

Cyber-
security
Munich



ORGANIZED BY



HOSTED BY



WELCOME!

Six Focus Areas – Four Locations – One Promise

**AI & Data Driven
Company**

**Resilient
Business**

**ESG
Transformation**

**Connected
Platforms**

**Transformation
Strategy**

**Future
Organization**

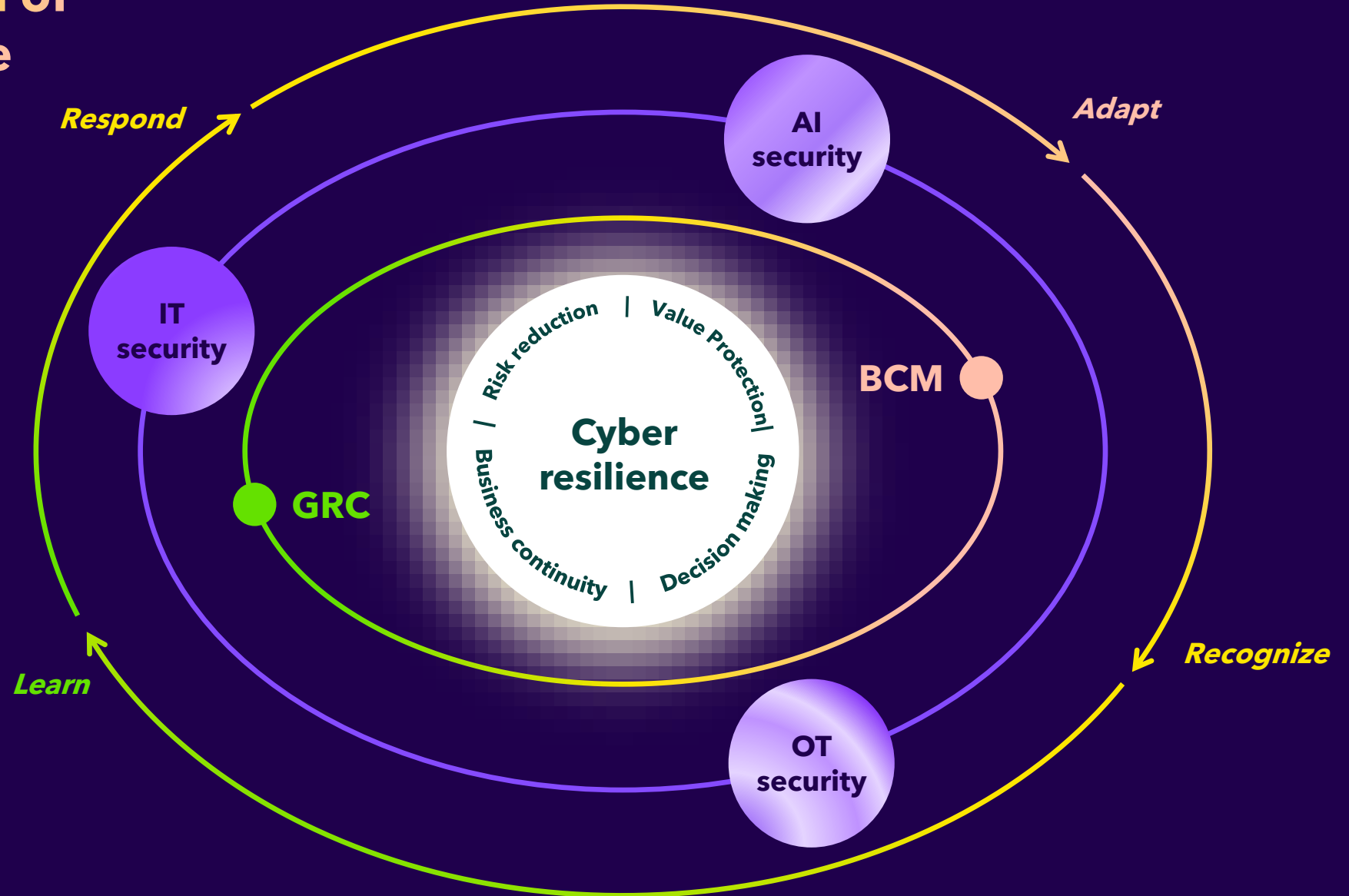


**We Shine a
New Light on
Future Viability**



metafinanz
technologie. kultur. netzwerke.

The Orbit Model of Cyber Resilience



From Cyber Attack to Existential Crisis

72 hours that decide the company



metafinanz
technologie. kultur. netzwerke.

A red emergency light is shown on the left side of the image, partially obscured by a dark blue overlay. The light has a white ring around its base and a red lens. The background is dark and out of focus, showing some structural elements.

Cyber Crisis Management

Why preparation is key



if...

when

From incident to crisis



Existential Threat

Business

Image

Legal

Finance

„IT Problem“ with business consequences

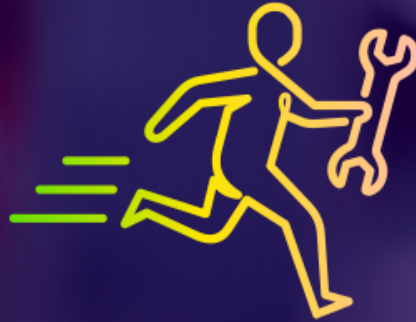


IT and CISO are NOT superheroes.

Who is steering the crisis?



Attackers



IR-Service Provider



Company



Decision Making Authority (DMA)

Key functions of the crisis team

Management Communication Legal Operations



Know your stakeholders

Internal
first

Customers

Partners

Public

Authorities
24h / 72h

5 To-Do's

1 Clarify external support and insurance at an early stage.

2 Define clear crisis organization and roles.

3 Prepare crisis-ready communication.

4 Align crisis management, business continuity management (BCM) and incident response (IR).

5 Test and practice regularly.

**AI has been around
for a long time.**

The only question is:
Who is in control?



metafinanz
technologie. kultur. netzwerke.

AI is growing faster than the governance behind it

From one customer example, we know that ...



... and the number keeps growing.

Latest headlines from the media

Ausbruch aus Testumgebung

KI von OpenAI steuert eigenständig Hackerangriff

Stand: 22.07.2026 • 07:46 Uhr

OpenAI spricht selbst von einem "beispiellosen Cybervorfall": KI-Modelle der Firma brachen eigenständig aus einer Testumgebung aus, verschafften sich Zugang zum offenen Internet - und hackten ein externes Unternehmen.

KÜNSTLICHE INTELLIGENZ

Samsung-Ingenieure geben ChatGPT vertrauliche Daten preis

Samsung hat ermittelt, dass drei seiner Ingenieure binnen kurzer Zeit mindestens dreimal bei der Nutzung von ChatGPT geheime Daten durchsickern lassen haben.

Air Canada

Chatbot verspricht Fluggast irrtümlich Rückerstattung – Airline muss zahlen

Er gewährte einen Rabatt, den es gar nicht gab: Weil ein Chatbot gegen die eigenen Richtlinien verstieß, wollte Air Canada einen Kunden auf dessen Kosten sitzen lassen. Nun entschied ein Gericht gegen das Unternehmen.

golem.de | tagesschau.de | spiegel.de

A hand holding a gold pen writing on a document, with a robotic hand visible in the background.

How can we help?

We combine **AI innovation** with **governance** to enable **sustainable business success.**

Usecase: Enabling rapid AI innovation without compromising governance

The situation

- AI development is **highly exploratory** and requires rapid experimentation
- New use cases must be **validated quickly** using realistic conditions and data
- Successful PoCs need a clear path **from experimentation to production**

The complication

- AI use cases often require access to **sensitive business data** and documents
- Data and security requirements **increase governance complexity**, resulting in longer time-to-go-live
- Anonymization can **limit the quality and reliability** of AI outcomes

The solution

- Establish dedicated environments for **AI experimentation**, validation, and production readiness
- Provide **access to production-like data**, AI services, and scalable infrastructure
- **Embed security and governance controls** throughout the AI development lifecycle

Key outcome

Faster validation and deployment of AI use cases.

Enable business data access without compromising security

Scale AI adoption through built-in governance and controls



Usecase: Example

- To **balance AI innovation and data protection**, the organization established a clear **separation between technology experimentation and business validation**.
- **Generic AI PoCs are executed on a dedicated platform** using synthetic data, while **validated use cases** requiring realistic conditions are tested on a **governed platform** with production-like or production data.

Access restrictions, developer guidance, and security controls ensure that innovation can scale without compromising governance, compliance, or data security.

Speed vs. security

Tech Test Plattform

Scenario

Generic /
Technical
PoC

Data

Synthetic
Data

Historic
Data

Dev Plattform

Scenario

Data PoC

Validated
Use cases

Feature
Development

Data

Anonymized
Data

Production-
like /
Customer
Data

Expert based AI scenario assessment



Your benefits

- **Support** for decision-making in AI risk management
- Creating **awareness** about the AI scenarios and their effects
- **Connecting** the different involved departments

AI has been around for a long time. The only question is: **Who is in control?**



Visible.

Transparency regarding use, relevance, and risk

- AI use case inventory
- Preliminary regulatory assessment
- Custom AI risk profile

Controllable.

Priority, responsibility, and next steps

- Roles & responsibilities
- Prioritized action plan
- AI risk navigator (KIRINA)

Future ready.

Governance, management, and strategic alignment

- AI use case management
- Robust AI governance framework
- Company-specific AI strategy

metafinanz
Informationssysteme
GmbH

Leopoldstraße 146
80804 Munich

Große Gallusstraße 16-18
60312 Frankfurt

Theodor-Heuss-Str. 30
70174 Stuttgart

Schönbrunner Straße 31/Top 26
1050 Vienna



How to Contact Us



LinkedIn



Instagram



Website