations have found that network-based tools provide the broadest visibility across the different parts of their environment.
- 53% of organisations have found that NDR tools provide the highest fidelity.
- 60% of organisations improved SOC analyst efficiency with NDR.

Corelight's Open NDR Platform was built to deliver these benefits to security teams of all sizes and levels of sophistication.

Why choose Corelight's Open Network Detection and Response (NDR) platform?

Corelight's Open NDR platform is unique in the industry because our detections and visibility engineering are community driven – with continuous content creation from Zeek®, Suricata IDS, and other Intel communities. Our integration with CrowdStrike XDR enables cross platform (EDR+NDR) analytics. This provides you with the most complete network visibility, powerful analytics, and threat hunting capabilities, and accelerates investigation across your entire kill chain.

Evidence is at the heart of security, and yet not all NDR solutions put network evidence at the centre of their operations. Corelight's Open Network Detection and Response (NDR) Platform, which is trusted by some of the biggest names in the industry including CrowdStrike, Microsoft, and Splunk, is the only solution that takes an evidence-based approach to cybersecurity. □

For more information, please visit
corelight.com

corelight

We don't have a malware problem, we have an adversary problem

Cyber-adversaries are finding new ways to broaden their reach and optimise attacks.

Zeki Turedi reports

Across the globe, cyber-adversaries are finding new ways to broaden their reach, optimise attacks and deepen their impact. According to CrowdStrike's Threat Hunting Report, these groups have adopted more aggressive tactics this past year, exploiting system vulnerabilities, and posing an ever-increasing threat to organisations across Europe.

The report found that adversary breakout time, which tracks the speed at which cybercriminals move laterally within a compromised system, plummeted to an all-time low of 79 minutes. This is a decrease from 84 minutes in 2022, with the fastest time coming in at a record of seven minutes. In less than the time it takes to step away from your desk and make a cup of coffee, this adversary had landed on an initial host and moved laterally into the broader victim environment.

CrowdStrike also observed that these incidents often began with an identity compromise. Adversaries are not relying solely on compromised valid credentials, either – rather, they demonstrated their capacity to abuse all forms of identification and authorisation, including weak credentials from the underground.

These findings are a stark reminder that CISOs must continuously ask their teams, "Are we fast enough at identifying, investigating, and remediating today's threats? Can we detect an adversary in seven minutes or even seven hours?"

Here, we analyse the key trends evident in the report and how CISOs across Europe can prepare for the year ahead as adversaries continue to work harder and smarter.

The European cybersecurity outlook

The financial sector in Europe is especially vulnerable, overtaking telecommunications to become the second-most attacked industry vertical, followed closely behind technology.

Adversaries are not relying solely on compromised valid credentials, either – rather, they demonstrated their capacity to abuse all forms of identification and authorisation, including weak credentials from the underground.

Meanwhile, the telecommunications vertical accounted for at least 10% of all intrusion activity with a significant proportion of intrusions attributed to Iran-nexus threat actors. Cobalt Strike, PsExec, ProcessHacker, Mimikatz and NetScan were the top five tools used in interactive intrusions.

Furthermore, overall e-crime threat actor, VICE SPIDER, was the most prolific in Europe, observed across an alarming 19 industry verticals.

Financial services sector on high alert

The volume of interactive intrusion activity targeting the financial services sector soared by over 80% in the past year.

North Korea-based culprits, especially the LABYRINTH CHOLLIMA group, have significantly ramped up their activities against the financial sector, chiefly targeting fintech organisations. They have now adapted their distinct methods to include tools specifically designed for Linux and macOS platforms.

While some adversaries focus on cryptocurrency and NFT heists, the predominant e-crime threats remain rooted in big game hunting (BGH) ransomware and expansive data theft campaigns.

Identity-based intrusions gain momentum

There is a clear trend indicating that cyber-adversaries are focusing on identity-based attacks. A significant 62% of interactive intrusions saw the exploitation of valid accounts. Disturbingly, there has been a 160% spike in efforts to secure secret keys and credentials via cloud instance metadata APIs.

Contributing to the massive escalation in identity-based intrusions is a 583% increase in Kerberoasting attacks, a technique adversaries can abuse to obtain valid credentials for Microsoft Active Directory service accounts, often providing actors with higher privileges and allowing them to remain undetected in victim environments for longer periods of time.

This technique poses a significant threat to organisations because adversaries do not need elevated privileges to execute this attack. In the past year, attacks against Kerberos were associated

The future of cybersecurity requires tight human-machine collaboration to deal with the speed, volume and advancing sophistication of the adversary.

predominantly with e-crime adversaries. VICE SPIDER was again the most prolific e-crime adversary, responsible for 27% of all intrusions that involved the Kerberoasting technique.

Nowhere to hide

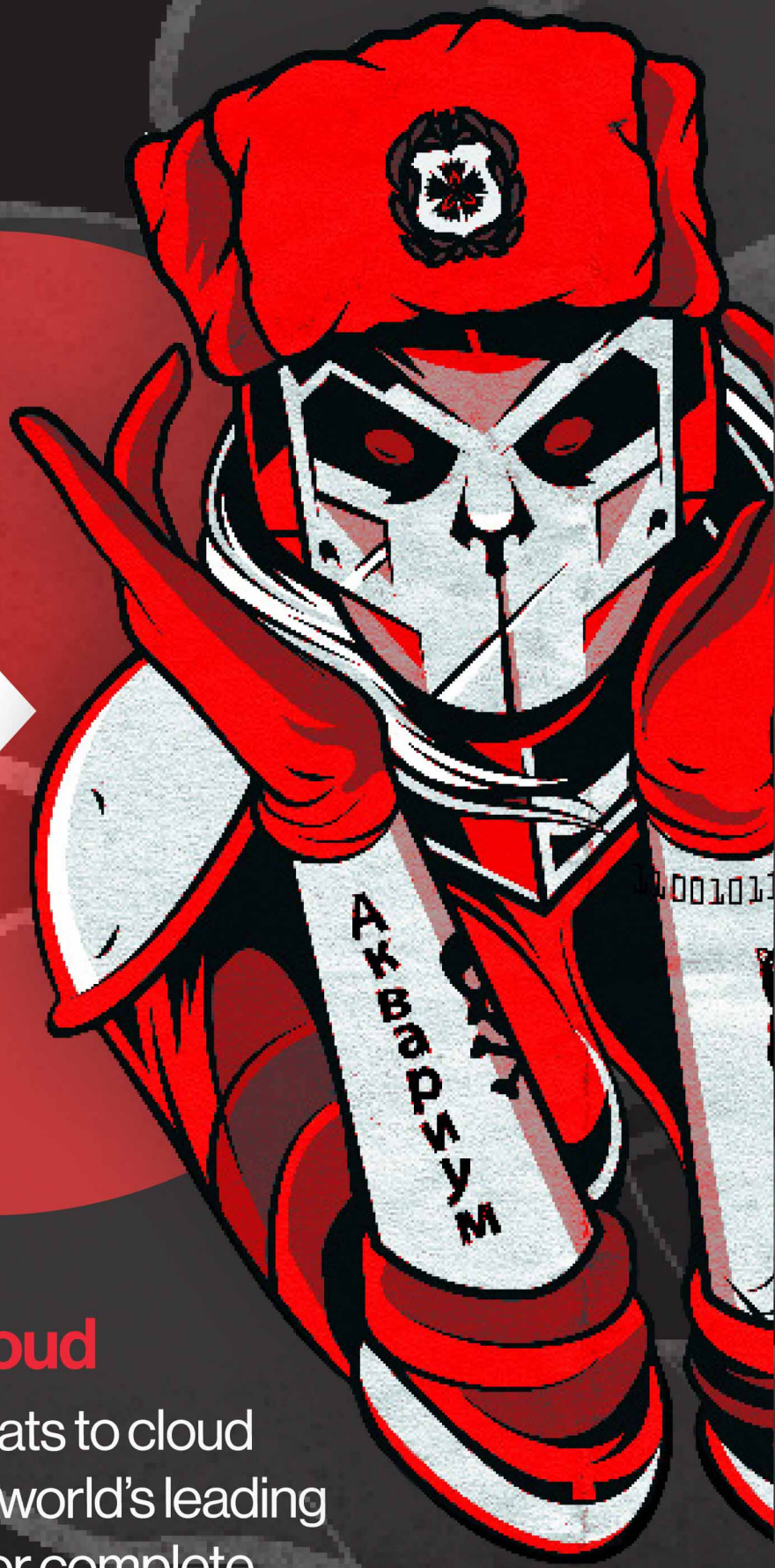
The findings of CrowdStrike's latest Threat Hunting Report show that adversaries in the threat landscape are more agile than a year ago and devastatingly fast. Cybersecurity teams across Europe need to prioritise working closely with their partners to develop strategies that stop breaches at even faster rates and give the modern adversary nowhere to hide.

The future of cybersecurity requires tight human-machine collaboration to deal with the speed, volume and advancing sophistication of the adversary. When executed correctly, teams can rapidly surface hidden threats, accelerate the decision-making of security analysts and streamline the detection process. When combatting a threat that can take control in just seven minutes, there is no room to compromise on security provision. □

Zeki Turedi is Field CTO Europe at CrowdStrike.

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

CROWDSTRIKE



Protecting the Cloud

Combat the rise in threats to cloud environments with the world's leading AI-powered platform for complete cloud security

www.crowdstrike.com


SentinelOne®
See, Protect,
and Resolve it All.
Go Beyond the Endpoint with Singularity XDR.
Learn How at SentinelOne.com

XDR: Reducing complexity and cost while improving incident response and remediation

Three key insights from CISOs to help you prioritise as you look to adopt XDR.

Extended Detection and Response (XDR) has generated a lot of buzz in recent times with security practitioners, analysts, and the vendor community. According to the Gartner Hype Cycle™ for Security Operations, 2022, XDR is at peak market interest, promising to deliver significant security visibility and response improvements to threat exposures.

XDR promises to reduce complexity and cost while improving incident response and remediation, and increasing productivity. Analysts and industry pundits say the potential of XDR is that it can make good on unmet security promises, like those made by SIEM (security information and event management) platforms, accelerating how security teams detect, investigate, and remediate threats with greater productivity and lower ownership costs.

And while many companies are interested in adopting XDR, what should organisations consider as they research the growing number of solutions in the market? Here are three key insights from CISOs we interviewed to help you prioritise as you look to adopt XDR.

Start with an XDR solution with roots in EDR

One common reason for implementing XDR is extending what works currently in their organisation to other attack surfaces – XDR that is based on a solid EDR foundation and all the benefits that brings. That means, for example, drawing on EDR's high-fidelity telemetry to provide critical supporting data from endpoints, as well as the real-time detection and remediation capabilities of EDR.

Good EDRs offer real-time behavioural detection and remediation, which can be deployed more broadly across the organisation with XDR. Alerts that might otherwise have been missed at an early stage can now be identified earlier and remediated before they have a significant impact. And it is easier to get a more complete understanding of what is happening within the whole enterprise security estate.

With SentinelOne's threat intelligence integration, threats are auto enriched from various sources, enabling customers to accelerate threat investigation and triage capabilities.

Look for an XDR solution that increases SecOps efficiency with various built-in integrations that extend functionality and lighten the burden on taxed security teams. Cybersecurity analysts are already overloaded and the situation is likely to get worse as threats increase, tools proliferate and the skills shortage continues to negatively impact the efficacy of security operations practitioners. That's why it's important to have a tool that automatically correlates related activity into unified alerts, which drastically simplifies the task for analysts. Central to the above points is automation improving threat detection, triage and response.

With SentinelOne's threat intelligence integration, threats are auto enriched from various sources, enabling customers to accelerate threat investigation and triage capabilities. Customers can also make use of an extensive library of threat hunting queries curated by SentinelOne research, which continually evaluates the latest methodologies to uncover new IOCs and Tactics, Techniques, and Procedures (TTPs).

And all of this can be consolidated into fewer alerts, which reduces the strain on security teams. For example, in the 2022 MITRE Engenuity's ATT&CK Evaluation, which tested leading XDR solutions against a range of benchmarks, SentinelOne's Singularity XDR consolidated two days of continuous testing into just nine campaign-level console alerts. This demonstrates the ability to alleviate SOC burdens by using machine speed to correlate and contextualise large numbers of alerts. In the end, fewer alerts, fewer clicks and fewer screens mean increased SOC efficiency.

Invest in an XDR that maximises existing security investments

A strong XDR solution helps maximise the value of your security investments. While a closed XDR requires the vendor to supply all the required sensors for typical use cases, an open XDR concentrates on backend analytics and workflow and integrates with the organisation's existing security controls.

That makes sense because many organisations have tools and technologies deployed in their SOC that it would be wasteful to simply decommission. These

SentinelOne reports

While it can sometimes be difficult to know how much difference a security tool or platform is making, XDR delivers clear, measurable benefits. It helps reduce costs, increases efficiency and improves visibility across the entire cybersecurity estate.

best-in-breed technologies provide point solution coverage and each comes with a steep learning curve and operational burden for SecOps efficiency. Switching those out for a new tool simply starts you on another learning curve with a new burden. XDR can allow you to make use of these existing tools, connecting them through simple built-in integrations.

SentinelOne's Singularity Marketplace makes it easy to add integrations to third-party systems such as SIEM or SOAR solutions, with just a few clicks. Email, identity management systems, cloud services and other third-party systems can all be brought into the XDR system, which is a huge improvement on having to secure each one individually and use a different dashboard to manage alerts. These integrations can then be enabled and automated without the need to write complex code.

On top of these benefits is a lower total cost of ownership for the organisation. XDR expands the powerful capability to the entire connected ecosystem of security tools across the enterprise. Automated response actions now extend to third-party applications. For example, you can force step-up authentication in your identity management tools when the system detects suspicious behaviour. Users will then be asked to submit additional forms of authentication. And you can automatically block email or web connectivity for suspicious resources or users based upon pre-defined rules and triggers. Automated one-click responses serve to reduce adversary dwell time and contain threats quickly.

Seeing beyond the buzz for measurable outcomes

When choosing an XDR, CISOs need to look beyond the buzz and focus on what really matters: the outcomes it can deliver. Identifying KPIs not only helps to determine the effectiveness of tools and processes but also to communicate that effectiveness to the leadership and board. Cybersecurity is not always something the board understands, but the leadership will be aware of the growing risk of attacks and will want to know that their defences are aligned with the company's risk profile and appetite.

XDR can improve common KPIs because of its faster, deeper and more effective threat detection and response than individual, disparate tools like EDR and SIEM. Drawing on a wider range of sources means that XDR can improve Mean Time to Detect (MTTD). XDR's central source of information and more manageable alert workload helps to reduce Mean Time to Investigate (MTTI) by accelerating triage and reducing time to investigate and scope. XDR's simple, fast and relevant automation reduces Mean Time to Respond (MTTR) by enabling simple, fast, and relevant automations to quickly contain threats.

Of course, the board is not just concerned with the effectiveness of cybersecurity measures. Its members have to worry about budgets, too. It can sometimes seem as if CISOs are constantly asking for the money to add yet more tools, so XDR's ability to reduce total cost of ownership is welcome. AI and automation mean that security analysts carry less of a burden, which means they can work more efficiently and be more productive.

While it can sometimes be difficult to know how much difference a security tool or platform is making, XDR delivers clear, measurable benefits. It helps reduce costs, increases efficiency and improves visibility across the entire cybersecurity estate. □

For more information, please visit
www.sentinelone.com

SentinelOne®

NDR and NIS 2 – How to transform an obligation in an opportunity

Meet the NIS 2 compliance requirements serenely with Gatewatcher.

The world of cybersecurity is constantly evolving: talent, products, technologies, but also regulatory requirements. It's an environment with new considerations to take into account almost every day.

At a time when the threat is becoming increasingly evolving and advanced, the spotlight is on the European Commission, which this year has to take a stand on a number of issues, particularly regulatory ones, to meet this need: the CRA – Cyber Resilience Act; the AI Act; DORA (Digital Operational Resilience Act), and more quickly NIS 2 (Network and Information Security).

NIS 2, a necessary evolution of the regulatory framework

Going well beyond the objectives of NIS 1, which provided a minimum of adequate security conditions for entities and sectors targeted by cyber-attacks, NIS 2 goes further.

Its objective is to strengthen our overall resilience in terms of cybersecurity by addressing new sectors and entities that are now critical targets. This is a necessary development in view of the growing and sophisticated threat, targeting players such as local authorities, public health establishments, higher education establishments and all players in the supply chain, not included in NIS 1.*

It will also make it possible to respond to the heterogeneous application of the old directive between Member States, which leads to a lack of coherence and a flagrant fragmentation in the treatment of cyber-attacks for sensitive sectors on a European scale.

Thanks to this new regulatory framework, clear improvements are expected:

- Harmonisation of the implementation of the Directive across Europe, with more precise regulations.
- A strengthening of the overall level of security, with strict and proportional criteria depending on the categorisation of the given organisation, between essential or important entities.
- Increased responsibility and powers of supervision, control and sanction for the Member States to ensure that these measures are properly implemented throughout the areas concerned.
- This responsibility is also shared by businesses, which must manage their own risks.

But as a company, how can we meet these compliance challenges quickly?

First of all, no concrete, binding measures have yet been taken (other than notification of contact persons, incident reporting procedures and the potential sharing of information). The Member States are currently in the process of transposing the directive at national level. However, there are a number of key elements that must inevitably be taken into account by the entities concerned, and these are essentially based on NIS 1.

A governance policy must be put in place to ensure adequate risk management for your IS (audit, risk analysis, security indicators, accreditation, mapping, etc.).

Certain key protection elements will need to be considered in relation to your security policies linked to your architecture itself, its administration, access (IAM), maintenance, etc. (network partitioning, access, etc.).

Finally, appropriate and reinforced detection measures, as well as incident response and management measures, must be put in place to maintain business continuity in a crisis situation should a cyber-attack occur on your networks (MCS, MCO, alert handling, crisis management policy, etc.).

In short, a good start to your compliance! These areas will have to be taken into account under NIS 2, but we need to wait for further details at European and national level, particularly in terms of correspondence with other legislation added to NIS 2 (DORA, CRA, AI Act, LPM in France, etc.).

These are essential compliance needs that Gatewatcher has been addressing since its creation in 2015. Gatewatcher first entered the compliance market, responding to the various legislative requirements that are still in force thanks to its 'secure by design' NDR.

Today, as a company, your challenges lie mainly in:

- Identifying and protecting your risks
- Protecting your data and sensitive information
- Investing in or strengthening your cybersecurity technologies

Gatewatcher reports

Gatewatcher's advanced technology enables you to build a consolidated, proactive defence mechanism based on advanced analysis, machine learning and artificial intelligence, including generative AI.

- Implementing incident management and CSIRT notification measures
- Training and awareness-raising for your employees

Gatewatcher's experience, along with the refinement and combination of its various NDR and CTI solutions, enables you to answer all these questions.

First and foremost, it is essential to maintain complete visibility of your information system, thanks to an inventory and mapping of all your assets and user behaviour on your network.

Once your risks and challenges have been identified, in particular the identification of your sensitive data and information, it is important to control your IS and comply with your security policies by adapting, for example, to your various restricted and confidential networks.

Whether you're investing in a cybersecurity solution for the first time or looking to strengthen your existing cyber-technologies, NDR, as a pillar of your strategy, enables you to reinforce your overall cybersecurity position. Simplified, seamless interconnection with your entire ecosystem (EDR, XDR, SIEM, SOAR, NGFW, etc.); proactive research; easy, rapid qualification and remediation of incidents by your cyber-experts to limit their overload; you have all the keys in hand to effectively manage cyber-threats in line with your environments.

In this way, we give you the power to protect your network and the peace of mind you need to focus on your business, and why not raise awareness and train your staff in key cybersecurity issues.

Compliance, an ongoing journey rather than a destination

Today, compliance must be seen as a strategic opportunity for companies, and not as an additional constraint to be met in order to comply with regulatory standards.

We need to take a long-term view. Achieving compliance not only enables you to build a comprehensive, up-to-date response to all your compliance needs (NIS, DORA, CRA, ISO 27001, etc.), but also to anticipate future regulatory developments. An NDR solution enables you to meet these challenges, but above all to go even further!

Beyond compliance, NDR enables you to raise your overall level of cybersecurity and optimise your investments for the most effective detection of and response to threats.

Building your cybersecurity strategy with NDR as a cornerstone means choosing a long-term cyber-strategy, with anticipation as the keystone. For cyber-attackers and defenders alike, time is of the essence. The aim is to be able to respond effectively to certain and potential future threats, thanks to an adapted and responsive defence system.

Think of NIS 2 as a guide to identifying and prioritising your risks and areas of weakness, as well as your cybersecurity strengths, in order to draw up a dynamic strategy to combat cyber-attacks. When compliance is approached strategically, it transforms from a necessity into a real opportunity and competitive advantage.

Rely on NDR

Imagine a cybersecurity strategy that not only reacts to threats, but also prevents them. In fact, as the vigilant guardian of your IS, Gatewatcher's NDR guarantees you:

- Enhanced real-time, 360° visibility
- Anticipated and advanced detection at every stage of the killchain of known, unknown (0-Day) and hidden threats (encrypted flows)
- Accelerated and prioritised investigations and remedies
- Control over your information and your cyber-risks
- Reduced attack surface and impact on your business
- An overall improvement in your cyber-score

Gatewatcher's advanced technology enables you to build a consolidated, proactive defence mechanism based on advanced analysis, machine learning and artificial intelligence, including generative AI.

So rely on NDR to turn this obligation into an opportunity for your business! □

* https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf

cyber security for business *serenity_*

At Gatewatcher, we give you the power to protect your network, so you can keep your data safe, shield your organization, and work securely.

In the end, we give you the peace of mind you need to focus on your business.

NDR_

CTI_

TAP_

gatewatcher.com

Sponsors and exhibitors

Corelight | Strategic Sponsor

Corelight transforms network and cloud activity into evidence so that data-first defenders can stay ahead of ever-changing attacks. Delivered by our Open NDR Platform, Corelight's comprehensive, correlated evidence gives you unparalleled visibility into your network. This evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

Our on-prem and cloud sensors go anywhere to capture structured, industry-standard telemetry and insights that work with the tools and processes you already use. Corelight's global customers include Fortune 500 companies, major government agencies, and research universities.

For more information, please visit www.corelight.com

CrowdStrike | Strategic Sponsor

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more at www.crowdstrike.com

Gatewatcher | Strategic Sponsor

Technological leader in real-time cyber-threat detection, Gatewatcher has been protecting the critical networks of the largest companies and public institutions since 2015.

Its vision is to offer a flexible (cloud, on-premise, hybrid), innovative and AI-friendly approach, without disrupting the existing architecture to allow cybersecurity teams to be more efficient in prioritising their remediation actions.

Our solutions provide an immediate improvement to current and future cybersecurity challenges by responding to the new detection needs of organisations. They combine machine learning algorithms with various network traffic analysis methods and are designed to be scalable and immediately operational for easy integration into SOCs.

Gatewatcher NDR is a network detection and response platform that can reliably identify malicious actions and suspicious behaviour by mapping all assets on the IS. Combining this capability with unprecedented encrypted network flow analysis, it provides a 360-degree model of the level of cyber-risk associated with each connection between assets and users, for an unprecedented level of detection and visibility.

Gatewatcher CTI is a threat intelligence offer aimed at providing an immediate improvement in your level of protection. Its exclusive technology combines machine learning and big data processing to generate in a very short time a high-quality information flow on cyber-threats specifically targeting your activity. The offer is also available as an analysis and investigation platform.

For more information, please visit www.gatewatcher.com

Illumio | Strategic Sponsor

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface.

The Illumio ZTS Platform visualises all communication and traffic between workflows, devices, and the internet in one console, automatically sets granular segmentation policies to control unnecessary and unwanted communications, and isolates high-value assets and compromised systems to proactively or reactively stop the spread of a breach.

ZTS is proven to help organisations of all sizes, from Fortune 100 to small business, stop breaches and ransomware in minutes, save millions in application downtime, and accelerate digital transformation projects.

Assume breach. Minimise impact. Increase resilience.

For more information, please visit www.illumio.com

KnowBe4 | Strategic Sponsor

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 50,000 organisations around the globe. Founded by IT and data security specialist, Stu Sjouwerman, KnowBe4 helps organisations address the human element of security by raising awareness about ransomware, CEO fraud, and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognised cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organisations rely on KnowBe4 to mobilise their end users as their last line of defence.

For more information, please visit www.knowbe4.com

Rubrik | Strategic Sponsor

Rubrik, the Zero Trust Data Security Company™, delivers data security and operational resilience for enterprises. Rubrik's big idea is to provide data security and data protection on a single platform, including: Zero Trust Data Protection, ransomware investigation, incident containment, sensitive data discovery, and orchestrated application recovery. This means data is ready at all times so you can recover the data you need, and avoid paying a ransom. Because when you secure your data, you secure your applications, and you secure your business.

For more information, please visit www.rubrik.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

Hoxhunt | Education Seminar Sponsor

Hoxhunt is a global leader in human risk management. The innovative Hoxhunt AI driven human risk platform scales your security culture and behaviour change that enables people to detect and report cyber-attacks that have bypassed your technical security layers, reducing the risk to organisations from sophisticated cyber-attacks targeting humans. Leading organisations of all sizes, including Bird & Bird, Airbus, Docusign, IGT, Nokia and Qualcomm all rely on Hoxhunt for their human risk management solutions that mitigate their most critical risks across email, cloud, social media, and the web.

For more information, please visit www.hoxhunt.com

Proofpoint | Education Seminar Sponsor

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber-attacks. Leading organisations of all sizes, including 80% of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

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

Recorded Future | Education Seminar 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

ReliaQuest | Education Seminar Sponsor

Our mission is to make security possible. By combining the power of a Security Operations Platform – ReliaQuest GreyMatter – with security expertise, our customers have increased visibility, the ability to confidently automate across the security lifecycle, and effectively measure and manage risk for continuous improvement.

ReliaQuest is the force multiplier of security operations. Our security operations platform, GreyMatter, automates detection, investigation, and response across cloud, endpoint, and on-premises tools and applications. GreyMatter is cloud-native, built on an open XDR architecture, and delivered as a service any time of the day, anywhere in the world. With over 700 customers worldwide and 1,000+ teammates working across six global operating centres, ReliaQuest is driving outcomes for the most trusted enterprise brands in the world. We exist to make security possible.

For more information, visit www.reliaquest.com

SoSafe | Education Seminar Sponsor

SoSafe empowers organisations to build a security culture and mitigate risk with its GDPR-compliant awareness platform. Powered by behavioural science and smart algorithms, SoSafe delivers engaging personalised learning experiences and smart attack simulations that turn employees into active assets against online threats. Comprehensive analytics measure ROI and tell organisations where vulnerabilities lie. The platform is easy to deploy and scale, fostering secure behaviour in every employee.

For more information, please visit sosafe-awareness.com

S-RM | Education Seminar Sponsor

S-RM is a corporate intelligence and cybersecurity consultancy. Founded in 2005, we have 400+ practitioners, serving clients across all regions and major sectors.

Headquartered in London, we have offices in Cape Town, Hong Kong, Manchester, New York, Rio de Janeiro, Singapore, Utrecht and Washington DC. We partner with leading organisations, supporting them at all levels, from CEOs and their boards through to front-line teams.

We support our clients by delivering intelligence that informs strategy and decision-making; by supporting them in building resilience to cyber-threats; and by providing rapid response to cyber-incidents and other organisational crises.

Our teams speak 45+ languages with backgrounds in intelligence, government, finance, journalism, military and academia. We deliver the best results for our clients by nurturing the brightest talent and bringing together the most relevant and experienced practitioners from across our business, creating teams designed to address unique problems and complex challenges.

Client service is at the heart of everything we do. We build long-term partnerships with our clients to gain a deep understanding of their challenges and goals. Our close relationships with the organisations we work with mean that we can respond quickly to their requirements and proactively adapt our approach as their business needs to develop over time.

Our advice is direct, honest and objective. We deliver tangible results and present our findings and advice in clear, straightforward language. Our pragmatic approach, combined with hard work, deep regional expertise and diverse experience means that our clients receive actionable recommendations, hands-on support and leadership, and sharper outcomes.

Find out more at www.s-rminform.com

AGENDA

08:00 Registration and networking break

08:50 Chairman's welcome

09:00 **Collaboration is key: Balancing regulation/compliance and security**

Claudia van den Beld, Advisor International Cooperation, National Cyber Security Centre of the Netherlands

- We strive to encapsulate the current threat landscape in laws and regulations, and the need for coordination is ever more relevant.
  Case study: From star-gazing to law-gazing – the Observatory
- We are trying to navigate this landscape through cross-border alliances which we sorely need.
  Case study: Choosing your cross-border partners – the Consortium
- Finally, there is a great deal we can learn from each other once we appreciate the need to share information.
  Case study: Lowering the thresholds to heighten the insight – the Platform

09:20 **Human machine teaming: The indispensable human element of cybersecurity**

Sjoerd de Jong, Senior Sales Engineer, SentinelOne

Artificial intelligence is a pervasive part of our lives today and cybersecurity teams and adversaries alike have learned to harness the speed and power of machines to strengthen their capabilities. With machine learning becoming one of the most important tools of defence, leaders must balance the overwhelming speed and accuracy advantage of AI with the need for measured and intuitive interactions with a real-world human element.

- What these trends mean for the hands-on practitioner
- When velocity of innovation outpaces the capabilities of human intellect
- The role of automation in the effective practice of securing our digital world

09:40 **Keeping your data incidents from becoming data breaches with Data Security Posture Management**

Filip Verloy, Field CTO EMEA & APJ Rx, Rubrik

- Data Security Posture Management (DSPM) is essential for securing data across diverse environments
- DSPM enables organisations to discover, protect, and manage data assets in on-premises, cloud, and SaaS environments
- Discover how by using DSPM, organisations can enforce security policies, ensure data sovereignty, and meet governance, risk, and compliance (GRC) requirements

10:00 **NIS2: Beyond compliance, a catalyst for transformation**

Arash Rahmani, CISO a.i., Nederlandse Zorgautoriteit

- The transformative opportunity of NIS2
- The strategic impact of NIS2
- The evolving role of the Chief Information Security Officer (CISO) in the age of NIS2

10:20 **Education Seminars | Session 1** **See pages 26 and 27 for more details**

Recorded Future	SoSafe
Generative AI: Amplifying attackers and defenders	**Hack the brain – Social engineering innovation in 2023**
Lewis Brand, Senior Sales Engineer, Recorded Future	**Bas van Erk,** Director Benelux & Nordics, SoSafe

11:00 Networking break

11:30 **Implementing robust measures to secure the supply chain**

Siegfried Moyo, Head of Cybersecurity EU, APAC, & LATAM, Americold Logistics

- Identifying potential threats & implementing physical security measures
- Conducting supplier and partner due diligence: Visibility and traceability
- Business continuity planning & employee awareness
- Compliance with regulations

11:50 **Living in a world of fakes**

Jelle Wieringa, Security Awareness Advocate, EMEA, KnowBe4

Deepfakes are here, and they are here to stay. And with technology ever advancing, it is no longer a matter of simply knowing what a deepfake is. Organisations will have to actively decide how they can utilise them to grow their business, and at the same time defend against the malicious use of this technology. In this talk, we'll be looking at:

- The evolving role of deepfakes in our lives
- What you can do with them
- How you can protect against them

12:10 **Nowhere to hide – Key insights into adversary tradecraft 2023**

John Spencer, Sales Engineering, CrowdStrike
- Get a frontline snapshot of the current threat landscape, threat actors and their victims
- Learn about the latest trends in adversary operations and tradecraft
- Understand why the human factor is more relevant than ever before
- Explore the 5 key steps to stay ahead of the threat actor

12:30 **NDR and NIS2: How to turn your compliance obligation into an opportunity**

Jürgen Verniest, Sales Director Benelux & Nordics, Gatewatcher
In this presentation, we will tackle:
- How we allow organisations, both essential and critical, to meet the NIS2 compliance requirements by providing full network and cloud visibility
- An unparalleled detection including the support of AI and ML, quick and effective response and compliancy support
- Concluding NDR serves as a key tool to enable a more secure and resilient infrastructure and ensure the desired business continuity and competitive edge

12:50 **Education Seminars | Session 2** **See pages 26 and 27 for more details**

ReliaQuest
The future of security operations
Rasham Rastegarpour, ReliaQuest

S-RM
The cyber-arms race: Staying ahead
Martijn Hoogesteger, Head of Cybersecurity, S-RM

13:30 Lunch break

14:30 **How to build a highly automated third-party security risk management (TPSRM) programme**

Elli Tsiala, Product Owner of Supply Chain Security, ABN AMRO Bank
- How to start your TPSRM with resources you already have
- How to increase your automation and minimise onboarding effort
- Lessons learned from our journey

14:50 **Using Zero Trust to improve cyber-resilience in the age of AI**

Trevor Dearing, Global Director of Critical Infrastructure Solutions, Illumio
As we transform our business models to deliver more agile services the increasing threat of AI generated attacks on critical infrastructure can potentially disrupt services causing an impact on society. Complying with any changes potentially coming with implementations of NIS2 could be complex and add cost. Taking a Zero Trust approach can simplify compliance and reduces costs. In this session, we will address the following topics:
- How to identify and define risk
- How to reduce the attack surface
- How to contain an attack
- How to respond and restore services during an attack

15:10 **Network evidence for defensible disclosure**

Nico Roosenboom, Systems Engineer, Corelight
- Do you consider network evidence a crucial part of your SOC strategy?
- How do you really know which alerts are the most serious?
- What's the best way to shift from responding to alerts to hunting for threats?
- Understand how to stay ahead of ever-changing attacks by using a data-first approach for detection and response

15:30 **Education Seminars | Session 3** **See pages 26 and 27 for more details**

Hoxhunt
The future of the human risk reduction
Petri Kuivala, Strategic Advisor, Hoxhunt

Proofpoint
Defending with an attacker's mindset
Boudewijn van Lith, Senior Manager Technical Sales, Proofpoint

16:10 Networking break

16:30 **CISO panel discussion**

Peter Avamale, Director, Cyber Strategy & Transformation Practice, PwC – Netherlands, (Moderator);
Marc Berns, CISO, Allianz Benelux;
Marnie Wilking, CISO, Booking.com;
Mario Beccia, Deputy CIO for Cybersecurity, NATO;
Daniela Lourenço, CISO, Tinka B.V
- Integrating cybersecurity into wider enterprise risk management frameworks
- Becoming a more strategic partner to the business
- Building resilience against third-party security threats
- Web 3.0 and the next generation of the internet: Securing new technologies and services

17:00 **Bypassing multi-factor authentication (MFA) via phishing techniques**

Manit Sahib, Ethical Hacker & **Raj Sandhu,** Ethical Hacker
- Introduction to MFA bypass phishing techniques
- Live demonstration of MFA bypass attack
- Countermeasures and best practices
- Conclusion of demo and presentation

17:30 Conference close

Education seminars

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

Session 1: 10:20–11:00

Recorded Future

SESSION 1
10:20–11:00

Generative AI: Amplifying attackers and defenders

Lewis Brand, Senior Sales Engineer, Recorded Future

Generative AI empowers scalable consumption and production for both attackers and defenders, ushering in a wave of surprising use cases. This presentation shifts the focus from potential malicious uses to practical takeaways. Join us to explore how generative AI can be harnessed for positive impact, providing you with actionable insights and strategies to navigate transformative possibilities.

Main topics to be discussed:

- Real world examples and use cases
- A practical lens for defenders
- Think about things differently
- Recorded Future AI in action

SoSafe

SESSION 1
10:20–11:00

Hack the brain – Social engineering innovation in 2023

Bas van Erk, Director Benelux & Nordics, SoSafe

The human factor remains a gateway for cybercriminals as phishing and ransomware attacks continue to increase. Cases like those of Uber and Rockstar Games have also shown how cybercriminals are evolving at a rapid pace, exploiting human psychology and our emotions – and hacking our brains. But how do attackers use behavioural science specifically against us? What can we do to protect those around us?

- *Emotional manipulation tactics:* Insight into how cybercriminals exploit emotions, emphasizing the need for psychological awareness in cybersecurity
- *Behavioural science in attacks:* Understanding how attackers use behavioural science for effective phishing and ransomware, highlighting the importance of this knowledge in defence strategies
- *Strengthening defences:* Practical strategies for enhancing resilience against social engineering, focusing on team education and recognition of sophisticated threats

Session 2: 12:50–13:30

ReliaQuest

SESSION 2
12:50–13:30

The future of security operations

Rasham Rastegarpour, ReliaQuest

Security operations are changing rapidly and require a more holistic approach to security. Streamlining threat detection, investigation, and response is a good start in managing risk, but also important are utilising threat intelligence and digital risk protection, reviewing suspect employee-submitted emails via the abuse mailbox, and measuring your programme to communicate better with your stakeholders and service providers.

Additionally, security operations will become more streamlined, with the automation of routine tasks and incident-response procedures becoming the norm. This session will help organisations achieve efficient and effective detection and response to security incidents.

Five benefits for delegates attending the session:

- How a security operations platform helps proactively detect and mitigate cybersecurity risks and support future changes in your business
- The benefits of complete visibility across cloud, on-premises, and endpoint environments to mitigate security risks and enable rapid remediation
- How automation at key junctures can streamline security operations, speed resolution, and reduce the risk of human error
- The need for a more collaborative approach between providers and enterprises that avoids a 'black box' method and provides measurable improvements in security operations
- How integration with existing security toolsets enables organisations to extract more value out of existing investments while streamlining security response

SR-M

SESSION 2
12:50–13:30

The cyber-arms race: Staying ahead

Martijn Hoogesteger, Head of Cybersecurity, S-RM

- Cybercriminals have had free reign for years, but organisations are better defended, driving them to develop new methods
- Understand the current lay of the cybercriminal landscape
- Learn about new techniques being used by ransomware groups
- Hear S-RM's insights on the future of cyber-threats

Session 3: 15:30–16:10

Hoxhunt

SESSION 3
15:30–16:10

The future of the human risk reduction

Petri Kuivala, Strategic Advisor, Hoxhunt

Cybersecurity comes together in a holy marriage of People, Processes and Technology. CISOs needs to engage people as their force multipliers as they will not survive alone in the constantly evolving world.

Join this interactive session to learn more about:

- The CISO veteran & start-up coach's thoughts about the People role in the future within the cybersecurity context
- Be ready with your phone having www.menti.com open to donate your ideas back into the conversation. "Hold on your chair as Texas is going bye bye….the Matrix".

Proofpoint

SESSION 3
15:30–16:10

Defending with an attacker's mindset

Boudewijn van Lith, Senior Manager Technical Sales, Proofpoint

The organisation chart is the new zero-day – and today, it's publicly available on social media.

- It's easier to find someone who will click a link than to find an exploit for an operating system. The attacker simply needs to know who has access to the data they want, then get creative
- Most security teams don't have the same perspective that the threat actors do – they think of their attack surface in terms of VLAN and IP address, instead of the department or job title
- Effective defence comes when you can anticipate your attackers' moves. By combining threat landscape insights with data on which of your users are targeted with which threats, organisations can build more effective security awareness training programmes, and users can better defend themselves from the threats they are most likely to see □

Easily manage human layer risk

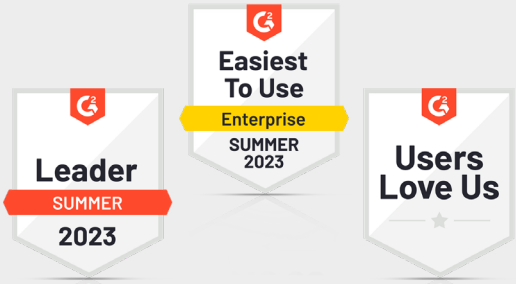
sosafe

Where technology meets real people, you want a solution that blends both too. With behavioral science in our DNA, the SoSafe platform creates automated and engaging cyber security awareness training programs at scale. Manage your human risk, at very low touch.

www.sosafe-awareness.com

European market leader

- 370+ employees
- 4,500+ customers across all industries and sizes
- 3,000,000+ users
- 60+ learning modules and videos
- 600+ phishing templates optimized for different industrie



Our platform

TEACH
Gamified e-learning

TRANSFER
Personalized phishing simulations

ACT
Risk cockpit and analytics

CONNECT
Sofie Rapid Awareness

Why customers love us

Driven by behavioral science

Story-based, gamified micro-learning for maximum engagement

Easy to use and scale

Seamless and customized experience for both admins and users

100% GDPR-compliant

Privacy-by-design approach with smart reporting functions, e.g., for ISO-27001

Trusted by leading global companies

MUSTANG · vitra. · CECONOMY · Marc O'Polo · ALDI MARKET · ROSSMANN

Speakers and panellists

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

Peter Avamale

Director, Cyber Strategy & Transformation Practice, PwC – Netherlands

Peter is a Director in the Cyber Strategy and Transformation practice of PwC in the Netherlands. He serves as a trusted advisor to C-level executives at major institutions in Europe, helping them ensure that security enables business innovation and success in the marketplace. He has consulted for over 50 organisations globally on topics including cybersecurity strategy, GRC, application security, security operations and information protection. Prior to joining PwC, Peter was a Technical Security Lead at Booking.com, and a regional cybersecurity services leader at EY. He is passionate about mentoring the next generation of cybersecurity professionals and sharing insights with industry colleagues.

Mario Beccia

Deputy CIO for Cybersecurity, NATO

Mr Mario Beccia is NATO's Deputy CIO for Cybersecurity, working in the Office of the Chief Information Officer. He holds a university degree in Economics and Management, an MBA in Management of Innovation, and several certifications in cybersecurity and information technology. He started his career in 1997 by joining a start-up company focused on the use of web technologies for businesses. He then worked as independent consultant on IT and information assurance projects in Italy and Belgium. He joined NATO Allied Command Transformation in 2006, where he worked on business transformation and capability development programmes. He supported the setup of the NATO Computer Incident Response Capability (NCIRC) and IT Modernization (ITM) programs by collecting and engineering requirements, championing the creation of an implementation roadmap for cloud computing and cyber-defence in NATO. He joined the European Defence Agency in 2018 as Chief Information Security Officer and Project Officer Cyber Defence, leading the creation of a cybersecurity practice in the Agency, the creation of a stronger classified information management ecosystem and the cyber-defence programme of the Agency. He led and supported several cross-domain and multinational projects under the PESCO (PErmanent and Structured COoperation) framework and other multinational initiatives. In 2020, he started the milCERTs Interactive Conference, a yearly cybersecurity exercise and conference aimed at creating a stronger military CERT interaction between EU military entities. In March 2021, he joined back NATO and, as of February 2022, he took on the role of Deputy CIO for Cybersecurity, leading a major cybersecurity transformation programme in NATO. He is passionate about martial arts, computer programming, crypto-currencies and electric vehicles.

Marc Berns

Chief Information Security Officer, Allianz Benelux

Marc is the CISO for Allianz Benelux, an insurance company based in Brussels, Rotterdam and Luxemburg, part of the Allianz SE group of companies. Throughout his career, he has worked in heavily regulated industries from investment banking to insurance. His focus is implementing risk-based governance over information security in IT operations outsourced to third parties.

Lewis Brand

Senior Sales Engineer, Recorded Future

Lewis Brand, Senior Sales Engineer at Recorded Future, has over nine years in the IT industry, where he has specialised in liaising with enterprise customers across EMEA. Before his career at Recorded Future, Lewis operated as a Sales Engineer at Tenable, with his primary focus centred around vulnerability management. He has previously provided IT support for SMBs, which gives him a unique perspective when engaging with customers by providing insight from both a vendor and end-user viewpoint.

Sjoerd de Jong

Senior Sales Engineer, SentinelOne

Trevor Dearing

Global Director of Critical Infrastructure Solutions, Illumio

Trevor Dearing has worked in networking and security for over 40 years. He has attended the birth of nearly all the technologies that we now take for granted including, ethernet switching, VPNs, firewalls and virtual networks. Originally an engineer working on some of the first network and cybersecurity systems, he is now the Global Director of Critical Infrastructure Solutions for Illumio.

Martijn Hoogesteger

Head of Cybersecurity, S-RM

Martijn Hoogesteger heads S-RM's office in the Netherlands as Head of Cybersecurity. He is responsible for building out the cyber-proposition in the Benelux and managing the team in the Netherlands. His mission is keeping organisations secure, and making sure they get the correct response when things have taken a turn for the worse. Prior to joining S-RM, Martijn had been in different roles in the cybersecurity field where he built and managed Incident Response and Offensive Security teams. He also takes part in the Dutch TV show 'Hunted', where he is a Digital Investigator, tracking down fugitive contestants through digital means. Martijn holds an MSc in Computer Science from the University of Twente, with a specialisation in Cybersecurity.

Petri Kuivala

Strategic Advisor, Hoxhunt

Petri Kuivala is an experienced CISO who led the establishment of the function at Nokia Corporation in 2008, where he later became CSO until 2012. He then established and oversaw the CISO function at NXP Semiconductors until 2021. Petri has considerable experience in mergers and acquisitions, having worked with companies including Microsoft, Qualcomm, and Siemens. He has also dealt with various security challenges, such as defending against Nation-State attackers, corporate espionage, and OT-security catastrophes. Petri has managed large-scale programmes to secure company assets, including Crown Jewels, OT-security, supply chain security, and cybersecurity more broadly. He currently coaches several start-up companies and was also a founding member of the Helsinki Police Department IT-Crime unit.

Daniela Lourenço

CISO, Tinka B.V.

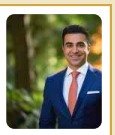
Daniela Lourenço (CISSP, CISM) is the Chief Information Security Officer for Tinka B.V. Daniela holds a master's degree in Communication and Cultural Studies and an executive master's degree in Cybersecurity. With multinational experience in compliance and information security, in the financial and automotive markets, 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. She is often found talking passionately about the cultural impact of cybersecurity and how rewriting the awareness and training methodology is urgent for private and public organisations.

Siegfried Moyo

Head of Cybersecurity EU, APAC, & LATAM, Americold Logistics

As the Head of Cybersecurity for EU, APAC, and LATAM regions at Americold Logistics, Siegfried is responsible for aligning the IT/cybersecurity roadmap with the business strategy and growth plans. He advises the regional senior leadership team on cyber-risk management and has a proven track record of designing and implementing pragmatic cybersecurity solutions that balance security risks with business needs and the cyber-cultural impact of risk management controls. He has also built in-house cyber-threat/incident response capabilities, focusing on threat intelligence, threat modelling, and threat hunting, to increase the cyber-resilience and effectiveness of the organisation. In addition, he is a mentor, an advisory board member, a founder and CEO of CyberNext Academy, an author, and a cyber-risk management researcher.

Arash Rahmani



CISO a.i., Nederlandse Zorgautoriteit

Arash believes that secure digital transformation adds value to the business, can help drive strategy execution and should be business-driven, not just IT-driven. He focuses on technology, people, processes, and culture to achieve organisational goals. Arash has a track record in increasing the digital resilience of large organisations and managing multidisciplinary teams. He is also a board member of ISACA NL and co-author of the EU-elections programme for one of the biggest Dutch political parties.

Rasham Rastegarpour

Sales Engineer,
ReliaQuest

Rasham Rastegarpour has over 21 years of experience in IT, which was mostly focused on enhancing the security stance of many organisations. Since the start of his career, Rasham has held multiple positions and therefore, he has been and participated in many different disciplines which makes him a jack of all trades and master of a few. With his education and experience ranging from operational to various training, consulting and managerial roles, he is able to speak the language of multiple stakeholders within security teams. His wealth of in-depth technical and organisational knowledge within multiple subject matters across many companies makes him a valuable asset to any type of organisation at any level of security maturity. Currently active as Sales Engineer for ReliaQuest, Rasham is solving complex challenges across IT, OT and Cloud environments by optimising Security ROI, increasing visibility, measuring team performance whilst improving the overall security posture for all types of organisations in EMEA.

Nico Roosenboom

Systems Engineer,
Corelight

Nico Roosenboom is a Systems Engineer at Corelight, inc., and has been in the security industry for more than a decade. He has broad experience in the most advanced cybersecurity fields with strong technical abilities, and is passionate about helping organisations improve their cyber-resilience and make the internet a safer place for everyone. Nico is recognised as a thought leader in the industry and has delivered keynote talks, workshops, and tech talks at national and international events.

Manit Sahib

Ethical Hacker

Manit is an experienced offensive security expert who is certified by UK's National Cyber Security Centre (NCSC) as well as His Majesty's CESG Check scheme (HMG CHECK). He has over 10 years professional experience in both UK Government and private offensive security operations. Formerly, Manit was the Head of Penetration Testing & Red Teaming at the Bank of England. He is contracted to Global Fund.

Raj Sandhu

Ethical Hacker

Raj Sandhu is a highly experienced Ethical Hacker with 15 years of expertise in intergovernmental, financial, and telecommunication organisations. As a consultant at the World Health Organization, he focuses on red teaming, penetration testing, vulnerability management, risk assessments, and security audits.

John Spencer

Sales Engineering,
CrowdStrike

A seasoned IT executive with 30 years of experience in the software industry technical and product teams, John has worked in large corporate and start-up organisations, and was previously CPO for a cyber-identity start-up and CTO for Northern Europe at Citrix. John currently leads the CrowdStrike Sales Engineering team for Northern Europe, possessing a deep understanding of the rapidly evolving cyber-landscape, while helping organisations stay ahead of the adversaries.

Elli Tsiala

Product Owner of Supply Chain Security, ABN AMRO Bank

Elli Tsiala is an enthusiastic third-party security expert. With over 12 years of experience in this domain, she has been at the forefront of developing innovative third-party security programmes across diverse industries. As the Product Owner of Supply Chain Security in ABN AMRO Bank, Elli has spearheaded multiple initiatives, resulting in significantly automated continuous monitoring of more than 450 third parties within the bank.

Claudia van den Beld

Advisor International Cooperation, National Cyber Security Centre of the Netherlands

Claudia van den Beld earned her Advanced Msc in International Relations and Diplomacy from Leiden University and the Clingendael Institute. After having worked at the Directorate for Innovation, Science and Strategy of the Dutch Ministry of Justice and Security, she is now a part of the National Cyber Security Centre of the Netherlands. There, she focuses on international cooperation and strategic vendor management.

Bas van Erk

Director Benelux & Nordics, SoSafe

Bas van Erk is Director Benelux & Nordics at SoSafe. His background in SaaS companies includes companies like Meltwater, Insided & Newzoo. His mission is to launch SoSafe's awareness solution in the mentioned markets and support local clients to create strong security cultures to build resilience against cyber-threats.

Boudewijn van Lith

Senior Manager Technical Sales, Proofpoint

Filip Verloy

Field CTO EMEA & APJ Rx, Rubrik

Filip Verloy serves as Field CTO EMEA & APJ for Rubrik X. In that role, Filip engages and advises customers, partners and the security industry at large, sharing his experience, insights, and strategies on data security. Prior to joining Rubrik, Verloy was the Global Field CTO at API security start-up Noname Security, and has previously served at various IT vendors including Citrix, Dell, Riverbed, and VMware in roles ranging from Staff Architect to Solutions Executive supporting some of the largest and most complex customer environments. He has been in the IT industry for over 20 years, spanning the customer-, consulting-, and vendor-side.

Jürgen Verniest

Sales Director Benelux & Nordics, Gatewatcher

Jürgen Verniest has more than 25 years of experience as Sales and Marketing Manager and held several high-profile positions at Alcatel-Lucent, Cisco and spotit. At spotit, Jürgen held the positions of Head of Sales and became CEO in 2020. Prior to spotit, Jürgen was responsible at Cisco for the cybersecurity line of business in Belgium and Luxembourg with focus on enterprise and public sector, with coverage of both technical and business decision makers (including CISO and CxO level).

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.

Marnie Wilking

Chief Information Security Officer, Booking.com

Marnie Wilking is the Chief Information Security Officer for Booking.com, where we make it easier for everyone to experience the world. Marnie has more than 20 years of experience aligning cybersecurity strategy with business objectives to support and accelerate growth. She has built and led cybersecurity and enterprise risk management programmes to meet business and regulatory needs for financial services, healthcare technology, and e-commerce companies worldwide. Marnie currently serves on the Board of Directors for Robert Half, International; non-profit organisations RH-ISAC and CyberCrime Support Network; and advises several cybersecurity startup companies. Prior to Wayfair, Marnie was Global Head of Privacy, Cybersecurity, and IT Risk Management for Wayfair; Global CISO for Orion Health; Senior Director of Security Compliance for Early Warning; and Information Security Officer for Wells Fargo Mortgage. She holds the CISSP, CISA, and CISM designations, as well as an MBA in Technology Management and a Bachelor of Arts in Mathematics and Statistics. □

How TomTom automatically navigated human cyber risk

tomtom

About

Billions of data points. Millions of sources. Hundreds of communities. TomTom is the mapmaker bringing it all together to build the world's smartest map. They provide location data and technology to drivers, carmakers, businesses, and developers.

Challenge

Serving some of the largest automotive and technology companies in the world, TomTom needed to quickly achieve regulatory and auditory compliance and level-up their security maturity to satisfy intensified requirements for doing business.

Solution

Hoxhunt supported TomTom achieving compliance targets and demonstrated measurable human risk reduction with a strategic focus on phishing, security behavior change training, and human risk management.

Results

- Successful phishing simulation reporting rates rose 151%
- Real threat detection surged from a few dozen to thousands per month
- Went from zero to compliance in 12 months, enabling their business shift to B2B

10x

Threat feed volume

99%

Threat feed automated noise reduction

Navigating new business and regulatory terrain to reach compliance at warp speed

Hoxhunt helped TomTom reach compliance in 12 months. As a result, the TomTom sees security as an integral part of its growth strategy, and a revenue enabler for B2B activity.

Real threat detection proves training works

The employee threat reports went from a dozen trickling in per month, to pouring in by the thousand: undeniable proof that their security behavior change program was working.

Driving behavior change

Hoxhunt's ongoing, personalized micro-trainings seamlessly integrated into corporate workflows, measurably boosted resilience, and uplifted company security culture. Built on an ethos of innovation and fast R&D, TomTom appreciated how quickly employees leveled-up their security skills without slowing down operations.

Putting SOC on auto pilot accelerates response

The Response Platform reduced threat feed noise by 99%. Incident response times were accelereated while hundreds of SOC hours saved, per month. The faster an incident is addressed, the better it's controlled.

> "We were a small security team tasked with building up security capabilities very quickly, and Hoxhunt has been extremely useful for us. The response platform is a force multiplier that does the initial triage for us without us having to scale out a massive team to look at every email being reported to us by our well-trained employees."

Behavior change for risk reduction

TRAINING PERFORMANCE

SUCCESS	FAILURE	RESILIENCE RATIO
↑ 151%	↓ 73%	↑ 843%
from 24% to 61%	from 15% to 4%	from 1.6 to 15.1

REAL THREAT DETECTION

THREAT DETECTION VOLUME	THREAT FEED AUTOMATED NOISE REDUCTION	SOC RESOURCE SAVINGS
↑ 10x	↓ 99%	2 FTEs
to 1000/month		

HOXHUNT

RESILIENCE, SIMPLE AND AUTOMATIC

Reduce your human cybersecurity risk

Discover how measurable improvements to human cyber behavior can deliver better results

Top 50 EMEA Companies BEST SOFTWARE AWARDS 2023

Protect

Change employee behavior to mitigate real risk. Stay at the cutting edge of an evolving threat landscape.

Detect

Turn real threats into instant learning. Use positive, people-first strategies to drive engagement.

Respond

Neutralize attacks with limited resources. Harness up-to-date threat data from a global sensor network.

Documented Risk Reduction

Build resilience with a complete picture of human risk and documented outcomes.

20x lower failure rates

90%+ engagement rates

75%+ detect rates

fortum DocuSign NOKIA nets IGT Deloitte. G2

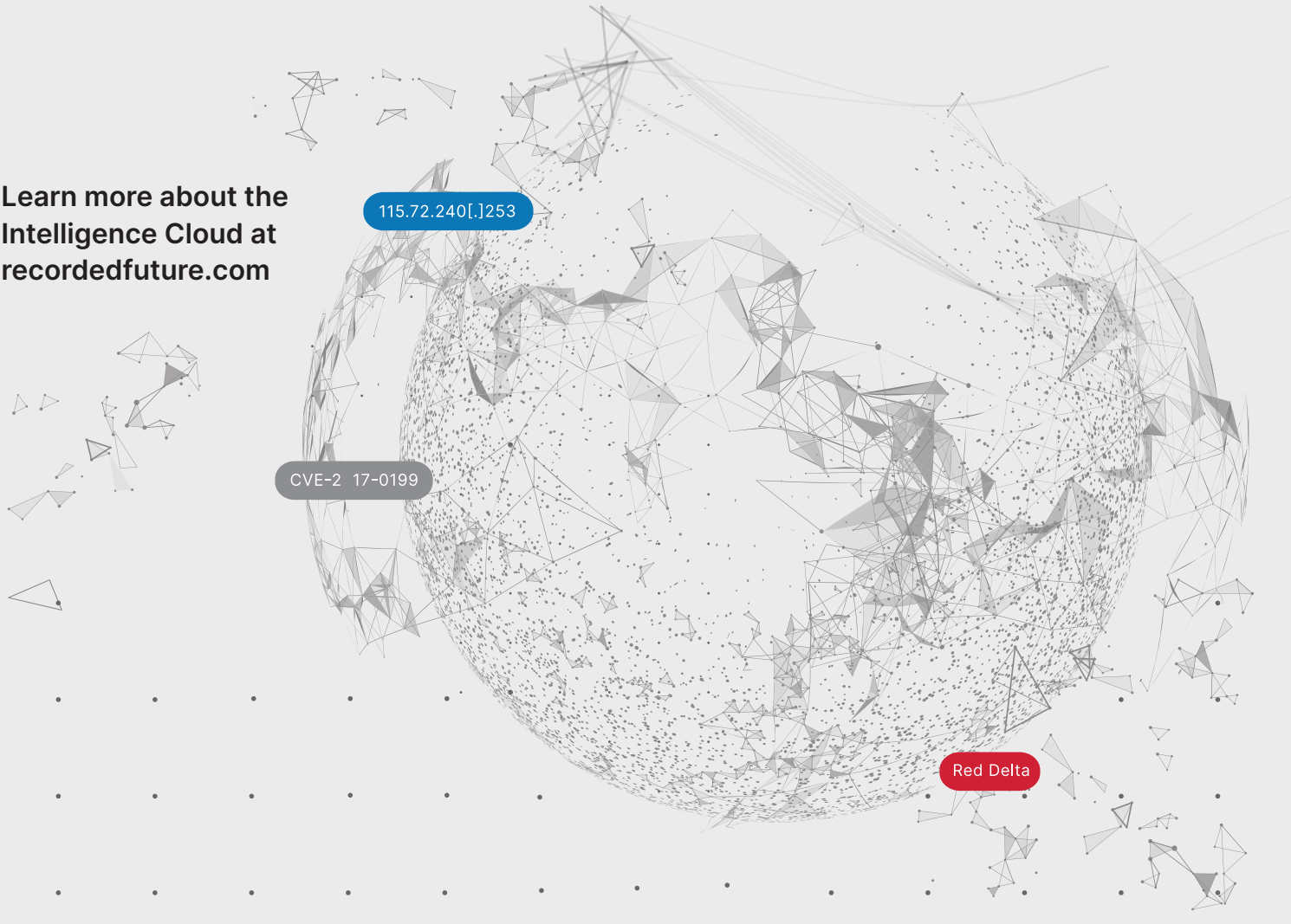
READ MORE: WWW.HOXHUNT.COM

Recorded Future®

Securing Our World With Intelligence

As threats accelerate and converge in the world around us, Recorded Future empowers your enterprise with real-time visibility into your changing attack surface and today's threat landscape so you can act with speed and confidence to mitigate business risks.

Learn more about the Intelligence Cloud at recordedfuture.com



From speed to consistency: The power of automation for your SOC

This article will provide insights from a conversation with experts from Recorded Future, Splunk, Ernst & Young, and NOV on automation best practices and tips on how to get started.

Meghan McGowan reports

As the cybersecurity industry constantly evolves and threat actors leverage AI and automation, defenders are challenged to stay ahead of the game. To address this challenge, organisations need to incorporate automation into their security strategy. Automation can reduce the burden of monotonous and repetitive work, while freeing up more time for high-value activities that drive security strategy forward.

Automation is not a one-size-fits-all solution, but it can improve the effectiveness of security teams. Successful implementation requires a culture that supports automation. This article will provide insights from a conversation with experts from Recorded Future, Splunk, Ernst & Young, and NOV on automation best practices and tips on how to get started.

Why should you have an automation strategy?

- *Speed:* Automation allows security analysts to respond to threats faster, which is crucial in today's fast-paced threat environment. Automation can enable a faster response and help prioritise and document alerts.

- *Analyst burnout:* Automation can reduce the burnout of security analysts who are inundated with too many alerts to handle effectively in a single day. As Tips for Selecting the Right Tools for Your Security Operations Center report from Gartner points out, "SOC teams face scalability challenges. Too many events and too much time spent on investigating complex incidents drive security leaders to seek tools for improving their SOC productivity." Automation is one of the strategies organisations are enlisting to improve their SOC team's efficiency.

- *Consistency:* Automation can help prioritise and document alerts, ensuring there is uniformity in the way they are triaged and managed. SOC Level 1 work can be offloaded to automation, allowing teams to focus on higher-value aspects of their role.

- *Deciding what to automate?* Deciding what to automate can be daunting, but by considering a few key factors, you can make informed decisions about where to start.

- *Cost of automation:* Determine if the process is worth automating by evaluating the time, energy, and resources required to develop and maintain the automation.

- *Cost of continuing with manual processes:* Take into account the impact of continuing with a manual process on your team's time and energy.

- *Orchestration:* Ensure that processes are well documented and well understood.

- *Identify good starting points:* Strategically choose your first automation use case, avoiding complex and time-consuming processes.

Automation can reduce the burden of monotonous and repetitive work, while freeing up more time for high-value activities that drive security strategy forward.

Importance of cultivating a culture of automation

As Gartner says, "There is a misconception that technologies powered by artificial intelligence (AI) and machine learning (ML), or any that promise to fully automate your SOC, would magically transform an SOC from low maturity to high maturity overnight. Tools alone won't solve all SOC challenges."

For organisations to see material improvements in SOC efficiency, consistency, and scalability, they must cultivate a culture of innovation and automation. Cultivating an entrepreneurial spirit to automation and empowering the team to participate in the implementation of those strategies leads to incredible outcomes.

Automation in practice

Here are some examples of how intelligence-driven automation can be operationalised across security workflows to accelerate identification, investigation, and prioritisation of threats:

- *Streamlined investigation of indicators:* The average SOC receives about 4,000 alerts per day,

By cultivating a culture of automation, security teams can operationalise intelligence-driven automation across security workflows and guard against cyber-threats in real-time.

which can be overwhelming and lead to alert fatigue. Automating the enrichment of indicators eliminates manual research and prioritises alerts, preventing resources from being drained by investigating non-critical alerts.

- *Automated cyber-threat hunting:* Automation can provide contextual information about threats, giving security teams a better understanding of attacks and the ability to formulate a more comprehensive response plan.

- *Monitoring digital risks to your brand:* Intelligence-driven automation streamlines the collection, analysis, and delivery of threat intelligence in real-time, enabling organisations to identify and respond to threats faster. For example, with Brand Intelligence, organisations can receive real-time playbook alerts on brand impersonation, including domain and logo abuse, packed with valuable context.

- *Remediating identity compromises:* By using automation to identify newly compromised credentials and initiate password resets, organisations can protect their critical assets in real-time.

Automation not only streamlines security workflows but also optimises productivity, allowing security teams to focus on high-value initiatives. By cultivating a culture of automation, security teams can operationalise intelligence-driven automation across security workflows and guard against cyber-threats in real-time. To learn how to get started with automation today, watch our on-demand webinar, Elevate Your SOC: Automation Trends & Best Practices or read Tips for Selecting the Right Tools for Your Security Operations Center report by Gartner. □

Gartner, *Tips for Selecting the Right Tools for Your Security Operations Center*, Al Price, Jeremy D'Hoinne, Angela Zhao, 1 November 2022 GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Meghan McGowan is Senior Product Marketing Manager at Recorded Future.

Learn more at **recordedfuture.com** and follow us on Twitter at @RecordedFuture.

Quick wins: 3 ways to act on security operations metrics

This blog provides three actionable steps for security teams to achieve desired metric outcomes, without significant time or resource investment.

Retired colonel and ReliaQuest CISO John Burger frequently says, "If you're not measuring, you're not operating." Metrics allow you to report on security programme outcomes, benchmark against your peers and industry, and identify next steps to mature your security operations programme. This blog provides three actionable steps for security teams to achieve desired metric outcomes, without significant time or resource investment.

1. What to do if your MTTR is flat or rising

One of the most frequently cited and most useful cybersecurity metrics is mean time to resolve (MTTR). MTTR assesses how well a security operations team responds to incidents.

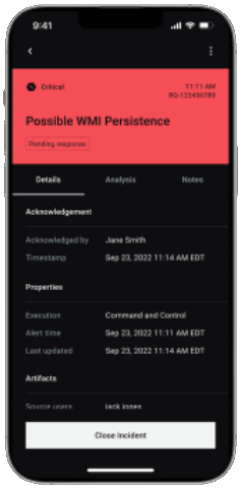
It is worth noting that MTTR can have different definitions across the industry. ReliaQuest defines MTTR as the time to **resolve** an incident, measured from the start of an incident to the time a customer closes it. Others in the industry, however, may define MTTR as the time to **respond**, measured from the initial incident to when a customer is notified of its escalation, even if the issue is not yet resolved. Comparing MTTR across the industry can be problematic given varying definitions.

Automating repetitive work enables your team to overcome 'high-time, low-brain' activities and focus on more important projects or priorities.

Actions to improve MTTR

A consistently prompt response to threats is a team effort. One tool ReliaQuest customers have used to improve those communications is a security operations mobile app that allows you to take action on the go – quickly evaluating an alert, closing out common alerts, and knowing when you need to crack open a laptop to do some deeper analysis. Many ReliaQuest customers find value in using the GreyMatter Mobile App.

GreyMatter Mobile App



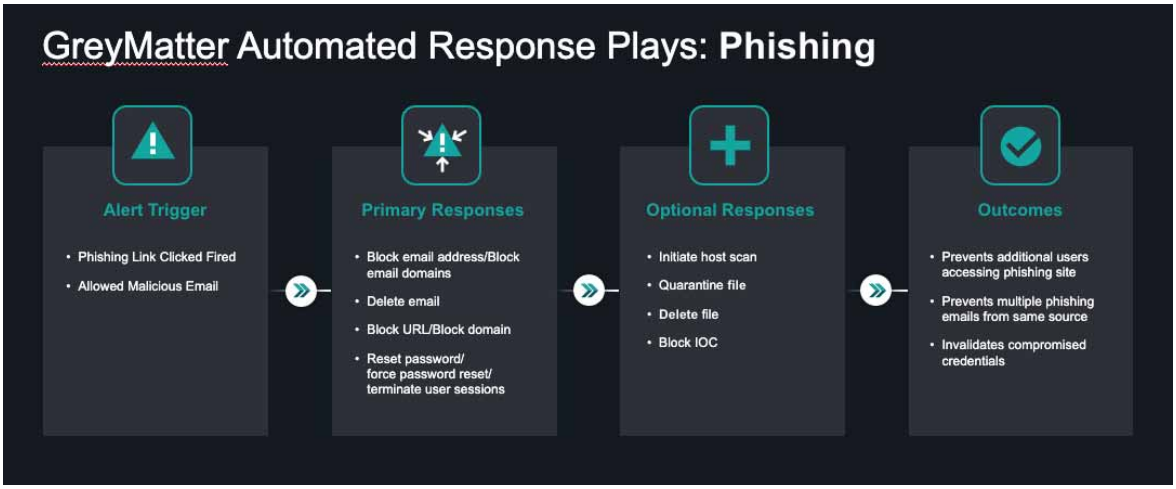
2. If automation and playbook utilisation is low

Automation across threat detection, investigation, and response workflows can act as a force multiplier for security teams. Automating repetitive work enables your team to overcome 'high-time, low-brain' activities and focus on more important projects or priorities.

Action to impact playbook utilisation

A quick action your team can take is to locate high-fidelity alerts and automate response. Automating response actions provides benefits ranging from improved threat response to reduced repetitive work.

GreyMatter Automated Response Plays for Phishing



ReliaQuest reports

Detection coverage is only as good as the visibility you have to support those detections. Increased visibility can require more logging and data ingestion, and data ingestion may come with a cost.

GreyMatter Security Model Index Summary of MITRE ATT&CK Coverage

When you can consistently identify true-positive alerts, it presents the opportunity to automate response actions. Based on an alert trigger, your security operations platform can usually take automated action through your existing tools, such as EDR, network security, identity (IAM/SSO), and email security.

3. If you are uncertain about your detection coverage

Visibility empowers organisations to detect, mitigate, and respond to threats effectively and efficiently. You can't monitor what you can't see, and you can't detect threats that slip through protective layers without adequate visibility.

MITRE ATT&CK is an open-source framework and global knowledge base of adversary tactics and techniques that is derived from real-world observations of cyber-threats. This comprehensive view of the organisation's security posture allows for prioritising security measures, mitigating risks, and proactively addressing blind spots in their systems.

Action to improve threat detection coverage

Evaluate your significant visibility gaps using MITRE ATT&CK coverage mapping and examine how to fill those gaps. However, there may be a cost-benefit trade-off that you will need to consider: Detection coverage is only as good as the visibility you have to support those detections. Increased visibility can require more logging and data ingestion, and data ingestion may come with a cost.

Summary

Metrics can provide valuable insights, enabling security leaders to make data-driven decisions, prioritise actions, and drive continuous improvement. This blog highlighted three pieces of 'low-hanging fruit' that you can immediately pluck to make a quick impact. Your environment is unique, and your 'low-hanging fruit' may be different. □

RELIAQUEST®

Drive Faster, **More Efficient** Security Operations

Visit **ReliaQuest.com**

Protect the new attack surface: How organisations can break the attack chain

Cybercriminals continue to target humans, rather than infrastructure and their attacks remain inherently 'people-centric'.

Proofpoint reports

Today, attackers realise it is cheaper, easier, and faster to steal credentials and log in than trying to hack through technical controls. Once an identity vulnerability is exploited, they can move laterally through systems and networks, amassing intelligence, distributing malicious payloads and exfiltrating data. It's currently far too easy for an attacker to turn one compromised identity into an organisation-wide ransomware incident or data breach.

Ultimately, identity is now being used by threat actors to further their cybercriminal gains. Quite literally following a pattern, or an 'attack chain'. Organisations must consider how they can break this attack chain, by halting initial compromise and stopping privilege escalation, thus securing data.

How are cybercriminals attacking identity?

The initial point of compromise is most often email, and Dutch organisations continue to see a high-volume of phishing attacks. Proofpoint's 2023 State of the Phish report revealed that among the Dutch organisations that experienced an attempted phishing attack in 2022, 90% of these were successful. Of these, 38% resulted in credential theft and/or account compromise, where employees invertedly expose their credentials, giving threat actors access to sensitive data and their business accounts.

Cybercriminals are also targeting employees at all levels of an organisation. Along with high-value targets such as administrators or finance contacts, modern threat actors also target unmanaged and misconfigured identities that are often not afforded the same protections. This can include service accounts, local and shadow admins, cached credentials and many others that often slip through the net of privilege and password security tools. By targeting identities like these, cybercriminals can bypass standard perimeter defences with minimal effort or technical knowhow.

The issue is the nature of these attacks is hard for organisations to detect. And the longer any malicious actor lays undetected, the greater their opportunity to traverse through identities – from privilege escalation to abuse of Active Directory and cloud environments. And the more potentially devastating the consequences.

Defending against identity-focused attacks

Attackers will continue to rely on the same technique – targeting employees with an email, to gain a foothold into an organisation and move laterally, doing as much damage as they can. They depend on this technique, because put simply, it works and will continue to do so unless organisations consider how they can break the links in the attack chain.

When we look at opportunities for organisations to break the attack chain, the first step is to stop the initial compromise in the first place. This is where a robust email security strategy is crucial. From Business Email Compromise (BEC) attacks, cloud account takeover or cybercriminals using trusted third parties to compromise the organisation through their supplier, an initial email can lead to compromise. After initial compromise, they have access to your domain, giving them access to email accounts and the ability to commit fraud.

Worryingly, compromised accounts can often go undetected, leaving no indicators of compromise or evidence of malware. And despite the deployment of privileged account management (PAM) and multifactor authentication (MFA), these attacks are still on the rise. If undetected, organisations are faced with an even bigger problem – that of privileged escalation and lateral movement within the networks.

To combat this, organisations need to implement technology to identify and respond to compromised users and remove what attackers need to complete their crime: privileged account access. A unique approach to identity threat detection and response (ITDR) will help organisations remediate privileged identity risks and understand the potential ramifications of compromise, such as access to critical data and intellectual property.

The result is a unified solution that extends protection across the entire attack chain for critical threats like ransomware and data breaches, gives organisations unprecedented insights into their privileged access attack surface and helps security teams better protect those at most risk of attack. □

For more information, please visit
www.proofpoint.com

proofpoint.

Break the attack chain

Aegis Threat Protection

Protect your people from advanced email attacks.

No. 1 cybersecurity solution of the Global 2000.

Identity Threat Defense

Defend sensitive data from theft, loss and insider threats.

Fastest-growing company in the information protection market.

Sigma Information Protection

Secure privileged identities and stop lateral movement.

Undefeated in 150 red-team exercises (and counting) to stop privilege escalation.

proofpoint.

Protect people. Defend data.

Learn more:
www.proofpoint.com/uk

S-RM

YOUR FIRST CALL FOR CYBER SECURITY

www.s-rminform.com

5 tips for cybersecurity success and ransomware resilience

Five tips every organisation should consider when protecting itself against cyber-threats

Martijn Hoogesteger reports

The cyber-threat landscape is constantly evolving. For businesses, particularly small or medium-sized enterprises, the effort needed to stay ahead of cyber-risk is daunting. However, there are practical exercises organisations of any size can undertake to protect themselves against cyber-threats.

Here Martijn Hoogesteger, Head of Cybersecurity, outlines five tips every organisation should consider when protecting itself against cyber-threats and offers specific advice on ransomware readiness – the most prolific of all the cyber-incidents we see at S-RM.

1. Understand that your data is attractive to attackers

An organisation's data is a very precious resource, and there is little surprise that regulations around data, particularly personal data, are growing and hardening. For any business collecting, storing, or processing customer, employee, or client data, you must understand that this is an attractive target for attackers and hence presents your greatest area of risk and liability.

2. Take steps to understand the evolving threat landscape

You don't have to be a technical cyber-expert to understand the evolving threat landscape. You can build knowledge and awareness incrementally. Focus on your industry and keep up to date with the risk businesses face – you can do this by subscribing to weekly risk bulletins, free alert services, and by signing up to receive material from organisations like the National Cyber Security Centre (NCSC) in the UK. As a next step, consider engaging a professional cybersecurity consultancy to help you understand your firm's threat profile.

For any business collecting, storing, or processing customer, employee, or client data, you must understand that this is an attractive target for attackers and hence presents your greatest area of risk and liability.

3. Understand and map your IT environment and attack surfaces

Are your printers networked? Do you use a third-party supplier to host your company website? It's important to map out your IT environment, which can get very complex – but you can't protect what you can't see or don't know is exposed. Making sure your IT team (be that internal or external) has up-to-date network diagrams, asset registers, public (and private) IP address inventories is important. Having these resources ready and available allows you to assess your own exposure to vulnerabilities accurately, implement mitigating controls, and also respond more quickly and effectively in the event of an incident.

4. Carry out a comprehensive review of your cybersecurity controls

Once you have mapped out your IT environment, you can start to carry out a risk assessment of each point of exposure. This will provide the foundation of a 'road mapping' exercise in which solutions can be intelligently focussed on known and prioritised weaknesses. However, there's no point in having a 'to do' list with no one assigned to carry out the tasks. So, when it comes to implementing changes, ensure that the programme is owned at the right level of leadership and resourced with appropriate expertise. We also recommend that companies align their roadmap against a well understood technical framework (for example CIS18, NIST, etc.) This will allow to make sure you have considered all control domains.

5. If time and budget are scarce, focus on quick wins

If there isn't time or budget to go through these steps, assume that an attack is *likely* to happen sooner rather than later and focus on quick wins:

- Provide security awareness training for your staff
- Arrange penetration testing to expose and remediate the flaws most visible to would be attackers
- Update and simplify your Incident Response plan
- Exercise response teams and processes with a simulated attack

Ransomware resilience

Of all the cybersecurity threats organisations face, ransomware remains one of the most pervasive, and

Of all the cybersecurity threats organisations face, ransomware remains one of the most pervasive, and is the key driver behind most incidents we respond to at S-RM.

is the key driver behind most incidents we respond to at S-RM.

In 2021, there was concern within the cybersecurity sector about the war in Ukraine and whether Russia-based hacking groups might step up new forms of attack on certain western targets as a result.

However, this did not materialise and the majority of organised cybercriminal groups continue to operate 'as normal' today, with ransomware groups continuing to target western companies indiscriminately.

Such groups will often scour the internet and use publicly available vulnerability scanning tools to identify 'low hanging fruit' to target – in other words, companies with weak security postures and exposed vulnerabilities.

You can minimise your chances of being impacted by a ransomware incident by implementing the following core security controls:

- Review your public facing infrastructure for vulnerabilities and ensure that the latest security updates and patches are applied and tested as fast as is feasible.
- Deploy multi-factor authentication (MFA) to all external services and remote access methods.
- Deploy and monitor an Endpoint Detection and Response (EDR) solution to increase your capabilities to detect and respond to threats as they occur. Remember that a tool like this is only as good as the time and resource you give to configuring and monitoring it properly.
- Maintain regularly tested backups of critical systems and data which are off-network or offline to reduce downtime in the event of a cyber-attack. These backups should be stored away from the core infrastructure with a segregated method of access management in place.
- Enable logging within the environment at the most granular level and with the longest retention feasible, particularly for network logs. This will mean that, in the event of an incident, you can easily and effectively investigate what vulnerabilities may have been exploited and how a threat actor may have gained access to your environment – in turn, this will mean you can emerge more resilient from an incident and remediate any security failings identified.
- Review your denial of service protections with your ISP and consider using web application firewalls where applicable.

S-RM is here to help organisations build their cyber-resilience. Please reach out to our experts to get your cyber-plans underway. □

Martijn Hoogesteger is Head of Cybersecurity at S-RM.

For more information, please visit **www.s-rminform.com**

e-Crime & Cybersecurity Congress 2024

"I thought the e-Crime & Cybersecurity Congress was absolutely fascinating! I'm new to the industry, so there was a lot for me to learn in a short time. Many of the topics discussed were advanced, but the speakers were excellent at explaining things and I was able to understand every point. The whole thing was so incredibly well organised and well run and I'm really looking forward to going back next year!"

Software Engineer, The Home Office

"Happy 21st! – great to be back in person at another well organised event providing short, punchy and educational presentations from some quality speakers."

Chief Compliance and Business Ethics Officer, Saint-Gobain

"Just wanted to let you know I thought it was a really good event!"

Information Security Programme Manager, Hiscox

2023 sponsors included:

Strategic Sponsors

Abnormal, BeyondTrust, corelight, CROWDSTRIKE, Forcepoint, GATEWATCHER, Integrity360, MENLO SECURITY, mimecast, proofpoint, RED SIFT, SentinelOne, SYNOPSYS, transmit security

Education Seminar Sponsors

CISCO, ESENTIRE, HOXHUNT, INTEL471, Kiteworks, noetic, OBSIDIAN, Ontinue, Opensystems, RISK LEDGER, SEARCHLIGHT CYBER, Silobreaker, VMRAY, ZEROFOX

Networking Sponsors

iZOOlogic, PERCEPTION POINT, ULTRARED

Branding Sponsors

agnostic intelligence, BSS, JT

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

Thank you to all our sponsors

Strategic Sponsors

corelight

CROWDSTRIKE

GATEWATCHER

illumio

KnowBe4
Human error. Conquered.

rubrik

SentinelOne

Education Seminar Sponsors

HOXHUNT

proofpoint

Recorded Future

RELIAQUEST

sosafe

S-RM