e-crime & cybersecurity SWITZERLAND

21st September 2023
Zurich, Switzerland

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Switzerland under attack

**It's been a year of intense cyber-bombardment.
Is Switzerland doing enough to fight back?**

Forthcoming events

e-crime & cybersecurity MID-YEAR 19th October 2023 London	e-crime & cybersecurity SPAIN 24th October 2023 Madrid	e-crime & cybersecurity NORDICS 31st October 2023 Copenhagen
e-crime & cybersecurity BENELUX 7th December 2023 Amsterdam	PCI LONDON 24th January 2024 London	SECURING FINANCIAL SERVICES 25th January 2024 London
SECURING THE LAW FIRM 25th January 2024 London	e-crime & cybersecurity GERMANY 30th January 2024 Frankfurt	e-crime & cybersecurity NORDICS 30th January 2024 Helsinki
e-crime & cybersecurity CONGRESS 28th & 29th February 2024 London	e-crime & cybersecurity CONGRESS 6th March 2024 Dubai	e-crime & cybersecurity NORDICS 25th April 2024 Stockholm

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

It's been a year of intense cyber-bombardment for Swiss organisations. In June, a pro-Russian hacking group took down several major websites, including key government sites such as parliament and the federal administration sites, as well as the one for Geneva Airport.

The country's National Cyber Security Centre (NCSC) described the intensity of the DDoS attack as 'exceptionally high' and warned some government websites could remain inaccessible. The attack coincided with preparations by the Swiss parliament for a video address by Ukrainian President Volodymyr Zelenskiy and with Switzerland's adoption of an EU sanctions package against Russia.

These were just the latest in an accelerating burst of attacks in the country. And these attacks have exposed weaknesses in Switzerland's cybersecurity readiness. One security solution provider recently reported that it had found 106,000 security holes among 3.5 million servers in Switzerland. It rated 50,000 weak points as extremely serious.

From the start of next year, Switzerland's NCSC will become a new federal office, reporting to the defence minister, and its budget will rise from CHF13.7m to CHF14.5m ($16.2m). However, few believe this is enough to keep up with the rate of growth in attacks.

In the private sector, just over half of Swiss firms told a survey that they plan to boost their cybersecurity budgets for 2023, as they expect a rise in ransomware and other attacks next year. That said, globally 65% of firms say that their budgets will rise and the willingness of Swiss firms to release sensitive information about hacks was lower than the global average.

So, what should Switzerland's public and private sector be doing next to counter these growing threats? How can firms build resilience quickly? Can third-party vulnerabilities be defended? And what about new AI-based challenges?

Today's e-Crime & Cybersecurity Congress will try to answer some of these questions. Join our real-life case studies and in-depth technical sessions from the security and privacy teams at some of the world's most admired brands.

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**

21st September 2023

Courtyard by Marriott Zurich North

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

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

Forum organiser:
AKJ Associates Ltd
4/4a Bloomsbury Square
London WC1A 2RP
e: simon.brady@akjassociates.com

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

Cyber Bedrohungen: Vorbeugen statt heilen

Die heutigen Täter so unterschiedlich wie die Motive, die sie antreiben.

Wer erinnert sich noch an die ersten Cyberangriffe? Das ist schwer zu sagen, da einige bis ins Jahr 1974 zurückreichen. Während sie damals eher das Werk junger Geeks waren, die nach Bekanntheit strebten, sind die heutigen Täter so unterschiedlich wie die Motive, die sie antreiben: auf der einen Seite politisch oder ideologisch engagierte Hacker, auf der anderen Seite die bei weitem zahlreichen Cyberkriminellen, deren bevorzugte Praxis die Geldbeschaffung durch verschiedene Formen von Ransomware ist, d. h. Schadsoftware, die Computerdaten sperrt, bevor die Täter ein Lösegeld verlangen, um sie wieder zugänglich zu machen.

Neben Krypto-, Locker- und Doxware-Ransomware gibt es auch DDoS-Ransomware (Distributed Denial of Service). Dabei drohen die Angreifer einer Website oder einem Netzwerk mit einem DDoS-Angriff, wenn sie nicht bezahlt werden. Diese Angriffe führen nicht nur zu erheblichen Unterbrechungen des Dienstes. Sie haben auch greifbare negative Auswirkungen auf die Geschäftstätigkeit und das Image der Zielorganisation. Wenn sie auf kritische Infrastrukturen wie Transport-, Telekommunikations-, Wasser-, Energie- oder Gesundheitssysteme abzielen, können sie erhebliche Auswirkungen auf die Menschen haben, die von diesen Systemen abhängig sind. So wurden in jüngster Zeit einige unserer öffentlichen und privaten Einrichtungen ins Visier genommen.

Kampf gegen Hochleistungs-Botnets

Wir haben gesehen, dass DDoS-Angriffe immer größer werden und immer häufiger eine Lösegeldzahlung beinhalten. Aber was steckt hinter diesen hyper-volumetrischen Angriffen, und wie können Unternehmen ihnen Einhalt gebieten?

Hyper-volumetrische DDoS-Angriffe werden immer größer und häufiger, da eine neue Generation von Botnetzen Virtuelle Private Server (VPS) anstelle von Internet-of-Things-Geräten (IoT) verwendet. Botnets sind ein Netzwerk von Computern mit bösartiger Software, die aus der Ferne gesteuert werden können, um einen Angriff zu starten. DDoS-Botnet-Malware kann verschiedene Formen und Zwecke annehmen; einige sind so konzipiert, dass sie die Kontrolle über ein Gerät vollständig übernehmen, während andere als Hintergrundprozess laufen und so konzipiert sind, dass sie unentdeckt bleiben, bis der Angreifer ihnen Anweisungen gibt. Botnets können sich sogar selbst verbreiten, indem sie über verschiedene Kanäle zusätzliche Bots rekrutieren, z. B. durch Ausnutzung von Schwachstellen in Websites oder durch Rekrutierung anderer Hardware-Geräte in der Umgebung eines infizierten Geräts.

Bislang waren diese Botnets auf ein relativ großes Netzwerk von IoT-Geräten angewiesen, die zusammenarbeiten, um genügend Datenverkehr zu erzeugen, um das Ziel zu stören. Die neue Generation von Botnets benötigt jedoch viel weniger Geräte, um ihre Arbeit zu verrichten. Insbesondere die Ausnutzung virtueller privater Server von Cloud-Computing-Anbietern ermöglicht es Angreifern, Botnets zu erstellen, die bis zu 5.000 Mal stärker sind als herkömmliche Botnets. Angreifer können sich über nicht gepatchte Server Zugang zu diesen virtuellen privaten Servern verschaffen und sich mit durchgesickerten API-Anmeldedaten in Verwaltungskonsolen einhacken, um enorme Mengen an bösartigem Datenverkehr zu erzeugen.

Das Internet zu einem besseren und sichereren Ort zu machen, ist eine Teamleistung, und die Zusammenarbeit ist der Schlüssel zur Zerschlagung der Botnetze, die für groß angelegte DDoS-Angriffe verantwortlich sind. Glücklicherweise arbeiten Cloudflare und Cloud Computing-Anbieter zusammen, um gegen diese Botnets vorzugehen. Unternehmen wie Cloud-Computing-Anbieter, allgemeine Service-Provider und Hosting-Provider sollten sich um eine kontinuierliche Sichtbarkeit von Angriffen bemühen, die aus ihren Netzwerken heraus gestartet werden, indem sie bewährte, spezielle Tools von zuverlässigen Marken verwenden. Durch Zusammenarbeit kann die Cybersicherheitsgemeinschaft gegen diese Botnets vorgehen und sicherstellen, dass wir den Angreifern immer einen Schritt voraus sind.

Die Kunst, seinen Feind zu kennen und erkennen

Um DDoS-Angriffe zu verhindern, müssen Organisationen wissen, wie sie funktionieren. Eine Website, die offline ist oder nur langsam auf Anfragen reagiert, ohne dass eine Wartung geplant wurde, ist ein verdächtiges Zeichen. Protokolle eines ursprünglichen Webservers, die Anfragen enthalten, die dem üblichen Besucherverhalten fremd sind, oder unerwartete Spitzen bei den Anfragen oder der Bandbreite, sind andere.

Leider sind die herkömmlichen Schutzlösungen auf Basis von Boxen nicht mehr für diese neuen Angriffsformen geeignet. Daher müssen Organisationen unbedingt dafür sorgen, dass ihre IT-Umgebung ständig auf dem neuesten Stand ist. Um Instanzen zu schützen, ohne den legitimen

Cloudflare berichtet

Datenverkehr zu gefährden, stützen sich effektive Tools auf einen Satz vorkonfigurierter Regeln, um bekannte Angriffsmuster und -werkzeuge, verdächtige Muster, übermäßigen Datenverkehr, der den Ursprung/Cache betrifft, Protokollverletzungen, Anfragen, die eine große Anzahl von Ursprungs Fehlern verursachen, und zusätzliche Angriffsvektoren in der Anwendungsschicht zu identifizieren.

Der Baum, der den Wald verdeckt

Neben dem Schutz vor DDoS-Angriffen müssen Organisationen auch sogenannte Zero-Trust-Dienste implementieren, da Cyberkriminelle oft aus mehreren Perspektiven angreifen. So kann beispielsweise ein DDoS-Angriff durchgeführt werden, um einen anderen zu verschleiern. Während die Sicherheitsteams mobilisiert werden, um den DDoS-Angriff zu bewältigen, findet der eigentliche Angriff statt, z. B. über eine SQL-Code-Injektion.

Kunden, die Zero-Trust-Technologien einsetzen, erklären, dass der Aktionsradius eines erfolgreichen Angriffs viel enger wird, was eine schnellere Rückkehr zum Normalzustand ermöglicht. Darüber hinaus wird eine Zero-Trust-Architektur dazu beitragen, dass sich Ransomware nicht im Netzwerk ausbreiten kann. Schließlich kann eine Lösung zum Schutz von E-Mails (Anti-Phishing), die in eine Zero-Trust-Technologie integriert und um Dienste der generativen künstlichen Intelligenz erweitert ist, sowohl die Mitarbeiter als auch das Unternehmen schützen. Phishing-Angriffe und die Kompromittierung von Geschäfts-E-Mails (Business Email Compromise, BEC) stellen nach wie vor ein großes Sicherheitsproblem für Unternehmen dar. 91 % aller Cyberangriffe beginnen mit einer Phishing-E-Mail (Deloitte). Trotz verschiedener Versuche, das Bewusstsein für die Gefahren von Phishing zu schärfen und die Nutzer darüber aufzuklären, wie sie solche E-Mails erkennen können, sind diese Angriffe nach wie vor erfolgreich. Als Reaktion darauf investieren Unternehmen in fortschrittlichen E-Mail-Schutz mit Link-Isolierung und Cloud-basierter Remote-Browser-Sanierungstechnologie als Sicherheitsnetz für die neuesten Phishing-Angriffe.

Die Bedeutung von Zero Trust als wichtige Cybersicherheitsstrategie

Es ist zwar klar, dass Cyberangriffe weiter zunehmen und raffinierter werden, doch es gibt Mittel und Wege, um sie abzuwehren. Ein Angriff ist kein unabwendbares Schicksal mehr. Das erfolgreiche Triptychon für eine Cybersicherheitsstrategie ist einfach: Anwendungen, Netzwerke und Mitarbeiter schützen, und zwar auf vollständig integrierte Weise.

Da die meisten Angriffe innerhalb von Unternehmen erfolgen, ist der traditionelle Ansatz der Überwachung und Prävention nicht mehr wirksam. Es werden fortschrittliche und strenge Lösungen benötigt, um diese Bedrohungen zu beseitigen. Für Unternehmen ist ein narrensicheres Sicherheits-Framework wie Zero Trust jetzt unerlässlich, um ihre digitale Transformation zu unterstützen. Zero Trust ist ein Sicherheitsmodell mit strengen Zugriffskontrollen nach dem Prinzip, standardmäßig niemandem zu vertrauen, auch nicht denjenigen, die sich bereits innerhalb des Netzwerkperimeters befinden. Die Philosophie hinter einem Zero Trust-Netzwerk geht davon aus, dass es sowohl innerhalb als auch außerhalb des Netzwerks Angreifer gibt. Also sollte keinem Nutzer oder Gerät automatisch vertraut werden. Zero Trust verifiziert die Identität und die Privilegien der Nutzer sowie die Identität und Sicherheit der Geräte. Anmeldungen und Verbindungen werden in regelmäßigen Abständen unterbrochen, sodass Nutzer und Geräte ständig neu verifiziert werden müssen.

Mitarbeiter ins Zentrum stellen

CIOs, CSOs und CISOs sollten darüber nachdenken, einen vollumfänglichen Schutz für ihr Unternehmen inklusive Webpräsenz, Unternehmensnetzwerk, Mitarbeiter und auch für die eigenen Produkte gewährleisten. Es gibt leider keine ruhige Minute. Man muss neugierig, aufmerksam und innovativ bleiben, aber im Allgemeinen ist das etwas, was CIOs, CTOs, CSOs und CISOs von Natur aus tun, es ist ein integraler Bestandteil der Eigenschaften, die sie für ihren Posten benötigen. Da sich die Bedrohungen ständig weiterentwickeln, gilt es, wachsam zu bleiben, seine Sicherheits-Lösungen zu testen und evaluieren, und sich auf einen vertrauenswürdigen Partner wie Cloudflare zu stützen. Ideal ist es, seine operativen Arbeitsbelastungen auf ein Minimum zu reduzieren, um sich auf die Cyber-Sicherheitsstrategie des Unternehmens oder der öffentlichen Organisation zu konzentrieren. Es erfordert gesellschaftliche und technologische Entwicklungen zu beobachten, um neue Anwendungen, schwache Signale und somit neue potenzielle Bedrohungen zu antizipieren.

Darüber hinaus sollten CIOs, CTOs, CSO und CISOs das Bewusstsein für Cyber-Sicherheit beim Vorstand und erst recht bei allen Mitarbeitern der Organisation schärfen. Wichtig ist es eine „no blame Culture" einzuführen damit die Mitarbeiter angstlos sofort bescheid geben wenn sie auf falsche Links oder Anhänge geklickt haben; letztendlich sind wir nur Menschen und dürfen auch etwas falsch machen weil wir neugierig waren oder abgelenkt oder weil wir unter Zeitdruck zu schnell gehandelt haben. Jeder in der Organisation soll so verantwortungsbewusst wie ein CSO/CISO sein. □

CLOUDFLARE

Protection in every direction

One global platform secures employees, applications and networks. Everywhere Security.

300+

Cities in 100+ countries, including mainland China

112B

Daily threats blocked

95%

of world's Internet users within **50ms** of our network

cloudflare.com

Break the attack chain

Aegis Threat Protection

Protect your people from advanced email attacks.

Trusted by 86 of the Fortune 100 to stop initial compromise.

Sigma Information Protection

Secure privileged identities and stop lateral movement.

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

Identity Threat Defense

Defend sensitive data from theft, loss and insider threats.

The fastest growing DLP and insider risk platform.

proofpoint.

Learn more:
proofpoint.com

Ways to safeguard your data in generative AI like ChatGPT

The approach to public gen AI tools varies by company.

Generative AI is revolutionising how people work. At Proofpoint, there's a lot of discussion about the future state of generative AI apps like ChatGPT. The use of AI and machine learning (ML) is not new at Proofpoint. These capabilities are built into our core platforms to protect people and defend data. With generative AI, or gen AI, we see multiple opportunities. Not only can gen AI drive even greater insights and efficiency for your teams, but it also presents Proofpoint with an opportunity to scale our products and drive the business forward.

But there are also risks to using these advanced tools. The approach to public gen AI tools varies by company and can range from acceptable use policies to mitigating controls.

Here are some questions we hear from our customers, and how Proofpoint can help:

1. Who is using ChatGPT in my company?

Proofpoint helps you understand who is accessing ChatGPT and how often – whether through proxy traffic or at the endpoint. ChatGPT is one of hundreds of AI apps on the market. Thanks to the built-in gen AI app category Proofpoint created, you can use our platform to efficiently gain visibility into this category of shadow IT and apply controls to more than 600 URLs. You can do this by user, group or department.

2. How can I block access to ChatGPT?

With Proofpoint, you can block users from accessing specific sites such as ChatGPT or gen AI app category. People-centric policies allow you to apply dynamic access controls based on user risk. That means you can dynamically block access for a user based on their:

- Vulnerability (such as failing security awareness training or exhibiting careless behaviour, like clicking on phishing links)
- Privilege (access to sensitive data)

There are very real concerns about the risk of data loss related to generative AI. Users can copy and paste almost six pages of 12-point font into the ChatGPT prompt.

3. How can I allow users to use ChatGPT while also preventing the loss of sensitive data?

There are very real concerns about the risk of data loss related to generative AI. Users can copy and paste almost six pages of 12-point font into the ChatGPT prompt. Prompt splitters can split even larger pieces of text into separate chunks.

Another layer to mitigate risk is by limiting copy/paste into the ChatGPT prompt. You can block pasting or limit the number of pasted characters allowed. This mitigates critical data leak scenarios, like users submitting large amounts of confidential source code into the chat to optimise it or pasting full meeting transcripts to summarise them.

You can also block all files or files with sensitive data from being uploaded into ChatGPT via browser extensions for analysis. Real-time notifications (pop-ups) to the user can let them know why their action was blocked. You can also include links to company policy on acceptable use.

4. How can I allow users to use ChatGPT while also monitoring its use?

Some businesses don't want to limit ChatGPT or generative AI website use. But monitoring for safe use or context of use for investigations is important. As users interact with the ChatGPT prompt, you can capture meta and screenshots for visibility. Layer in visibility into the files in use and the source of those files, and you quickly gain a picture of the potential risks.

You can also set up alerts on visits to gen AI sites to signal that further investigation is needed. Alerts can be triggered for any or a subset of your users, such as high-risk users.

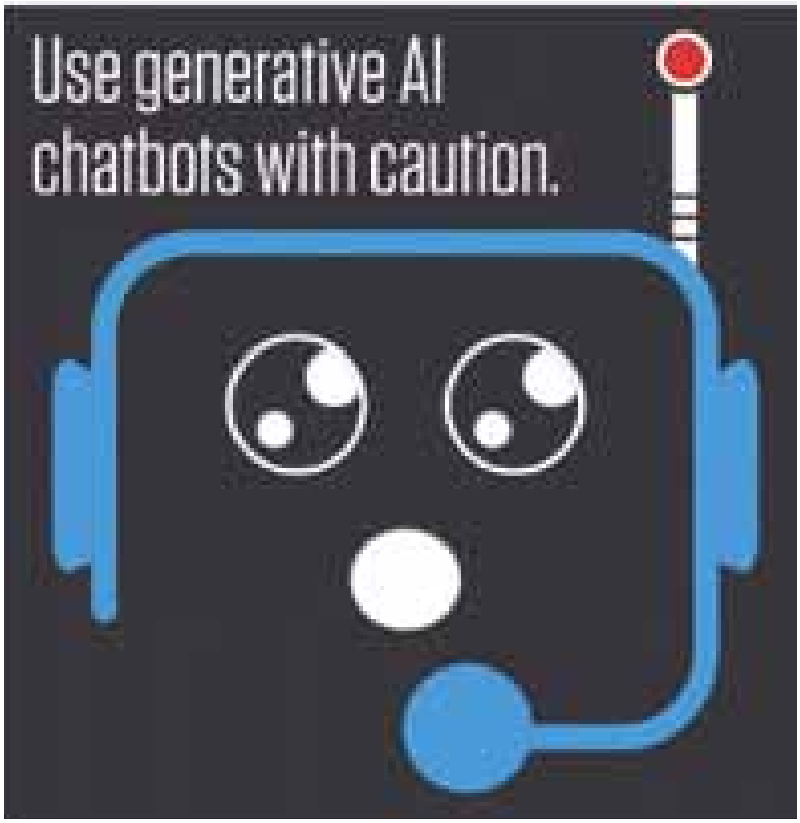
5. Where do I start? And how can I educate users?

You can start your journey by first communicating an acceptable use policy with employees. An explicit policy enables employee awareness and fosters accountability. Here are some steps to consider:

- Publish a list of pre-approved use cases that list what type of data inputs are acceptable for public versus company-hosted (or third-party hosted internal) generative AI tools. For example, call out that only public data can be input in public tools while customer data is out of bounds.

Proofpoint reports

Proofpoint can help you educate users on the safe use of generative AI with our security awareness kit and training module. With Proofpoint, you get tailored cybersecurity education online that's targeted to the vulnerabilities, roles and competencies of your users.



- Make sure users review and revise the output from generative AI tools and not just copy and paste.
- Create a process to review and approve new generative AI tools and use cases.
- Inform users that you reserve the right to monitor and record the use of these tools if that's part of your plan.

Proofpoint can help you educate users on the safe use of generative AI with our security awareness kit and training module. With Proofpoint, you get tailored cybersecurity education online that's targeted to the vulnerabilities, roles and competencies of your users. We provide education in bite-sized chunks, so it creates sustainable habits. And you get all the metrics that your CISO needs. □

Learn more
We invite you to reach out to your account team to find out more about how Proofpoint can help you to safeguard your data in generative AI like ChatGPT. For more information visit our website **www.proofpoint.com**

proofpoint.

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.

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.

SentinelOne berichtet

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. □

SentinelOne®

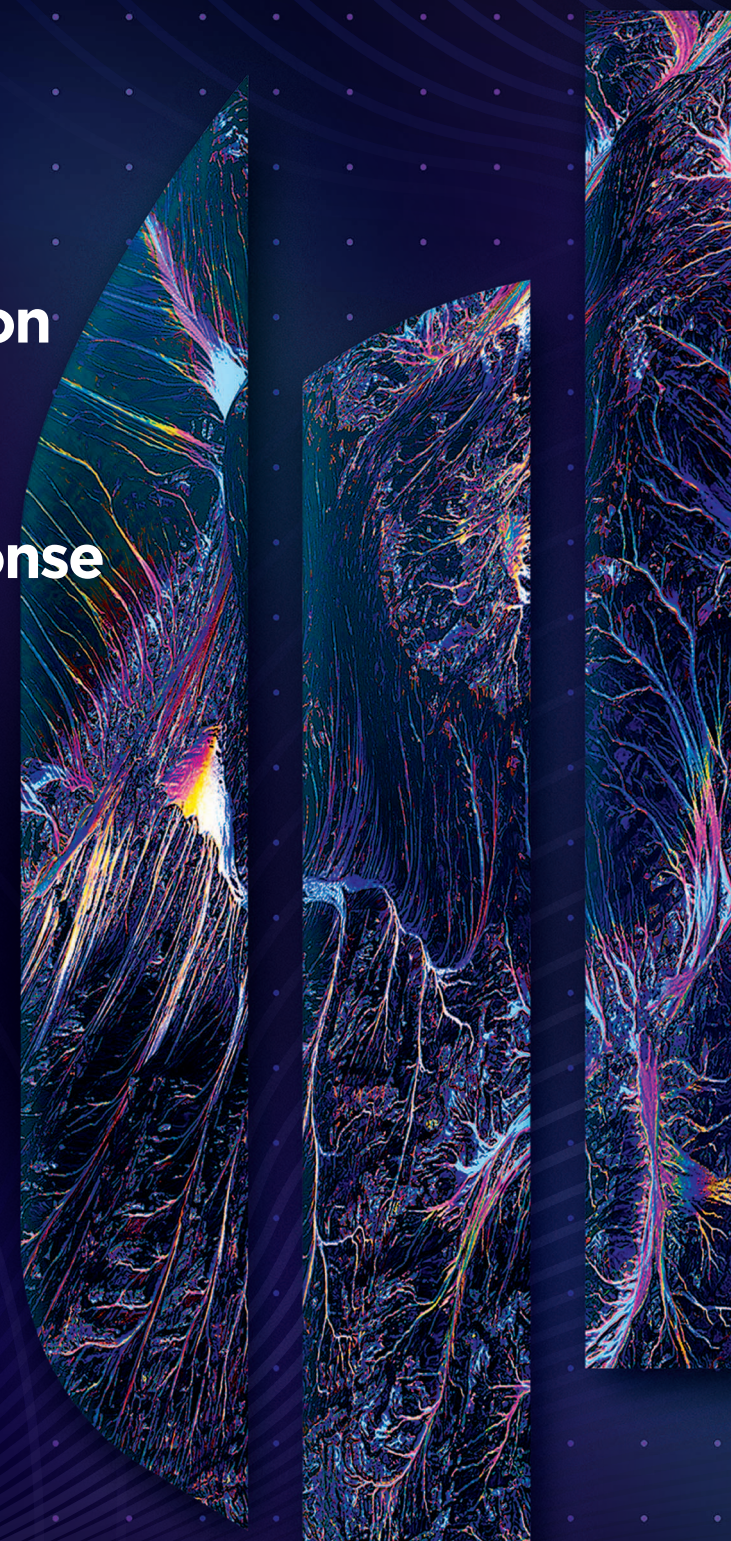
Smarter, stärker, schneller... autonom.

REAL TIME
Endpoint Protection

ACTIVE
Detection & Response

AUTONOME
Network Visibility & Control

NATIVE
Cloud Security



sentinelone.com

Why mid-market financial services firms are pivoting to MXDR services

Effective cybersecurity requires more than tools.

Craig Jones reports

For those in the financial services sector, cybersecurity is especially challenging, given the extraordinarily high stakes, due to the nature of the data these firms handle. Mid-market companies in this sector find themselves in the throes of a crucial decision: construct an internal Security Operations Centre (SOC) or entrust a managed extended detection and response (MXDR) service. Although each path presents compelling benefits, financial services firms may want to explore MXDR services for the reasons discussed below.

SOC: Build vs. Buy

An in-house SOC offers the perception of control through a customised defence architecture, fused with existing IT infrastructure, wielding a sovereign grip on sensitive financial data. However, this enticing control masks a host of challenging realities.

Developing an SOC demands a substantial initial outlay and persistent operational expenses. Staffing an SOC sufficiently demands a range of specialised experts: cyber-analysts, incident responders, and threat hunters, often supervised by a CISO. For financial services firms, these costs can quickly add up. And retaining these experts is costly.

MXDR services: A pragmatic alternative

By contrast, MXDR services offer benefits tailor-made for mid-market companies in the financial services sector.

- *Expertise:* First, MXDR service providers offer a team of cyber-experts who keep abreast of the latest threat intelligence and are well-versed in applying the most current counterstrategies. This provides customers with access to top-level cybersecurity expertise without the need to assemble their own in-house teams. This is particularly important for financial services firms, which are challenged by a threat landscape that is both highly complex and which is always evolving. Their sole focus on threats makes MXDR teams exceptionally skilled in resolving these incidents with a proficiency internal teams can't match.
- *Scalability and flexibility:* MXDR service providers can scale with a company's fluctuating requirements, an indispensable approach for growing mid-market financial services firms. MXDR services costs are often more manageable and predictable. The upfront and operational costs associated with an SOC give way to a subscription model, transitioning CAPEX into OPEX, making this an attractive proposition for managing the bottom line.
- *24/7 coverage:* MXDR service providers offer 24/7 surveillance, an exceptionally resource-intensive feat for an in-house team. Constant vigilance significantly enhances threat detection and accelerates response times. This reduces the potential for damages, a critical aspect for firms dealing with financial transactions and sensitive customer data.

MXDR: A strategic imperative for financial services

Choosing between an in-house SOC and outsourcing to an MDR service isn't a one-size-fits-all decision. It's shaped by numerous factors, including a company's risk profile, budget, and business model. However, for most mid-market financial services firms, MDR services present a compelling case.

MXDR services offer a streamlined, cost-efficient model, providing robust security without the rigours of building and maintaining an SOC. The level of expertise and around-the-clock protection is extremely difficult for most mid-market financial services companies to manage in-house.

As IT leaders in the financial sector chart their course through the SOC decision maze, they must remember that effective cybersecurity requires more than tools. Cybersecurity hinges on the expertise to understand and react to security incidents. This is where MXDR service providers prove their worth, blending security expertise with advanced technology, delivered as a scalable, manageable service.

For most mid-market financial services companies, the SOC build-or-buy problem tilts decisively towards the buy side. With rapidly developing cyber-threats, an evolving regulatory landscape, and the escalating cybersecurity skills gap, choosing an MXDR service is not only strategic but imperative. □

Craig Jones is Vice President, Security Operations at Ontinue. Learn more about the advantages of MXDR services and how the Ontinue ION MXDR service can meet the needs of financial services firms at **www.ontinue.com**

Ontinue

The MXDR Service to Optimise your Microsoft Security Investments.

Accelerate detection & response

70%

of high-severity incidents resolved automatically

Optimise daily SecOps

2 Days

of time per week, on average, is saved by analysts

Maximise SecOps cost efficiencies

50%

savings on SecOps data costs with Microsoft Sentinel cost optimisation

See the power of Ontinue ION

Generative AI apps and the risk of accidental data exposure

The number of users accessing AI apps in the enterprise is growing exponentially, and with that, the risk of accidental exposure of internal information is growing too.

Netskope reports

As businesses explore how to balance the benefits of AI with the associated risks, the Netskope Threat Labs have released a new report focused on 'AI Apps in the Enterprise'. The report examines the risks from AI apps such as the increased attack surface and accidental data leaks.

Given all the media hype, it is unsurprising the report found that the number of users accessing AI apps in the enterprise is growing exponentially, and with that, the risk of accidental exposure of internal information is growing too. According to the study, during May and June 2023, the percentage of enterprise users accessing at least one AI app each day increased to a total increase of 22.5% over the time period. ChatGPT tops the charts, with more than eight times as many daily active users as any other AI app. Organisations with more than 10,000 users utilised on average five AI apps per day with 1 out of 100 enterprise users interacting with an AI app each day.

This rapid growth is largely driven by the potential AI apps have to provide productivity benefits such as reviewing code for bugs, assisting in editing written content, and making better data-driven decisions. But organisations and IT leaders face a dilemma: the balance between security and productivity.

Source code is the most frequently exposed type of sensitive data

The biggest risk the report found was users accidentally sharing sensitive information or intellectual property with AI apps. The data shows an organisation can expect around 660 daily prompts to ChatGPT for every 10,000 users, with source code being the most frequently type of sensitive data exposed, generating on average 158 incidents every month.

It is no surprise that Samsung decided to ban the use of generative AI apps by its employees (and develop its own AI applications) after users accidentally leaked sensitive data via ChatGPT. However, very few companies have the resources needed to follow Samsung and develop their own AI tools in-house, and need to find the trade-off between the security risks and the opportunities for the enterprise.

Even when users are not the source of the leak, the platform itself may have security flaws. At the end of March 2023, OpenAI, the company behind ChatGPT, provided details of a data breach caused by a bug in an open source library, which forced it to take the generative AI app temporarily offline. The data breach exposed payment-related information of some customers, and also allowed titles from some active user's chat history to be viewed.

Organisations and IT leaders face a dilemma: the balance between security and productivity.

Putting controls in place to safely enable generative AI applications

In response, organisations put in place specific controls around access ChatGPT and other generative AI applications with highly regulated industries, such as financial services and healthcare, preferring a more conservative approach with 18% of organisations enforcing a complete block on the use of generative AI apps. Technology companies in contrast, prefer a more nuanced approach based on DLP controls to detect if specific types of sensitive information such as source code and PPI is being posted to ChatGPT. Using granular DLP policies in combination with real-time user coaching around company policies and the risks of AI apps, will likely be the preferred approach as companies look to unleash the full potential of AI apps and mitigate the related risks.

Armed with these basic principles of cloud security, companies should be able to test and experiment with various AI app use cases with the confidence that their users are not unwittingly exposing proprietary corporate IP and data. □

For more information, please visit
www.netskope.com

Sponsors and exhibitors

Cloudflare | Strategic Sponsor

At Cloudflare, our mission is to help build a better Internet. Cloudflare's global cloud platform delivers a broad range of network services with integrated, purpose-built products to enterprises, making them more secure, enhancing the performance of their business-critical applications and eliminating the cost and complexity of managing individual network hardware. Cloudflare protects entire corporate networks, helps customers build Internet-scale applications efficiently, accelerate any website or Internet application, ward off DDoS attacks, and can help you on your journey to Zero Trust.

Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network with data centres in over 270 cities, which gets smarter with every request. As a result, customers like Allianz and Thomson Reuters and many more, are seeing significant improvements in performance, reliability and a decrease in attacks.

For more information, please visit www.cloudflare.com

Ontinue | Strategic Sponsor

Ontinue is on a mission to be the most trusted, 24/7, always-on security partner that empowers customers to embrace the future by operating more strategically and with less risk. Grounded in an intelligent, cloud-delivered SecOps platform, Ontinue offers superior protection that goes well beyond basic detection and response services.

Ontinue is the only MDR provider that leverages AI-driven automation, human expertise, and the Microsoft security platform to continuously assess and protect your environment and advance your security posture for digital transformation.

Continuous protection. Always-on prevention services. Nonstop SecOps. That's Ontinue.

Learn more at www.ontinue.com

Proofpoint | Strategic Sponsor

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber-attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

More information is available at www.proofpoint.com

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

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

eb-Qual | Education Seminar 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

Netskope | Education Seminar Sponsor

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organisations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimised access and zero trust security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivalled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organisational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com

Recorded Future | Education Seminar Sponsor

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

Learn more at recordedfuture.com

ReliaQuest | Education Seminar Sponsor

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, please visit www.reliaquest.com

Seclore | Education Seminar Sponsor

Seclore is a leading provider of data-centric security solutions, enabling organisations to control and protect their sensitive information wherever it goes, both within and outside of the organisation. Founded in 2008, the company is headquartered in United States with global offices in India, the United Kingdom, the Middle East, and Asia Pacific.

Seclore's data-centric security platform provides persistent, granular, and dynamic data-centric security for enterprises. Its flagship product, the Seclore Data-Centric Security Platform, empowers organisations to manage the usage and distribution of their sensitive information, regardless of its format or location. The platform seamlessly integrates with existing enterprise systems to provide persistent protection for files shared internally and externally, including emails, documents, and images.

The platform provides advanced data classification and rights management capabilities, enabling organisations to define policies and controls around who can access, edit, and share their sensitive information. The platform also provides audit trails and granular reporting capabilities, giving organisations visibility into the usage and distribution of their sensitive information.

Overall, Seclore's data-centric security solutions enable organisations to achieve their strategic objectives by protecting their sensitive information, enhancing their regulatory compliance posture, and improving their overall security posture.

For more information, please visit www.seclore.com

SUSE | Education Seminar Sponsor

SUSE is a global leader in innovative, reliable and secure enterprise-grade open source solutions, relied upon by more than 60% of the Fortune 500 to power their mission-critical workloads. We specialise in Business-critical Linux, Enterprise Container Management and Edge solutions, and collaborate with partners and communities to empower our customers to innovate everywhere – from the data centre, to the cloud, to the edge and beyond.

SUSE puts the 'open' back in open source, giving customers the agility to tackle innovation challenges today and the freedom to evolve their strategy and solutions tomorrow. The company employs more than 2,000 people globally. SUSE is listed on the Frankfurt Stock Exchange.

For more information, please visit www.suse.com

Menlo Security | Branding 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

SpyCloud | Branding Sponsor

SpyCloud is the leader in operationalising Cybercrime Analytics™ to protect businesses from cyber-attacks, prevent consumer fraud losses, and power cybercrime investigations.

Our focus is recapturing data from the deepest layers of the darknet, processing and analysing billions of cybercrime elements with our proprietary engine, and delivering automated solutions that thwart ransomware, account takeover, and online fraud.

For more information, please visit spycloud.com

AGENDA

08:00	Registration and networking break
08:50	Chairman's welcome
09:00	**Feeling secure or being secure? That is the question** **Philipp Grabher,** CISO, Canton Zurich • What do we understand when speaking about Security Theatre? • How can we address Security Theatre in our organisations? • Three concrete use-cases
09:20	**The new cyber-threat landscape Switzerland** **Sammie Walden,** Banking Expert DACH, Cloudflare • Cyber-threat landscape international and Switzerland • Why employee security training falls short • What can you do today to shut down one of the biggest attack vendors?
09:40	**What is the key to successfully engage on cybersecurity with executive and supervisory boards?** **Marcel Zumbühl,** CISO, Swiss Post • As CISO you meet with executive and supervisory boards, what do these boards expect from you? • How do you prepare to make these encounters a win for the cybersecurity of your company?
10:00	**Education Seminars | Session 1** **See pages 20 and 21 for more details** **Netskope** **Understanding the cloud-native threat landscape** **Paolo Passeri,** Principal Sales Engineer and Cyber Intelligence Specialist, Netskope **Seclore Technologies** **Know, protect and control your data** **Jasbir Singh,** Partner and Managing Director Europe, Seclore Technologies
10:40	Networking break
11:10	**EXECUTIVE PANEL DISCUSSION** **CISO panel discussion** **Juan Carlos Lopez Ruggiero,** CISO, Bouygues Energies & Services, (Moderator); **Fabian Wuest,** Head of Security, Bank CIC; **Philipp Grabher,** CISO, Canton Zurich; **Rebecca Gibergues,** Regional Director, France & Southern Europe, FS-ISAC; **Javier Gonzalez,** Senior Information Security Analyst, Roche • Learning from a recent cyber-attack on Swiss federal agencies and state-linked companies • Third-parties risks and threats for Switzerland • Overcoming the skills shortage in the Swiss market • Are CISOs under budget pressure? Is there pressure to outsource?
11:40	**Generative AI: What will change with the rise of GPT in cybersecurity?** **Theus Hossmann,** Director of Data Science, Ontinue, and **Nevena Lazarevic,** Security Technology Specialist, Microsoft • The impact of generative AI like GPT on security operations • Innovative use-cases beyond detection of malicious activity • The inevitable prospect of attackers using AI
12:00	**Break the attack chain: Strengthening defences and safeguarding people and data** **Tom Kretzschmar,** PreSales Engineer, Proofpoint • People are the primary targets of today's advanced attacks. But most organisations aren't centering their security strategy around their people • It is critical to align protection with risks targeting users throughout the attack chain – from initial compromise to lateral movement to impact • In this session, you will get an overview of the evolving threat landscape and proactive strategies you can implement to protect your organisation and break the attack chain at every stage

AGENDA

12:20	**Education Seminars | Session 2**	**See pages 20 and 21 for more details**
	Recorded Future **Unspoken words with immense criminal potential** **Joël Giger,** Intelligence Consultant, Recorded Future	**SUSE** **Importance of Zero Trust security in Kubernetes environments** **Holger Moenius,** NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE, and **Dieter Reuter,** Solutions Engineer, NeuVector, SUSE
13:00	Lunch and networking break	
14:00	**Shaping the future of Cyber TPRM by unlocking the potential of automation & digitalisation – lessons learned & best practices, case study**	
	Monika Atanasova, Global Head of Cyber TPRM, Raiffeisen Group – Switzerland • Main aspects of the Cyber TPRM programme • Security assessments workflow automation • Comprehensive Cyber TPRM profiling • Reporting: KPIs/KRIs cyber-risk cockpit • AI & threat intelligence	
14:20	**Human-machine teaming – AI in cybersecurity: Why the human element will always be indispensable in cybersecurity**	
	Thomas Wüst, Sales Lead Switzerland, SentinelOne • What the current AI trends mean for the hands-on practitioner • When velocity of innovation outpaces the capabilities of human intellect • The role of automation in the effective practice of securing our digital world	
14:40	**Bypassing multi-factor authentication (MFA) via phishing techniques**	
	Raj Sandhu, Ethical Hacker, Contracted to World Health Organisation, and **Manit Sahib,** Ethical Hacker, Contracted to Global Fund • Introduction to MFA bypass phishing techniques • Live demonstration of MFA bypass attack • Countermeasures and best practices • Conclusion of demo and presentation	
15:00	**Education Seminars | Session 3**	**See pages 20 and 21 for more details**
	CrowdStrike **Nowhere to hide – key insights into adversary tradecraft 2023** **Philipp Wachinger,** Sales Engineer, CrowdStrike	**ReliaQuest** **The future of security operations** **Andreas Grzess,** ReliaQuest
15:40	Networking break	
16:10	**EXECUTIVE PANEL DISCUSSION** **Crypto CISOs open questions**	
	Jeff Schiemann, CISO, SEBA Bank AG (Moderator); **Dominik Raub,** CISO, Crypto Finance AG **Mark Impini,** Head of Information Security, Swissquote • What is the impact of crypto fraud and crime? • What is our focus for the next 6–9 months? • What is 'a day in the life' of a crypto CISO like?	
16:40	Chairman's closing remarks	
16:50	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: 10:00–10:40

Netskope

SESSION 1
10:00–10:40

Understanding the cloud-native threat landscape

Paolo Passeri, Principal Sales Engineer and Cyber Intelligence Specialist, Netskope

The consolidated adoption of cloud services and the distribution of the workforce have led to a new paradigm in the threat landscape. Threat actors are capitalising on the fact that users access their data from any location and any device, even the personal ones, and also on the fact that they have progressively replaced human interactions with digital interactions. The attackers are launching evasive campaigns that exploit the trust on cloud services and collaboration tools, but they are also dusting off more traditional techniques such as sophisticated social engineering and SEO poisoning campaigns that exploit the unconditional trust on search engines and online tools in general.

Join this session to:

- Understand what are cloud-native threats and why they are more evasive than traditional web-based threats
- Understand the most common attack techniques
- Gain a comprehensive view of the current threat landscape
- Learn how to mitigate the risks with a security culture and a cloud-delivered security model

Seclore Technologies

SESSION 1
10:00–10:40

Know, protect and control your data

Jasbir Singh, Partner and Managing Director Europe, Seclore Technologies

In the fast-paced digital age, safeguarding digital assets has become more crucial than ever. This education seminar delves into the key topics essential for effective data protection. Jasbir Singh introduces an approach that revolves around understanding the data landscape within an organisation: The key to establishing a robust security framework and compliance includes to set labels to the documents, track and visualise the usage but always to protect & control confidential information.

By understanding the value of data, classifying it, and implementing usage controls based on classification labels, organisations can stay one step ahead of cyber-threats and safeguard their digital assets effectively. A safeguard that goes beyond the security perimeter of an organisation, allowing usage control updates and even remote revocation of shared data at any time. The seminar will also outline why classification can act as a first layer of security and the importance of dynamic watermarks to deter or detect data leakage.

In this session, you will learn:

- Why we need data-centric security in today's landscape
- How to know, protect and control sensitive information
- Example: An integration of data-centric security into the M365 landscape

Session 2: 12:20–13:00

Recorded Future

SESSION 2
12:20–13:00

Unspoken words with immense criminal potential

Joël Giger, Intelligence Consultant, Recorded Future

The recent boom in artificial intelligence capability has led to the creation of beautiful art and writing of essays within seconds, but threat actors have not stood idly by.

In this session, you will learn about:

- The rise of Voice-Cloning-as-a-Service offerings, a new form of commodified cybercrime
- Current use cases, future potential and possible impact for your organisation
- Not all is lost – old mitigation techniques work against new threats, at least for now

SUSE

SESSION 2
12:20–13:00

Importance of Zero Trust security in Kubernetes environments

Holger Moenius, NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE, and **Dieter Reuter,** Solutions Engineer, NeuVector, SUSE

Deep network visibility is the most critical part of run-time container security. In traditional perimeter-based security, administrators deploy firewalls to quarantine or block attacks before they reach the workload. Inspecting container network traffic reveals how an application communicates with other applications and it's the only place that can stop attacks before they reach the application or workload. SUSE NeuVector is the only 100% open source Zero Trust container security platform with continuous audits throughout the full lifecycle.

- Perform deep packet inspection (DPI)
- Real-time protection with the industry's only container firewall
- Monitor 'east-west' and 'north-south' container traffic
- Capture packets for debugging and threat investigation

Session 3: 15:00–15:40

CrowdStrike

SESSION 3
15:00–15:40

Nowhere to hide – key insights into adversary tradecraft 2023

Philipp Wachinger, Sales Engineer, CrowdStrike

Your ability to defeat advanced cyber-threats rests almost entirely on your understanding of the problem. And the problem isn't malware – it's the adversaries. While technologies and security products that organisations rely on are evolving, they struggle to keep up with the alarming pace at which adversary tooling and tradecraft is evolving. In all incidents observed by CrowdStrike's specialist teams, adversaries looked for ways to broaden their reach, optimise their tradecraft and deepen their impact on targets. To gain access, the intrusion attempts often started with an identity compromise or the exploitation of vulnerable software. In addition, adversaries have been quick to learn how to take advantage of common misconfigurations in public cloud services. To stop these adversaries, it is imperative that security teams understand how they operate.

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

ReliaQuest

SESSION 3
15:00–15:40

The future of security operations

Andreas Grzess, ReliaQuest

Security operations are changing rapidly and require a more holistic approach to security. Streamlining threat detection, investigation, and response is a good start in managing risk, but also important are utilising threat intelligence and digital risk protection, reviewing suspect employee-submitted emails via the abuse mailbox, and measuring your programme to communicate better with your stakeholders and service providers. Additionally, security operations will become more streamlined, with the automation of routine tasks and incident-response procedures becoming the norm. This session will help organisations achieve efficient and effective detection and response to security incidents.

Five benefits for delegates attending the session:

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

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.

Monika Atanasova

Global Head of Cyber TPRM, Raiffeisen Group – Switzerland

Monika is an experienced security strategist in highly regulated sectors, adept in designing and implementing Cyber TPRM strategies and programmes, with long-term international expertise in contractual negotiations and stakeholder management within electric mobility, cybersecurity and renewable energies.

Rebecca Gibergues

Regional Director, France & Southern Europe, FS-ISAC

Rebecca is a Regional Director with FS-ISAC (Financial Services ISAC). Based in Geneva, she is responsible for Switzerland, France and French-speaking markets. Rebecca has spent her career in financial technology, working for banks and asset managers in Europe and the US. Prior to moving to Switzerland in 2018, she was Head of Technology for a private bank in Monaco for eight years. Her fascination with cybersecurity started when she was assigned to the Monaco Government's working group for critical infrastructure cyber-policy. Rebecca holds a degree from the University of Edinburgh (Social Science/Economics), a post-graduate diploma in Digital Finance Law from the University of Geneva, and will be completing a CAS in Digital Forensics and Cyber Investigation with the Bern University of Applied Sciences in the coming months.

Joël Giger

Intelligence Consultant, Recorded Future

Joël Giger is an Intelligence Consultant at Recorded Future with over 10 years of experience in security and crime prevention. His journey in the field of 'Intelligence' began during his studies in Psychology and Informatics in Switzerland. Among other roles, he has worked for several years in fraud prevention and in the area of security vetting for the Swiss Army. Prior to joining Recorded Future, he spent several years in the field of open source intelligence in London, catering to clients from the financial sector.

Javier Gonzalez

Senior Information Security Analyst, Roche

Javier is a Senior Information Security Analyst at Roche. He is a seasoned information security professional with significant expertise in various aspects of security, including design, implementation, project management, and IT security tools management. He previously worked for Santander Tecnología, TSHA and SESCAM in IT security.

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.

Andreas Grzess

ReliaQuest

Andy Grzess is a cybersecurity expert with over 10 years of experience. He advises clients at the highest level on political, business, technical and architectural issues related to security. With innovative concepts, he helps to provide cyber-defence technologies and services for corporate customers. Andy has a passion for photography and travel.

Theus Hossmann

Director of Data Science, Ontinue

Theus Hossmann is Director of Data Science for Ontinue. He is responsible for everything around data, data science and AI, and leads Ontinue's team of expert data scientists and data engineers. Theus has published dozens of papers on applied AI and

machine learning for top-tier conferences and journals such as ACM and IEEE. Theus earned his PhD in Applied Machine Learning from ETH Zürich, Switzerland.

Marc Impini

Head of Information Security, Swissquote

As the Head of Information Security for Swissquote Bank, Marc oversees the protection of the bank's digital infrastructure. With a particular emphasis on crypto, he leads a specialised team, ensuring the security of clients' digital assets and contributing to the cutting-edge landscape of financial technology.

Prior to Swissquote, Marc worked for over 15 years in the security industry as an Engineer, Consultant and Auditor in the technology, humanitarian and financial sectors.

Tom Kretzschmar

PreSales Engineer, Proofpoint

Tom Kretzschmar is PreSales Engineer at Proofpoint where he focuses on topics like 'identity threat detection and respone', 'securing email – the number one threat vector' and on 'data loss prevention'. Before Proofpoint, he worked for VMware as a Networking & Security Specialist and for other companies like Infinigate, Networkers AG and was a CISO at a stock listed German real estate company. Tom Kretschmar has more than 20 years of experience in IT security.

Nevena Lazarevic

Security Technology Specialist, Microsoft

Nevena is a Technical Security Specialist at Microsoft bringing into play experience in both offensive and defensive security. She is passionate about leveraging her strong technical expertise, advisory skills, and her analytical and detail-oriented mindset to empower every organisation to be more secure, while ultimately transforming security into a business enabler. As a firm believer in continuous learning and growth, she remains at the forefront of the rapidly evolving cybersecurity landscape, constantly exploring new avenues and staying ahead of the game. Armed with Big 4 experience, Nevena excels at collaborating with cross-functional teams and effectively communicating complex technical concepts to non-technical stakeholders in a clear and concise manner.

Juan Carlos Lopez Ruggiero

CISO, 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. Juan Carlos owns a strong international and multicultural background, having lived and worked in North/South America, Europe, Africa and the Middle East.

Holger Moenius

NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE

As a Sales Director DACH, I have been fortunate enough to have worked with several startup companies in the network and security solutions space over the last 20 years. My experience in selling network and security solutions has given me a deep understanding of the industry, as well as a large network of contacts in various sectors, including financial services, insurance, pharmaceuticals, healthcare, telecommunications, and gaming. Throughout my career, I have collaborated with leading service integrators such as NTT Group, T-Systems, and Deloitte Digital Solutions to provide cutting-edge solutions to clients. This has enabled me to stay up-to-date with the latest trends and technologies in the industry and develop innovative solutions that meet the specific needs of my clients. I have previously deployed successful IT and security solutions for companies such as Cybersprint, Eperi, and Secure Islands, which has given me the confidence and expertise to take on new challenges in the industry. My ability to work with clients to understand their specific needs, and then provide them with the solutions that will best meet those needs, has been the key to my success in the industry. In my personal life, I have always been passionate about football and continue to play in a local senior league. Additionally, living close to the Alps has given me the opportunity to enjoy skiing during my free time. I believe that maintaining a work-life balance is essential for personal and professional growth, and I always make time for my hobbies and interests outside of work. Overall, my experience as a Sales Director DACH has given me a deep understanding of the network and security

solutions industry, and a large network of contacts in various sectors. I am passionate about providing innovative solutions that meet the specific needs of my clients and I look forward to continuing to work in this dynamic and challenging industry.

Paolo Passeri

Principal Sales Engineer and Cyber Intelligence Specialist, Netskope

Paolo Passeri, cyber-intelligence principal in Netskope, is a consultant, blogger, and security professional with over 20 years of experience in the information security arena. His current interests include cloud threats and advanced malware detection and mitigation. Paolo is also the founder and maintainer of hackmageddon.com, a collection of timelines and statistics of the main cyber-attacks that have occurred since 2011. The blog is considered a primary source of data and trends in the threat landscape across the Infosec community.

Dr Dominik Raub

CISO,
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.

Dieter Reuter

Solutions Engineer – NeuVector, SUSE

Dieter is an experienced container security specialist working as a Solutions Architect at SUSE NeuVector. He has 30+ years IT experience and began using containers back in 2014 when containers started to get popular with the Docker project. With further adoption of containers in Kubernetes, Rancher and OpenShift environments he was constantly working with all security-related aspects for using containers in datacentres.

Manit Sahib

Ethical Hacker

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

Raj Sandhu

Ethical Hacker

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

Jeff Schiemann

CISO,
SEBA Bank AG

As a board reporting CISO, with more than 20 years of experience in information security working for global companies, Jeff's focus is bringing consensus between Board members and Executive teams to implement solutions for technology & cyber-risks that unlocks competitive advantage. His daily goal is to limit the chance of material impact from cyber-threats upon customers, employees and assets of the bank. Empowering executives by advising, assessing and assuring good business decisions faster than the speed of digital transformation.

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.

Philipp Wachinger

Sales Engineer,
CrowdStrike

Philipp looks back on over 10 years of experience in the cybersecurity industry with a strong focus on customer success. Since 2022, he is supporting CrowdStrike as Sales Engineer for the DACH region. With his broad knowledge and understanding of Cloud- and IT-infrastructure, he is helping and consulting security professionals in the choice and set-up of security solutions that best fit their requirements and stop breaches from happening.

Sammie Walden

Banking Expert DACH,
Cloudflare

Sammie Walden is Cloudflare's Banking Expert in the DACH region. He joined Cloudflare in 2021. Over the last 18 years, Sammie Walden has held various expert roles for some of the world's largest technology providers, with the last five years dedicated exclusively to the banking sector. Sammie's background is in various IT technologies ranging from DC/Cloud technologies to cybersecurity, risk and compliance.

Fabian Wuest

Head of Security,
Bank CIC

Fabian Wuest is the Head of Security at Bank CIC (Switzerland) Ltd and, as such, responsible for a broad range of tasks within the 2nd line of defence. Bank CIC is a subsidiary of the French financial group Crédit Mutuel and is independently operating in Switzerland. Originally a certified Chartered Accountant working for one of the big four, he moved to the internal audit department of the Bank CIC in 2009 and successfully achieved certification as an IT auditor. Shortly after, he took over as head of the newly created 2nd line security team and built it up from scratch with a focus on the pivot between IT and business. Thanks to constantly growing requirements and regulation, he has not become bored even after 13 years in this function and is still learning.

Thomas Wüst

Sales Lead Switzerland,
SentinelOne

For over a year now, Thomas Wüst has led the SentinelOne Sales Team in Switzerland. Before joining SentinelOne, Thomas took care of Strategic Accounts at Tanium and BMC Software. Thomas is very experienced and passionate about leveraging disruptive technology to create tangible business outcome for his customers

Marcel Zumbühl

CISO,
Swiss Post

Marcel Zumbühl is Swiss Post Group's CISO. He is also a Certified Board Member of Hacknowledge SA, Swiss Post's Cybersecurity affiliate. Marcel is Co-President of the Information Security Society Switzerland (ISSS), Switzerland's largest network of cybersecurity professionals. He lectures at ETH Zurich on risk management and risk communication, and at the University of Lucerne on CISO organisations. Marcel holds a master's degree in Computer Science and is alumni of the University of Rochester-Bern, as well as the International Institute for Management Development (IMD). He has held positions in Accenture, Swisscom and Credit Suisse, working in Switzerland, Germany, Denmark and Greece. □

Data-centric security: Safeguarding your organisation's most valuable assets

In today's rapidly advancing digital era, data has become the lifeblood of organisations.

Seclore reports

Confidential information, such as intellectual property, financial records, and customer data, holds immense value and requires robust protection. As cyber-threats continue to evolve, the conventional perimeter-based security approach is no longer sufficient. In this landscape, data-centric security emerges as a crucial paradigm shift to ensure the safety and integrity of sensitive data. Let us explore how knowing, protecting, and controlling confidential data through data-centric security can fortify your organisation's defences.

1. Know your data: The power of classification

Knowing your data is the first step in data-centric security. Data classification involves identifying and categorising information based on its sensitivity, value, and risk level. By classifying data, organisations gain a clear understanding of their data landscape, allowing them to implement appropriate security measures for different data types.

Through proper data categorisation and classification, organisations can prioritise resources and focus on protecting high-value assets. For instance, sensitive data can be encrypted, and access controls can be tightened, while less critical data can have more relaxed security measures. This approach enables efficient resource allocation and minimises chances of overlooking critical security gaps.

2. Protecting confidential data: dynamic watermarking as the first security layer

Protecting data at its source is the next step and paramount to data-centric security. Dynamic watermarking can serve as an effective first security layer to safeguard confidential data from unauthorised access and distribution. This innovative technology involves embedding visible watermarks within documents, enabling organisations to track data usage throughout its lifecycle. Dynamic watermarks contain essential details such as the user's identity, date of access, and classification label. Even if a document is leaked or shared without authorisation, the watermark can reveal the source, discouraging potential data breaches.

Furthermore, data-centric security grants organisations greater control over their sensitive data, both within and beyond traditional network perimeters. Whether data is accessed, it provides continuous protection, mitigating the risk of data exposure.

3. The art of data control: Empowering security and collaboration

Finally, data-centric security emphasises granular control over data access. It ensures that only authorised personnel can view, edit, or share confidential information, minimising the risk of insider threats and accidental data leakage.

The dynamic control extends to data shared with external parties. With traditional security measures, once data leaves the organisation's network, maintaining control becomes challenging. Data-centric security, however, allows organisations to set specific access rights for external recipients. Consequently, sensitive information remains protected even when shared with partners, clients, or collaborators. An important benefit is that organisations can also revoke access to the shared data any time. This heightened level of data control fosters secure collaboration among remote teams, enabling seamless sharing of information without compromising data security.

Conclusion: Securing the foundation of your organisation

In the digital age, data-centric security emerges as a critical approach to protect the lifeblood of organisations – confidential data. Knowing, protecting, and controlling data empowers organisations to fortify their cybersecurity defences effectively.

Jasbir Singh, Managing Director of Seclore Europe, highlights the significance of data-centric security in the current IT landscape, stating, "The cloud, collaboration, and remote work have shattered traditional security parameters. Today, the data itself must become the new security parameter."

As cloud adoption, remote work, and collaboration continue to redefine the modern workplace, data-centric security proves to be the most relevant and robust approach. By embracing data-centric security, organisations can safeguard their most valuable assets and stay one step ahead in the ever-evolving cybersecurity landscape. Remember, in this digital era, your organisation's security begins and ends with the data itself. □

For more information, please visit
www.seclore.com

SECLORE

Know, protect and control your most sensitive digital assets wherever they go. Any user. Any device. Any app. Any cloud.

The Seclore platform takes a data-centric approach to security by giving you the ability to see, protect, and control your digital assets — wherever they go.

Know Your Risk

Seclore provides visibility into your enterprise's most sensitive assets.

Protect Your Sensitive Digital Assets

Enable seamless collaboration while protecting your digital assets.

Control How Your Digital Assets Are Used

Assign and revoke access and permissions to digital assets with ease.

The booming access broker business

It is important that corporate IT security professionals understand the tactics and objectives of cybercriminals and use technology and intelligence to assess the threat landscape and actively combat it.

Zeki Turedi reports

The rise in e-crime activity has been an ongoing issue for years and is a concern for businesses worldwide. The latest Threat Hunting Report 2023 from CrowdStrike once again makes it clear that the threat from the cyber-underworld is becoming ever greater: Our Counter Adversary Operations Team is now tracking over 200 actors, including several e-Crime groups. A key role in the modern e-crime threat landscape is played by so-called access brokers.

Access brokers steal access data and sell them to other e-crime actors in underground forums. They act as a kind of middleman in the criminal ecosystem and facilitate countless e-crime activities with their services, as buying access data saves many e-crime groups time and resources. Ransomware actors in particular are among the regular customers of access brokers. They often work closely with Big Game Hunting (BGH) ransomware operators who specialise in extorting large, high-profile corporate targets, or with partners in Ransomware-as-a-Service (RaaS) programmes. The ransomware actors use the purchased credentials to collect data from a target company, encrypt systems and extort large sums of ransom. To increase the pressure to pay, many e-crime actors also exfiltrate sensitive company data and threaten to publish it, increasing the pressure on victim companies to pay the sums demanded.

The strong increase in the number of observed advertisements in underground forums proves how the business of access brokers is flourishing. Last year, there was a 147% increase in access broker advertisements on the dark web. Access to companies from the education, technology, industry, manufacturing, financial services, telecommunications, government and healthcare sectors were particularly frequently offered for sale. The reason is obvious: they are particularly easy to sell, because identity-based cyber-attacks are the top attack vector. Identity-based attacks are now among the biggest threats to businesses and can be seen in nearly 80% of all cyber-attacks.

The price of credentials offered by access brokers depends on several factors, and asking prices vary significantly by industry, country and access broker. Generally, a higher price is paid for access with extended privileges, and the same is true for access to large companies with higher annual revenues or for listings from established access brokers. For some brokers, the sale takes place via an auction process in which they offer an immediate purchase price or by trying to trigger a veritable bidding war. Strikingly, in 2022, access brokers increasingly offered access in larger quantities, while other brokers remained faithful to the 'one-access one-auction' method. The sectors with the highest average asking prices for access included government, financial services, and industrial and engineering firms. In general, we have already observed prices for access data ranging from five-digit amounts to a value of 10 BTC.

The listings on offer on the deep and dark web provide an interesting snapshot of an increasingly lucrative component of the e-crime ecosystem, where both reputation and timing play an important role. There is undoubtedly an opportunistic element to access brokers' operations, such as the availability of exploitable vulnerabilities or the validity of stolen credentials that facilitate intrusion.

CrowdStrike Intelligence predicts that big game hunting will remain the dominant threat in the e-crime landscape and will continue to shift towards the use of RaaS networks, which will also continue to fuel the business of access brokers.

Threat actors are relentless. They are constantly evolving their techniques, adapting to current developments, regrouping and spawning their own business models. It is important that corporate IT security professionals understand the tactics and objectives of cybercriminals and use technology and intelligence to assess the threat landscape and actively combat it. Only then is there a chance to stay one step ahead of the sophisticated and fast adversaries. □

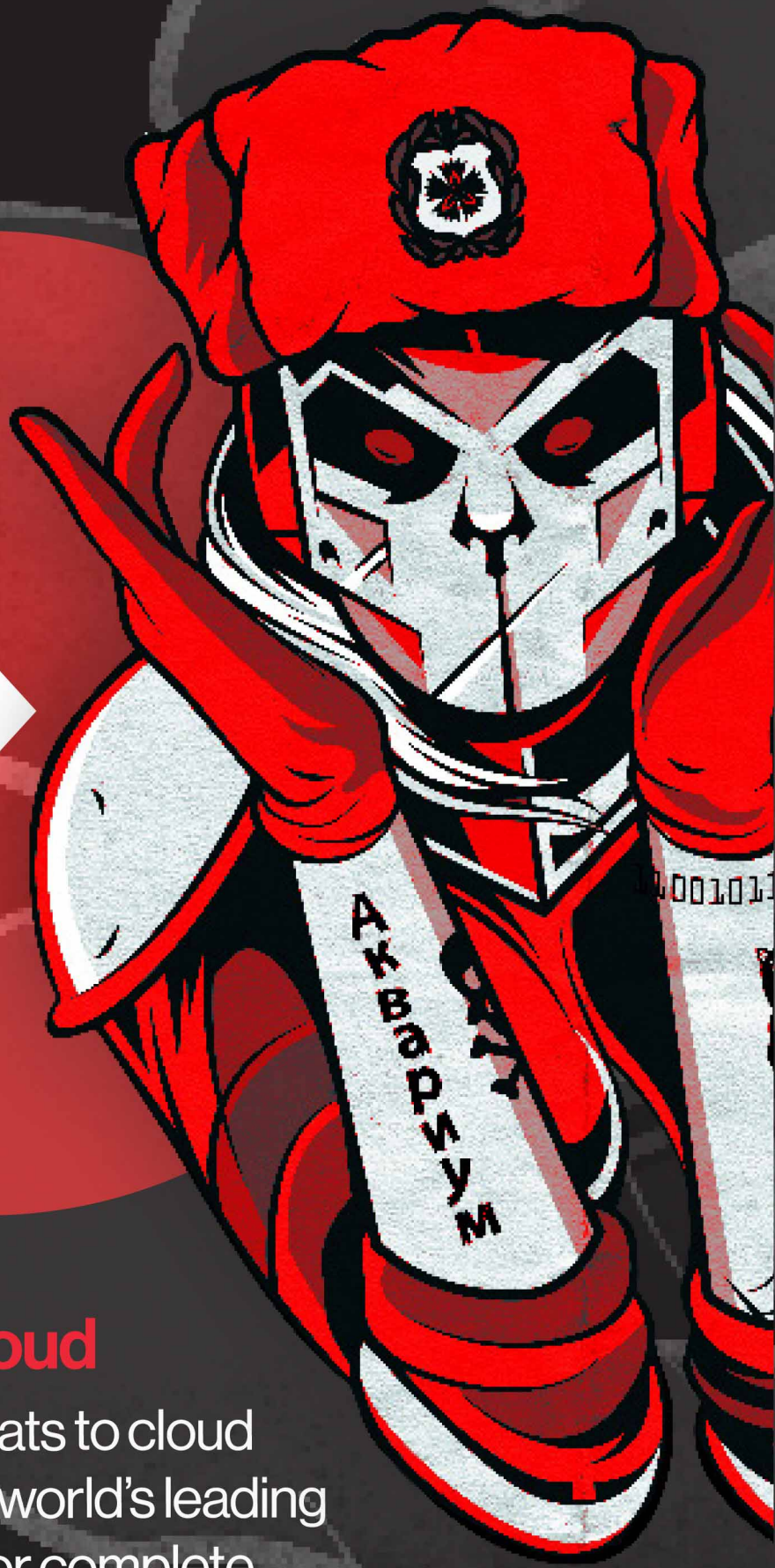
Sources: Global Threat Report 2023, Access Broker Blog Post

Zeki Turedi is Field CTO Europe at CrowdStrike.

For more information, please visit
www.crowdstrike.com

CROWDSTRIKE

CROWDSTRIKE



Protecting the Cloud

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

www.crowdstrike.com

Absicherung des digitalen Unternehmens mit Anwendungssicherheit

Seit über 30 Jahren vertrauen weltweit führenden Unternehmen auf SUSE, um ihre unternehmenskritischen Workloads sicher zu betreiben.

SUSE berichtet

Als ein weltweit führender Anbieter von innovativen und sicheren Open-Source-Lösungen für Unternehmen hat sich SUSE auf drei miteinander verbundene Produktfamilien spezialisiert: Geschäftskritisches Linux, Enterprise Container Management und Edge-Lösungen. Die Bereiche dieses sicheren Technologie-Stacks umfassen eine Reihe von Lösungen, die sowohl in der Cloud, als auch on-premises implementiert werden können, um die Sicherheit der wichtigsten Geschäftsanwendungen zu gewährleisten.

Mit Enterprise Linux, Cloud-nativer Transformation und Edge-Implementierungen verfügt SUSE über einen branchenführenden Ansatz für die Anwendungssicherheit auf allen Ebenen der Infrastruktur. Daher entscheiden sich Kunden in stark regulierten und Compliance-gesteuerten Umgebungen, die eine umfassende und robuste End-to-End-Sicherheitslösung benötigen, für SUSE Linux Enterprise. Kunden profitieren von den Vorteilen einer der weltweit sichersten Linux-Plattform für Unternehmen, die nach Common Criteria EAL 4+ zertifiziert ist, einschließlich einer zertifizierten Software-Supply-Chain. SUSE bietet das erste Enterprise-Linux, das Pakete nach dem anspruchsvollen Supply-Chain-Standard SLSA Level 4 (Supply-Chain Levels for Software Artifacts) liefern kann. Mit Rancher und SUSE NeuVector betreiben Kunden sicher ihre modernen Container-basierten Workloads und schützen so vertrauliche, finanzielle und geschäftskritische Daten vor hoch komplexen Angriffen.

Absicherung des gesamten Stacks

Bei einem ganzheitlichen Ansatz muss die Anwendungssicherheit in die gesamte Infrastruktur – den Stack – sowie in die Lieferketten-Pipelines integriert werden, die Anwendungen in die Produktion überführen.

Mit SUSE NeuVector, der marktführenden Container-Sicherheitsplattform für den gesamten Lebenszyklus, können Kunden gewährleisten, dass Anwendungen in der Pipeline sicher erstellt und implementiert werden und in der Produktion durch eine Zero-Trust-Sicherheitsarchitektur geschützt sind. Diese Architektur ermöglicht es NeuVector, dynamische Anwendungssicherheit zu bieten, die in der Container-Pipeline automatisiert wird. Einzigartig sind die tiefe Netzwerktransparenz und -segmentierung, eine Kubernetes Layer 7 Application Firewall, Data Loss Prevention (DLP) und Web Application Firewall (WAF). Zu den Audit- und Compliance-Funktionen gehören Risikoprofile, Schwachstellen-Scans, Compliance- und Konfigurations-Audits sowie Berichte zu Standards wie PCI, GDPR und NIST. NeuVector vereinfacht das Sicherheitsmanagement selbst für die größten, geografisch verteilten Kubernetes-Umgebungen. Dazu gehört die Kubernetes-Bereitstellung eines Public-Cloud-Anbieters mit bis zu tausend Knoten in einem einzigen Cluster ebenso wie Edge-Implementierungen mit Hunderten von Clustern in Edge-Umgebungen.

Laut Gartner* werden bis 2025 rund 45 Prozent der Unternehmen weltweit Angriffe auf ihre Software Lieferkette erlebt haben. SUSE sorgt mit einem sicheren, SLSA-konformen Open Build Service (OBS) für sichere Software-Lieferketten für seine Produkte und bietet ein geschütztes Ökosystem für Kunden, die kritische öffentliche und kommerzielle Infrastrukturen implementieren und betreiben.

Die Nachfrage nach einer Cloud-nativen Transformation wächst und damit auch der Bedarf an sicheren Container-Management-Lösungen. Rancher von SUSE unterstützt jede CNCF-zertifizierte Kubernetes-Distribution: On-Premises-Workloads und in Public-Cloud-Distributionen, einschließlich EKS, AKS und GKE, sowie in Edge-Umgebungen. Rancher ermöglicht überall sicheres Multi-Cluster-Kubernetes-Management mit konsistenten Abläufen, Workload-Management und Sicherheit auf Unternehmensniveau – vom Rechenzentrum über die Cloud bis hin zur Edge und darüber hinaus.

SUSE setzt einen starken Fokus auf Sicherheit und bietet ganzheitliche Lösungen zur Sicherung des gesamten Stacks – mit geschäftskritischem Linux, Enterprise Container Management und Edge Computing.

Ein aktuelles Beispiel für das Engagement von SUSE für Innovationen ist Confidential Computing, das es ermöglicht, ganze virtuelle Maschinen (VMs) verschlüsselt auszuführen und mit entsprechender Unterstützung durch das Betriebssystem, eine kryptografische Remote-Attestierung zu erreichen, selbst wenn die VM auf der anderen Seite des Globus läuft.

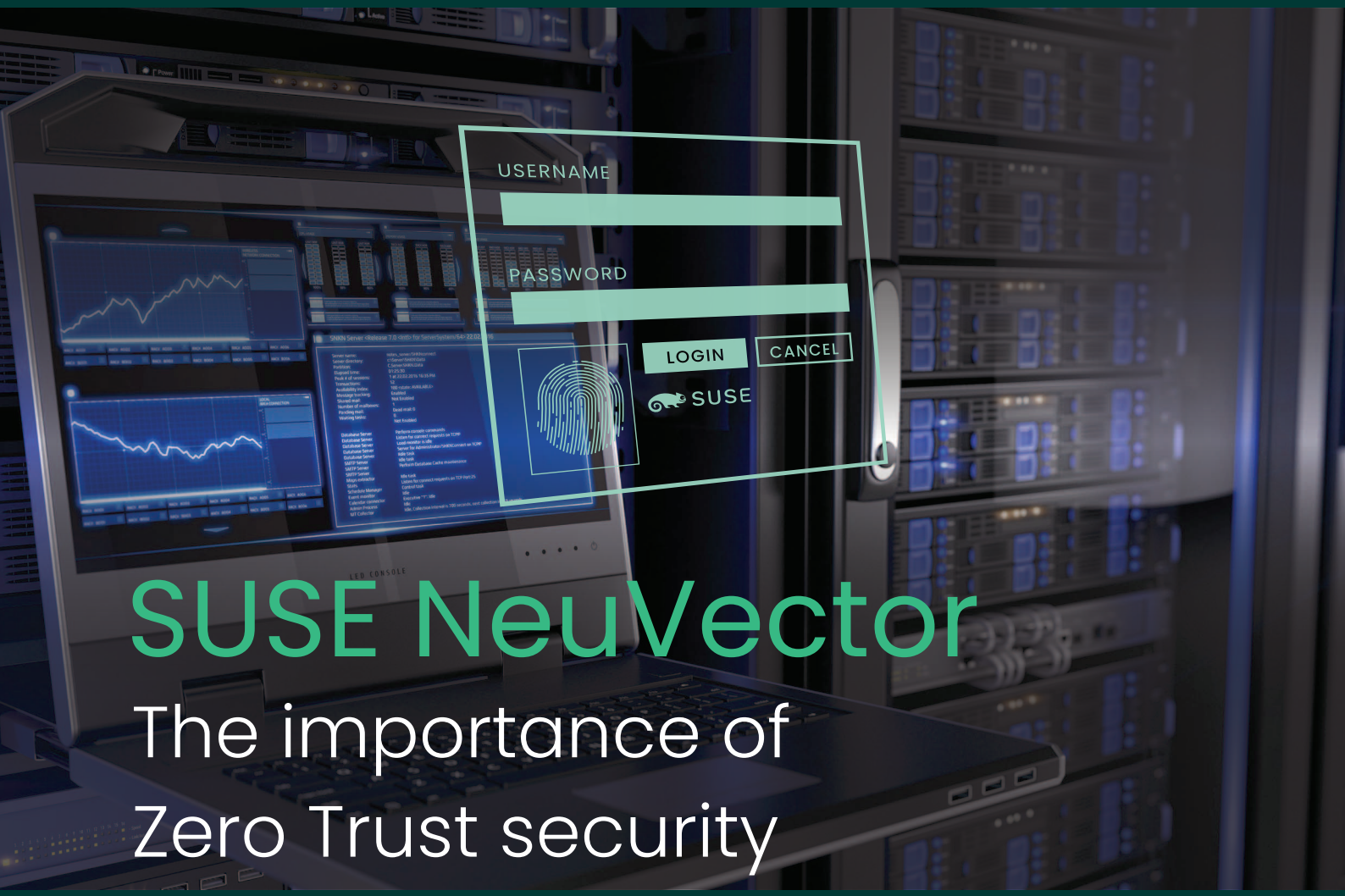
SUSE leistet Pionierarbeit bei Open Source-Innovationen und arbeitet eng mit branchenführenden Partnern wie Google, AMD, Microsoft und Nvidia zusammen, um Kunden auf jeder Plattform maximale Sicherheit zu bieten. □

* Gartner 7 Top Trends in Cybersecurity for 2022 Article, April 2022

Weitere Informationen unter
www.suse.com

SUSE

SUSE



SUSE NeuVector

The importance of Zero Trust security between Kubernetes environments

Scan QR code to learn more

Die wichtigsten Ransomware-Trends, auf die Sie 2023 achten sollten

Hier ist, was Sie über die Zukunft von Ransomware.

Jonathan Echavarria berichtet

Ransomware-Angriffe haben in diesem Jahr einen steilen Anstieg erlebt, 13 % mehr als im Jahr 2021, und es ist nicht zu erwarten, dass sich dieser Trend in absehbarer Zeit verlangsamen wird. Hier ist, was Sie über die Zukunft von Ransomware und Mindset-Strategien wissen müssen, die Sie anwenden können, um Ihre Chancen zu verbessern sich effektiv gegen Ransomwareangriffe zu schützen.

Ransomware-Gruppen und die Entwicklung des Ransomware-Marktes

Ransomwareangriffe haben sich von der einfachen Verschlüsselung von Geschäftsdaten zu einem zusätzlichen Fokus auf die Datenexfiltration verlagert. Es gibt ein paar gängige Möglichkeiten, wie Angreifer von diesen gestohlenen Daten profitieren können: Erpressung, bei der ein Angreifer sagt: „Ich habe Ihre Kundenliste gestohlen und in meine Infrastruktur exfiltriert. Zahlen Sie mir 200.000 Dollar, oder ich verrate es." Der andere Weg wäre, Ihre exfiltrierten Daten direkt zu verkaufen, z.B. indem Sie einen Benutzernamen- und Passwort-Dump in einem Darknet-Forum zum Verkauf anbieten.

Doppelte Erpressungsangriffe, bei denen Bedrohungsakteure sowohl Ihre Daten gegen Lösegeld einbehalten, als auch damit drohen, sie online zu veröffentlichen, sind seit ihrer Einführung im Jahr 2019 zu einem großen Trend geworden. Das Threat-Intelligence-Unternehmen Digital Shadows deckte 11 neue Erpressergruppen auf, die sich ausschließlich auf Datenlecks im Jahr 2022 konzentrierten .

Um nicht ins Rampenlicht zu treten, können berüchtigte Ransomware-Gruppen (denken Sie an REvil, Conti usw.) einfach ihre Namen ändern. Laut KrebsonSecurity ist „Neuerfindung eine grundlegende Überlebensfähigkeit im Geschäft mit Cyberkriminalität."
Schützen Sie die Webpräsenz Ihres Unternehmens mit ReliaQuest Digital Risk Protection >

Ransomware-Abwehrstrategien für 2023

Die Rekrutierung für Ransomware-Gruppen verlangsamt sich nicht. Um mit der sich entwickelnden Verteidigungslandschaft Schritt zu halten, stellen diese Gruppen ständig neue Entwickler und Pentester ein.
Auf der Verteidigungsseite gibt es einige Strategien, die dazu beitragen können, das mit Ransomware-Angriffen verbundene Risiko zu mindern.

Annahme einer Mitigations-Denkweise

Gehen Sie immer davon aus, dass ein Verstoß möglich ist, unabhängig von Ihrem Schutzniveau. Man sollte sich immer um Prävention bemühen, aber Angriffserkennung und -eindämmung können eine effektivere Ressourcennutzung sein. Für diese Strategie gibt es eine Reihe von Taktiken, die Sie anwenden sollten:

- Betrachten Sie jede Phase der Infektion aus der Angriffsperspektive.
- Führen Sie regelmäßige Tabletops mit verschiedenen Teilen der Organisation durch.
- Haben Sie ein Spielbuch parat für Zwischenfälle und führen Sie regelmäßige Übungen dazu durch.
- Bilden Sie ein fundiertes Verständnis über die Basislinien Ihrer Unt*ernehmensinfrastruktur*, um Anomalien schnell zu erkennen und einzudämmen.

Verteidigung in der Tiefe

Um einen umfassenden Schutz zu erreichen, sollten Sie eine mehrschichtige Verteidigungsstrategie haben, einschließlich mehrschichtiger Erkennungspipelines, Sicherheitsmechanismen und Kontrollen durch das Netzwerk.

Layered Detection Pipelines sind die logischen Prozesse, die Sie einsetzen, um Ereignisse in Ihrer Umgebung zu erfassen, zu verarbeiten, zu analysieren und darauf zu reagieren. Das kann Ihnen helfen, Prioritäten zu setzen, auf welche Erkennungspipelines Sie sich konzentrieren müssen, zum Beispiel:

- Prozessprotokollierung
- Protokollierung der Netzwerkkommunikation
- Authentifizierungsprotokollierung

Als nächstes sprechen wir über Sicherheitskontrollen. Aktive Kontrollen wie Firewalls und E-Mail-Gateways können Ihnen helfen, Risiken innerhalb der Umgebung zu mindern. Andere Kontrollen wie EDR können Ihre Erkennungspipelines aktiver bedienen.

Schließlich umfasst die Tiefenverteidigung auch ein mehrschichtiges Sicherheitsdesign. Die Einführung neuer Technologien kann neue Angriffspfade in das Netzwerk einführen. Diese Pfade sollten berücksichtigt werden. Viele Sicherheitsteams gehen dieses Problem mit einem „Zero Trust"-Ansatz an.

Investition in eine Security Operations Platform.

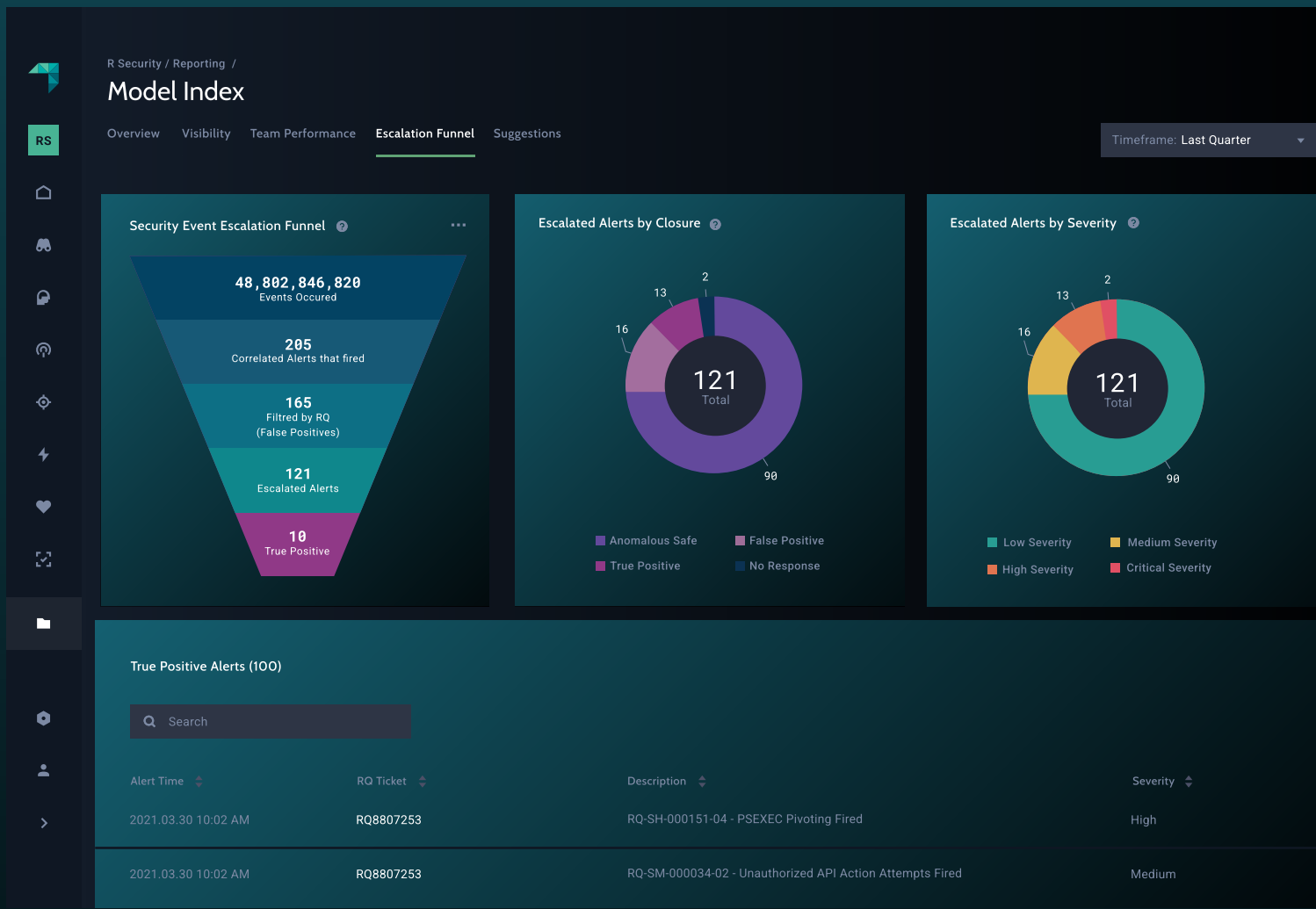
Beim Schutz vor Ransomware sind Transparenz und Flexibilität entscheidend. Die SOC-Plattform von ReliaQuest, GreyMatter, unterstützt Ihr Sicherheitsteam in jeder Phase des Ransomware-Lebenszyklus.

- *Ersteingabe stoppen.* GreyMatter automatisiert die Analyse von Phishing-Vorfällen, die Ihr E-Mail-Sicherheits-Gateway passieren.
- *Stoppen Sie die Ausbreitung.* GreyMatter bewertet den Zustand Ihres EDR und bestimmt, welche Schritte Sie unternehmen sollten, um Ihre Erkennungsinhalte am effektivsten an die jeweilige Bedrohungslandschaft und korrespondierende TTPs abzustimmen.
- *Antwort automatisieren.* GreyMatter kann bösartige E-Mail-Domains automatisch blockieren, Hashes verbieten, Dateien löschen oder Hosts unter Quarantäne stellen.
- *Ständige Überwachung.* ReliaQuest bietet eine einheitliche Ansicht, um Bedrohungen aus Ihrer gesamten Umgebung (On-premises, Cloud, und Hyrbid) sofort und umfassend zu erkennen und darauf zu reagieren.

Erfahren Sie mehr über ReliaQuest GreyMatter für Ransomware >

ReliaQuest exists to
Make Security Possible

ReliaQuest GreyMatter is a security operations platform built on an open XDR architecture and designed to help security teams increase visibility, reduce complexity, and manage risk across their security tools, including on-premises, clouds, networks, and endpoints.



RELIAQUEST®

RedLine Stealer: Informationen zur Malware und den illegalen Handel mit Identitätsdaten im Web

Die wachsende Bedrohung für Organisationen: Angriffe auf Zugangsdaten und Datenlecks.

Recorded Future berichtet

Mit der ständigen Erweiterung der Angriffsfläche durch Bedrohungsakteure und der anhaltenden Berichterstattung über Cloud-Systeme und Angriffe auf Lieferketten eröffnen sich immer mehr Möglichkeiten für Angreifer, in schützenswerte IT-Assets Ihrer Organisation einzudringen. Die Überprüfung von Benutzeridentitäten und die Kontrolle des Zugriffs auf sensible Daten sind von entscheidender Bedeutung für die Sicherheit Ihrer Organisation, können jedoch schwierig zu erreichen sein. Gestohlene Unternehmensdaten wie Benutzeranmeldeinformationen landen regelmäßig auf Paste-Seiten und im Darknet und ermöglichen es Cyberkriminellen, die Daten zu erwerben und möglicherweise für den Zugriff auf das Netzwerk oder die Systeme einer Organisation zu verwenden. Angesichts des wachsenden Ansturms von Angriffen und der kontinuierlichen Überwachung des Darknets nach sensiblen Informationen sind Organisationen oft nicht in der Lage, proaktiv zu handeln. Dadurch bleiben sie finanziellen, rechtlichen und reputativen Konsequenzen ausgesetzt.

Die Bedrohung durch gestohlene Identitätsdaten und raffinierte Angriffe

Das Problem beschränkt sich dabei nicht nur auf die schiere Menge an Angriffen, sondern auch auf die wachsende Raffinesse der Angriffe, wobei fortschrittliche Täuschungsmanöver die Erkennung erheblich erschweren. Bedrohungsakteure finden immer wieder neue Möglichkeiten, Zugangsdaten zu erfassen und im Darknet an den Meistbietenden zu verkaufen. Aus diesem Grund benötigen Organisationen eine größere Transparenz über die Taktiken von Bedrohungsakteuren zum Erfassen von Zugangsdaten und eine Echtzeitüberwachung von Datenlecks aus allen Quellen, einschließlich krimineller und nur auf Einladung zugänglicher Webseiten.

RedLine Stealer: Eine Infostealer-Malware zur Erfassung von Identitätsdaten

Die Recorded Future Analystengruppe Insikt Group hat vor Kurzem einen Bericht über RedLine Stealer veröffentlicht, eine Infostealer-Malware, die seit ihrer ersten Veröffentlichung Anfang 2020 eine wichtige Quelle für Identitätsdaten ist, die auf Online-Kriminellenforen vermarktet und verkauft werden. Es ist nur ein Beispiel von vielen Infostealern, die die Insikt Group im letzten Jahr analysiert hat und die Bedrohungsakteure derzeit verwenden, um Zugriff auf kompromittierte Identitäten zu erhalten und betrügerische Aktivitäten durchzuführen.

Verbreitung und Funktionsweise von RedLine Stealer

RedLine Stealer wird häufig über Phishing-E-Mails sowie über Nachrichten in sozialen Medien verbreitet. Die Köder der Phishing-E-Mails sind oft topaktuell oder betreffen Ereignisse wie COVID-19-Informationen oder Informationen zum Krieg in der Ukraine. RedLine stiehlt dann die Daten des Opfers, einschließlich Benutzernamen, Passwörter, Cookies, Zahlungskarteninformationen und Informationen zu Kryptowährungswallets, die leicht durch direkte Verwendung oder Verkauf an andere Kriminelle zu Geld gemacht werden können. Der Verkauf dieser gestohlenen Daten erfolgt häufig über Untergrundmärkte, die für Kriminelle, die Identitätsdiebstahl betreiben, eine Art Ein-Stop-Shop bieten.

Maßnahmen zur Prävention von Identitätsdiebstahl

Um Identitätsdiebstahl durch schädliche Tools wie RedLine Stealer zu erkennen und zu verhindern, benötigen Organisationen Unterstützung bei der Überwachung verschiedener Webquellen nach relevanten Bedrohungen, die auf sie abzielen. Eine effektive Lösung besteht darin, Identitätsinformationen automatisch zu sammeln, zu korrelieren und zu priorisieren, um die Zeit, die für die Erkennung, Priorisierung und Reaktion auf reale Risiken erforderlich ist, drastisch zu reduzieren.

Für Organisationen, die proaktiv Identitätsdiebstahl und Datenlecks bei Zugangsdaten verhindern möchten, bietet Recorded Future Zugang zu handlungsfähiger, Echtzeit- und automatisierter Identity Intelligence, unterstützt von der Insikt Group, unserem globalen Team von Threat-Intelligence-Experten, die Zugang zu geschlossenen, internen Foren im Open, Deep und Dark Web identifizieren und aufrechterhalten. □

Wenn Sie mehr erfahren möchten, laden Sie den vollständigen Bericht über RedLine Stealer herunter und fordern Sie eine Demo des Identity Intelligence-Moduls an.

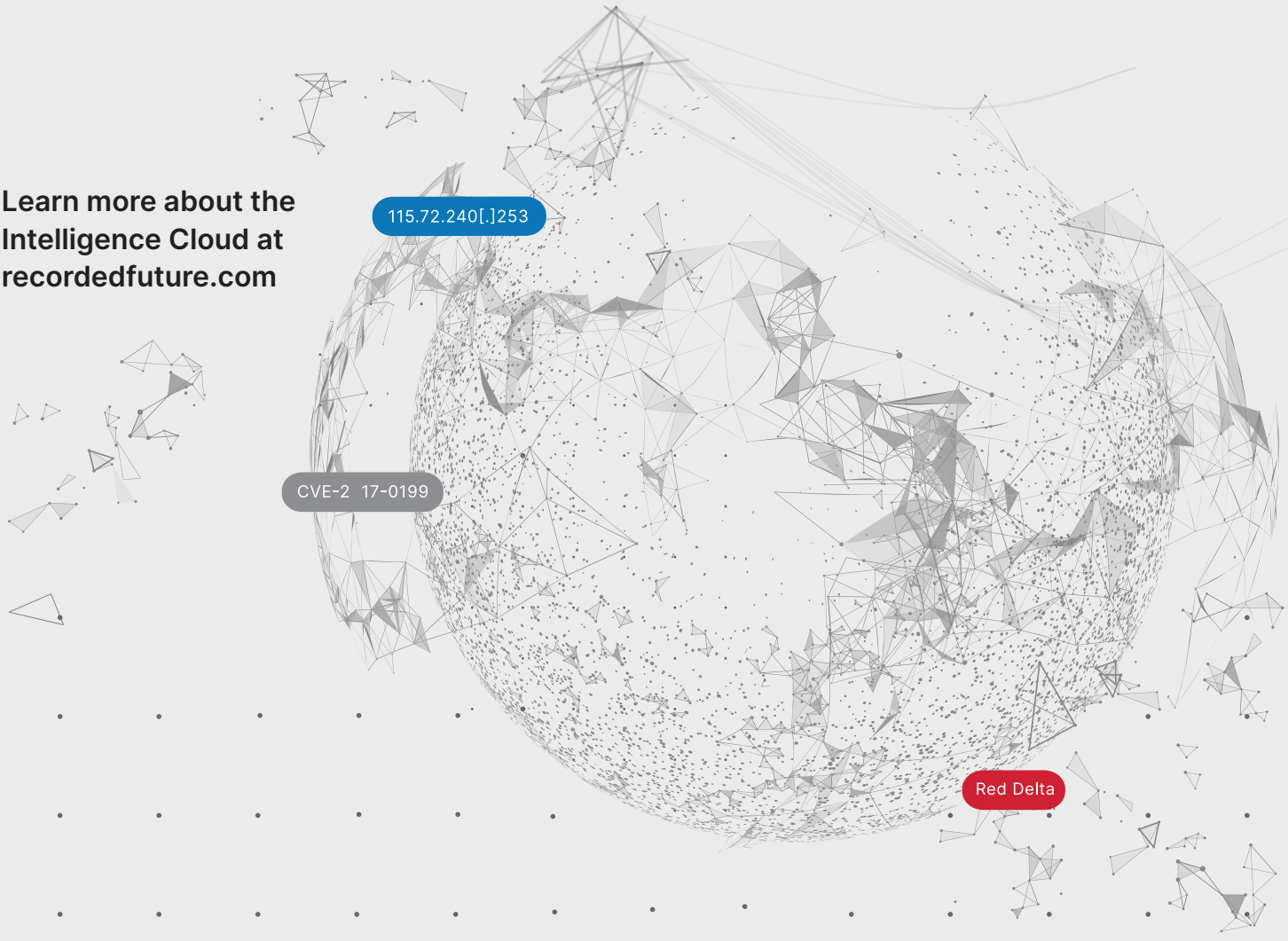
Weitere Informationen unter
www.recordedfuture.com

Recorded Future®

Securing Our World With Intelligence

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

Learn more about the Intelligence Cloud at recordedfuture.com



e-Crime & Cybersecurity Germany 2024

"I found the day very interesting, as always. My conclusion would then be: e-Crime offers a great mix of lectures, from information on the subject of threat risks to the best products to protect yourself. Networking opportunities are of course always the best. The lecture from the BSI was particularly interesting from a different perspective, instead of always dealing with day-to-day business to get busy."
Head of Development

"As always, the e-Crime Congress in Frankfurt was a very good event, with very good speakers and lectures, and an excellent supporting programme (industrial exhibition and catering) – I really liked it. Keep it up!"
Business Information Security Officer

"Many thanks for the valuable and very well organised event. For me personally, the following lectures were the most valuable:
- Forescout: 'Why automated visibility...'
- Client: 'Why threat intel for your company too...'
- ReliaQuest: 'The future of security operations...'"
Leader CERT Team

"Many thanks. I really liked the event again and, although AKJ Associates has held excellent digital events in recent years, the face-to-face format is better suited for networking in addition to dealing with the content of the topics. I was able to have very good conversations again. It's nice that the BSI was represented with its annual report and the other contributions also gave me plenty of impetus for the challenges of 2023."
CISO

2023 sponsors included:

Strategic Sponsors

BeyondTrust
corelight
LastPass
MANDIANT NOW PART OF Google Cloud
proofpoint.
SECLORE

Education Seminar Sponsors

CROWDSTRIKE
FORESCOUT
RAPID7
RELIAQUEST

Networking Sponsor

mnemonic

Branding Sponsor

RED BUTTON

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

Thank you to all our sponsors

Strategic Sponsors

Education Seminar Sponsors

Branding Sponsors