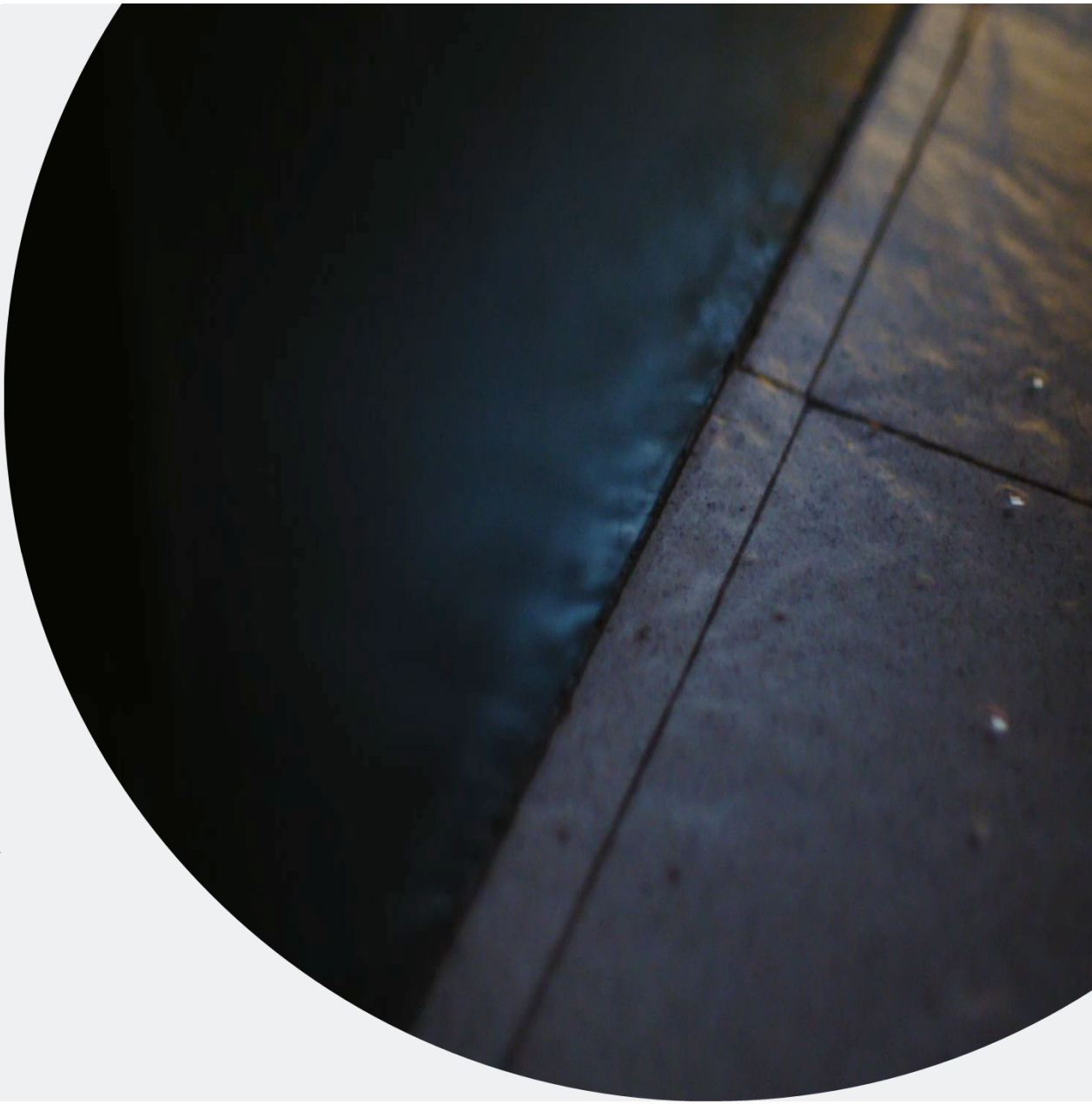

ZURICH
Meet tomorrow prepared.
With Zurich Resilience Solutions


wie

ZURICH

Vorsprung durch Prävention

Strategien gegen die Cyberbedrohungen von morgen



Datum: 09.04.2024
Referent: Michael Guiao – Senior Cyber Risk Engineer

Meet tomorrow prepared.

ZURICH

Agenda

1 | Herausforderungen in der Cyber-Sicherheit

2 | Strategien zur Risikominderung

3 | Cyber Risk Quantification (und KI)

Meet tomorrow prepared.

Introduction

Die digitale Welt, in der wir uns heute bewegen, ist geprägt von einer ständig wachsenden Zahl an Cyber-Bedrohungen. Von ausgeklügelten Ransomware-Angriffen bis hin zu raffinierten Phishing-Versuchen – die Komplexität dieser Gefahren nimmt stetig zu. Doch anstatt nur zu reagieren, müssen wir proaktiv handeln, um Organisationen und Systeme effektiv zu schützen.

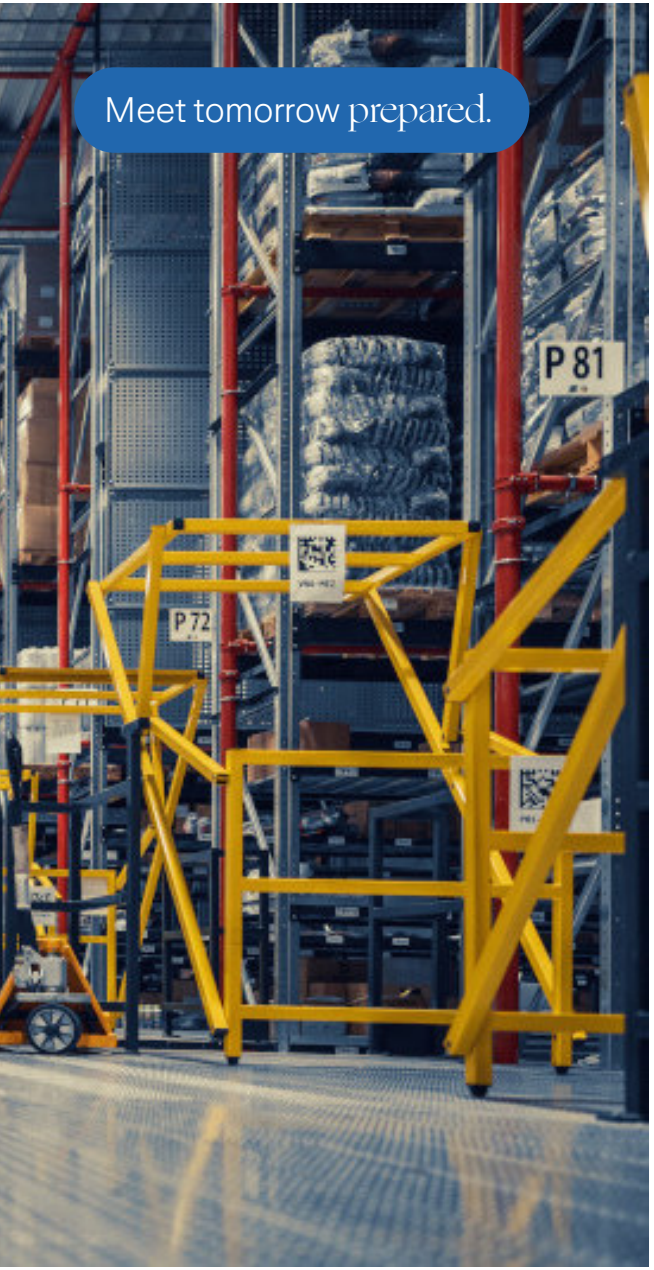
Meet tomorrow prepared.

ZURICH

Bundesamt
für Sicherheit in der
Informationstechnik

"Insgesamt zeigte sich im aktuellen Berichtszeitraum eine angespannte bis kritische Lage. Die Bedrohung im Cyberraum ist damit so hoch wie nie zuvor. […]"

BSI, "Die Lage der IT-Sicherheit in Deutschland 2023"
November, 2023



Die Komplikation:
Anonymisierter Fall eines Cyberangriffs

ZURICH

- **12. / 13. Februar 2024**: Cyberangriff trifft [redacted] Produktions- und IT-Systeme werden abgeschaltet (SecurityWeek) (BleepingComputer). Einrichtung einer Task Force aus Sicherheitsexperten (SecurityWeek).

- **14. Februar 2024**: Produktionsstillstand mit unklarem Zeitplan für die Wiederaufnahme (BleepingComputer).

- **15. März 2024**: [redacted] kündigt an, die Veröffentlichung des Jahresfinanzberichts für 2023 aufgrund des Cyberangriffs zu verschieben. Die Veröffentlichung, ursprünglich für den 28. März 2024 geplant, wird wahrscheinlich erst nach dem 30. April 2024 erfolgen (EQS News).

- **Analystenbewertungen und Aktienkursentwicklung**: Seit dem 16. Februar 2024 herrscht eine negative Analystenhaltung. Der Aktienkurs erlebte einen Rückgang der relativen 4-Wochen-Performance um ca. -5% (finanzen.net).

- **Finanzielle Auswirkungen**: [*Unabhängig vom Angriff*] Für das Jahr 2023 wird ein Nettoverlust von -87 Millionen Euro prognostiziert, mit einer weiteren negativen Prognose für 2024 bei -27 Millionen Euro. (MarketScreener).

ZURICH

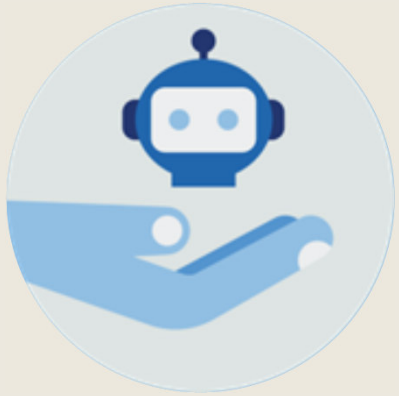
Herausforderungen in der Cyber-Sicherheit

Vier Treiber im Cyber-Umfeld und 12 daraus resultierende Bedrohungsszenarien wurden als relevant identifiziert.

Fortschreitende **Professionalisierung** organisierter Cybercrime-Kartelle.

Zunehmende **geopolitische Spannungen und Konflikte** zwischen regionalen Mächten.

Wachsender **Mangel an qualifiziertem Personal** zur Bekämpfung der Bedrohungen.



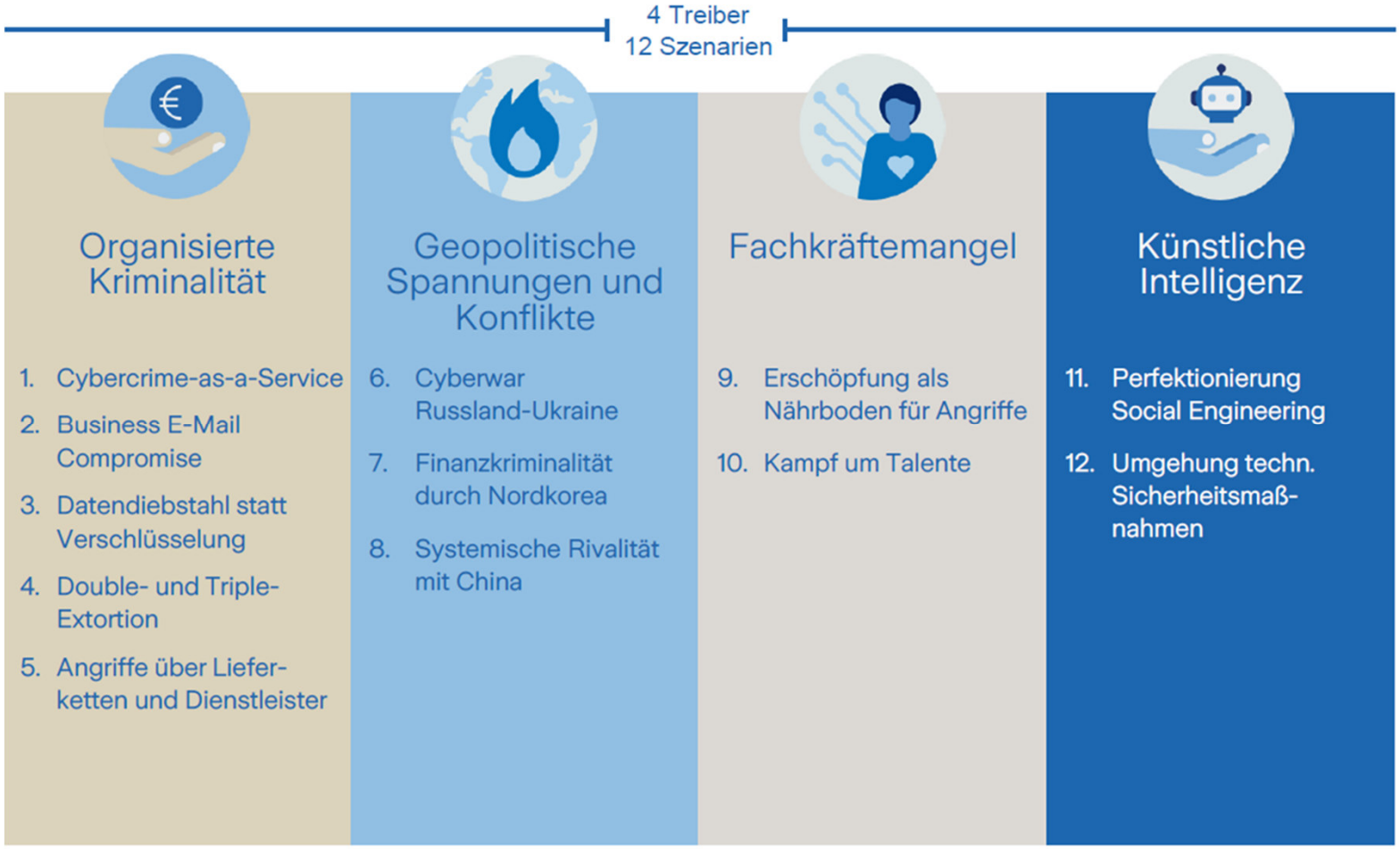
Rasante Weiterentwicklung von Technologien im Bereich der **künstlichen Intelligenz**.

Meet tomorrow prepared.

ZURICH

Bedrohungslandschaft

Treiber und Szenarien



ZURICH

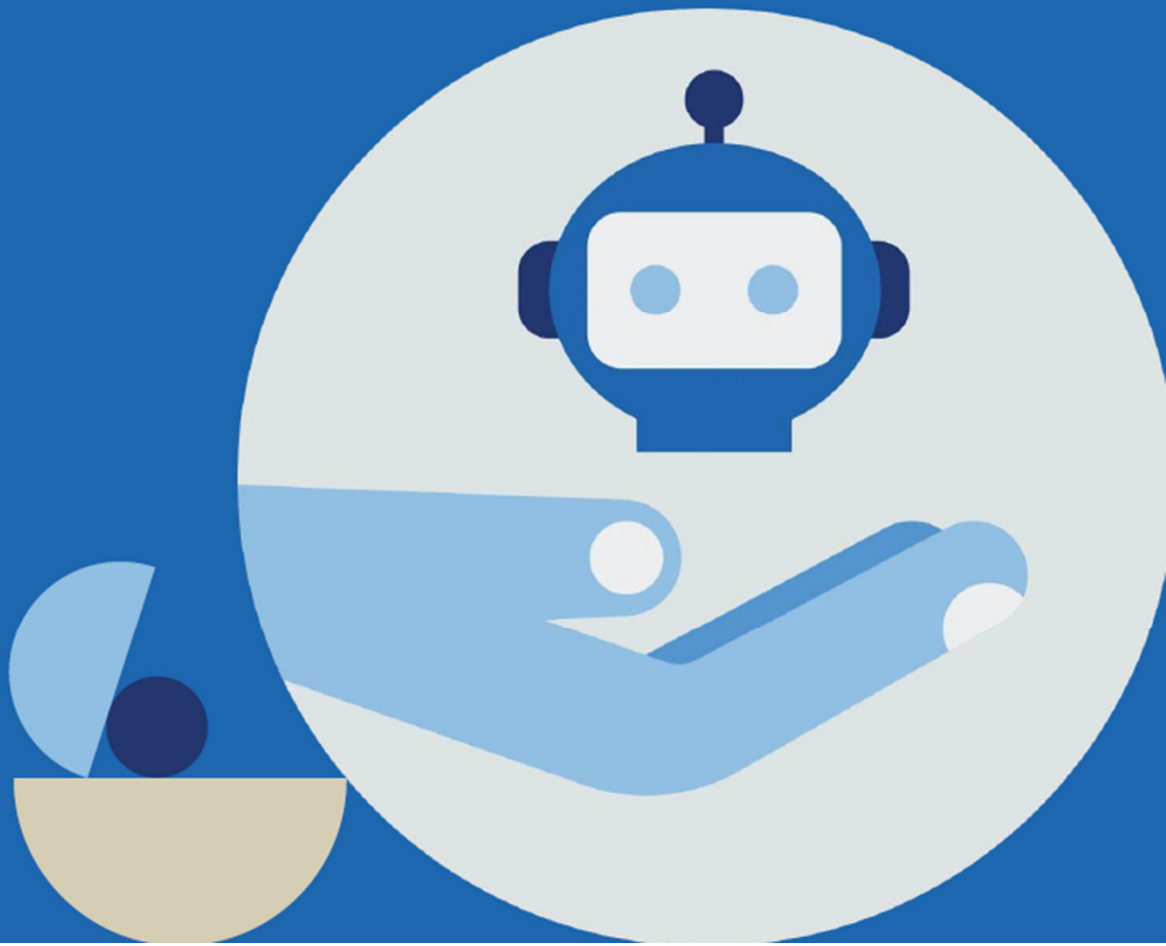
Organisierte Kriminalität

1. Cybercrime-as-a-Service
2. Business E-Mail Compromise
3. Datendiebstahl statt Verschlüsselung
4. Double- und Triple-Extortion
5. Angriffe über Lieferketten und Dienstleistern

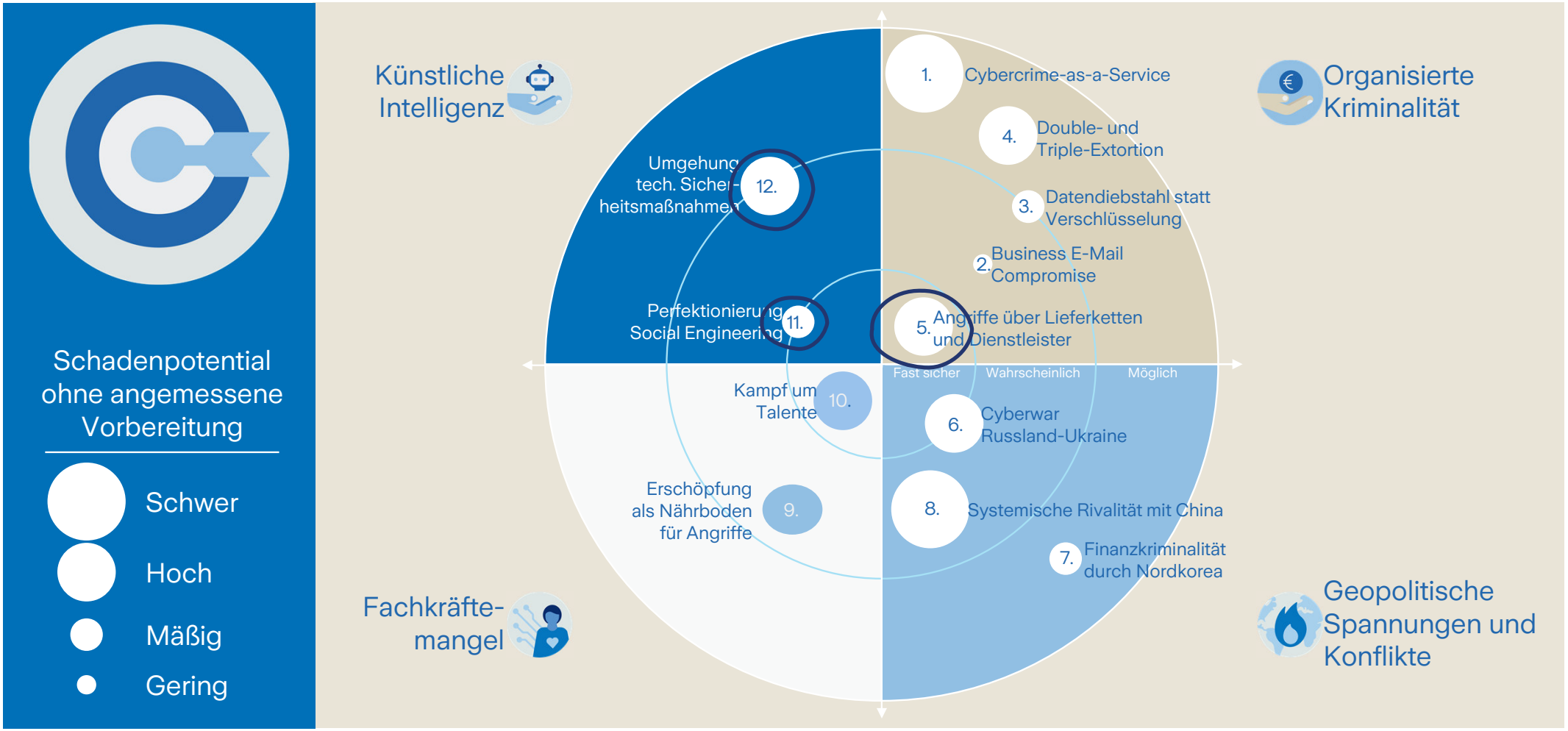
ZURICH

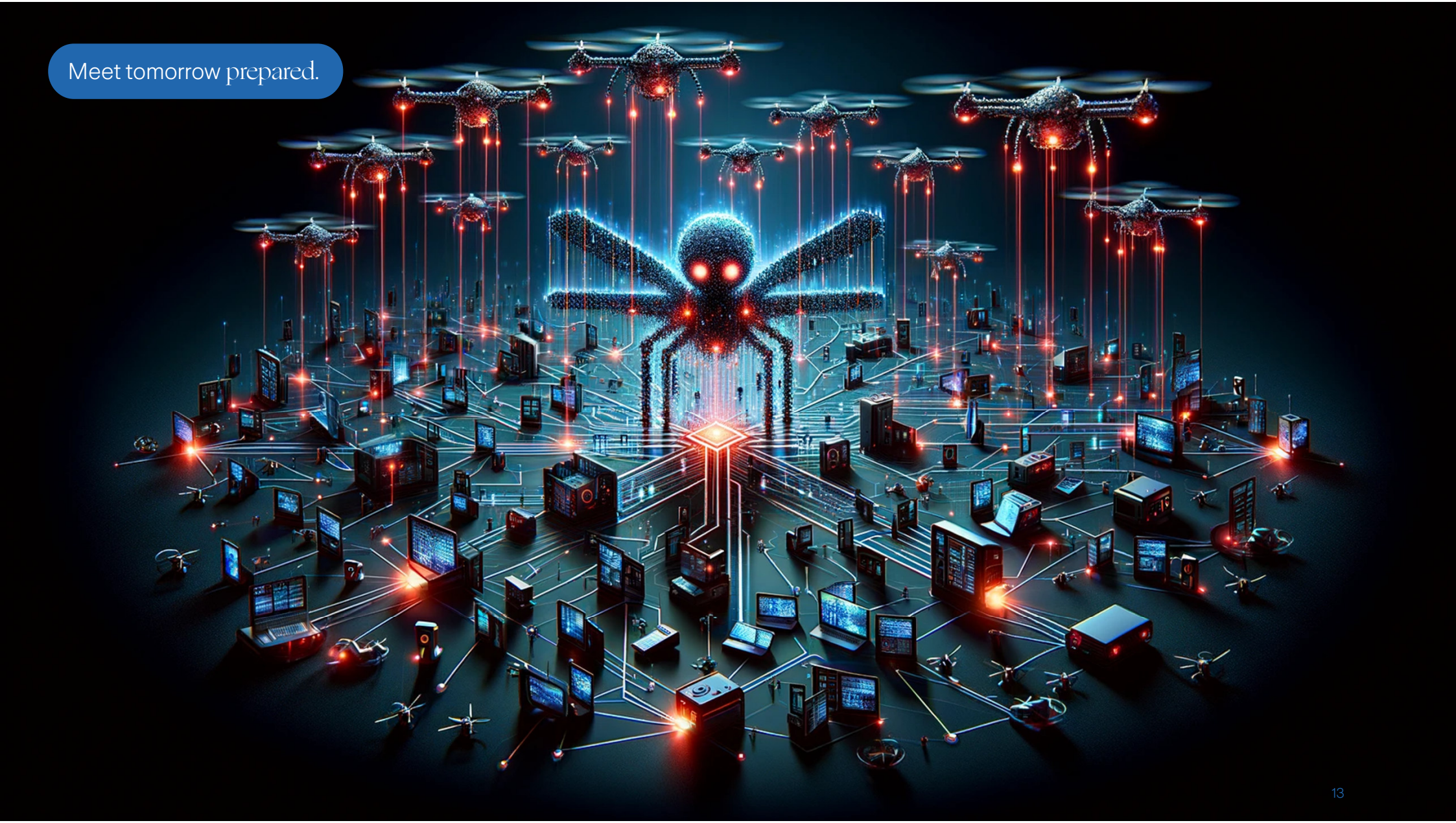
Künstliche Intelligenz

11. Perfektionierung Social Engineering
12. Umgehung technischer Sicherheitsmaßnahmen



ZURICH

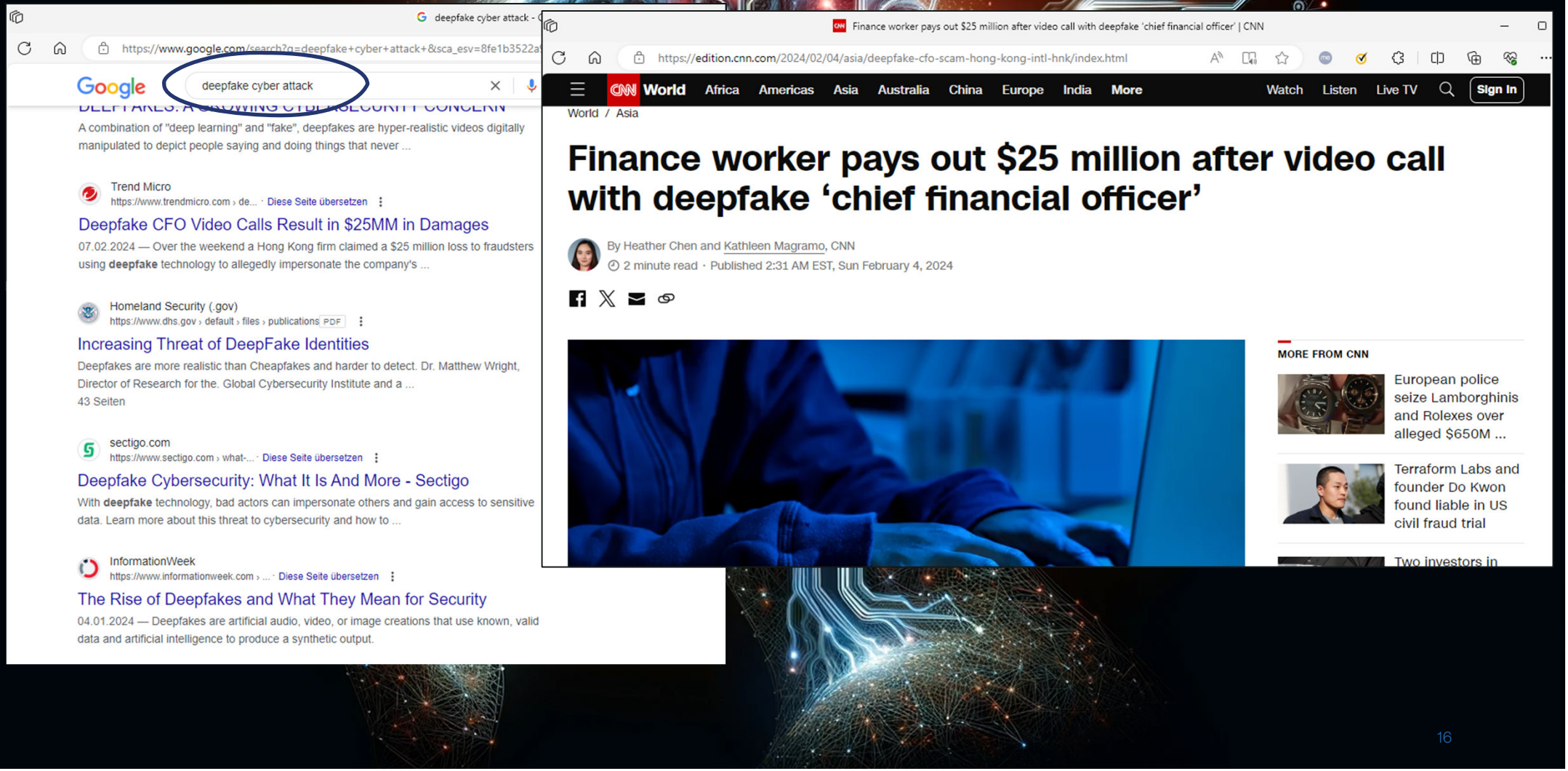


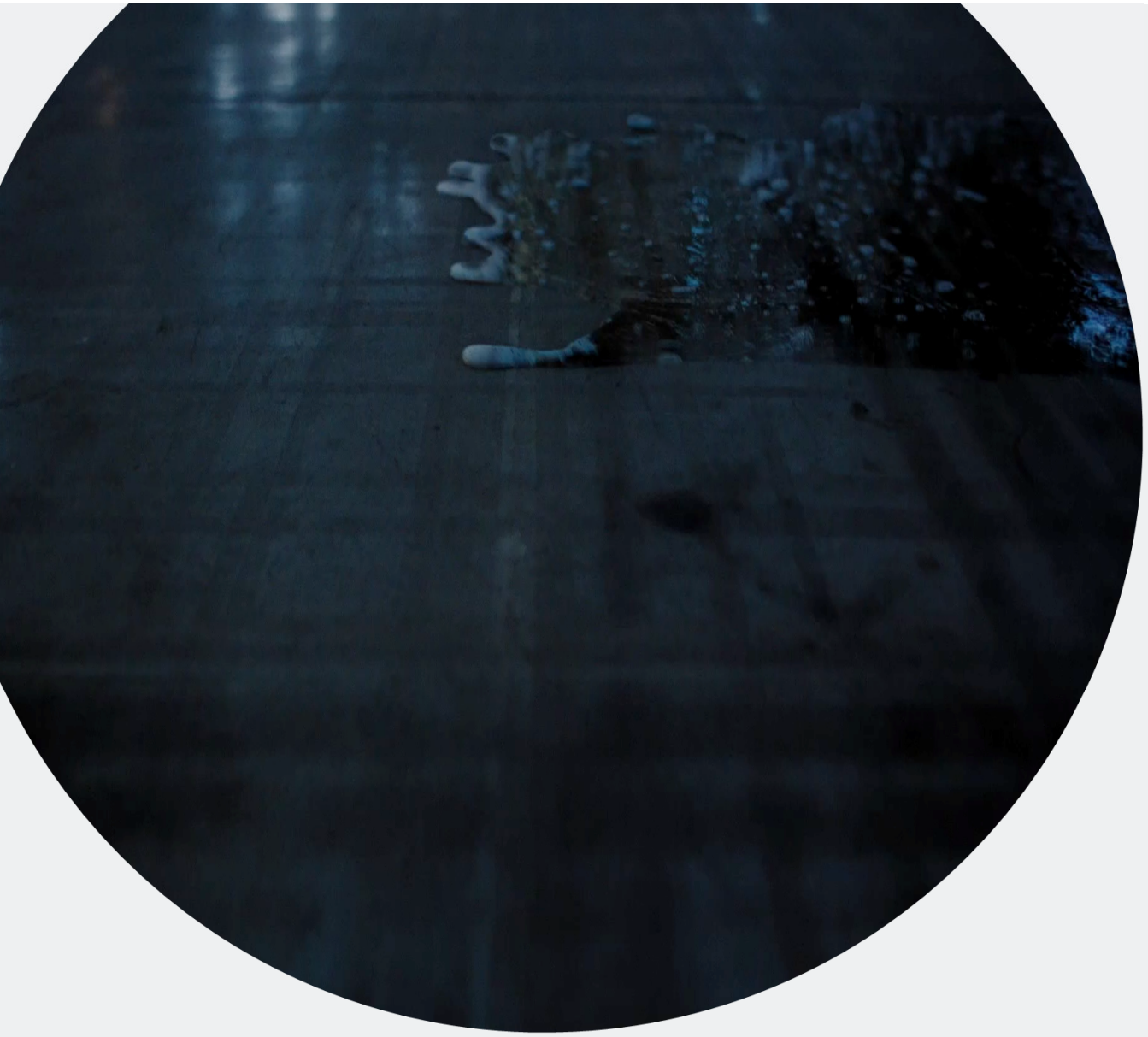

Meet tomorrow prepared.


sky news
.COM.AU
DEEPFAKE
After Trump declared that he was about to get arrested (he wasn't) deepfakes flooded social media showing Trump's arrest (didn't happen) and attempts to flee (also, not real). Get ready for AI-generated 2024 drama.
First Edition
DEEPFAKES OF TRUMP ARREST EMERGE ON TWITTER
REAL NEWS, HONEST VIEWS.

Meet tomorrow prepared.

Meet tomorrow prepared.





ZURICH

Be ready for every challenge – meet tomorrow prepared

Strategien zur Risikominderung

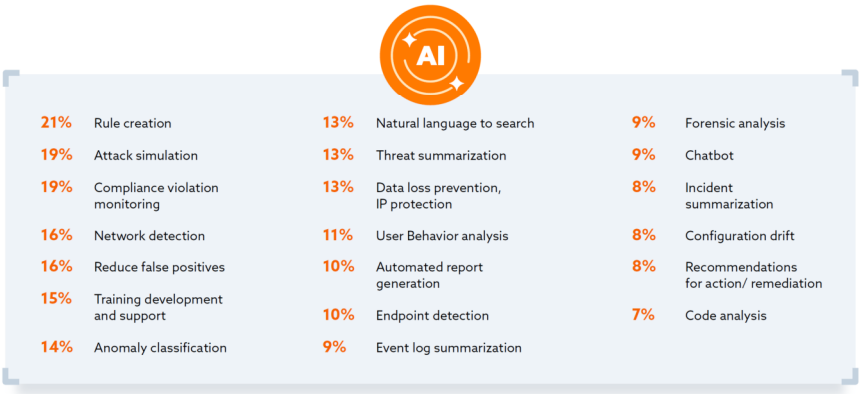
Gemäß Studie

ZURICH

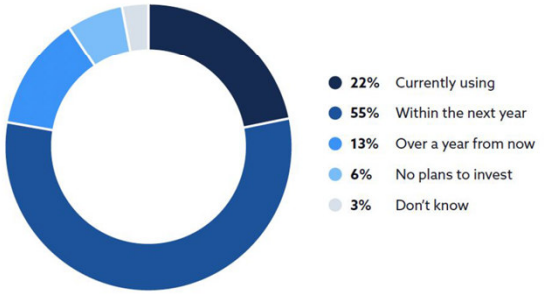
Key Finding 4: 2024 Is the Year for AI Implementation – Get Ready for the Revolution

- Over half (55%) of organizations are planning to implement gen AI solutions in the next year
- A diverse range of use cases are being explored with the top use cases: rule creation (21%), attack simulation (19%), and compliance violation detection (19%)
- Biggest hurdle to AI implementation is the skills gap and staff shortage, as reported by 33% of respondents

How does your organization plan to use Generative AI for cybersecurity? (Select top 3 use cases)



In general, is your organization using or planning to use Generative AI solutions?



Strategien zur Risikominderung

Gemäß Studie

How does your organization plan to use Generative AI for cybersecurity? (Select top 3 use cases)

21%	Rule creation	13%	Natural language to search	9%	Forensic analysis
19%	Attack simulation	13%	Threat summarization	9%	Chatbot
19%	Compliance violation monitoring	13%	Data loss prevention, IP protection	8%	Incident summarization
16%	Network detection	11%	User Behavior analysis	8%	Configuration drift
16%	Reduce false positives	10%	Automated report generation	8%	Recommendations for action/ remediation
15%	Training development and support	10%	Endpoint detection	7%	Code analysis
14%	Anomaly classification	9%	Event log summarization		

Strategien zur Risikominderung

Unsere Services

Was ist meine Reife in Bezug auf Cyber- und Datenschutz?

Risikoanalyse

Welche Kosten würden bei einem Cyber-Angriff entstehen?

Finanzielles Risiko

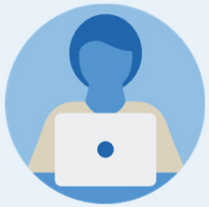
Ist meine IT-Infrastruktur sicher?

Penetrationstest

Bin ich auf einen Cyber-Angriff vorbereitet?

Krisensimulation

Erkennen meine Mitarbeiter einen Phishing-Versuch?



Schulung

Wie stoppt man die nächste Generation von Schadsoftware?

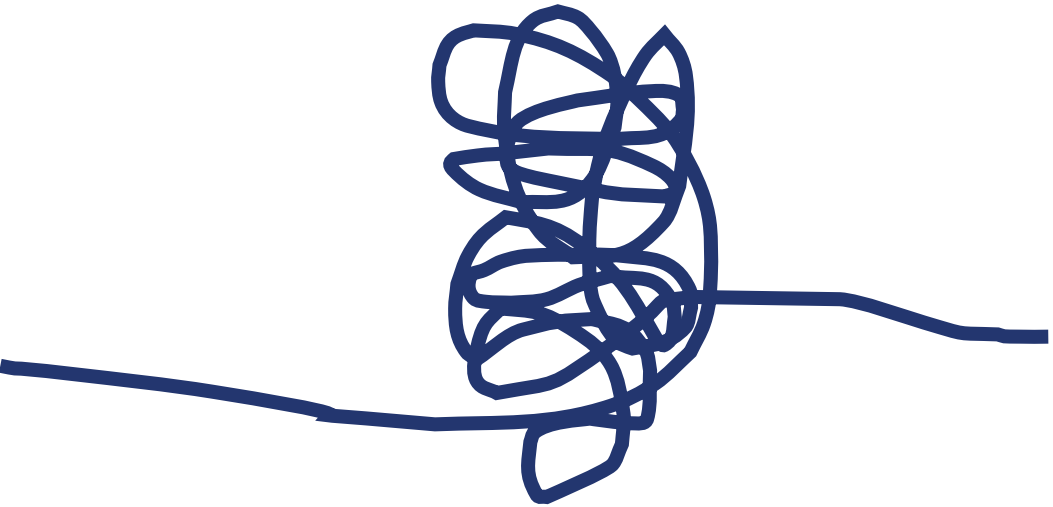
Cyber-Toolbox

Sind meine Partner auf Cyber-Bedrohungen vorbereitet?

Bewertung von Drittanbietern

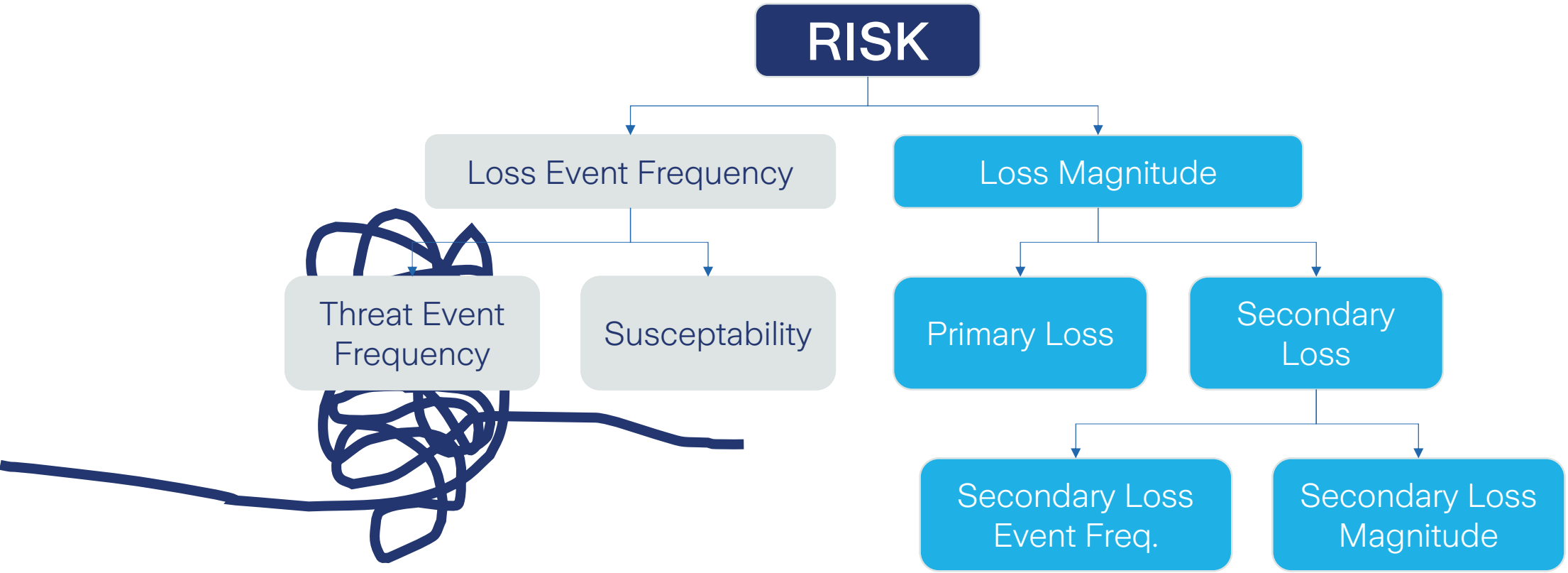
Strategien zur Risikominderung

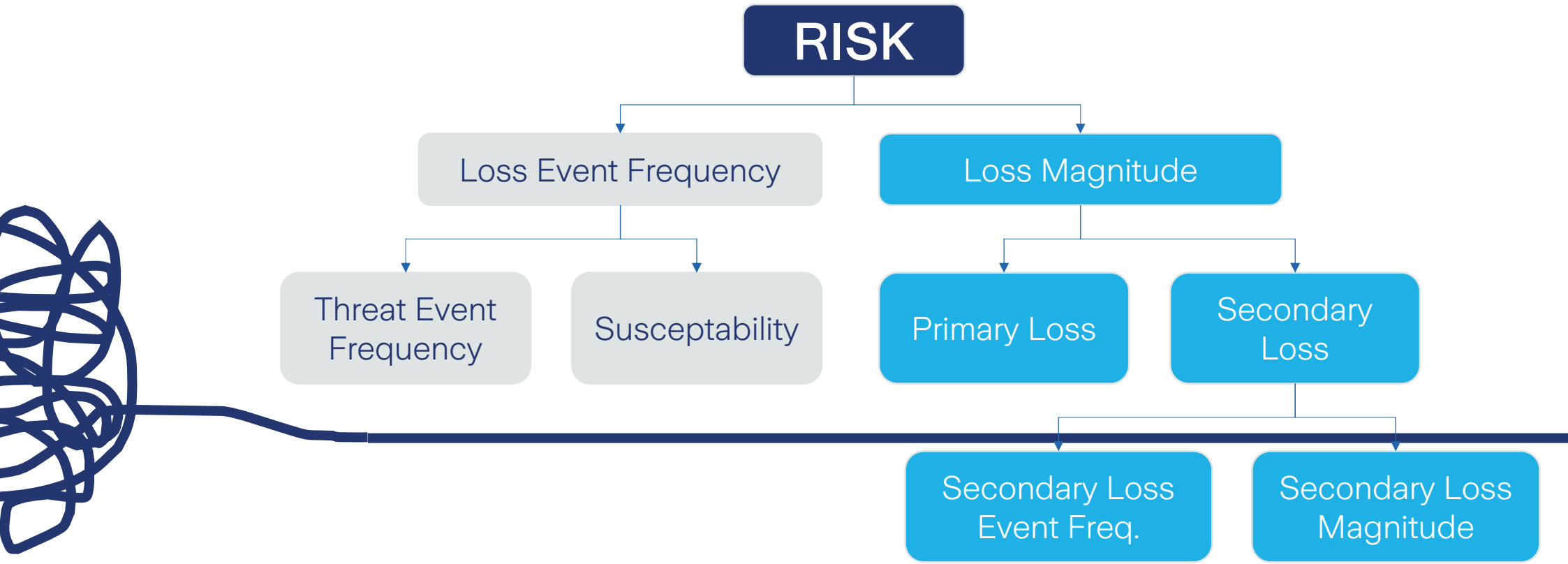
Die Rolle der Cyber Risk Quantification



Strategien zur Risikominderung

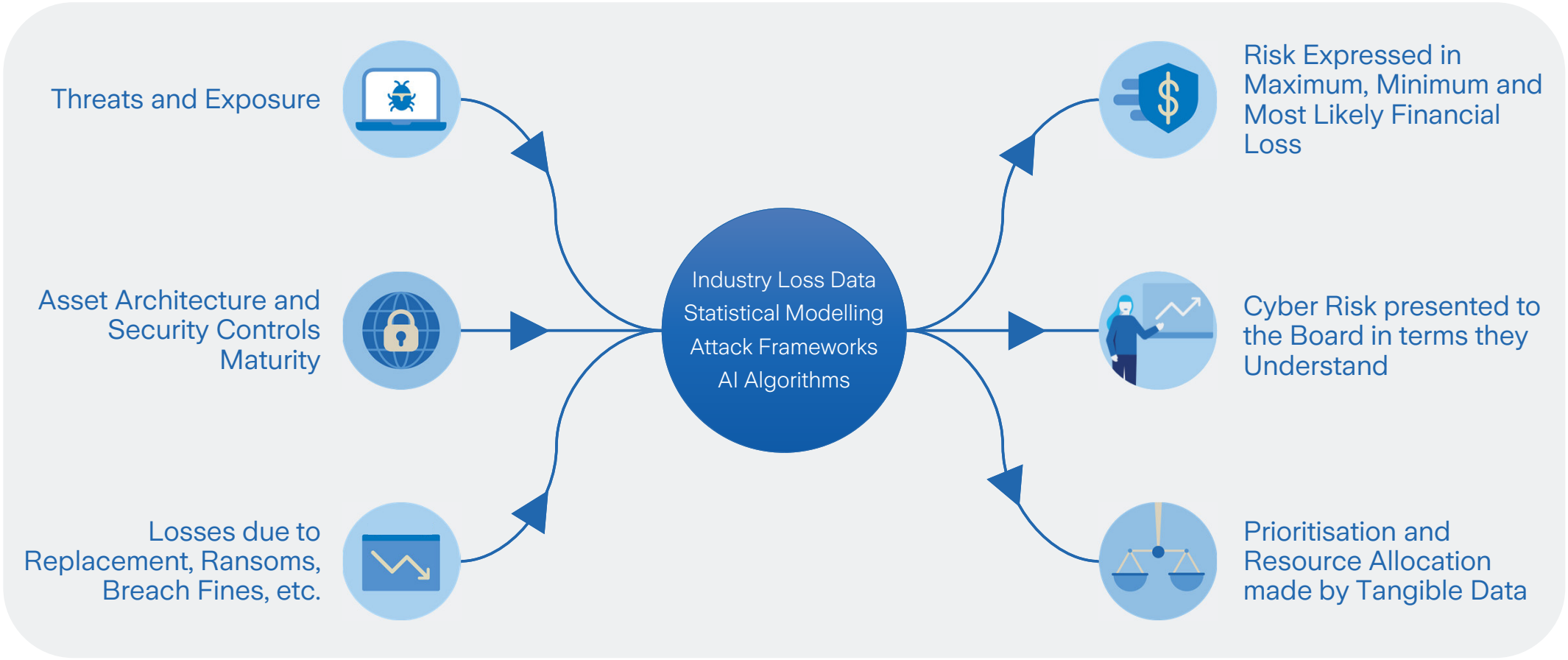
Die Rolle der Cyber Risk Quantification




RISK
Loss Event Frequency
Loss Magnitude
Threat Event Frequency
Susceptability
Primary Loss
Secondary Loss
Secondary Loss Event Freq.
Secondary Loss Magnitude

CRQ und KI

Ein dynamisches Duo gegen Cyber-Bedrohungen



Meet tomorrow prepared.

ZURICH

Ihre Vorteile mit unserer Cyber Risiko Quantifizierung

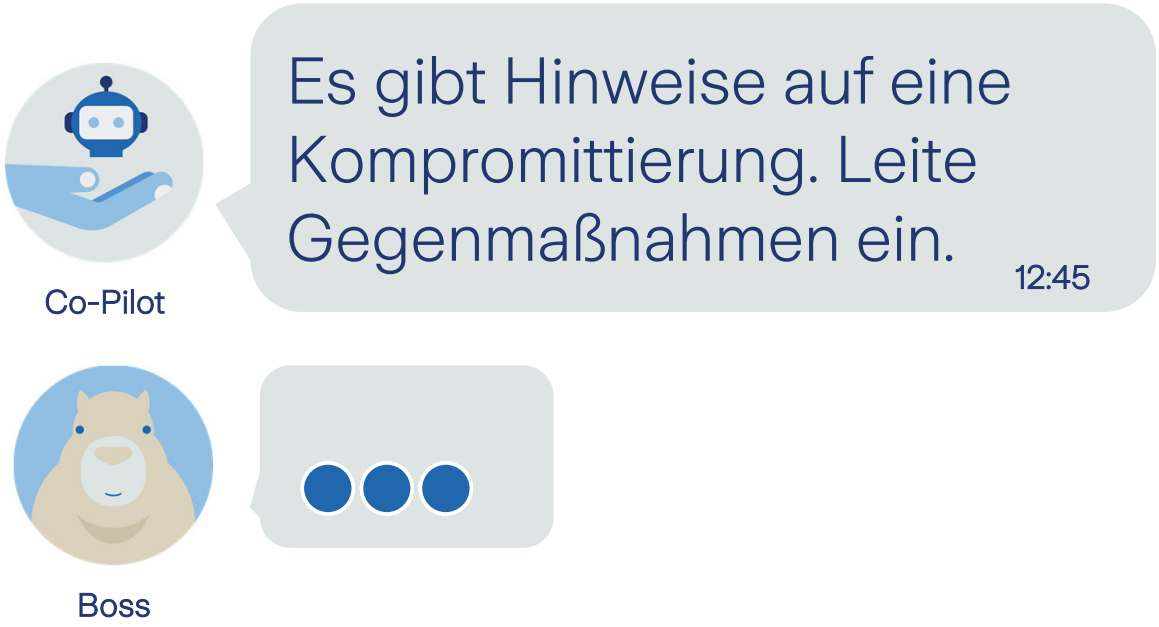
1 | Machen Sie Ihre Cyber-Risiken greifbar und messbar

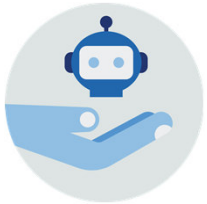
2 | Begründen Sie Ihre Budgets und Investitionen überzeugend

3 | Erhalten Sie eine klare Steuerungsperspektive auf Risiken und dem Behebungsplan

4 | Steuern Sie Drittanbieterrisiken und gewinnen Sie vollständige Einsicht in Ihr Ökosystem

5 | Verankern Sie Risikobewusstsein wirkungsvoll in der Unternehmensspitze


Es gibt Hinweise auf eine Kompromittierung. Leite Gegenmaßnahmen ein.
12:45
Co-Pilot
Boss



Co-Pilot

Es gibt Hinweise auf eine Kompromittierung. Leite Gegenmaßnahmen ein.

12:45

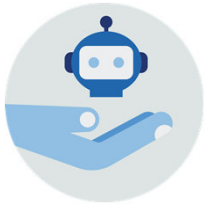
Boss

Mike, das ist Internet funktioniert nicht mehr!

12:47

12:48

Ich



Co-Pilot

Es gibt Hinweise auf eine Kompromittierung. Leite Gegenmaßnahmen ein.

12:45

Boss

Mike, das ist Internet funktioniert nicht mehr!

12:47

Ja, wir sind dran

12:48

Ich

@Chef, die Werke stehen still.

12:55

Ich

Boss

/&§$!” 12:56

@Co-Pilot, Status

12:57

Ich

Gerne. Die Systeme wurden erfolgreich isoliert. Wiederherstellung wurde initiiert. Test steht aus. Normalbetrieb wird in 3 Wochen erwartet.

12:59

Co-Pilot

/&§$!”

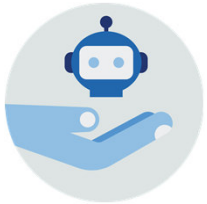
13:03

Boss

@Co-Pilot, Berechne den finanziellen Schaden.

13:04

Ich



Co-Pilot

Der Schaden wird auf 30,000 Euro geschätzt.

13:06

Boss

Das geht ja.

13:08

Sehe ich auch so.

13:09

Ich

Innovation durch Conversational AI und Risikovisualisierung

Dann gehe ich jetzt z'Mittag.
En guete. 🙏

👍
12:48

Ich

ZURICH

Thank you

You can’t wish disaster away

But you can meet tomorrow prepared

ZURICH

Michael Guiao
Senior Cyber Risk Engineer

E-Mail:
michael.guiao@zurich.com

LinkedIn:
https://www.linkedin.com/in/michael-guiao

ZURICH
Resilience Solutions

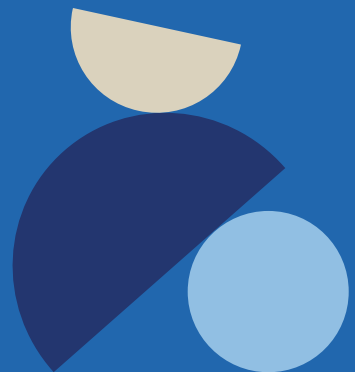
ZURICH
Resilience Solutions

This is a general description of (insurance) services such as risk engineering or risk management services by Zurich Resilience Solutions, which is part of the Commercial Insurance business of Zurich Insurance Group, and does not represent or alter any insurance policy or service agreement. Such (insurance) services are provided to qualified customers by affiliated companies of Zurich Insurance Company Ltd, including but not limited to: Zurich American Insurance Company, 1299 Zurich Way, Schaumburg, IL 60196, USA; The Zurich Services Corporation, 1299 Zurich Way, Schaumburg, IL 60196, USA; Zurich Insurance plc, Zurich House, Ballsbridge Park, Dublin 4, Ireland; Zurich Commercial Services (Europe) GmbH, Platz der Einheit, 2, 60327 Germany; Zurich Management Services Limited, The Zurich Centre, 3000b Parkway, Whiteley, Fareham, Hampshire, PO15 7JZ, UK; Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland; Zurich Australian Insurance Limited, ABN 13 000 296 640, Australia.

The opinions expressed herein are those of Zurich Resilience Solutions as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible, but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its affiliated companies (Zurich Insurance Group) as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment, or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group.

Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties, and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product, nor will it ensure coverage under any insurance policy.

Zurich Resilience Solutions



Strategien zur Risikominderung

Die Rolle der Cyber Risk Quantification

Cyber Risk Quantification

- **Individuelle Bedrohungsanalysen** initiieren **Risikomodellierung.**
- **Quantifizierung** durch Bewertung operativer Risiken.
- **Cyber-Sicherheitsstandards** prüfen, um **Reife** zu bestimmen.
- **Klarheit** durch top **Empfehlungen** in unserem Bericht.

1

Cyber Strategy Management Support

- **Laufende Neubewertung** der Cyber-Exposition, einschließlich **Lieferantenrisiken**.
- **Regelmäßige Audits** und Überprüfung von **Mitigationsplänen.**
- Erstellung **detaillierter Berichte** über Risiken und deren finanziellen Auswirkungen nach **Implementierung** der Maßnahmen.
- **Begleitung** bei der Entwicklung der **Cybersecurity-Strategie**, unter Berücksichtigung der **Ökosystemrisiken.**
- **Zugriff** auf unsere Plattform für die **Visualisierung von Risiken** und das **Reporting in Echtzeit.**

2