e-crime & cybersecurity SWITZERLAND

28th September 2022
Zurich, Switzerland

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Securing critical business sectors

Finance, healthcare, infrastructure and local government are all key targets: are they doing enough?

Forthcoming events

e-crime & cybersecurity MID-YEAR

19th October 2022
London

1st November 2022
Copenhagen

e-crime & cybersecurity NORDICS

e-crime & cybersecurity SPAIN

15th November 2022
Madrid

8th December 2022
Amsterdam

e-crime & cybersecurity BENELUX

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

Switzerland, arguably, came late to cybersecurity. It was only in 2019 that the Federal Council created the NCSC, which is part of the FDF General Secretariat. But more recently, the growing significance of cybersecurity to the country and core sectors such as finance has become clear. This year, the Federal Council is looking to reinforce and restructure the NCSC and turn it into a Federal Cybersecurity Office.

In addition, the government has just announced the establishment of a financial sector cybersecurity association, aimed at increasing the cyber-resilience of the country's financial sector. A new Swiss Financial Sector Cybersecurity Centre (Swiss FS-CSC) has been established in Zurich, which is open to all banks, insurance companies, and other entities that are registered in Switzerland and authorised by The Swiss Financial market supervisory authority (Finma).

The drivers of these changes are clear: Switzerland is increasingly a target for cyber-attacks. In February Swissport, the world's largest airport ground services and cargo handling company, was targeted by ransomware.

So how can vendors, governments and CISOs work together to build a better model for cybersecurity? In the US, a new cybersecurity act for the healthcare sector has been proposed; resilience is the key buzzword in finance, and regulators want to force companies to put CISOs on their boards. In Europe, DORA and other regulatory updates are increasing mandatory security measures. And new technologies and cybersecurity architectures are being developed to try to keep up with the hackers, at the same time as the market moves to digital assets and the metaverse. But is this enough?

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

Simon Brady | Editor

@eCrime_Congress **#ecrimecongress**

28th September 2022

Courtyard by Marriott Zurich North

3 The business of fraud: Bank fraud
Recorded Future analysed current data between March 2021 and March 2022 to observe and identify how threat actors are conducting and advertising the following types of bank fraud: accounting, loan, checking, and wire transfer.
Recorded Future

7 Security operations: New terminologies for old problems?
6 easy steps decision-makers should emphasize in the orientation & decision-making process
GATEWATCHER

9 A new home front: The part we all play in a modern cyber-war
The degree to which modern war efforts can be influenced by individual threat actors is a new and disconcerting symptom of the modern cyber-landscape.
Darktrace

12 Schutz vor Ransomware: Awareness ist entscheidender Faktor
Um Unternehmen über die Prävention von Ransomware-Angriffen zu informieren und ihnen dafür die Grundlagen an die Hand zu geben, veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den „Maßnahmenkatalog Ransomware". Das BSI verpasst hier jedoch womöglich eine große Chance, indem es sich in seinen Empfehlungen nur auf die Eindämmung von Ransomware konzentriert.
KnowBe4

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

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

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

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

14 Preventing highly evasive threats that lead to ransomware
Ransomware continues to torment cybersecurity leaders around the world.
Menlo Security

17 Protecting global events when the world is watching
Defending against cyber-threats must be an important consideration for organisers and is no longer something we can bury our heads in the sand about.
Mandiant

19 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.

28 Speakers and panellists
Names and biographies.

33 Mensch und Maschine in der Cybersicherheit: Partner oder Gegner?
Viele Organisationen und deren Sicherheitszuständige haben inzwischen verstanden, dass sie sich dringend auf den Fall einer auf sie gerichteten Cyberattacke vorbereiten und entsprechende Schutzmaßnahmen entwickeln müssen, da es nur eine Frage der Zeit ist, bis es soweit ist.
SentinelOne

35 Distributed Cloud Services: Einheitliche Sicherheitskontrollen für verteilte Infrastrukturen
Eine neue SaaS-basierte Plattform vereinfacht das Security Management für sämtliche Anwendungen in allen Umgebungen.
F5

38 Testing early and often can reduce flaws in app development
Security needs to be much more than an afterthought.
Synack

40 Drei Tipps zur Verbesserung der Cloud-Sicherheit
Cloud-Dienste Cloud-Dienste nicht nur ein wesentlicher Bestandteil der digitalen Infrastruktur von modernen Unternehmen sondern auch bei Angreifern sehr beliebt.
CrowdStrike

42 How aligning Security Awareness and Security Operations can reduce dwell time
It is time Security Awareness takes its rightful place next to Security Operations as partners in reducing dwell time and keeping email phishing attacks out of employee inboxes.
Cofense

44 Data Centric Security oder Information Rights Management 2.0
Ein neuer Ansatz zum Schutz und zur Kontrolle vertraulicher Unternehmensdaten überwindet die größten Probleme klassischer IRM-Systeme.
Seclore

45 Verbesserte Sicherheit der Betriebstechnologie mit Cyber Deception
Die Deception-Technologie bietet eine effektive weitere Schutzschicht.
CounterCraft

The business of fraud: Bank fraud

Recorded Future analysed current data between March 2021 and March 2022 to observe and identify how threat actors are conducting and advertising the following types of bank fraud: accounting, loan, checking, and wire transfer.

Recorded Future analysed current data from the Recorded Future® Platform, dark web and special-access sources, and open-source intelligence (OSINT) between March 2021 and March 2022 to observe and identify how threat actors are conducting and advertising the following types of bank fraud: accounting, loan, checking, and wire transfer. This report expands upon findings addressed in the first Insikt Group Fraud Series report, "The Business of Fraud: An Overview of How Cybercrime Gets Monetised".

Executive summary

Bank fraud is the use of illegal means to obtain money, assets, or other property owned or held by a financial institution or individual by fraudulently posing as a bank, another financial institution, or another individual. As the financial sector has incorporated online and internet-connected banking into its business model, traditional means of fraudulently acquiring funds from a bank have been replicated and updated to target today's online banking employee and consumer. Throughout Recorded Future's 'Business of Fraud' series of reports, we have identified many tactics, techniques, and procedures (TTPs) being used by cybercriminals to facilitate online criminal activities. Many of these same TTPs, from harvesting and using compromised personally identifiable information (PII) to social engineering, are also being used to conduct banking and online banking account fraud. In this report, we examined cybercriminal activities around the following types of bank fraud due to them often being overlooked and to identify parallels with other types of financial-related fraud: accounting, loan, check, and wire transfer.

Key findings

Threat actors are offering services and selling how-to guides and tutorials that include instructions on how to manipulate financial records, get approval for loans, and purchase compromised accounts that contain loan application information. Hackers-for-hire include the capability of accessing and manipulating records and documentations in their advertisements.

Counterfeit checks are still in high demand and are often coupled with threat actors looking to conduct wire transfers or cash out. The means of creating a counterfeit check has become more automated and customised, with threat actors operating shops that focus on this service and whose user interface is easy to follow.

Threat actors continue to use instant messaging platforms to advertise, negotiate, and sell services and listings that facilitate check, loan, wire transfer, and accounting frauds. These messaging platforms are all-encompassing when compared to the traditional dark web ecosystem (forums, marketplaces, and shops) in that they provide instantaneous communication, greater control in adding and removing listings, and are more readily available.

Background

Bank fraud is the use of illegal means to obtain money, assets, or other property owned or held by a financial institution, or to obtain money from depositors by fraudulently posing as a bank or other financial institution. While the specific elements of banking fraud laws vary depending on jurisdictions, the term 'bank fraud' applies to actions that employ a scheme or artifice, as opposed to bank robbery or physical theft. For this reason, bank fraud is sometimes considered a white-collar crime. Online banking services now allow customers to access bank accounts and records via personal computers and mobile devices. This convenience has not only increased the attack surface but has allowed cybercriminals to creatively leverage new and old methods for conducting nefarious activities.

Threat actors gain access to online banking accounts in multiple ways, such as using a stolen identity (identity theft) to open new accounts (application fraud) or obtaining valid credentials to existing accounts (account takeover) through phishing, credential reuse, different types of malware, or

Recorded Future reports

A majority of bank related fraud involves compromised payment data and accounts, compromised PII data and bypass methods (among others) used in accounting, loan, checking, and wire transfer. These types of fraud are being actively sought after and advertised across the entirety of the dark web criminal ecosystem.

purchasing them from dark web sources. Given the previous reporting done by Recorded Future that relates to financial crimes (laundering funds, using compromised PII and counterfeit documentation to open accounts, using sniffers, bank injects/overlays, infostealers to harvest banking credentials to take over accounts and payment cards, and recruiting mules and cashout services), this report will not focus specifically on compromised payment card data or one of the aforementioned topics. Rather, this report will examine how cybercriminals are conducting operations across a variety of dark web and special-access sources to facilitate the following types of bank fraud, which are not as commonly known or popularised: check, loan, wire transfer, and accounting fraud.

Types of bank fraud

Many of the aspects covered throughout our Fraud Series overlap with TTPs being used by threat actors to facilitate bank fraud:

- A majority of threat actors are not specifically advertising services for the 4 types of bank fraud addressed in this report; rather, are offering services and methods that include these activities in conjunction with other types of financial fraud.
- Like with most types of fraud, compromised credentials and PII to create or gain control of accounts are the lifeblood of bank fraud. Threat actors advertising these types of compromised data are using the same forums, marketplaces, and shops (both as sellers and buyers) to facilitate other types of fraudulent cybercrimes.

Threat actors are lately interested in synthetic identities, a type of fraudulent identity that combines the proprietary PII (such as date of birth, Social Security number) of several individuals to make a single, new identity. Although this report does not specifically investigate synthetic identities, the amount of compromised PII data widely available across dark web sources coupled with the widely shared knowledge of performing fraudulent activities (social engineering, phishing, among others) makes this attack vector an attractive tactic to be used by criminals in the future, specifically those wanting to commit bank and financial-related crimes such has registering account or loan applications. According to our data sets, there are multiple tutorials and how-to guides on creating synthetic identities across different dark web and special-access sources.

Outlook

The 4 types of fraudulent activities that facilitate bank fraud covered in the full report showcase how different types of fraud are using similar methods and require similar data to facilitate activities. A majority of bank related fraud involves compromised payment data and accounts, compromised PII data and bypass methods (among others) used in accounting, loan, checking, and wire transfer. These types of fraud are being actively sought after and advertised across the entirety of the dark web criminal ecosystem, with threat actors continuing to incorporate instant, encrypted messaging platforms into their methods for advertising, discussing, seeking, and selling services and products.

As highlighted in Recorded Future's 2020 series on the automation and customisation of the dark web, the threat actors highlighted in this report (as well as the many others) are continuing to customise their services, host automated shops and marketplaces with easy-to-use interfaces, and update their attack vectors to defeat security measures. We believe threat actors will continue to incorporate automation and customisation into their business model so as to attract customers and make profits. As the demand for these services show no signs of dissipating, we recommend working with Recorded Future so as to receive timely updates and notifications of events or listings that may affect your brand. Once an alert is received, we recommend triaging it for severity and working with us to identify solutions and steps to be taken in the future to harden your security measures.

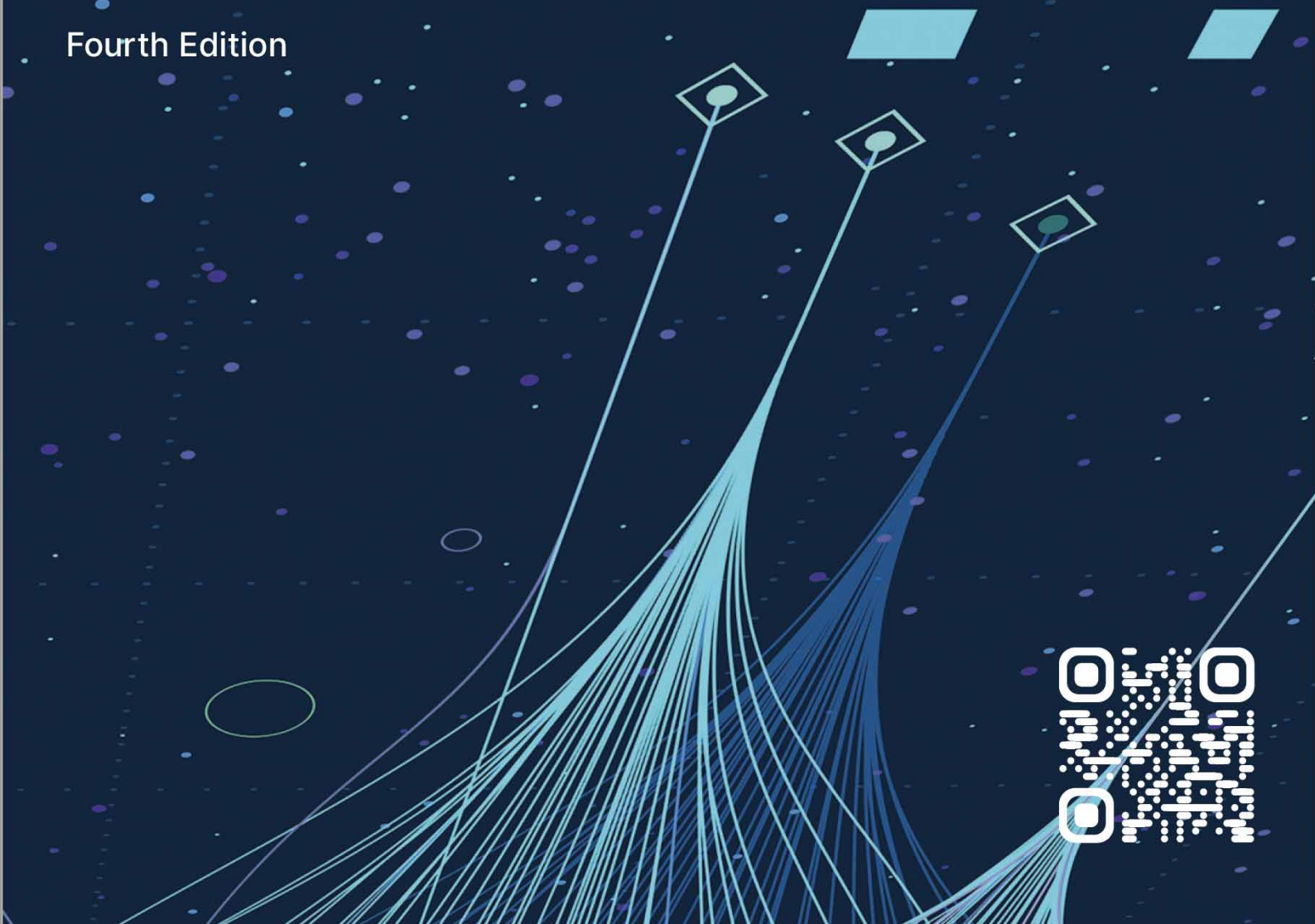
Editor's note: This article is an excerpt of a full report. Click the PDF link to read the entire analysis. □

Recorded Future®

THE INTELLIGENCE HANDBOOK

A Roadmap for Building an Intelligence-Led Security Program

Fourth Edition



GATEWATCHER

HIGHLIGHT CYBER THREATS BEFORE THEY **DARKEN** YOUR BUSINESS

AIONIQ®

AUGMENTED DETECTION

NDR with behavorial and mapping analysis powered by AI

AIONBYTES®

DYNAMIC ANALYSIS

Sandboxing with dedicated and monitored environment

LASTINFOSEC®

SMARTER DETECTION

CTI with enriched streams analysis

+ 600

INFRASTRUCTURES PROTECTED

100M

FILES SCANNED PER DAY

+ 20Bn

EVENTS PROCESSED PER DAY

www.gatewatcher.com

Security operations: New terminologies for old problems?

6 easy steps decision-makers should emphasize in the orientation & decision-making process

The cybersecurity industry numbers almost 4,000 software vendors worldwide. Despite the approximately 15% that leave the market each year, the number is growing every year – and there is no end in sight. This also applies to terminologies, which increase every year. As a result, it is becoming increasingly difficult for decision-makers to get an overview.

It is the same with vendors as it is with terminologies

Between real successful companies there are many soldiers of fortune and 'snake oil' – and just as much marketing wordings and 'business bullshit', as aptly described in the recently published book by Jens Bergmann. The market is flooded with new terminology and marketing messages, which on closer inspection, turn out to be empty phrases and artificial words.

Business bullshit in all cybersecurity spheres?

This applies not only to the market as a whole, but also to niches such as security operations centres (SOC). Want an example? The list is long... Here is a small sample of acronyms:

- SIEM (Security Information and Event Management)
- SOAR (Security Orchestration, Automation and Response)
- NDR (Network Detection and Response)
- EDR (Endpoint Detection and Response)
- XDR (Extended Detection and Response)
- MDR (Managed Detection and Response)
- CTI (Cyber Threat Intelligence)
- Attack surface
- Threat hunting
- Zero Trust

To understand: The current 'buzzwords' MDR & XDR are ultimately just evolutions of the long-established SIEM, SOAR, EDR & NDR, which denoted relevant data collection on end and network devices with a central consolidation of data, at best events, to support SOC teams and automate their operations. What for? So that organisations with as small a team as possible can, operate current technologies in a way that – in addition to automated detection – also detects anomalies that are difficult to realise as early status of an attack as automated detections without too high a number of *false positives*.

There is rarely anything new behind the new terminologies

The current terms denote in very few cases really new technologies; at best 'repackagings' or commercialisations of previous open source or personal projects. Technology providers partly do what technically interested, knowledgeable people have been doing for years and put this into paid, ready-made packages – which hopefully will be maintained and further developed in line with the times.

Is there such a thing as the 'jack of all trades' of the cybersecurity scene?

Many vendors of such next-gen solutions – augmented intelligence, artificial intelligence, machine learning, supervised/unsupervised, deep learning, etc. – claim to be able to cover and fulfill everything. Here it is important not to confuse their visions with the reality.

AI as a panacea? – dream or reality in the near future?

With respect to AI, most of the cybersecurity industry was convinced early on that AI was the cure for all bad. Industry experts continue to promise that AI can solve all of the pressing problems of the day. From the labour shortage, to fully automating the security team through autonomous operations, to detecting 'unknown unknowns' – and even protecting against non-existent adversaries – AI is supposed to fix all of it.

Experts know: In reality, more AI has been written in PowerPoint than in code

One approach may be to view AI less as '**artificial** intelligence' and more as '**augmented** intelligence' – and to use it. It is true that AI can already solve many things better than humans. But is not yet good enough. Moreover, the human = the natural intelligence, continues to be the decisive factor of the artificial.

Well-founded decision-making aids show the way through the cybersecurity jungle

How are IT decision-makers supposed to orient themselves in the confusing jungle and choose the right one now from the [seemingly novel] offers and possibilities? How can they efficiently find the answers to the most important questions?

- Which solutions & tools do companies really need?
- Which cybersecurity systems significantly increase the level of security?
- What processes facilitate the work of cybersecurity departments and specialists?

GATEWATCHER reports

- Which selection criteria are relevant for medium-sized companies, and which should corporate decision-makers pay attention to?

In short: CXOs, head of IT departments and all responsible stakeholders need decision-making aids to identify what is pure marketing gimmick – and what actually promises sense & benefit for the entire organisation or the interacting systems.

New terms & solutions – old strategies

While the terminology in the IT industry has changed, the way decision-makers work has remained the same. And that's a good thing! Because anyone who really decides on budgets must not be guided by highly motorised marketing promises, but must decidedly deal with the technological aspects, talk to several qualified providers and test different solutions.

IT decision-makers under time pressure – or – Marketing always wins!

The problem: Because decision-making deadlines are getting shorter and shorter, expectations are getting higher and higher, and the urgency for quick solutions has increased exorbitantly in recent years, IT architects, analysts and decision-makers often have far too little time in reality to make truly solid decisions. The result: the best-known vendor, who often shines through marketing, gets the deal. And not the perhaps more inconspicuous provider, who does not put his budget into marketing, but into innovation and function.

Decision criterias & filter options

The crux of 'brand recognition of a provider versus depth of technical knowledge' raises new questions in the selection process:

- How can decision makers escape the 'marketing trap'?
- How can decision-making times be reduced to a minimum without risk?
- According to which filter criteria should one select in order to find individual *state of the art solutions*?

In principle, what has always been true applies:

> *Security does not begin with technologies and even less with products; security begins with a process. And which technologies fulfill this process and thus ultimately contribute to security is decided by the process and the individual circumstances of each individual IT landscape.*

The future certainly belongs to AI, ML & Co., but it still seems in many parts of the industries that their real, reliable and useful usability is still a long way off.

Security by obscurity – AI (still) in the twilight

What use is it if a large part of the alleged AI is nothing more than rule-based expert systems that generate a vast number of *false positives* and take systems offline on a daily basis even though there was no threat at all? What's more, essential processes often still run in a black box. But *security by obscurity has never been* a good tactic.

TIPS

You are an IT decision maker and responsible for cybersecurity in your company? GATEWATCHER will be happy to support you in your decision-making process.

1. Take enough time to identify the relevant players in the cybersecurity scene.
2. Don't be blinded by full-bodied marketing promises.
3. Analyse your needs accurately.
4. Check out the professional journals and rankings.
5. Don't give up your goals for vendor promises!
6. If necessary, engage suitable consulting partners who know the international cybersecurity market inside out.

There is a fundamental difference between a company pretending to be an AI company – and companies that are proven to use mature details associated with the term 'AI' – to solve cybersecurity problems.

Protection against known threats no longer sufficient

The fact is that mere protection against known threats and attacks is no longer sufficient by a long shot.

> *IT is like health: It is better to always live a healthy life – and not to react only when an illness has already occurred.*

IT decision-makers should therefore make sure that their system is not infiltrated and keep it 'healthy'. After all, if they have to act hastily – in the event of an attack – it is usually already too late. The damage has already been done. □

A new home front: The part we all play in a modern cyber-war

The degree to which modern war efforts can be influenced by individual threat actors is a new and disconcerting symptom of the modern cyber-landscape.

Marcus Fowler reports

Cyber-warfare is increasingly being conducted outside of centralised military or government efforts. In Ukraine, without direct government supervision, thousands of private individuals and organisations are involving themselves in the cyber-war against Russia. Yurii Shchyhol is Head of Ukraine's State Service of Special Communications and Information Protection. Speaking to Politico, he commends a group of "more than 270,000 volunteers who are self-coordinating their efforts and who can decide, plan, and execute any strikes on the Russian cyber-infrastructure without Ukraine getting involved in any shape or form".

'Hacktivists' have existed since the 1990s, but the term seems ill-suited to the scale and approach Shchyhol is describing. They might instead be labelled an auxiliary cyber-force, playing a supportive role in a larger military effort. Shchyhol himself calls them 'an army'.

Open-source warfare

In the modern cyber-landscape, anyone with a computer and a basic skill set can contribute to a war. Depending on who and perhaps where you are, this fact is inspiring, concerning, or a little of both. The challenge of distinguishing between official nation-state attacks and hacktivists raises certain issues, making it possible, for instance, for nation-states to conduct devastating attacks against critical national infrastructure from behind a mask of proxy criminal organisations. The ties between nation-states and these organisations may be suspected, but any accusations are rarely confirmed.

The converse problem is seen when idealistic individual actors launch provocative attacks with the potential to stoke tensions between nation-states. Recent DDoS and defacement attacks against Taiwanese government sites and businesses are largely being attributed to Chinese hacktivists, but with the perpetrators unidentified, these attacks remain a concerning question mark and do little to ameliorate sharply rising tensions. A spokesperson for Taiwan's ruling party has already said in a statement that these attacks are "unilaterally raising the situation in the Taiwan Strait." Official Taiwanese websites, like that of the Presidential Office, the Ministry of National Defense, and a municipal Environment Protection Bureau have all been targeted, the latter defaced with five Chinese national flags.

A spate of similar defacements preceded Russia's February invasion of Ukraine, with more than a dozen Ukrainian national websites made to display threats like, "be afraid and expect the worst". Once again, the perpetrators of this attack remained unconfirmed, with Ukrainian government institutions accusing the Russian Federation, and Russia denying all involvement. The degree to which modern war efforts can be influenced by – or concealed behind – individual threat actors is a new and disconcerting symptom of the modern cyber-landscape. There are, however, more official ways in which cyber-warfare has moved beyond government and military organisations as well.

Calling in a private cavalry

Just 15 months after it was opened by President Volodymyr Zelensky, the UA30 Cyber Center in Ukraine lies largely empty. It is located in an unsafe part of the war-torn country, and its operations have had to be moved elsewhere. In the time between its opening and Russia's invasion in February, however, the centre was able to host more than 100 cybersecurity training sessions. These sessions, which involved realistic cyber-attack simulations, hackathons, and other competitions, were attended by some military operators, but also by large numbers of civilian contractors and private sector representatives. Their attendance was part of an intentional and significant effort to involve the private sector in Ukraine's cyber-defence efforts.

Shchyhol explains, "a lot of private sector IT cybersecurity experts are either directly serving in the Armed Forces of Ukraine or my State Service or otherwise are indirectly involved in fighting against cyber-attacks." This is the realisation of the UA30 Cyber Center's aim: using crucial assistance and expertise from the private sector in national cyber-

For private sector organisations, auxiliary cyber-forces, and hacktivists alike, focusing on defensive rather than offensive action will be the surest way to win the battle and the war.

defence efforts, and bolstering the security of those organisations on which Ukraine's critical national infrastructure depends. As we have seen with attacks against Ukrainian telecom and internet providers, organisations operating the infrastructure which underpins a population's daily life are often the first – and most appealing – targets for attackers looking to create disorder within a nation.

It is not only Ukraine's own private sector which is lending a hand. International organisations like and Amazon have contributed to Ukraine's efforts by providing technology and infrastructure, as well as their own expertise and services. In its report on Early Lessons from the Cyber War, Microsoft suggests that "defence against a military invasion now requires for most countries the ability to disperse and distribute digital operations and data assets across borders and into other countries". With cloud services provided by Amazon, Microsoft and others, and data now hosted across Europe, Ukraine is managing to do just that. Like its army of guerilla cyber-fighters, the involvement of private organisations is dispersing and bolstering Ukraine's war effort.

The new home front

Beyond these direct contributions, however, Shchyhol also notes those private sector organisations supporting the cyber-war 'indirectly'. These indirect efforts have been a focus of US government statements on cybersecurity since the beginning of the conflict. A statement from President Biden in March read, "I urge our private sector partners to harden your cyber-defences immediately", a message which has been repeated and reinforced by CISA.

The great responsibility that private organisations have for critical national infrastructure has been highlighted in attacks like that on Colonial Pipeline last year, but organisations in every industry can offer opportunities for nation-state attackers. When more organisations are sufficiently prepared for cyber-attacks, the nation as a whole becomes stronger.

In its report, Microsoft calls for 'a common strategy' to thwart modern cyber-threats, which includes the need for greater public and private collaboration and advances in digital technology, Artificial Intelligence (AI), and data. By adopting stronger defences, and employing well-suited emerging AI technologies, organisations can accelerate the detection and prevention of threats, and contribute to national security in the face of constantly developing international cyber-threats.

When cyber-attackers are provided with funding, coordination, and thorough threat security intelligence, they can create scores of never-before-seen attacks, which circumvent pre-established security rules and avoid detection. As attackers develop their approach, so must defenders — not just by employing the latest technologies, but by embracing the changes in defensive strategy that those technologies enable. Defenders need to pivot away from focusing on patterns and predictions, and concentrate on understanding the landscapes and 'normal' operations of their digital environments. With this approach they can harden attack paths, visualise their internet-facing attack surface, detect the smallest deviations from 'normal', and disrupt attackers before damage is done.

For private sector organisations, auxiliary cyber-forces, and hacktivists alike, focusing on defensive rather than offensive action will be the surest way to win the battle and the war. □

Marcus Fowler is SVP, Strategic Engagements and Threats at Darktrace.

As SVP of Strategic Engagements and Threats, Marcus works closely with senior security leaders across industries on cybersecurity strategy and business resilience, including across Darktrace's Federal Division. Marcus focuses his research and analysis around emerging and next generation cyber-threats, trends, and conflicts. Prior to joining Darktrace in 2019, Marcus spent 15 years at the Central Intelligence Agency developing global cyber-operations and technical strategies. He has led cyber efforts with various US Intelligence Community elements and global partners. Prior to serving at the CIA, Marcus was an officer in the United States Marine Corps. Marcus has an engineering degree from the United States Naval Academy and a master's degree in International Security Studies from The Fletcher School. He also completed Harvard Business School's Executive Education Advanced Management Program.

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

CYBER SECURITY ISN'T A PRODUCT. IT'S A STATE OF BEING.

We believe that cyber security should cover you from all angles, all the time. It's why Darktrace detects threats, responds to them, and helps proactively prevent them. And it's all powered by our industry-first Cyber AI Loop - which uses Self-Learning AI to constantly optimize your state of security.

DARKTRACE

Evolving threats call for evolved thinking

Darktrace.com

Schutz vor Ransomware: Awareness ist entscheidender Faktor

Um Unternehmen über die Prävention von Ransomware-Angriffen zu informieren und ihnen dafür die Grundlagen an die Hand zu geben, veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den „Maßnahmenkatalog Ransomware". Das BSI verpasst hier jedoch womöglich eine große Chance, indem es sich in seinen Empfehlungen nur auf die Eindämmung von Ransomware konzentriert.

Jelle Wieringa berichtet

Der kürzlich veröffentlichte BSI-Leitfaden ist eine großartige Initiative – jedoch ist seine Zielgruppe für so etwas oft nur schwer zu begeistern. Es gilt daher, diese Gelegenheit, die Leser mit einem Ransomware-Leitfaden zu erreichen, bestmöglich zu nutzen. Man muss sicherstellen, alles Wichtige einzubeziehen und eine umfassende Perspektive zu bieten. Security Awareness ist ein entscheidender Faktor bei der Eindämmung von Ransomware, weshalb das BSI gut daran getan hätte, einige Punkte zu diesem Thema in die Empfehlungen mitaufzunehmen.

Die Rolle von Social Engineering bei Ransomware-Attacken

Ransomware gelangt fast immer über den Faktor Mensch in ein Unternehmen. Beispielsweise erhalten Nutzer eine Phishing-E-Mail mit einem Link, der sie auf eine Website führt, die ihren Rechner mit Ransomware infiziert, oder sie bekommen eine Datei mit einem bösartigen Anhang geschickt. Bei dieser Art schädlicher Software handelt es sich um eine sehr verheerende Form von Malware. Sie kann ganze Unternehmen lahmlegen, sowohl durch Ausfallzeiten als auch durch den Verlust von Reputation.

Der Ransomware-Maßnahmenkatalog enthält zwar viele nützliche Informationen darüber, wie man sich von einem Ransomware-Angriff erholen kann, aber er thematisiert nicht die Vorbeugung eines solchen Angriffs. Natürlich kann Vorbeugung niemals zu 100 Prozent garantiert werden – ein Handbuch für die Reaktion auf Ransomware ist also grundsätzlich wertvoll. Doch bereits die richtige Prävention kann Unternehmen dabei helfen, eine Menge Ressourcen zu sparen.

Security Awareness Trainings als vorbeugende Maßnahme

Schulungen zum Sicherheitsbewusstsein schaffen eine Belegschaft, die sich über die Gefahren im Cyberraum bewusst ist. Sie ermöglichen es den Mitarbeitern, ein aktiver Teil eines Sicherheitsprogramms zu werden. Die Teilnehmer werden in die Lage versetzt, Cyber-Bedrohungen zu erkennen und auf sie zu reagieren. Die Trainings vermitteln ihnen sowohl das Wissen als auch die Fähigkeiten, die in der heutigen digitalen Welt erforderlich sind.

Aus wirtschaftlicher Sicht ist es wesentlich besser Ransomware vorzubeugen, als sich von einem Angriff zu erholen. Schulungen sind für jeden zugänglich, da sie online angeboten werden. Auf jedem Gerät, zu jeder Zeit und überall. Die Trainings sind kostengünstig, führen nachweislich zu Ergebnissen und können auf die individuellen Fähigkeiten eines jeden Teilnehmers abgestimmt werden. Es wäre enorm wertvoll, wenn die Regierung ihre derzeitigen Bildungskampagnen um Security Awareness Trainings erweitern würde – eine solche Entwicklung würde deutschlandweit die digitale Hygiene und Sicherheit deutlich verbessern. Auch ein Sensibilisierungstool wie der Ransomware-Maßnahmenkatalog sollte sich darauf konzentrieren, auf Maßnahmen wie Schulungen aufmerksam zu machen, die auf allen Ebenen eines Unternehmens umsetzbare Erkenntnisse liefern.

Das Bewusstsein der Menschen zu schärfen, führt jedoch nicht automatisch dazu, dass sie auch nach den neuen Erkenntnissen handeln. Der Schwerpunkt von Schulungen sollte daher nicht nur auf der Vermittlung von Wissen liegen. Es bedarf langfristiger Bemühungen, um Organisationen und Verbraucher zur Teilnahme zu bewegen, und es muss viel Aufwand betrieben werden, um die Bereitschaft und Motivation zu schaffen. Das Endziel ist es, die Menschen zu einem sichereren Verhalten zu bewegen, damit sie bessere Sicherheitsentscheidungen treffen. Durch das Verständnis für den Zweck der Übung sollen die Teilnehmer motiviert werden, das Gelernte anzuwenden.

Fazit

Ransomware wird häufig als etwas Beängstigendes wahrgenommen und oft missverstanden. Viele denken, man könne derartige Angriffe schlichtweg nicht verhindern. Dieser Irrglaube ist wahrscheinlich einer der Hauptgründe, warum sich der Maßnahmenkatalog des BSI auch auf die Prävention konzentrieren sollte. Denn jeder weiß, dass die Prävention eines Vorfalls besser ist, als sich mit seinen Folgen auseinandersetzen zu müssen. □

KnowBe4
Human error. Conquered.

Why security awareness training?

RANSOMWARE
PHISHING
CEO FRAUD
COMPLIANCE

That's why.

TEST

TRAIN

PHISH

RESULTS

KnowBe4, Inc. | 855-566-9234 | www.KnowBe4.com | sales@KnowBe4.com

Preventing highly evasive threats that lead to ransomware

Ransomware continues to torment cybersecurity leaders around the world.

Menlo Security reports

More than 70% of organisations were hit by ransomware attacks in 2021, according to the 2022 CyberEdge Cyberthreat Defense Report – a staggering increase from 55% in 2018. These attacks shut down businesses, disrupt public infrastructure, and cost organisations billions of dollars in ransom payments.

Attackers know that ransomware is incredibly easy to execute and scale, and new digital payment methods such as cryptocurrencies make it easy to hide identities and bury a paper trail – all of which has put CISOs on high alert.

The surge in these attacks can be attributed to multiple factors:

- *Ransomware is more targeted than ever before.* Threat actors no longer have to rely on the inefficient 'spray and pray' approach – social engineering allows them to gather volumes of data on targets and craft personalised content to entice a user to click on a malicious link.
- *Ransomware can hide in plain sight.* Today's ransomware attacks are sophisticated and evasive, leveraging seemingly innocuous technologies such as Java communications and VPNs to spread laterally throughout the network. Threat actors are targeting web browsers with a new category of threats, termed Highly Evasive Adaptive Threats (HEAT), which bypass traditional security defences. These HEAT attacks can be used to deliver ransomware payloads and take advantage of today's expanded attack surfaces.
- *Ransomware is extremely lucrative.* Threat actors aren't content with the small fish anymore. Over the past two years, the average ransomware payment skyrocketed from $12,000 to $322,000 as targets shifted from individuals to large organisations with deep pockets, according to the 2022 CyberEdge Cyberthreat Defense Report.

How to prevent ransomware

Preventing ransomware requires that organisations shift from a traditional detect-and-respond approach to a Zero Trust mindset powered by isolation technology. This proactive, preventative approach safeguards mobile, distributed, and often unmanaged endpoints by routing all content through the Secure Web Gateway (SWG), where it's executed in an elastic sandbox in the cloud. Given that many of us now spend around three-quarters of our day using a web browser, isolation can also protect users against HEAT attacks from delivering malicious payloads leading to ransomware.

Here are three ways that Zero Trust powered by isolation technology can help stop ransomware attacks:

1. **Isolation automatically closes vulnerabilities.** Unfortunately, the expansion of attack surfaces means that it's virtually impossible for security leaders to completely close off initial access points for ransomware. With isolation, however, it doesn't matter if these access points are closed, because all traffic – whether it's suspicious or not – is routed through the isolation layer in the cloud and is never executed on the endpoint.

2. **Isolation helps detect abnormal behaviour.** Routing all traffic through an abstracted layer in the cloud gives organisations the visibility they need to identify and stop abnormal behaviour that, on the surface, may seem innocuous. Visibility into entities, where they are located, and the commands they are executing, enables a Zero Trust approach to cybersecurity.

3. **Isolation allows you to execute a recovery plan.** When mistakes happen, it's critical that CISOs have a recovery plan in place to determine how to respond. Answering questions like "*Can we recover lost data?*" and "*Should we pay the ransom?*" requires visibility into the network. Isolation technology makes this possible.

Take action today

Ransomware is a top concern among businesses today, and it will continue to vex security leaders in the future. Taking a Zero Trust to security and coupling it with isolation technology while it's delivered through an SASE framework provides the best defence against these highly-evasive and disruptive attacks. □

For more information, please visit
www.menlosecurity.com

MENLO SECURITY

HEAT attacks: The new era of web threats

Highly Evasive Adaptive Threats (HEAT) are currently evading multiple layers of security detection in current security stacks.

The result is the delivery of ransomware payloads and account takeovers. Discover how Menlo Security helps prevent these attacks and protect productivity, allowing your users to work without limits, while you work without worry.

Learn more at
menlosecurity.com

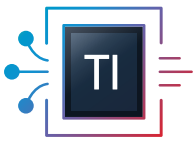
MENLO SECURITY

MANDIANT®

YOUR CYBERSECURITY ADVANTAGE

Put world-leading threat intelligence and frontline expertise to work with any security controls and at any organization.

Deliver dynamic cyber defense with the Mandiant Advantage SaaS platform.



Threat Intelligence

Attack Surface Management

Security Validation

Automated Defense

mandiant.com

Protecting global events when the world is watching

Defending against cyber-threats must be an important consideration for organisers and is no longer something we can bury our heads in the sand about.

Stuart McKenzie reports

Geopolitical summits, elections and sporting meets are some of the most visible events whether they're taking place on an international, national, or regional scale. They also present unique cybersecurity challenges for critical infrastructure and supply chains. From a summer of sporting events running through to the FIFA World Cup, as well as the G20 and COP27 summits this winter, no matter whether these last from a single day to multiple weeks or months, defending against cyber-threats must be an important consideration for organisers and is no longer something we can bury our heads in the sand about.

Defending these kinds of societal events requires active defences backed up by the latest intelligence on potential attackers. Organisers need to have strategic security programmes plus the right technical solutions in place to harden their security posture prior to an event and to support operations once it kicks off. Delivering resilient cyber-capabilities in a compressed timeframe under intense public attention and scrutiny is a major challenge that requires focus and investment to properly plan and implement.

There are three key phases to think about here, in the run up to and during a major event:

- *Understand the environment:* Prepare, harden and exercise
- *Anticipate threats:* Test, monitor and defend
- *Survive attacks:* Respond, contain and remediate

Understand the environment

This phase should take place before a major event, with the aim of proactively protecting and hardening the event's security posture. Do you know enough about the potential adversaries and have you prepared your people, processes and technologies in the right way?

Delivering resilient cyber-capabilities in a compressed timeframe under intense public attention and scrutiny is a major challenge that requires focus and investment to properly plan and implement.

Some of the critical things to think through in the preparation phase include:

- Ensure you can monitor and investigate alerts, proactively hunt for attackers and contain and remediate threats
- Deploy endpoint and network detection technologies across the entire environment and multi-factor authentication across all accounts and external facing services
- Create alerts for emerging and currently exploited vulnerabilities as well as current and imminent threats based on the latest information about the threat landscape
- Monitor social media, blogs, forums, news sites and chat apps for threats, misinformation and disinformation campaigns
- Coordinate with relevant national agencies to obtain and contribute related intelligence.

When it comes to hardening infrastructure, conduct compromise assessments and validate controls to check the security and integrity of the environment and the key data that needs protecting. Think about what all the different ways into that environment might be, and make sure to log and regularly scan all externally facing assets on the network.

In the heat of the moment, you don't want to be struggling to think who should be involved, so make sure you've designated a crisis-response team and that you've got the right organisational, executive and communications support. Conduct a tabletop exercise to ensure that all participants understand their roles and responsibilities during an incident, and test backup procedures to ensure that critical data can be rapidly restored and critical business functions can remain available.

Anticipate threats

Once the major event has begun, and there will be an increased risk of destructive or disruptive cyber-attacks. This is when you should go into an elevated active defence mode – or 'shields up'. Key priorities will include continuously validating security controls and defending critical assets. It's all about inhibiting the access an adversary needs to leverage to achieve their goal.

A prepared and practiced cyber-strategy and playbook helps ensure a favourable outcome not just for the hosts, but all participants, spectators, and those watching on from around the world.

Testing is important again here – whether that's ad-hoc penetration testing exercises on all externally facing assets, testing the internal team and technology's ability to detect, prevent and respond, or testing the incident response team's reaction times against real adversarial methods.

Monitoring what's happening in real time is key in this phase:

- Establish a situation room to bring together operations, intelligence and external organisation information and communications
- Continuously monitor, analyse and report relevant data and analysis from intelligence sources
- Conduct enhanced hunting and monitoring for indicator-less behaviours; assume attacks are happening and technical controls have missed something
- Continuously validate security controls effectiveness against active attack behaviours.
- Restrict egress communications on critical systems

Ultimately, the focus should be on protecting critical assets – what are your crown jewels and what might an adversary go after? Protect specific high-value infrastructure and network architecture to limit or remove adversary access to critical systems, and make sure you have offline backups in place to use if needed.

Survive attacks

By this stage, you've hopefully spent a long time prepping, building and testing defences, and now it's all about being ready to respond and providing continuity.

During the major event, national, international and social media coverage often parallels real-time activity. Having extensive intelligence on existing and emerging threat actor tactics, techniques and procedures enables you to have an effective and efficient incident response.

Effective incident and breach response extends beyond technical investigation, containment and recovery and includes executive communication and crisis management, such as legal, regulatory and public relations considerations. Doing this requires taking a potential adversary's view of the situation.

Preparing for an incident from only one side, without invoking real-world experience and known data on threats, solves only half the equation.

Following the major event, take time to detail successes, challenges and recommendations. We can always continue learning from similar events and try to share as much information as possible to avoid future similar circumstances.

The cybersecurity challenges we face today are often too big to tackle alone and the necessary cyber-defence operations maturity and capacity require significant, sustained focus and investment. These challenges become even more acute during major events. Protecting such events means having rapid and adaptable cyber-defences under unique duress and pressure.

A prepared and practiced cyber-strategy and playbook helps ensure a favourable outcome not just for the hosts, but all participants, spectators, and those watching on from around the world. □

Stuart McKenzie is EMEA SVP, Consulting at Mandiant.

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

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Sponsors and exhibitors

Darktrace | Strategic Sponsor

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a mission to free the world of cyber-disruption. Breakthrough innovations in our Cyber AI Research Centre in Cambridge, UK have resulted in over 100 patents filed and research published to contribute to the cybersecurity community. Rather than study attacks, our technology continuously learns and updates its knowledge of 'you' and applies that understanding to optimise your state of optimal cybersecurity. We are delivering the first ever Cyber AI Loop, fuelling a continuous end-to-end security capability that can autonomously spot and respond to novel in-progress threats within seconds. Darktrace employs over 2,000 people around the world and protects over 7,400 customers globally from advanced cyber-threats. Darktrace was named one of TIME magazine's 'Most Influential Companies' in 2021.

To learn more, visit https://darktrace.com

F5 | Strategic Sponsor

F5 (NASDAQ: FFIV) is a multi-cloud application security and delivery company that enables our customers – which include the world's largest enterprises, financial institutions, service providers, and governments – to bring extraordinary digital experiences to life.

F5 is a trademark, service mark, or tradename of F5, Inc., in the US and other countries. All other product and company names herein may be trademarks of their respective owners.

For more information, go to f5.com. You can also follow @F5 on Twitter or visit us on LinkedIn and Facebook for more information about F5, its partners, and technologies

GATEWATCHER | Strategic Sponsor

European leader in intrusion detection and advanced threat detection, GATEWATCHER has been protecting the critical networks of large- and medium-sized companies and public institutions since 2015.

Our vision is to offer a flexible (cloud, on-premise, hybrid), scalable, innovative, open to new technologies and artificial intelligence without disrupting the existing architecture. But also, to facilitate the operations of cybersecurity teams to allow them to be more efficient in prioritising their remediation actions.

Our solutions provide an immediate improvement to current cybersecurity issues and a response adapted to the new detection needs of organisations thanks to a 360° vision of cyber-threats. They combine machine learning algorithms with various network traffic analysis methods. They are designed to be scalable and immediately operational for easy integration into SOCs.

For more information, please visit www.gatewatcher.com

KnowBe4 | Strategic Sponsor

KnowBe4 is the world's largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering.

The KnowBe4 platform is user-friendly and intuitive. It was built to scale for busy IT pros that have 16 other fires to put out. Our goal was to design the most powerful, yet easy-to-use platform available.

Customers of all sizes can get the KnowBe4 platform deployed into production twice as fast as our competitors. Our Customer Success team gets you going in no time, without the need for consulting hours.

For more information, please visit www.knowbe4.com

Mandiant | Strategic Sponsor

Since 2004, Mandiant has been a trusted partner to security-conscious organisations. Effective security is based on the right combination of expertise, intelligence, and adaptive technology, and the Mandiant Advantage SaaS platform scales decades of frontline experience and industry-leading threat intelligence to deliver a range of dynamic cyber-defence solutions. Mandiant's approach helps organisations develop more effective and efficient cybersecurity programmes and instills confidence in their readiness to defend against and respond to cyber-threats.

For more information, please visit www.mandiant.com

Recorded Future | Strategic Sponsor

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

Learn more at recordedfuture.com

SentinelOne | Strategic Sponsor

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

For more information, please visit www.sentinelone.com

Cofense | Education Seminar Sponsor

Millions of ransomware, business email compromise and credential harvesting attacks bypass expensive email security solutions every year. They are in your users' inboxes right now.

Cofense is the only company that combines a global network of 30 million people reporting phish with advanced AI-based automation to stop phishing attacks fast. That's why over half of the Fortune 500 trust us.

We're Cofense. We Stop Phish.

Our Phishing Detection and Response platform catches the phishing emails that your secure email gateway inevitably misses. We deliver the technology and insight needed to detect, analyse, and stop phishing attacks.

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organisations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of nearly 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organisations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defence, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise.

For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn

CounterCraft | Education Seminar Sponsor

CounterCraft is the next generation of threat intelligence. The CounterCraft Cyber Deception Platform offers active defence powered by high-interaction deception technology. CounterCraft detects threats early, collects personalised, actionable intelligence, and enables organisations to defend their valuable data in real time. The award-winning solution, fully integrated with MITRE ATT&CK®, fits seamlessly into existing security strategies and uses powerful automation features to reduce operator workload.

Founded in 2015, CounterCraft is present in London, New York, and Madrid, with R&D in San Sebastian, Spain. CounterCraft recently raised additional funding from venture capital firms including cybersecurity-specific funds Adara Ventures, eCAPITAL, In-Q-Tel and Evolution Equity, bringing the total investment to date to $10 million.

Learn more at www.countercraftsec.com

CrowdStrike | Education Seminar Sponsor

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

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

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

Learn more at www.crowdstrike.com

Menlo Security | Education Seminar Sponsor

Menlo Security protects organisations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Our cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions.

For more information, please visit www.menlosecurity.com

Seclore | Education Seminar Sponsor

Seclore offers the market's first fully browser-based Data-Centric Security Platform, which gives organisations the agility to utilise best-of-breed DLP, CASB, and Classification solutions in concert with our flagship Rights Management solution to discover, identify, protect, and audit the usage of data wherever it goes, both within and outside of the organisation's boundaries. The ability to automate the data-centric security process enables organisations to fully protect information with minimal friction and cost. Over 2,000 companies in 29 countries are using Seclore to achieve their data security, governance, and compliance objectives.

Find out more at www.seclore.com

Synack | Education Seminar Sponsor

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

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

eb-Qual | Networking Sponsor

eb-Qual SA is specialised in ICT security and network services in the public and private sector in Switzerland. Founded in 2002, eb-Qual SA specialises in consulting, planning and implementation of sophisticated IT security network solutions. The company, which is based in Givisiez/FR and Kloten/ZH, employs qualified and experienced professionals and rigorously selects high-quality and globally recognised products and solutions. eb-Qual's customers include medium to large companies as well as multinationals. eb-Qual SA is one of the leading specialists in the field of IT and network security in Switzerland.

For more information, please visit www.eb-qual.ch

Exclusive Networks | Networking Sponsor

Die Exclusive Networks Group verbindet neue und wachsende globale Technologie-Anbieter für den paneuropäischen Markt durch ihr Modell des „Super Value Add Distributors". Das Unternehmen ist spezialisiert auf Sicherheits-, Netzwerk-, Infrastruktur- und Storage-Lösungen für das 'Smarter Social Enterprise'. Bekannt als Early Adopter und Technikexperten vertreiben wir Produkte führender und aufstrebender Hersteller aus Europa, USA und Fernost ausschließlich über den indirekten Kanal.

Mit unserer integrierten Lösungsplattform CARM (Cyber Attack Remediation and Mitigation) befinden wir uns an vorderster Front der 'Post-Breach'-Security, also einer nach entstandenen Lücken einsetzenden Sicherheit. Diese einzigartige Plattform bringt Anbietertechnologien nahtlos in einer umfassenden, vollständig nachweisbaren End-to-End-Lösung zusammen und ermöglicht so Unternehmen, die Auswirkungen von Sicherheitslücken zu identifizieren, einzudämmen, auf sie zu reagieren, sie zu beseitigen und einzuschränken.

Die Frage ist nicht 'ob', sondern 'wann' eine Lücke entsteht. Und wenn sie entsteht, müssen Sie die richtigen Anbieter für integrierte Sicherheit zur Hand haben, die entsprechend agieren können – Zeitpunkt und Ort der Lücke identifizieren und entscheiden, was als nächstes getan werden soll. Die Cyber Attack Remediation & Response Plattform (kurz CARM) von Exclusive Networks sorgt dafür, dass Sie vorbereitet sind, wenn das Unvermeidbare geschieht!

Fuer weitere Informationen, besuchen Sie uns auf: www.exclusive-networks.com

Forescout Technologies | Networking Sponsor

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

Learn how at www.forescout.com

RangeForce | Networking Sponsor

RangeForce develops the world's most comprehensive cybersecurity training and cyber-skills assessment programme. RangeForce believes in the power of skilling up SOC and cybersecurity professionals through advanced cyber-defence training, combining this with the ability to accurately and quantitatively assess your team's genuine preparedness to combat real cyber-attacks. Every day, hackers invent new creative techniques, with regulators administering increasingly significant fines. Using our Battle Skills individual training platform in combination with the Battle Fortress team event cyber range, we help companies mitigate their cybersecurity risk and boost the effectiveness and efficiency of their security operations. Our advanced threat training covers the very latest attack and defence techniques, all delivered through a browser and on real infrastructure. No prep, no set-up, no testing, no kit, no downtime, no hassle. All you have to do is log in, learn, assess and transform – for a fraction of the cost of traditional learning.

For more information, please visit www.rangeforce.com

ReliaQuest | Networking Sponsor

ReliaQuest, a global leader in cybersecurity, helps organisations achieve consistent security outcomes. ReliaQuest GreyMatter is a SaaS-based, unified threat detection, investigation and response platform aimed at reducing security complexity. Enhanced threat detection speeds response by force multiplying teams with curated integration and automation applied across the security operations process. Hundreds of security leaders trust ReliaQuest to deliver Open XDR outcomes – driving greater efficacy, efficiency and resilience, giving them the confidence to proactively advise on and manage risk for the business. ReliaQuest is a private company headquartered in Tampa, Fla., with five global locations.

For more information, visit www.reliaquest.com

AGENDA

08:00 Registration & networking

08:50 Chairperson's welcome

09:00 **Securing the digital citizen: A public sector view**

Philipp Grabher, Chief Information Security Officer, Canton of Zurich
- Cybersecurity strategy for the Canton of Zurich
- Supporting and inter-sector cooperation: raising awareness
- The big three areas – what to focus on

09:20 **The 2022 malware and vulnerability threat landscape**

Julian Kanitz, Lead Sales Engineer, DACH, Recorded Future

The presentation examines trends in Malware use, distribution, development and high-risk vulnerabilities disclosed by major hardware and software vendors in the first half of 2022. It will cover:
- An overview of the threat landscape of malware and vulnerabilities
- Top referenced malware variants associated with cyber-attacks
- Top vulnerabilities associated with cyber-attacks
- Tips on how to to strengthen your security posture and advisement for threat hunting teams and security operations centre teams
- Outlook for the rest of 2022 based on H1 2022 observations

09:40 **Debunking common myths about XDR**

Manuel Wolf, Security Expert, Alps, SentinelOne
- What is XDR and why should I consider the technology in my enterprise security stack?
- What should I expect from vendors who claim to have built the perfect mousetrap?
- What is reality, and what is just hype?
- This session is intended to debunk a few common myths that continue to muddy the water for security teams

10:00 **The vulnerability vector: An opportunity for the hacker and a challenge for the CISO**

Juan Carlos López Ruggiero, CISO, Bouygues Energies & Services
- Malicious actors are so much better organised (and financed) than company CISOs
- How do we survive the threats and stay one step ahead?
- What works and what doesn't when facing the challenges in an ever changing scenario?

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

Seclore Technologies
Data-centric security for data protection | Every digital asset | Everywhere
Jasbir Singh, Partner and Managing Director Europe, Seclore Technologies

Synack
Staying secure in the midst of the talent crisis
Wade Lance, Field CISO, Synack

11:00 Networking break

11:30 **EXECUTIVE PANEL DISCUSSION** **Balancing regulation/compliance and security**

Tom Schmidt, Partner, EY (Moderator); **Aneta Podsiadla,** Data Protection & Compliance Officer, Vorwerk; **Juan Carlos Lopez Ruggiero,** Chief Information Security Officer, Bouygues Energies & Services; **Ralf Winzer,** Group Information Security Officer/ Group Data Protection Officer, Zehnder Group International AG; **Olivier Busolini,** CISO, Sygnum Bank; **Dr. Dominik Raub,** Chief Information Security Officer, Crypto Finance AG
- How do new resilience regulations help in the battle against cybercriminals (NIS2 and DORA) and the impacts of the coming complete revamp of the FINMA 2008/21 circular for Swiss banks?
- Does cybersecurity fit naturally into the three lines of defence model?
- Third-party dependency

11:50 **Distributed cloud services: Uniform security controls for distributed infrastructures**

Andrea Arquint, Senior Solutions Engineer, F5 Switzerland GmbH
- Distributed cloud –> the infrastructure should become completely transparent, allowing customers to move seamlessly between environments
- An overlay that helps improve the quality of each individual cloud, with a single, central system that interconnects them all
- Spend less time fiddling with infrastructure
- Release new applications faster
- Reduce annual expenses
- Do not limit the ability of innovators to use best-of-breed services

12:10 How AI can think like an attacker

Marcel Gill, Account Director and **Marcel Wuestner,** Account Director, Darktrace

- In the face of skyrocketing cyber-risk, detecting and responding to attacks is no longer enough
- Organisations must take proactive steps to prevent threats before they happen, and to recover if compromised
- Darktrace unveils an ambitious new approach to security, with core engines powering AI technologies to prevent, detect, respond, and ultimately heal from attacks
- Together, these engines combine to strengthen organisations' security posture in a virtuous AI feedback 'loop,' which provides powerful end-to-end, bespoke, and self-learning solutions unique to each organisation

12:30 It's more than phishing – how to supercharge your security awareness programme

Javvad Malik, Lead Security Awareness Advocate, KnowBe4

- Why you need to brand the security department the right way
- The psychological approach to getting your message across
- Practical advice on building a strong security culture

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

Cofense
Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for Swiss organisations
Alain Salesse, Senior Sales Engineer, Cofense

CounterCraft
Adversary driven threat intelligence: Understand how cyber-deception will help your organisation make intelligent business-driven decisions
Conrado Crespo, Senior Sales Engineer, CounterCraft

13:30 Lunch & networking break

14:30 The cloud security journey

Olivier Busolini, Chief Information Security Officer, Sygnum Bank

- The implicit choices of starting a cloud(s) journey
- The key cloud security risks to evaluate
- The most important security principles and measures when running workloads in cloud(s)
- The implications of the shared responsibility model of data protection

14:50 Activating cyber-threat intelligence

Albert Brauchli, Country Manager, Mandiant Switzerland

Mandiant responders are on the frontlines every day, investigating and analysing the latest attacks and threats, and understanding how best to respond to and mitigate them. Everything we learn is passed on to our customers through our various services, giving them a much needed advantage in a constantly evolving threat landscape.

- Mandiant identified trends
- Cyber-threat intelligence provides tactical, operational and strategic support
- Cyber-threat profile
- Defender's advantage

15:10 Getting out of the terminological confusion around security concepts: What is really new and relevant?

Achim Kraus, Technical Solution Architect, GATEWATCHER

- Security operations: Latest terminologies (SIEM, SOAR, NDR; EDR, XDR, MDR...) – so what ?
- Zero Trust & attack surface: 'Threat hunting' – way before detection
- Team efficiency will come from integration of data and automation
- Where to start: Levels of maturity and deployment

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

CrowdStrike
Understanding the true threats to identity against the modern threat actor
Florian Hartmann, Senior Sales Engineer, CrowdStrike

Menlo Security
The next class of browser-based attacks
Brett Raybould, EMEA Solutions Architect, Menlo Security

16:10 Networking break

16:30 Securing client assets – in the context of escalating cyber-threat

Dr. Dominik Raub, Chief Information Security Officer, Crypto Finance AG

- Blockchain vs classical assets from a cyber-threat exposure perspective
- Information security threat landscape and securing client assets as central protection goals for a blockchain asset company
- Using secure hardware and sound security architecture to mitigate risks and secure client assets
- Residual risks to client assets and further recommended defences

16:50 SENIOR LEADERSHIP PANEL What's on the horison?

Simon Brady, Managing Editor, AKJ Associates (Moderator); **Philippe Vuilleumier,** Chief Security Officer, Swisscom; **Captain Patrick Ghion,** Head Regional Cyber Competence Center for Western Switzerland (RC3); **Klaus Haller,** Senior Security Architect, AXA; **Michele Federici,** Head of IT Security, Dialetic AG

- What's on the horizon, and how to we ensure security in a complex ecosystem?
- How do we ensure customer trust and strive to make society more cyber-immune?
- How do we protect artificial intelligence in the future?
- How do we cope with the fact that computing power will put our current encryption mechanisms at risk, etc.?

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

Seclore Technologies

SESSION 1
10:20–11:00

Data-Centric security for data protection | Every digital asset | Everywhere

Jasbir Singh, Partner and Managing Director Europe, Seclore Technologies

IT environments digital borders have shifted significantly over the last years. WFH, BYOD, Cloud, collaboration plus evolving hacker tactics and new compliance regulations are causing a lot of pressure on organisations. What should the boundaries of your IT environment look like today, with evolving technology and remote workforces?

Jasbir Singh will discuss the challenges of traditional security solutions in a world of disappearing borders and how data-centric-security can address these challenges in a centralised and transparent way.

We will explore:

- How to protect your organisation against insider threats
- How to ensure secure collaboration
- Mitigating third-party risk by protecting your data everywhere
- Data-centric security as a cornerstone to staying compliant

Synack

SESSION 1
10:20–11:00

Staying secure in the midst of the talent crisis

Wade Lance, Field CISO, Synack

The worldwide cyber-talent shortage is real and growing. Just in the US there are 1 million people employed as cybersecurity professionals, but over 700,000 unfilled job postings and that number is growing at an alarming rate. Globally, the gap is at least 2.7 million. Initiatives are underway to address the shortage spanning government, industry groups, and the private sector, however the short-term cybersecurity implications are alarming. The lack of skilled practitioners extends beyond the issue of headcount – deficiencies exist in capability, diversity, morale and more. But effective and innovative solutions can bridge the talent gap and address both near term and longer term needs.

In this session, we will discuss:

- Current options to increase the cyber-talent capacity required to meet organisations' current and future security needs
- Broadening the diversity of available security skill sets to cover the full scope of vulnerabilities for on-premise, cloud, networking, hosts, mobile, applications, etc.
- The challenges, and importance, of establishing a continuous testing practice to keep pace with the continuous application development and deployment methodologies
- The advantages of leveraging a global researcher community as part of your security operations
- The importance of standard testing frameworks and operational transparency in leveraging untapped and available security talent

Session 2: 12:50–13:30

Cofense

SESSION 2
12:50–13:30

Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for Swiss organisations

Alain Salesse, Senior Sales Engineer, Cofense

- *What is an adaptive security architecture and what are the objectives?* – With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation. We'll walk you through the benefits and objectives of implementing an adaptive security architecture and risk framework.
- *The current situation in email and phishing security* – We'll share some of the latest insights from the industry and what we're seeing through

our unique combination of artificial, human, and high-fidelity intelligence.
- *Implementing adaptive security architecture and risk framework with Cofense* – We'll talk through how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity.

CounterCraft

SESSION 2
12:50–13:30

Adversary driven threat intelligence: Understand how cyber-deception will help your organisation make intelligent business-driven decisions

Conrado Crespo, Senior Sales Engineer, CounterCraft

Join this session to find out more on:

- Limited value in generic intelligence: why is the traditional threat intelligence broken?
- Can deception technology really provide actionable intelligence? How does it work?
- What are the risks involved in adopting this approach?
- Am I mature (from a security operations perspective) enough to leverage this approach?

Session 3: 15:30–16:10

CrowdStrike

SESSION 3
15:30–16:10

Understanding the true threats to identity against the modern threat actor

Florian Hartmann, Senior Sales Engineer, CrowdStrike

Modern adversaries no longer break in, they login. An attacker with compromised credentials has free reign to move about an organisation and carefully plan their attack before they strike.

In more than 80% of modern attacks, threat actors are using valid credentials. It's not zero days or phishing that should be your concern from attackers, it's that they already have the keys to your kingdom.

Join us to further understand:

- The history of identity and identity architecture
- The identity threat landscape
- Identity attack techniques by e-crime and nation-state actors
- Best practices for solving the identity problem

Menlo Security

SESSION 3
15:30–16:10

The next class of browser-based attacks

Brett Raybould, EMEA Solutions Architect, Menlo Security

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

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

In this session, you will:

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

Speakers and panellists

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

Andrea Arquint

Senior Solutions Engineer, F5 Switzerland GmbH

With over 20 years' experiences in IT, I am planning and building application delivery networks including security, high availability and modern architecture concepts for business solutions. I am significantly experienced within the areas of security, automation and risk management. My conceptual and analytic way of thinking helps me to abstract complex interrelationships to transport knowledge to the market/customers with my social competence. I love to get in contact with people/customers, talk about challenges and finding valuable solutions that fit their needs. My qualifications include a postgraduate master's degree in Information Security from Lucerne University of Applied Sciences and Arts. Prior to joining F5, I was building data centre IT infrastructures as a Network and Security Engineer for auction and university platforms.

Albert Brauchli

Country Manager, Mandiant Switzerland

At Mandiant, we are committed to providing our customers with a legitimate sense of security and control over their infrastructures at challenging times. We'll help you protect your crown jewels, but we'll also help you identify and get rid of the supposedly successful attackers. I myself have been in IT for over 30 years and have worked in IT security and cloud security for over 20 years. For the past two years, I'm Mandiant's representative in Switzerland.

Olivier Busolini

Chief Information Security Officer, Sygnum

Olivier Busolini has been involved in IT security for 25 years, in the private and public sectors, across several industries in France, the UK and Switzerland. He experienced different business dynamics, and developed leadership in IT risk, (cyber)security, privacy and resilience management, as an integrated part of operational risks, data governance and digital business activities. He has been holding CISO roles for Swiss banks for the last 13 years. He focuses on managing technology risks and security from a business risk perspective, to deliver cost-efficient risk assurance.

Michele Federici

Head of IT Security, Dialetic AG

Michele Federici is a long-time tech enthusiast and programmer. Over the years, he focused primarily on the security aspects of IT, developing a recognised expertise in design and review of security-critical code and systems such as digital assets and blockchain projects, secure key ceremonies and custody solutions, wallet software and payment gateways. He is currently Head of IT Security at Dialectic, a futuristic family office focusing on cutting edge portfolios. Previously, he led SEBA Bank's blockchain team and helped in designing the bank's custody infrastructure from scratch. He is also an independent advisor and active in several communities and software projects.

Captain Patrick Ghion

Head Department of Forensic Sciences at Geneva State Police, Head Regional Cyber Competence Centre for Western Switzerland (RC3), Deputy Director Swiss Network for Police Cyber coordination (NEDIK)

Attached to the Geneva Criminal Police, the Department of Forensic Sciences is made up of six Divisions, which are Homicide, Crime Scene Investigation (CSI), Criminal Intelligence, Cyber Investigations, Computer Crime and Evidence Management. After working five years in a couple of Swiss banks, he spent some time in Asia as a diving instructor before joining the Criminal Police in 1997. His hobbies include scuba diving and aviation.

Marcel Gill

Account Director, Darktrace

Philipp Grabher

CISO,
Canton Zurich

Philipp Grabher is the Chief Information Security Officer (CISO) of the Canton Zurich and is responsible for its cybersecurity strategy. Further tasks include ensuring an adequate cybersecurity resilience in the cantonal administration, planning and carrying out security assessments and audits, raising awareness and developing the necessary security policies. He holds a PhD in Information Security from Bristol University, UK.

Klaus Haller

Senior Security Architect,
AXA

Klaus works as a Senior Security Architect at AXA in Switzerland with a focus on cloud and information security. Additional areas of expertise are project management, organising IT operations, and data management and AI. Recently, he published a book on organising AI departments titled 'Managing AI in the Enterprise'.

Florian Hartmann

Senior Sales Engineer,
CrowdStrike

Florian Hartmann joined CrowdStrike as a Senior Sales Engineer supporting Southern Germany and Switzerland. For more than 20 years he worked closely with international companies and their global IT Security and Network teams building considerable expertise in network, network security and cloud security. Prior to CrowdStrike, he worked for A10 Networks, Zscaler and Forescout.

Julian Kanitz

Lead Sales Engineer,
Recorded Future

Julian Kanitz is Lead Sales Engineer at Recorded Future supporting the DACH region. He holds a Master of Science in Industrial Engineering and served 12 years in the German Military. He has been evangelising threat intelligence for various enterprise security programmes for the past three years.

Achim Kraus

Technical Solution Architect,
GATEWATCHER

Over the past 30 years, Achim has been essential in introducing, deploying and operating high-tech solutions in the cybersecurity space for end customers working across Europe. He was fortunate to work for companies including IronPort Systems and Palo Alto Networks who changed markets at their time.

Wade Lance

Field CISO,
Synack

Wade Lance is Field CISO at Synack. Wade has been productising new technologies in cybersecurity, education and healthcare for over 20 years. He has diverse experience in security solution design for global 1000 organisations, and a passion for mentoring and developing cybersecurity leaders. Prior to his career in information technology, Wade was a professional mountain guide, and developed a new method for technical rock and ice climbing instruction that is still used to teach advanced skills for the most dangerous environments.

Juan Carlos Lopez Ruggiero

Chief Information Security Officer,
Bouygues Energies & Services

Juan Carlos is a results-driven CISO with 20+ years of experience in managing all facets of information security management, cybersecurity, risk management, regulatory compliance, and quality assurance.

He is an executive with a proven track record of establishing and implementing information security strategies, identifying potential risk factors, and delivering robust strategic action plans to senior leadership.

He has demonstrated excellence in implementing strategic security initiatives, supporting evaluation, deployment, and management of current and future security technologies. He has a strong international and multicultural background, having lived and worked in North/South America, Europe, Africa and the Middle East.

Conrado Crespo

Senior Sales Engineer,
CounterCraft

Javvad Malik

Lead Security Awareness Advocate,
KnowBe4

Javvad Malik is Lead Security Awareness Advocate at KnowBe4 and is based in London. Malik is an IT

security professional with over 20 years of experience as an IT security administrator, consultant, industry analyst and security officer. He is also a multiple award winner and currently holds the Guinness World Record for the most views of a cybersecurity lesson on YouTube within 24 hours.

Malik is passionate about helping people understand the value of cybersecurity and how each department and individual can play their part. He frequently educates his audience through blog posts, videos, podcasts, and at public events. Malik holds SACP and CISSP certification.

Aneta Podsiadla

Data Protection & Compliance Officer, Vorwerk International & Co

Aneta Podsiadla is the Data Protection & Compliance Officer for Vorwerk International & Co. KmG. Aneta has overall 14 years of multi-sectoral and cross-jurisdictional experience in data protection, information security and IT law. She is skilled in building and maintaining data protection & compliance programmes, establishing strategies for effective data management and compliance, and supporting organisations in various business and IT transformations. She is a frequent speaker at international conferences (ISACA EuroCACS; IAPP European Data Protection Congress; TrendMicro CloudSec; Cloud Computing Summit, Brand Protection Excellence Forum). In 2012, she was awarded an advanced research scholarship from the Fulbright U.S. Scholar Program at the John Marshall Law School in Chicago, where she worked on the topic of products liability and AI & robotics. Last but not least, she is the former expert for the European Commission's Policy Expert Groups: Cloud Computing, Internet of Things, ENISA's European Private-Public Partnership for Resilience and EuroPriSe (European Privacy Seal) certification body for IT products and IT based services.

Dr. Dominik Raub

Chief Information Security Officer, Crypto Finance AG

Dr. Dominik Raub is a seasoned information security professional with over 10 years of experience in the financial industry. He is currently serving as Chief Information Security Officer (CISO) for Crypto Finance AG in Zurich. Crypto Finance AG is part of Deutsche Börse Group and a licensed broker and asset manager dealing in blockchain assets that prides itself on its high security custody and crypto asset storage solution. As a security professional Dr. Raub takes a 'can do' approach, enabling the business by striking a healthy, risk-based balance between cost, security, and usability. Dr. Raub holds a PhD in Information Security and Cryptography from ETH Zurich, and his professional experience includes security architecture and operational risk and security roles at UBS AG and Cembra AG in Zurich and Singapore. From researching and authoring biannual global reports on cybercrime for UBS AG, Dr. Raub has gained detailed insight into global cybercriminal threats to the financial industry. He passes on his experience as speaker and as an instructor for the Swiss Federal Diploma Cyber Security Specialist. In his free time, he enjoys hiking, travel, and martial arts.

Brett Raybould

EMEA Solutions Architect, Menlo Security

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

Alain Salesse

Senior Sales Engineer, Cofense

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

Tom Schmidt

Partner, EY

Tom Schmidt has more than 30 years' experience in information technology and more than 20 years of practical information security/cybersecurity and cyber-risk management experience. He has extensive experience in leading and providing cybersecurity assessments, cybersecurity consulting projects,

cloud risk and cloud security projects, IT security audits, IT and Cyber-risk management projects, third party risk management (TPRM) and general IT audit and consulting services for national and international clients in the financial services and industry sectors. In addition, Tom is a member of the technical board and lecturer at the MAS Cyber Security, University of Applied Science, Lucerne.

Jasbir Singh

Partner and Managing Director Europe, Seclore Technologies

Jasbir Singh is Partner and Managing Director of Seclore Europe, the international leader in rights management. Jasbir brings Seclore over 30 years of international business and security technology expertise. A recognised computer and IT expert, he holds patents in identity security solutions and has founded and grown numerous successful, European-based IT companies. Examples include firms in single-sign-on, digital content management, computer-aided design and systems management technology sectors. After a successful career spanning 25 years of building and running IT tech companies, Jasbir then spent roughly five years as a strategic advisor and investor in high-growth ventures in Germany, Switzerland, the United Kingdom and United States. Since 2018, he leads Seclore's sales and operations for the Europe region and is part of the executive management team setting overall company go-to-market and product strategy.

Philippe Vuilleumier

Chief Security Officer, Swisscom

Philippe Vuilleumier has worked at Swisscom for more than 15 years and assumed overall responsibility for Swisscom Security as Head of Group Security in September 2015. He was Head of Network & IT Operations at Swisscom Switzerland from 2008, before being appointed CEO of subsidiary Alphapay in 2013. His qualifications include a master's degree in Business Telecommunications from Delft University of Technology. Prior to joining Swisscom, Philippe Vuilleumier held various management positions at Zurich Insurance Group, Equant and IBM. Philippe is currently on the Board of Directors of Electrosuisse, participates actively in several organisations related to physical and cybersecurity and served as President of the Board of Directors of SEC Consult Switzerland AG.

Ralf Winzer

Group Information Security Officer/ Group Data Protection Officer, Zehnder Group International AG

Ralf Winzer is responsible for information security and data protection at group level at Zehnder Group. He has many years of experience in information security, risk management and data protection. He has worked for several companies as CISO as well as in security advisory and IT audit, especially with Ernst & Young. He is interested in the more and more challenging interaction between governance, risk management and compliance in the context of security and data protection.

Manuel Wolf

Security Expert, Alps, SentinelOne

Marcel Wuestner

Account Director, Darktrace

Marcel Zumbühl

Chief Information Security Officer, Swiss Post

Marcel Zumbühl works for Swiss Post as Chief Information Security Officer (CISO) and member of the IT Board since 2018. He is responsible for the information security of the Swiss Post Group. He was also recently appointed to the Board of Directors of Hacknowledge, a cybersecurity affiliate of Swiss Post Group. Marcel holds a master's degree in Computer Science with a minor in Business Administration. After studying at the University of Berne, he worked both in Switzerland and abroad for various companies such as Accenture, Swisscom and Credit Suisse. He lectures at ETH Zurich on risk management and risk communication and HSLU on CISO organisations. Since 2020, Marcel Zumbühl is Co-president of the Information Security Society Switzerland (ISSS). □

SentinelOne®

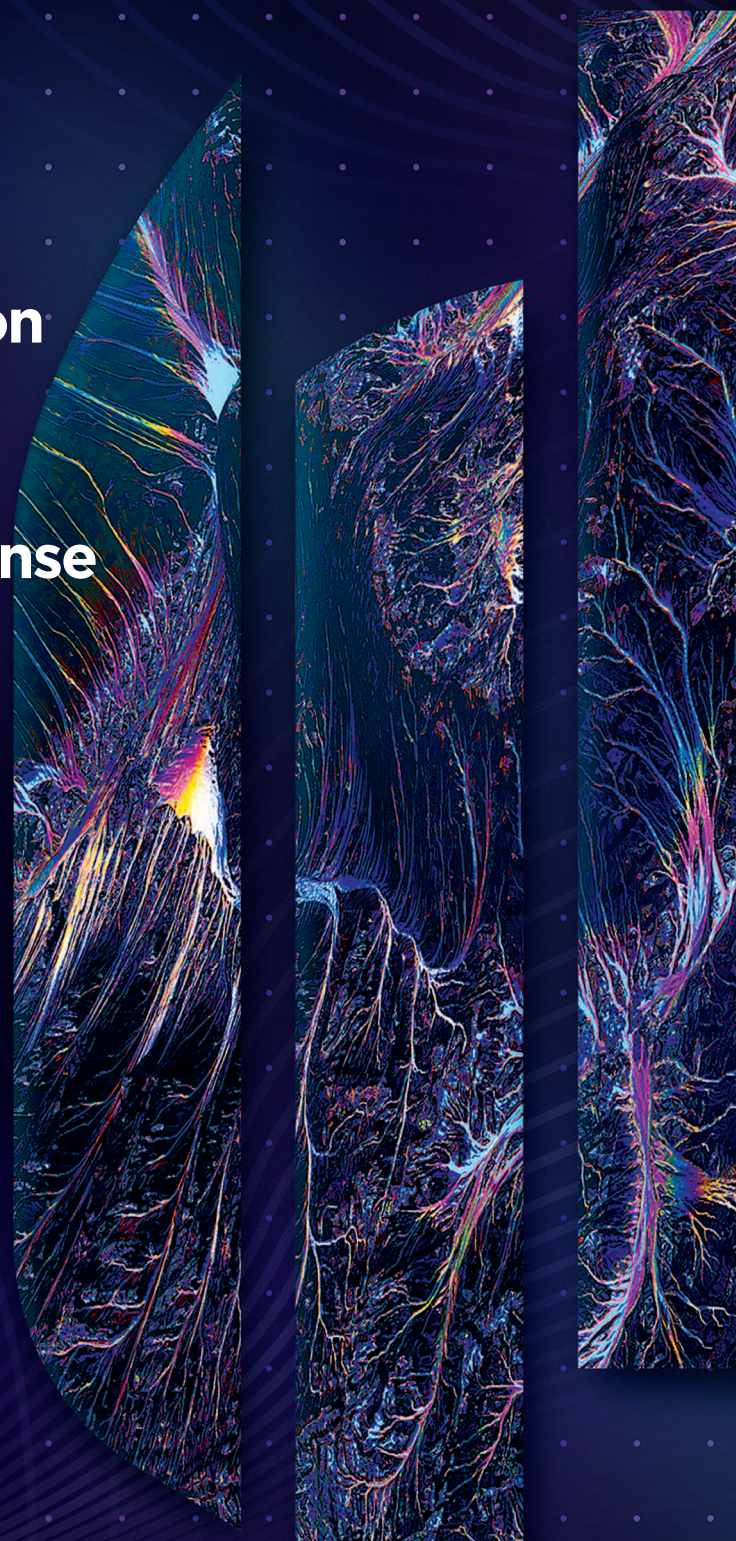
Smarter, stärker, schneller... autonom.

REAL TIME
Endpoint Protection

ACTIVE
Detection & Response

AUTONOME
Network Visibility & Control

NATIVE
Cloud Security



sentinelone.com

Mensch und Maschine in der Cybersicherheit: Partner oder Gegner?

Viele Organisationen und deren Sicherheitszuständige haben inzwischen verstanden, dass sie sich dringend auf den Fall einer auf sie gerichteten Cyberattacke vorbereiten und entsprechende Schutzmaßnahmen entwickeln müssen, da es nur eine Frage der Zeit ist, bis es soweit ist.

SentinelOne berichtet

Wir leben im Zeitalter zunehmender Kriminalität im Cyberraum. Es vergeht kaum ein Tag, an dem nicht das Auftauchen einer gefährlichen Sicherheitslücke, ein neuartiger und hochentwickelter Ransomware-Angriff oder eine großangelegte Cyberattacke auf Unternehmen, Organisationen und Staatskörper zu verzeichnen ist. Das Phänomen der ansteigenden Zahl der Vorfälle zieht sich quer durch alle Industrien und Unternehmensgrößen. Über alle Branchen hinweg ist daher heutzutage ein klarer Wandel in der Denkweise der Sicherheitsexperten zu beobachten. Es geht nicht mehr darum, „ob" Hacker das eigene Unternehmen angreifen werden, sondern darum „wann" dies geschehen wird. Viele Organisationen und deren Sicherheitszuständige haben inzwischen verstanden, dass sie sich dringend auf den Fall einer auf sie gerichteten Cyberattacke vorbereiten und entsprechende Schutzmaßnahmen entwickeln müssen, da es nur eine Frage der Zeit ist, bis es soweit ist.

Den Angreifern einen Schritt voraus zu sein, ist allerdings ein zunehmend komplexes Unterfangen, da die Bedrohungsakteure ständig neue Angriffsvektoren nutzen. Von kleineren Ransomware-Gruppen bis hin zu ausgeklügelten Angriffen auf die Lieferkette wie bei dem SolarWinds-Vorfall oder der aktuellen und hochbrisanten Sicherheitslücke Log4Shell – die Gefahren, mit denen wir heute konfrontiert sind, sind nicht mehr mit denen früherer Tage zu vergleichen. Angriffe können aus einer komplexen Reihe von Aktionen bestehen, bei denen die Infektion nur der erste Schritt von vielen ist, was die Bemühungen der Sicherheitsteams bei der Erkennung und Reaktion erschwert.

Einer der wesentlichen Faktoren, der es den Cyberkriminellen ermöglicht, immer gefährlichere Malware in Systeme einzuschleusen und immer effektiver zu agieren ist der Einsatz von KI (Künstliche Intelligenz). Die Technologie entwickelt sich stetig weiter, doch selbstverständlich nicht nur bei den Bösewichten, sondern auch bei den Sicherheitsexperten. Beide Parteien befinden sich in einem dauerhaften Wettrüsten, denn für beide geht es um nichts Geringeres als das (finanzielle) Überleben.

Einer der wesentlichen Faktoren, der es den Cyberkriminellen ermöglicht, immer gefährlichere Malware in Systeme einzuschleusen und immer effektiver zu agieren ist der Einsatz von KI (Künstliche Intelligenz).

Unter diesem Gesichtspunkt stellt sich die Frage nach der Stellung von KI und Automatisierung in der Security: Welche Chancen bietet uns moderne Technologie? Wie ist es um die Rolle des Menschen in der Cybersicherheit bestellt? Was ist der Wert von KI und wird sie uns bald ablösen? Der Schlüssel zur Beantwortung dieser Fragen liegt im Diskurs rund um die Themen Mensch und Maschine – und der komplexen und wechselseitigen Beziehung dieser zwei grundverschiedenen Entitäten.

Die Maschine ermöglicht das Erstellen und Nachvollziehen von Kontext

Kommt es zu einem Angriff auf ein Unternehmen, gibt es eine ganze Reihe an Fragen, die beantwortet werden müssen, um zu verstehen, um welche Art von Bedrohung es sich handelt. Es gibt auch viele Fragen dazu, wie man sich nun am besten verhält, um der Gefahr bestmöglich zu begegnen und den Schaden zu minimieren. Einige der Fragen, die sich stellen könnten lauten: „Wie ist der Angriff erfolgt?", „War er erfolgreich, und wenn ja, warum?", „Wer oder was trägt die Schuld daran, dass das System kompromittiert wurde?" und „Wie können die Auswirkungen behoben werden?".

Derartige Fragen sind von enormer Wichtigkeit, denn sie zu stellen ist unabdingbar, um ein Verständnis dafür zu entwickeln, wie ernst die Situation ist, womit genau es die Sicherheitsexperten zu tun haben und welche Maßnahmen wie eingeleitet werden sollen. Die Antworten auf diese Fragen liegen vor allem in der Analyse gesammelter Informationen im Netzwerk. Der Vorfall muss also untersucht werden, und zwar in der Regel ausgehend vom Endpunkt, den die Cyberkriminellen als Einfallstor genutzt haben, um Zugang zum Netzwerk zu erhalten. Mithilfe von EDR-Tools (Endpoint Detection Response) wird dann versucht, auf Basis von Vorfallsdaten eine isolierte Aktivität mit weiteren Punkten im System zu verknüpfen, bis sich ein klareres Bild des Vorfalls als Ganzes herauskristallisiert und festgestellt werden kann, wie weitreichend der Verstoß ist.

Auch wenn es in der IT-Sicherheit kein Patentrezept gibt, ermöglicht der Einsatz von moderner Technologie und KI den Unternehmen, im Wettrüsten der Cybersicherheit endlich die Nase vorn zu haben.

Das Lösen des Rätsels und das Verstehen der Zusammenhänge in einer Flut von Unternehmensdaten ist jedoch eine Aufgabe, die für einen menschengesteuerten Ansatz zu mühsam ist. Die überwältigende Menge an Daten über eine Vielzahl von Endpunkten bedarf mehr Rechenleistung für eine ausreichend detaillierte Analyse, als es einem einzelnen (oder sogar einer Vielzahl von) Menschen möglich wäre, aufzubringen. Zudem sind die Sicherheitsteams zumeist bereits mit einer Fülle anderer Aufgaben überlastet, so dass ihnen gar nicht erst die Zeit bleibt, Vorfälle und Bedrohungen eingehend zu untersuchen. Der einzige Weg der Situation Herr zu werden: Der Einsatz intelligenter Technologie, die die menschlichen Experten bei ihrer Arbeit unterstützt.

Automatisieren dessen, was für den Menschen zu aufwändig ist

Es ist offensichtlich, dass eine manuelle Alarmtriage heutzutage nicht mehr ausreichend ist. Vollkommen unmöglich und fehlgeleitet wäre der Versuch, jeden Endpunkt manuell zu überwachen, zu groß sind das Ausmaß und die Raffinesse der Angriffe, um sich auf einen rein menschengesteuerten Ansatz zu verlassen. Stattdessen ist die Kontextualisierung aller Datenpunkte zu einem einzigen Handlungsstrang der beste Weg, um eine umfassende Verteidigung gegen moderne Cyberattacken zu ermöglichen. Diese Aufgabe übernehmen intelligente Technologien, die in der Lage sind, einen komplexen Angriff, der möglicherweise über eine Vielzahl von Vektoren erfolgt, zu analysieren und eine adäquate Reaktion einzuleiten. Durch den Einsatz von KI und Automatisierung kann so das gesamte Spektrum an Bedrohungen aus verschiedenen Angriffsvektoren in Echtzeit erkannt und neutralisiert werden.

Wettrüsten im Cyberraum: Auf die Technologie kommt es an

Bedrohungsakteure nutzen die neuesten Innovationen in Technik und Technologie, um ihre Angriffe stets weiterzuentwickeln und noch gefährlicher zu machen. Cybersicherheitsteams in Unternehmen müssen dasselbe tun und Feuer mit Feuer bekämpfen. Nur durch den Einsatz möglichst leistungsfähiger Technologien können sie darauf vertrauen, den Angreifern einen Schritt voraus zu sein und Attacken proaktiv zu verhindern. Da der Angriff auf ein Unternehmen innerhalb von Sekunden erfolgen kann, muss auch die Erkennung und Abwehr mit dieser Geschwindigkeit mithalten können. Durch den Einsatz von KI können Unternehmen Angriffe in Echtzeit erkennen, darauf reagieren und wiederherstellende Maßnahmen einleiten.

Bei der Modellierung von Bedrohungen in Echtzeit, der Korrelation von Vorfällen und der Analyse von Taktiken, Techniken und Verfahren (TTP) liefert KI angereicherte Informationen über den Kontext einer Attacke. Es können benutzerdefinierte Erkennungsregeln geschrieben werden, die sich mit neuen oder gezielten Bedrohungen befassen, z. B. mit solchen, die für bestimmte Branchen oder Unternehmen spezifisch sind, so dass sofort eine angemessene Reaktion erfolgt und den menschlichen Sicherheitsexperten dennoch die vollständige Kontrolle über den Prozess erhalten bleibt, sollten sie selbst eingreifen müssen.

Proaktivität bei der Verteidigung

Durch den Einsatz von KI und Automatisierung wechselt die Cybersicherheit von einer rein reaktiven Maßnahme hin zu einer proaktiven. Bedrohungen können automatisch erkannt und unerwünschte Prozesse blockiert werden. Darüber hinaus wird ein Endpunkt vom Netzwerk getrennt und sogar ein selektives Rollback des Systems auf einen Punkt vor dem Vorfall durchgeführt. Auf diese Weise hilft die Maschine dem Menschen - z. B. in Form eines SOC-Analysten - dabei Angriffe zu verhindern, bevor sie auftreten können, und die Auswirkungen eines erfolgreichen Einbruchs zu beheben.

Auch wenn es in der IT-Sicherheit kein Patentrezept gibt, ermöglicht der Einsatz von moderner Technologie und KI den Unternehmen, im Wettrüsten der Cybersicherheit endlich die Nase vorn zu haben. Ein menschlicher Analyst benötigt jahrelange Erfahrung und Ausbildung, um die notwendigen Fähigkeiten zur Erkennung und Isolierung von Bedrohungen zu entwickeln. Die Maschine soll den Menschen nicht in allen Aspekten ersetzen, sie soll ihn vielmehr bei seiner Arbeit unterstützen und es ihm ermöglichen, sich auf die wirklich wichtigen Arbeiten zu konzentrieren. Diese Symbiose ist das eigentliche Ziel der Technologie, denn sie ist der Schlüssel zu einem optimalen und ergebnisorientierten Ansatz in der Cybersicherheit. □

Distributed Cloud Services: Einheitliche Sicherheitskontrollen für verteilte Infrastrukturen

Eine neue SaaS-basierte Plattform vereinfacht das Security Management für sämtliche Anwendungen in allen Umgebungen.

Andrea Arquint/F5 berichtet

Die IT-Komplexität steigt, denn Unternehmen nutzen zunehmend sowohl herkömmliche als auch moderne Anwendungen in Multi-Cloud-Implementierungen. So zeigt der State of Application Strategy Report 2022 von F5, dass 88 Prozent der Befragten sowohl monolithische als auch Microservices-basierte Anwendungsarchitekturen betreiben. Zudem verwenden 70 Prozent mehrere Clouds.

Eine wachsende Komplexität erhöht jedoch die Gefahr für Sicherheitslücken. Denn Unternehmen müssen getrennte und oft inkonsistente Security-Kontrollen in verschiedenen Umgebungen einsetzen. Dabei sind Anwendungen und die damit bereitgestellten digitalen Angebote zu einer unverzichtbaren Grundlage für die menschliche Kommunikation und Arbeit sowie für geschäftliche Innovationen geworden.

Von on-Premises über Multi-Cloud bis zum Edge

Klar ist daher, dass Unternehmen ihre Anwendungen optimal absichern und hochverfügbar bereitstellen müssen. Doch neben traditionellen Applikationen in on-Premises Rechenzentren verwalten sie auch Services von verschiedenen Cloud-Providern. Hinzu kommen vermehrt neue IoT-basierte Lösungen am Edge.

Dabei erschwert der Fachkräftemangel vor allem im Bereich der IT-Security das Installieren und Betreiben geeigneter Sicherheitslösungen. Kein Wunder, dass sich manche Unternehmen überlegen, auf Innovationen und neue Technologien zu verzichten, weil sie nicht zu bewältigende Schwachstellen fürchten. Dies gilt gerade für Branchen mit sensiblen Daten wie Finanz- und Gesundheitswesen oder die öffentliche Hand.

Einheitliche Oberfläche

Aber das muss nicht sein. Denn inzwischen gibt es Lösungen, die eine zentrale Konsole zur Verwaltung von Anwendungen bietet. Dabei spielt es keine Rolle, ob die Applikation im eigenen Rechenzentrum, der Public Cloud oder am Edge läuft. Die End-User Experience ist über alle Lokationen hinweg immer identisch. Sicherheit und Verfügbarkeit der Anwendung lassen sich dabei zentral mit einem Mausklick gewährleisten.

Der Trick liegt in einer abstrahierten Sicherheit für die Applikationen. So lassen sich Telemetrie-Informationen auf einfache Weise weltweit über eine Oberfläche managen. Zudem ist ein umfassendes Reporting unabhängig vom Public Cloud Provider möglich. Entsprechend können Microservices- und Container-basierte Applikationen heute in AWS, morgen in Azure und übermorgen in GCP laufen – je nach aktuellen Anforderungen und Angeboten. Auch die Installationen on-Premises und am Edge lassen sich über das einheitliche Dashboard managen.

Verteilte Cloud-Dienste

Die Grundlage für diese Lösung bilden Distributed Cloud Services. Sie bieten Sicherheit, Multi-Cloud-Networking und Edge-basierte Funktionen auf einer einheitlichen Software-as-a-Service (SaaS)-Plattform. Die Cloud-nativen, SaaS-basierten Dienste für die Absicherung und Bereitstellung von Applikationen werden zentral verwaltet. Sie stehen jedoch überall dort zur Verfügung, wo die Anwendung benötigt wird.

Die F5 Distributed Cloud Services basieren auf einer Kombination aus der Plattform und den Diensten von Volterra sowie den branchenführenden Sicherheitsservices von F5 und Shape. Sie können nativ in Multi-Cloud-, Rechenzentrums- und Edge-Umgebungen eingesetzt werden. Die Lösung bietet End-to-End-Transparenz und Richtlinienkontrolle für alle Anwendungen in einem Dashboard. Zudem stellt sie ein integriertes globales privates Netzwerk in mehr als 20 grossen Metropolregionen bereit.

Schutz von Web-Anwendungen und APIs

Der erste neue Dienst im Rahmen der Distributed Cloud Services ist WAAP (Web Application and API Protection). Er umfasst mehrere Security-Funktionen verschiedener F5-Technologien, um das Sicherheitsmanagement zu vereinfachen und Prozesse zu automatisieren.

Das SaaS-basierte Angebot konsolidiert Funktionen von Web Application Firewall (WAF), Bot- und DDoS-Abwehr sowie API-Schutz durch Machine-Learning-basierte Auto-Discovery und Anomalie-Erkennung in einer einfach zu implementierenden Lösung. So können SecOps- und DevOps-Teams konsistente Sicherheitsrichtlinien durchsetzen, wo auch immer sie Applikationen bereitstellen, und Anwendungsteams sich auf die Bereitstellung von Funktionen konzentrieren. Die Distributed Cloud Services für Bot Defense, DDoS Mitigation, WAF und API Security stehen auch einzeln zur Verfügung.

Weitere Services

Neben WAAP sind weitere Distributed Cloud Services erhältlich. Multi-Cloud Transit ermöglicht Multi-Cloud Networking (MCN)-Funktionalität mit sicherer und hochperformanter Konnektivität zwischen Clouds und einer Netzwerk-Firewall. Load Balancer and Kubernetes Gateway bietet einen integrierten Load Balancer mit Kubernetes- und API-Gateways zur

einfachen Bereitstellung moderner Workloads und Microservices über verteilte Cluster, Standorte und Cloud-Anbieter hinweg.

Die Plattform verfügt ausserdem über Cloud-native Funktionen für Edge Computing, die als App Delivery Network (ADN) bekannt sind. Sie verbessern die User Experience durch die Verteilung von Anwendungen auf das globale F5-Netzwerk aus Edge Points of Presence (PoPs). Damit lassen sich die Latenzzeiten um mehr als 80 Prozent reduzieren.

Sicherheit zum Mieten

Distributed Cloud Services stehen dabei als Mietlösung bereit, die auf F5-Servern gehostet wird. Für besonders sensible Bereiche lassen sich die Dienste aber auch als White-Label-Lösung kaufen und on-Premises installieren, so dass die Plattform inhouse läuft.

Gerade Branchen mit hohen Sicherheitsanforderungen wie Behörden, die Vorschriften zur strengen Datenklassifizierung unterliegen, profitieren von dieser Variante. So setzen Kunden diese Lösung bereits erfolgreich in der Praxis ein. Sie erhalten damit die Vorteile einer umfassenden, zentral administrierbaren SaaS-Lösung wie in der Cloud und können durch lokales Hosting gleichzeitig strenge Vorgaben einhalten, etwa die DSGVO.

Schnell und einfach

Bei der Entwicklung und Bereitstellung von Anwendungen ist eine schnelle Markteinführung der Schlüssel zum Erfolg. Doch dabei muss eine hohe Sicherheit gewährleistet sein. Mit Distributed Cloud Services lassen sich Security-Funktionen sehr schnell in neue Anwendungen einbinden und überprüfen. Damit sind Container-basierte Applikationen frühzeitig und weitgehend automatisiert geschützt.

Gleichzeitig können Unternehmen ihre digitale Transformation beschleunigen. Traditionelle on-Premises installierte Anwendungen lassen sich schnell und einfach in die Public Cloud migrieren, um sie flexibel zu skalieren. Insbesondere bei Multi-Cloud-Ansätzen ist die Gewährleistung einer homogenen Sicherheitsarchitektur mit einheitlichen Regeln eine enorme Herausforderung. Da Distributed Cloud Services jedoch Anwendungen unabhängig von der darunter liegenden Plattform automatisch erkennen und in die übergreifende Security-Struktur integrieren, lässt sich die Migration auf einfache Weise erledigen.

Übersichtlicher Sicherheitsstatus

Zudem erhalten Unternehmen durch die zentrale, einheitliche Oberfläche einen umfassenden Überblick über ihren aktuellen Sicherheitsstatus. Eine automatisierte, Machine-Learning-basierte Erkennung vermeidet weitgehend False Positives und entdeckt neuartige Bedrohungen aufgrund von Anomalien.

Dies funktioniert auch im eigenen Rechenzentrum. Doch beim Hosting über dedizierte Data Center von F5 werden die Security Incident und Response Teams des Anbieters eingebunden. Diese unterstützen die Erkennung und Abwehr von Gefahren, indem sie die automatisierten Funktionen der Lösung mit aktuellen Informationen und Daten zur Bedrohungslage ergänzen.

Alles aus einer Hand

Da F5 sämtliche Software und Hardware für die Distributed Cloud Services selbst entwickelt und herstellt, erhalten Unternehmen inklusive Security Support alles aus einer Hand. Dabei können sie flexibel einzelne Module und Services nutzen, diese beliebig miteinander kombinieren, skalierbar erweitern und bei Bedarf mit zusätzlichen Services ergänzen. Die SaaS-Plattform lässt sich im eigenen Rechenzentrum oder Cloud-basiert oder hybrid in beiden Varianten gleichzeitig nutzen.

So erhalten Unternehmen maximale Flexibilität, um die Lösung massgeschneidert an ihre individuellen Anforderungen und Bedürfnisse anzupassen. Dabei profitieren sie von einem Security-Ansatz aus einem Guss, da keine Abhängigkeit von Drittanbietern oder weiteren Cloud-Providern besteht. Zudem handelt es sich um eine bewährte Lösung, die bereits europaweit bei mehr als 50 Kunden, teilweise in Hochsicherheitsbereichen, im Einsatz ist.

Zahlreiche Vorteile

Diese profitieren von zahlreichen Vorteilen: Dank eines integrierten Satzes von SaaS-basierten Diensten in jeder Umgebung verkürzen sie die Markteinführungszeit um das bis zu 12-Fache. Die mehrinstanzenfähige Plattform ohne Integration von Cloud-Providern oder Drittanbietern ermöglicht dabei eine Kostenersparnis von bis zu 70 Prozent.

Self-Service-Funktionen mit Aufgabentrennung erleichtern eine offene Zusammenarbeit zwischen Entwicklern, DevOps-, NetOps- und SecOps-Teams. Diese erhalten über ein gemeinsam genutztes Portal einen ganzheitlichen Überblick über die Sicherheit und Leistung von Anwendungen. Machine Learning reduziert Bedrohungen und setzt Security-Richtlinien in verteilten Umgebungen durch. Zudem können Anwendungen und Workloads näher am Nutzer bereitgestellt werden.

Fazit

Distributed Cloud Services bieten eine moderne SaaS-basierte Plattform, die mehrere Dienste über monolithische und Microservices-Anwendungen hinweg konsolidiert. Dies vereinfacht die Anwendungsverwaltung, Sicherheit und Netzwerkkonnektivität in einer verteilten Infrastruktur aus on-Premises, Multi-Cloud und Edge. Ausserdem erhalten Unternehmen mit einer einheitlichen End-User Experience erweiterte Security-Kontrollen, die deutlich über die nativen Dienste von Cloud-Anbietern hinausgehen. □

Andrea Arquint, Senior Solutions Engineer, F5.
Weitere Informationen unter **www.f5.com**

Protecting Your Web Apps and APIs Across Distributed Environments

Secure your web applications and APIs deployed across a multi-cloud and on-prem infrastructure with a comprehensive, easy-to-use SaaS security solution.

Testing early and often can reduce flaws in app development

Security needs to be much more than an afterthought.

Kirsten Gibson reports

Security is too often an afterthought in the software development process. It's easy to understand why: Application and software developers are tasked with getting rid of bugs and adding in new features in updates that must meet a grueling release schedule.

Asking to include security testing before an update is deployed can bring up problems needing to be fixed. In an already tight timeline, that creates tension between developers and the security team.

If you're using traditional pentesting methods, the delays and disruption are too great to burden the development team, who are likely working a continuous integration and continuous delivery process (CI/CD). Or if you're using an automatic scanner to detect potential vulnerabilities, you're receiving a long list of low-level vulnerabilities that obscures the most critical issues to address first.

Instead, continuous pentesting, or even scanning for a particular CVE, can harmonise development and security teams. And it's increasingly important. A shocking 85% of commercial apps contain at least one critical vulnerability, according to a 2021 report[1], while 100% use open-source software, such as the now infamous Log4j. That's not to knock on open-source software, but rather to say that a critical vulnerability can pop up at any time and it's more likely to happen than not.

If a critical vulnerability is found – or worse, exploited – the potential fines or settlement from a data breach could be astronomical. In the latest data breach settlement, T-Mobile agreed to pay $350 million[2] to customers in a class action lawsuit and invest additional $150 million in their data security operations.

This is why many companies are hiring for development security operations (DevSecOps). The people in these roles work in concert with the development team to build a secure software development process[3] into the existing deployment schedule. But with an estimated 3.5 million cybersecurity jobs globally that are likely went unfilled in 2021[4], it might be hard to find the right candidate.

If you want to improve the security of your software and app development, here are some tips from Synack customers:

- *Highlight only the most critical vulnerabilities to the dev team.* The development team has time only to address what's most important. Sorting through an endless list of vulnerabilities that might never be exploited won't work. Synack delivers vulnerabilities that matter by incentivising our researchers to focus on finding severe vulnerabilities.
- *Don't shame, celebrate.* Mistakes are inevitable. Instead of shaming or blaming the development team for a security flaw, cheer on the wins. Finding and fixing vulnerabilities before an update is released is a cause for celebration. Working together to protect the company's reputation and your customers' data is the shared goal.
- *Embrace the pace.* CI/CD isn't going away and the key to deploying more secure apps and software is to find ways to work with developers. When vulnerabilities are found to be fixed, document the process for next time. And if there's enough time, try testing for specific, relevant CVEs. Synack Red Team (SRT) members document their path to finding and exploiting vulnerabilities and can verify patches were implemented successfully. SRT security researchers can also test as narrow or broad a scope as you'd like with Synack's testing offerings and catalogue of specific checks, such as CVE and zero day checks.

Security is a vital component to all companies' IT infrastructure, but it can't stand in the way of the business. For more information about how Synack can help you integrate security checkpoints in your dev process, request a demo. □

1 https://venturebeat.com/business/85-of-commercial-software-apps-have-critical-vulnerabilities-study-finds/#:~:text=85%25%20of%20commercial%20apps%20have,'%20vulnerabilities%2C%20study%20finds%20%7C%20VentureBeat

2 https://apnews.com/article/technology-lawsuits-class-action-8f03e9f76fa75f474f1a2584ce3a55f0

3 https://niccs.cisa.gov/education-training/catalog/security-innovation/secure-software-development

4 https://cybersecurityventures.com/jobs/

Kirsten Gibson is Senior Content Marketing Manager at Synack.

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

Synack

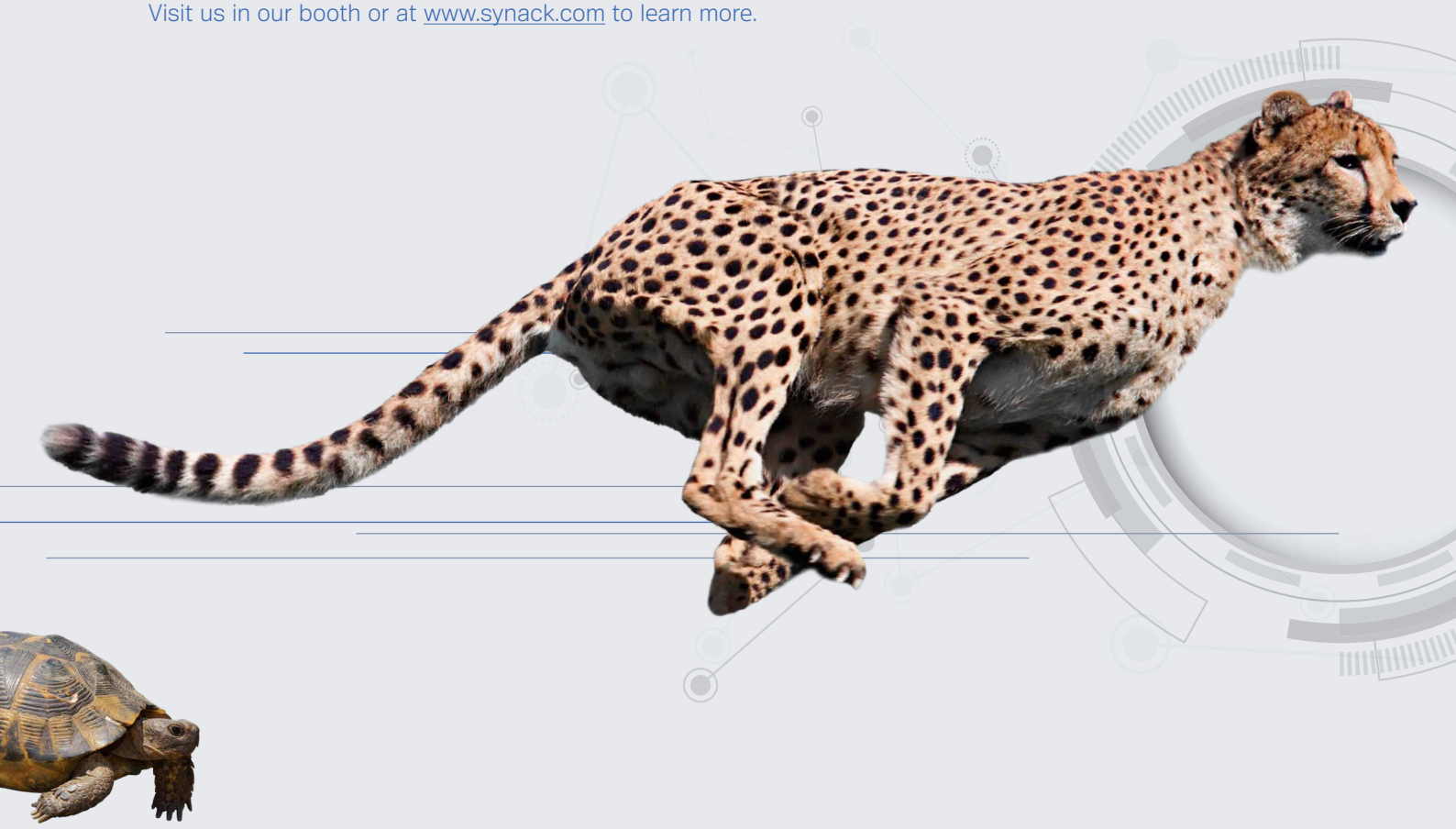
THE PREMIER SECURITY TESTING PLATFORM

A BETTER WAY TO PENTEST

Traditional pentesting is like a turtle chasing a cheetah

Find the vulnerabilities that matter with continuous and on-demand security testing.

Visit us in our booth or at www.synack.com to learn more.



Drei Tipps zur Verbesserung der Cloud-Sicherheit

Cloud-Dienste Cloud-Dienste nicht nur ein wesentlicher Bestandteil der digitalen Infrastruktur von modernen Unternehmen sondern auch bei Angreifern sehr beliebt.

Aris Koios reports

Der Einsatz von Cloud-Diensten hat zwar vielen Unternehmen mehr Möglichkeiten für Kollaboration, Flexibilität, Skalierbarkeit und Kosteneinsparungen gebracht, aber zugleich auch eine neue Angriffsfläche geschaffen. Denn mit der wachsenden Beliebtheit der Dienste hat sich auch der Fokus von Angreifern verschoben. Immer mehr Cyber-Akteure missbrauchen Cloud-Dienste für ihre Machenschaften. Zu den häufigsten Cloud-Angriffsvektoren, die von eCrime-Angreifern und anderen Eindringlingen verwendet werden, gehören:

- die Ausnutzung von Cloud-Schwachstellen
- Diebstahl von Anmeldeinformationen
- Missbrauch von Cloud-Diensteanbietern
- die Nutzung von Cloud-Diensten zum Hosten von Malware und Command and Control (C2)
- die Ausnutzung falsch konfigurierter Image Container

Ein weiterer Trend laut des Global Threat Report: Cloud Security 2022 sind Angriffe auf stillgelegte oder vernachlässigte Cloud-Infrastrukturen, um sensible Daten abzugreifen. Mangelnde oder fehlende Sicherheitskontrollen wie Überwachung, detaillierte Protokollierung, Sicherheitsarchitektur und -planung sowie Behebung von Schwachstellen machen diese Umgebungen zu einem attraktiven Ziel.

Manchmal enthalten vernachlässigte Cloud-Infrastrukturen immer noch wichtige Geschäftsdaten und -systeme. Angriffe auf solche Systeme haben in der Vergangenheit zu sensiblen und meldepflichtigen Datenlecks geführt, die eine kostspielige Aufarbeitung und Reputationsschäden nach sich zogen. Stellen diese Systeme noch kritische Dienste bereit, können diese Angriffe folgenschwere Dienstausfälle verursachen.

Leider sind viele traditionelle Sicherheits- und Netzwerktools, die in vielen älteren Umgebungen funktionierten, in der Cloud nicht einsetzbar. Infolgedessen haben sich viele Unternehmen für eine Mischung aus selbst entwickelten und veralteten Ansätzen entschieden, die Silos schaffen und die Verwaltung erschweren. Unzureichende Transparenz bedeutet, dass Sicherheitsrisiken unbemerkt bleiben, die Angreifern Tür und Tor öffnen können. Sicherheitsteams, die Einblick in die Tools und Taktiken von Angreifern haben, können Bedrohungen schneller erkennen und stoppen.

Diese drei zentralen Grundsätze der Cloud-Sicherheit gilt es zu beachten:

1. *Laufzeitschutz aktivieren und Sichtbarkeit in Echtzeit ermöglichen:* Unternehmen können sich nicht vor dem schützen, was sie nicht sehen können – dazu gehört auch Infrastruktur, die kurz vor der Stilllegung steht. Von zentraler Bedeutung für die Sicherung der Cloud-Infrastruktur zur Verhinderung von Sicherheitsverletzungen sind der Laufzeitschutz und die Transparenz, die Cloud-Workload-Schutz bietet. Es bleibt entscheidend, Workloads mit Endpunktschutz der nächsten Generation zu schützen, einschließlich Servern, Workstations und Containern, unabhängig davon, ob sie in einem lokalen Rechenzentrum oder in der Cloud gehostet werden.
2. *Konfigurationsfehler beseitigen:* Die häufigste Ursache für das Eindringen in die Cloud sind nach wie vor menschliche Fehler und Versehen, die während allgemeiner Verwaltungsaktivitäten auftreten. Wichtig ist der Aufbau einer neuen Infrastruktur mit Cloud-spezifischen Prozessen und Audit-Maßnahmen, die einen sicheren Betrieb erleichtern. Eine Möglichkeit, um einfach neue Unterkonten und Abonnements zu erstellen, bietet die die Verwendung einer Cloud Account Factory. Diese Strategie stellt sicher, dass neue Konten auf vorhersehbare Weise eingerichtet werden, wodurch eine häufige menschliche Fehlerquelle vermieden wird. Die Einrichtung von Rollen und Netzwerksicherheitsgruppen verhindert weiterhin, dass Entwickler und Betreiber ihre eigenen Sicherheitsprofile erstellen müssen und versehentlich neue Schwachstellen schaffen.
3. *CSPM-Lösung verwenden:* Unternehmen sollten sich vergewissern, dass ihre Cloud-Account-Factory eine detaillierte Protokollierung und ein Cloud Security Posture Management (CSPM) mit Warnmeldungen an die verantwortlichen Parteien ermöglicht, einschließlich Cloud-Operations- und Security Operations Center (SOC)-Teams. Nicht verwaltete Cloud-Dienste sollten aktiv gesucht und identifiziert werden. Es ist wichtig, dass jegliche Cloud-Schatten-IT entweder stillgelegt oder in das CSPM eingebunden und vollständig verwaltet wird. Um fortlaufende Transparenz für Operation-Teams zu gewährleisten, sollte das CSPM für die gesamte Infrastruktur bis zu dem Zeitpunkt verwendet werden, an dem das Konto oder Abonnement vollständig außer Betrieb genommen wird.

Die Verteidigung der Cloud wird wahrscheinlich noch komplexer werden, da sich nicht nur Cloud-Dienste permanent weiterentwicklen, sondern auch Angreifer verstärkt versuchen Cloud-Infrastruktur, -Anwendungen und -Daten zu kompromittieren. Mit einem umfassenden Ansatz, der auf Transparenz, aktuellen Bedrohungsinformationen und Cloud-spezifischer Bedrohungserkennung basiert, haben Unternehmen jedoch die besten Chancen, die Cloud zu nutzen, ohne die Sicherheit zu gefährden. □

Aris Koios, Technology Strategist DACH bei CrowdStrike.
Weitere Informationen unter
www.crowdstrike.com

CROWDSTRIKE

We stop **breaches**

Maximale Sicherheit
aus der Cloud
für die Cloud, Identität &
Endgeräte
vereint in einer Lösung.

crowdstrike.com

How aligning Security Awareness and Security Operations can reduce dwell time

It is time Security Awareness takes its rightful place next to Security Operations as partners in reducing dwell time and keeping email phishing attacks out of employee inboxes.

Cofense reports

Email phishing attacks pose a large threat to every organisation around the world and make up 91% of all cyber-attacks. The most effective way for organisations to reduce their risk is to ensure that all aspects of their phishing programme are focused on resiliency and preparing for the attacks that have the highest likelihood of reaching them. Suggested metrics to define and understand include human resiliency, mean time to detect (MTTD), mean time to respond (MTTR), and dwell time.

While MTTR falls under the purview of Security Operations and is a central focus in analysing and remediating attacks, MTTD also should be considered and is often a secondary metric. To fight email phishing attacks, both metrics must be primary objectives of the information security programme. The Security Awareness function can make an impact to these metrics by increasing the resiliency of the humans at the organisation to ensure that the threats bypassing traditional email controls are quickly recognised, reported, and placed in the hands of the security operations and response teams.

The first step to reducing dwell time is improving MTTD and can be accomplished by conditioning your employees to be the first line of defence by becoming human sensors to report any email they suspect is malicious. Most security awareness programmes focus on susceptibility, a measure of how many employees click on a simulation. Instead, security awareness programmes should focus on resiliency, which compares the number of employees who reported the simulation to the number of employees who clicked the link. Email phishing attacks can only be removed if Security Operations is aware of them – positioning Security Awareness in the centre of Security Operation's strategy.

The second step to reducing dwell time can be accomplished by enabling Security Operations to analyse the most-likely malicious emails first. While increased reporting rates are a positive change and increase visibility into the threat landscape, it also means threat analysts must spend more time reviewing emails for actual attacks. Various email security vendors provide tools for Security Operation Centres (SOCs) to respond to reported emails, but don't provide the best approach. While most organisations take an approach of 'scoring' threats based on their internal threat intelligence, this does not account for the power of your internal reporters. With highly trained employees as the first line of defence, they become the best 'eyes' of an organisation, and employees with the highest likelihood to spot a phishing email should have their reports analysed first. Combining threat scoring and reporter scoring further emphasises the importance of Security Awareness while making it easier for Security Operations to stop email phishing attacks.

Security Awareness is more than compliance – it is an integral part in reducing dwell time of the most active and successful threat vector facing every organisation – email phishing attacks. With services such as those provided by DFI in collaboration with Cofense, organisations can create a partnership between the Security Awareness and Security Operations teams. DFI and Cofense can enable Security Awareness to build resiliency across the organisation with simulations derived from real phish that are updated every month. Cofense is the only vendor that delivers simulations when an employee is active in their inbox, doubling report rates across our customer base. Cofense Phishing Detection and Response (PDR) takes these reported emails and automatically helps analysts in SOCs sift through the noise by scoring reported emails based on indicator of compromise (IOC) scoring and 'reporter reputation', enabling threat analysts to investigate reported emails from employees with the greatest track record of reporting real phish. It is time Security Awareness takes its rightful place next to Security Operations as partners in reducing dwell time and keeping email phishing attacks out of employee inboxes. □

For more information, please visit
www.cofense.com

COFENSE

COFENSE

in Partnerschaft mit

DFi Data First

GROUPE CHEOPS TECHNOLOGY

Aufbau einer Cyberresistenteren Welt

Stärken Sie Ihre Cybersicherheit mit einem Expertenteam und Zugang zu einem Netzwerk von über 32 Millionen Bedrohungsmeldern. Mit Services, die auf Ihre Bedürfnisse zugeschnitten sind, können wir Ihnen helfen:

- Identifizieren Sie Risiken und Bedrohungen
- Schutz vor Bedrohungen
- Erkennen Sie Cyberangriffe
- Reaktion auf Vorfälle

Einblicke in die neuesten E-Mail-Bedrohungen...

Identifizieren, erkennen und reagieren Sie auf die neuesten E-Mail Bedrohungen mit dem Cofense Q2 Phishing Intelligence Trends Review. **Laden Sie jetzt Ihr kostenloses Exemplar herunter:**

LADEN SIE IHRE KOPIE JETZT HERUNTER

Data Centric Security oder Information Rights Management 2.0

Ein neuer Ansatz zum Schutz und zur Kontrolle vertraulicher Unternehmensdaten überwindet die größten Probleme klassischer IRM-Systeme.

Seclore reports

Der Spagat zwischen Sicherheit und Produktivität ist für Unternehmen nicht leicht zu meistern. Die zunehmende Digitalisierung, besonders der stetige Ausbau von Cloud-Lösungen, erlaubt es Unternehmen, einfach und firmenübergreifend an gemeinsamen Projekten zu arbeiten.

Doch während Mitarbeiter die neuen Möglichkeiten des Datenaustausches schätzen, bereitet diese Entwicklung den CISOs und CEOs zunehmend Probleme. Vertrauliche Daten, die die eigenen Firmengrenzen verlassen und unbemerkt zum Wettbewerber gelangen, sind seit jeher eine große Gefahr. Doch neben den klassischen Gefahren, etwa der unabsichtliche Versand einer E-Mail, das Kopieren auf USB-Sticks, unzufriedene Mitarbeiter und Identitätsdiebstahl kommen neue Problemfelder, die sich nicht mit Firewalls oder DLP-Tools lösen lassen, hinzu. Durch die Verwendung von Cloud-Diensten, BYOD, das Teilen von Informationen mit Dienstleistern und Geschäftspartnern fließen Daten automatisch aus den Unternehmen und entziehen sich der Kontrolle. Ein Datenleck scheint nur eine Frage der Zeit.

Grenzenlose Sicherheit in Zeiten wegfallender Grenzen?

Information Rights Management (IRM) Systeme können in Zeiten wegfallender Unternehmensgrenzen Dateien vor Missbrauch effektiv schützen, indem sie eine sichere Zugriffskontrolle mit Nutzungsrechten verbinden. Das Dokument selbst wird verschlüsselt und ist damit unabhängig von Speicherort oder Übertragungsweg geschützt. Granulare und zentral verwaltete Berechtigungen ermöglichen es die Verwendung (z.B. Lesen und Editieren), den Zeitraum sowie den Verwendungsort einzuschränken. Diese Berechtigungen sind jederzeit anpassbar, egal wo sich das Dokument befindet.

Dennoch zögern viele Firmen bzw. scheitern daran, ein IRM-System erfolgreich einzusetzen. Die Technologie ist nicht das Problem, sondern die zersplitterte und gewachsene Anwendungslandschaft. IRM Systeme sind jedoch nur dann effizient und produktiv, wenn sie plattformübergreifend eingesetzt werden. Hieraus ergeben sich 3 große Herausforderungen:

1. *Daten schützen:* Es mag banal klingen, aber ein IRM System ist nur sinnvoll, wenn vertrauliche Daten auch konsequent geschützt werden. Überlässt man diese Aufgabe den Mitarbeitern, entsteht hoher Schulungsaufwand und die Gefahr das Daten nicht oder nur inkonsequent geschützt werden. Data Centric Security von Seclore ermöglicht Unternehmen eine einfache Integration mit bestehenden Datenschutzlösungen (wie DLP, CASB, eDiscovery) und anderen Unternehmensanwendungen (wie CMS, File Sharing und E-Mail-Systeme), um Dokumente automatisch zu schützen, sobald sie identifiziert, heruntergeladen und weitergegeben werden.
2. *Benutzerfreundlichkeit sicherstellen:* Neue Möglichkeiten des Datenaustausches dürfen nicht durch IRM Systeme ausgebremst werden. Ist die Anwendung zu kompliziert wird das Vorhaben mittelfristig im Unternehmen scheitern. Besonders externe Nutzer müssen in der Lage sein, einfach und ohne Installation auf geschützte Dokumente zuzugreifen. Mittels nativer Applikation oder komplett browserbasiert, Seclore erlaubt es Nutzern geschützte Dateien auf jedem OS und jedem Gerät einfach und sicher zu verwenden.
3. *Einfache Administration:* Implementierung, Wartung und die Richtlinienverwaltung dürfen zu keinem signifikanten Mehraufwand für die Unternehmen führen. Doppelte Nutzerverwaltung und separate Erstellung von Zugriffsrechten sind ein nicht zu unterschätzender Mehraufwand, der die Nutzung unnötig erschwert. Dank des Seclore Unified-Policy-Manager werden Identitätsmanagement, Richtlinienmanagement und Aktivitätsberichte über die Dokumentnutzung koordinierbar. Wenden Sie beispielsweise SharePoint-Berechtigungen automatisch auf entsprechende Dateien an, wenn diese das System verlassen. Ganz ohne doppelte Verwaltungsaufwand.

Abwarten ist keine Option mehr

Die Gefahr durch unkontrollierten Datenabfluss ist ein immer noch unterschätztes Risiko für viele Unternehmen. Die Nutzung von Cloud-Diensten und mobilen Endgeräten, erschwert die Kontrolle sensibler Daten zusätzlich. Der Gesetzgeber hat die Gefahr erkannt und erhöht durch verbindliche Datenschutzverordnungen den Druck.

Die Lösung ist Data Centric Security von Seclore. Ein IRM-System muss heutzutage kein hochkomplexes und ressourcenfressendes IT Monster mehr sein. Automatisierung und Integration in bestehende Systeme sind der Schlüssel für eine erfolgreiche Implementierung. Mitarbeiter werden nicht belastet, Daten aber konsequent und rechtzeitig geschützt. Hohe Nutzerfreundlichkeit und minimale Administration gewährleisten Flexibilität, ohne dabei die Kontrolle über die Dokumente zu verlieren. Datenschutz ist kein Selbstzweck sondern eine elementare Teildisziplin in der IT Sicherheit. □

For more information, please visit
www.seclore.com

Verbesserte Sicherheit der Betriebstechnologie mit Cyber Deception

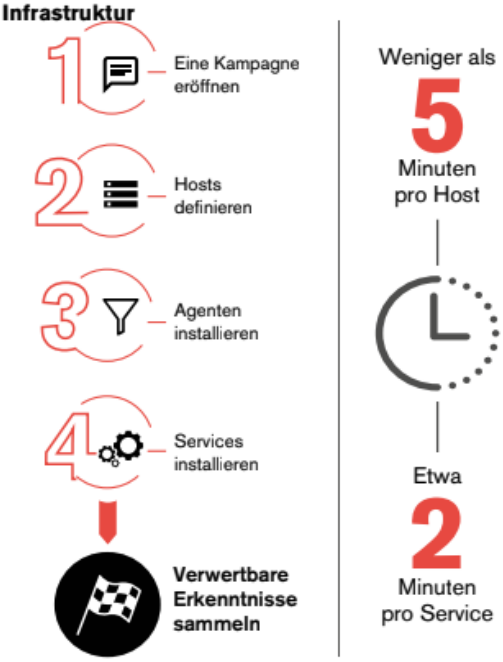
Die Deception-Technologie bietet eine effektive weitere Schutzschicht.

Cyber-Angriffe auf kritische Infrastrukturen und physische Systeme kommen immer häufiger vor. Beispiele wie der Angriff auf das amerikanische Ölpipelinesystem Colonial Pipeline und der Hacker- Angriff auf ein Wasserwerk in Florida haben gezeigt, wie unmittelbar die Gefahr ist. Das hat dazu geführt, dass die US-Behörde für Cybersicherheit und Infrastruktur (CISA) mehrere Warnungen ausgesprochen hat, wie z. B. im Oktober 2021 die Warnung über „Anhaltende Cyberbedrohungen für Wasser- und Abwassersysteme in den USA".

Betriebstechnologie-Netzwerke (OT-Netzwerke) wie SCADA und industrielle Kontrollsysteme (ICS) besitzen viele einzigartige.

Eigenschaften, die die Abwendung solcher Cyber-Angriffe besonders herausfordernd machen. Die höchste Priorität hat bei solchen Systemen die Betriebskontinuität. Die Verwendung von veralteten und physisch isolierten Geräten und die unvermeidliche Zusammenführung von IT und OT machen diese Umgebungen besonders anfällig sowohl für Bedrohungen von innen als auch für externe Angriffsversuche. Zudem entstehen zusätzliche Herausforderungen für die Sicherheit, die in reinen IT-Umgebungen selten vorkommen.

Die nötigen Schritte für eine Kampagne bei kritischer Infrastruktur



Verwertbare Erkenntnisse:

- IP-Adressen
- Ursprungsland
- Domain-Namen
- Benutzeragenten
- Betriebssystem
- Browser
- Sicherheitsevents: Netzwerkscans, Exploitversuche usw.
- Benutzernamen und Passwörter
- Ausgeführte Binärcodes
- Ausgeführte Befehle
- Neu erstellte Prozesse
- Erstellte Dateien
- Erstellte Netzwerkverbindungen
- Veränderungen am Betriebssystem
- Änderungen an Benutzern und Rechten
- Sicherheitsevents: Netzwerkscans, Exploitversuche usw.
- Änderungen an der Systemintegrität
- Änderungen in der Registry (Windows)
- Bösartige Prozessaktivität (Code-Einschleusung, Remote-Threads usw.)

OT-Netzwerke gehören zur kritischen Infrastruktur, sind teils anfällig und verwenden häufig veraltete IT-Technologie. Die Lebensdauer von Industriemaschinen beträgt oft viele Jahre.

- Teilweise werden Betriebssysteme verwendet, die vom Hersteller gar nicht mehr unterstützt werden.
- Ein Netzwerk mit „Air Gap" ist manchmal keine Option, z. B. wenn auf diesen Geräten Daten liegen, auf die zugegriffen werden muss.
- Patches sind nicht immer kompatibel oder benötigen eine Verbindung zum Internet oder einem zentralen Patch-Server.
- Viele HMI-Systeme laufen auf einfachsten Betriebssystemen und auf Hardware, die auf das absolut Notwendige „optimiert" wurde.

Diese Netzwerke sind schwer zu schützen und sind somit ein gefundenes Fressen für Angreifer. Daher ist es unabdingbar, neue Sicherheitslösungen zu finden. Da OT ein so kritischer Bestandteil des Systems ist, muss es um jeden Preis geschützt werden. Die Deception-Technologie bietet eine effektive weitere Schutzschicht.

Hauptvorteile

Deception kann beim proaktiven Schutz von

CounterCraft reports

Die CounterCraft Cyber Deception-Plattform kann verwendet werden, um das System ohne Einfluss auf bestehende Systeme sicherer zu machen und um aus erster Hand wertvolle Threat Intel über die Angreifer Ihres OT-Systems zu gewinnen.

kritischen Assets helfen, ohne den normalen Betrieb der Services zu belasten.

- Eine Deception-Umgebung hat keinen Einfluss auf bestehende Systeme
- Es besteht kein Risiko für die Betriebskontinuität
- Sie ermöglicht die Erkennung von bösartigen Aktivitäten und das Sammeln wertvoller Threat Intel
- Sie reagiert in Echtzeit auf feindliche Aktivität

Unsere Lösung

Deception-Technologien können eine zusätzliche Schutzschicht für OT-Netzwerke bieten. Die CounterCraft Cyber Deception-Plattform kann verwendet werden, um das System ohne Einfluss auf bestehende Systeme sicherer zu machen und um aus erster Hand wertvolle Threat Intel über die Angreifer Ihres OT-Systems zu gewinnen. Der Ansatz von CounterCraft erfordert keine Veränderungen am bestehenden SCADA-Netzwerk.

Es werden keine zusätzlichen Inline-Geräte benötigt.

Deception-Assets werden einfach wie jedes andere System an das Netzwerk angeschlossen und so eingerichtet, dass die ausgeführten Services so aussehen wie andere Geräte in Ihrem SCADA-Netzwerk. Es werden wichtige Informationen aus den Aktionen des Angreifers gewonnen. Dies liefert Einsicht in die Ziele und verwendeten TTPs des Angreifers. Andere Deception-Hosts wie physische WLAN-Router oder SPS-Emulationen können ebenso ein effektiver Teil einer Deception-Kampagne sein.

Die CounterCraft Cyber Deception-Plattform basiert die Erkennung nicht auf bekannten Signaturen oder Traffic-Analysen, sondern auf menschlichen Aktionen.

Das bietet eine Deception-Umgebung

Proaktiver Schutz: Sorgt für proaktiven Schutz von kritischen Assets und verhindert den Erfolg des Angreifers, ohne den normalen Betrieb der Services zu belasten.

Überzeugende Echtheit: Kann so konfiguriert werden, dass sie wie bestimmte Geräte in einem typischen SCADA-Netzwerk aussieht.

Genau die richtigen Informationen: Ermöglicht die Überwachung von Angriffen, die speziell auf die aktuelle Infrastruktur abzielen.

Frühe Erkennung: Gleichzeitig werden die Sicherheitslücke und das gefährdete Asset sofort identifiziert.

Verwertbare Erkenntnisse: Das Wissen über die TTPs des Angreifers ermöglicht das direkte Teilen mit SIEM, SOAR und dem restlichen Sicherheitsteam. □

CounterCraft ist die nächste Generation von Threat Intel – dank einer Deception Plattform, die aktiven Schutz durch hochinteraktive Deception-Technologie bietet.

Kontaktieren Sie uns gerne für weitere Informationen zu CounterCraft **www.countercraftsec.com**

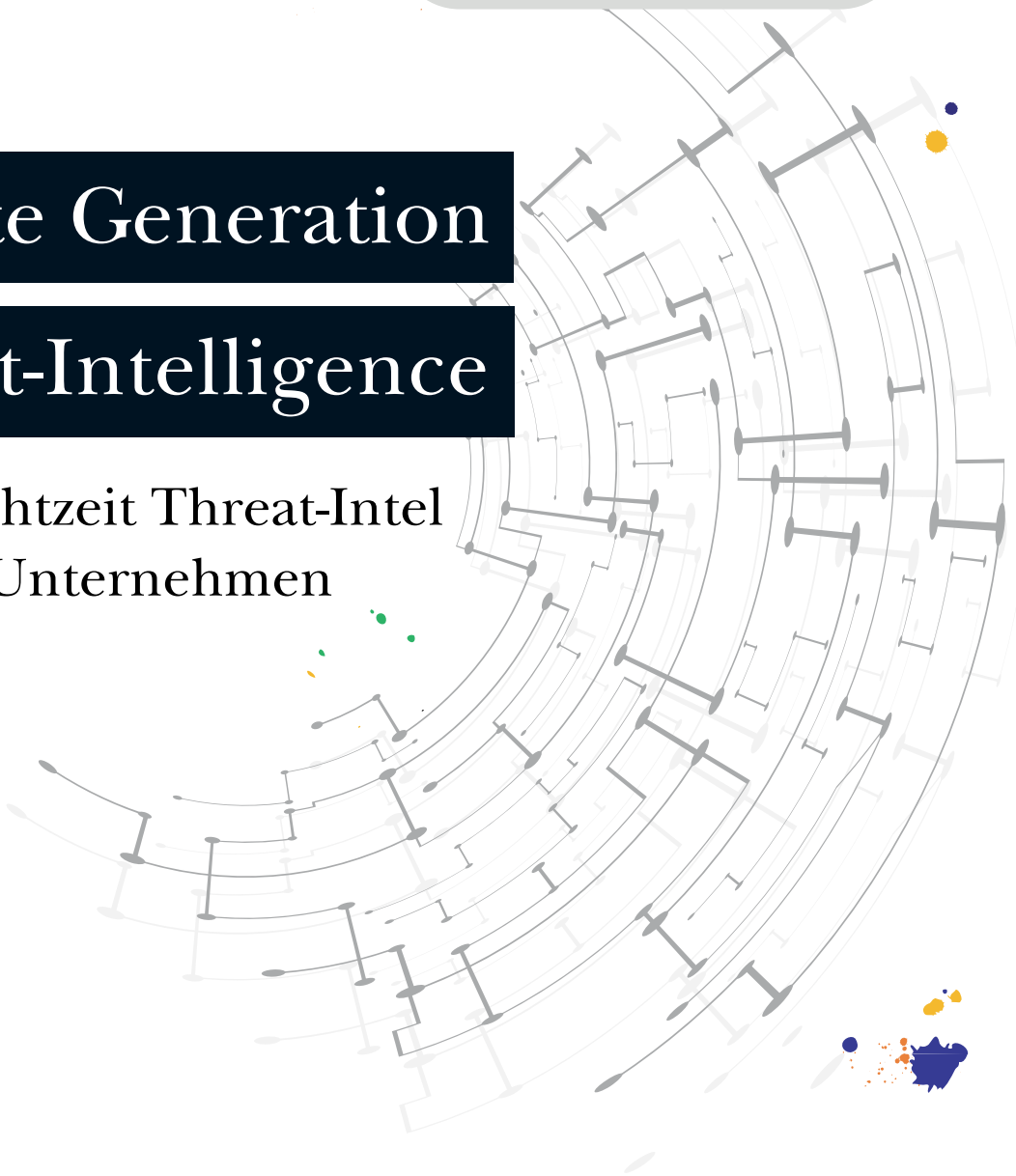
CounterCraft

CounterCraft

BESUCHEN SIE UNS IN
DER AUSSTELLUNGSHALLE

Die nächste Generation von Threat-Intelligence

Umsetzbarer Echtzeit Threat-Intel speziell für Ihr Unternehmen



Sicherheitsteams auf der ganzen Welt vertrauen CounterCraft

Weltbekannte Finanzinstitute, Regierungsbehörden, Pharma-, Einzelhandels-, Industrie- und Strafverfolgungsbehörden verteidigen ihre Organisationen mit CounterCraft. Trete ihnen bei!

Gartner COOL VENDOR 2021

OVERALL LEADER
LEADERSHIP COMPASS 2021

INFOSEC AWARDS WINNERS
CYBER DEFENSE MAGAZINE
2019

Follow us: @countercraftsec
@countercraft
@countercraftsec

www.countercraftsec.com
New York - London - Madrid - San Sebastian

e-Crime & Cybersecurity Mid-Year Summit 2022

"Insightful, relevant and thought provoking; no hard sells, sensible practical approaches to current day cybersecurity challenges."

Head of Information and Cyber Security, McArthurGlen Group

"Thanks, very enjoyable. Look forward to my invitation to the March event. Thanks to everyone making this possible in these difficult times. I actually spent the whole day on it!"

Director of Global Security, American Express

"Thank you for the update and the invitation to join yesterday's session. I found the conference to be very informative (as always) and covered the threat landscape in a timely manner. The presenters were excellent and the introduction/ continuity was executed to perfection. The content was superb [...] Thank you for the invitation again and I hope to catch up with you in person at the March 2022 event."

Information Security, AIB Group Technology Services

"It's been a wonderful experience to attend this virtual conference. Many thanks for organising the event."

Information Security Officer/ Data Protection Manager, Jein Solicitors

2021 sponsors included:

Principal Sponsor

F-Secure

Strategic Sponsors

BeyondTrust
DARKTRACE
MENLO SECURITY
okta
proofpoint
Recorded Future
SentinelOne

Education Seminar Sponsors

appgate
axis security
bitglass
corelight
CybelAngel
CyGlass by NOMINET
DEVO
CISCO | KENNA Security
onelogin
PICUS
RANGEFORCE
RED SIFT

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

Thank you to all our sponsors

Strategic Sponsors

DARKTRACE

f5

GATEWATCHER

KnowBe4
Human error. Conquered.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Recorded Future®

SentinelOne™

Education Seminar Sponsors

COFENSE

CounterCraft

CROWDSTRIKE

MENLO SECURITY

SECLORE

Synack

Networking Sponsors

eb-Qual

EXCLUSIVE NETWORKS

FORESCOUT

RANGEFORCE

RELIAQUEST