Lessons from Real-World Pentesting and Emerging Threats

Securing Critical Infrastructure in the Era of Sovereign Cloud

Presenter: Sebastian Kokott | IT Security Consultant

Securing Critical Infrastructure in the Era of Sovereign Cloud

Agenda

01 Introduction

02 Sovereign Cloud Concepts

03 Critical Infrastructure (KRITIS) Overview

04 Legal & Regulatory Framework

05 DELOS Cloud Case Study

06 Key Security Challenges

07 Security by Design

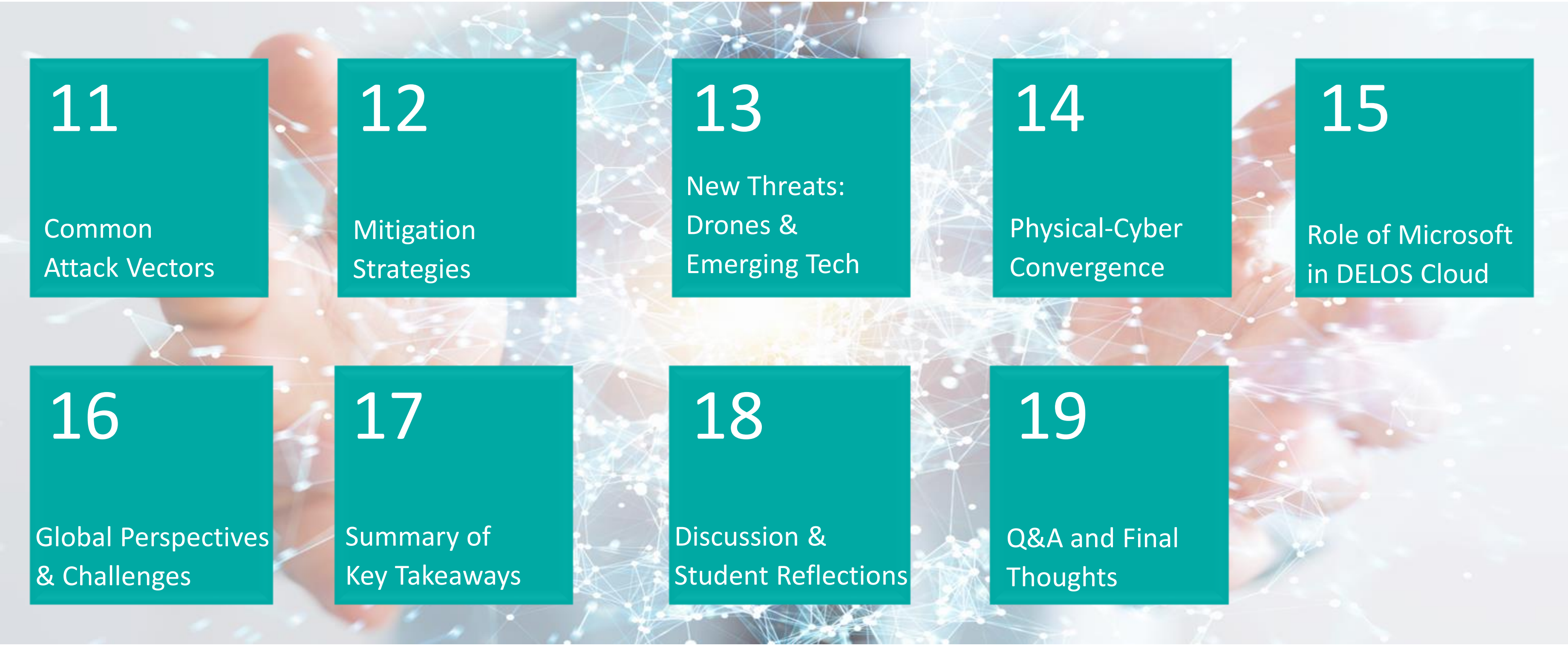
08 Penetration Testing KRITIS

09 Real-World Pentest Scenarios

10 Ethical & Legal Boundaries

Securing Critical Infrastructure in the Era of Sovereign Cloud

Agenda



11
Common Attack Vectors

12
Mitigation Strategies

13
New Threats: Drones & Emerging Tech

14
Physical-Cyber Convergence

15
Role of Microsoft in DELOS Cloud

16
Global Perspectives & Challenges

17
Summary of Key Takeaways

18
Discussion & Student Reflections

19
Q&A and Final Thoughts

Welcome!

Talk Goal: Bridge Cloud Security & Critical Infrastructure

Founded in 1987

> 2,000 employees

> 300 million euros annual sales

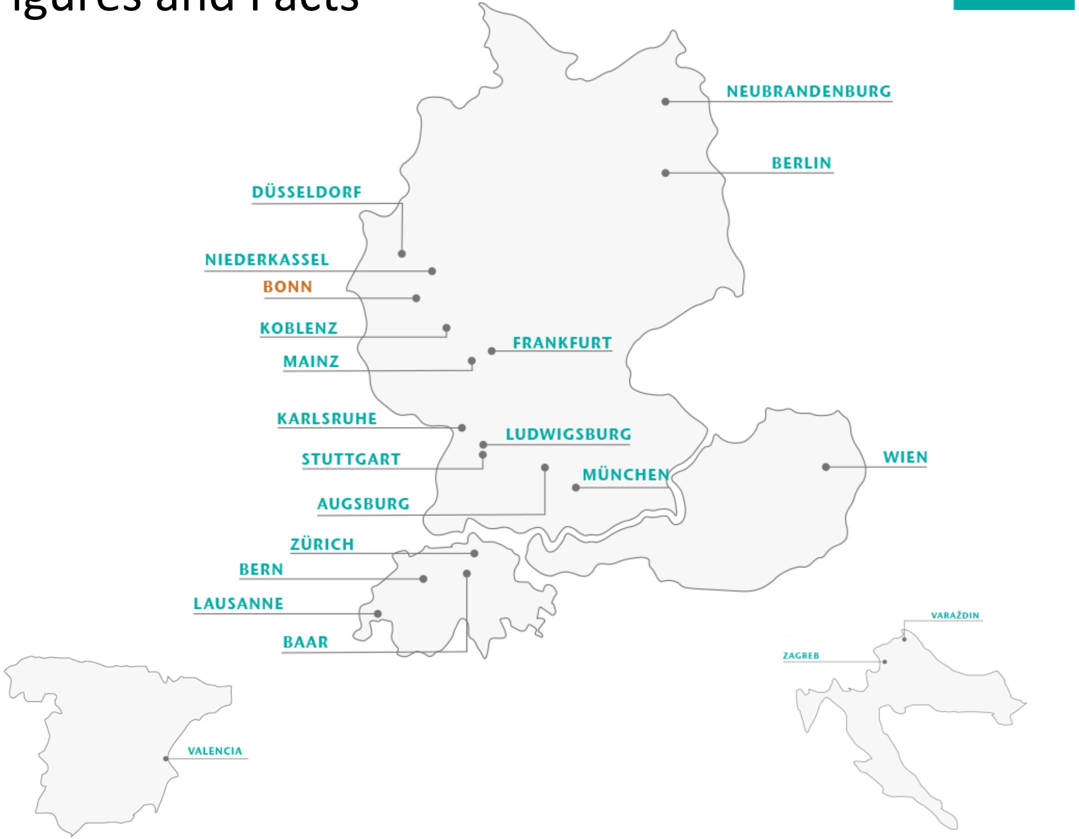
21 locations in Germany, Austria, Switzerland, Spain & Croatia

Headquarter Bonn

The CONET Group:

Figures and Facts

CONET



www.conet.de

Sovereign Cloud: What & Why

Definition:

- National control over data & infrastructure

Importance:

- **Compliance, Independence, Trust**

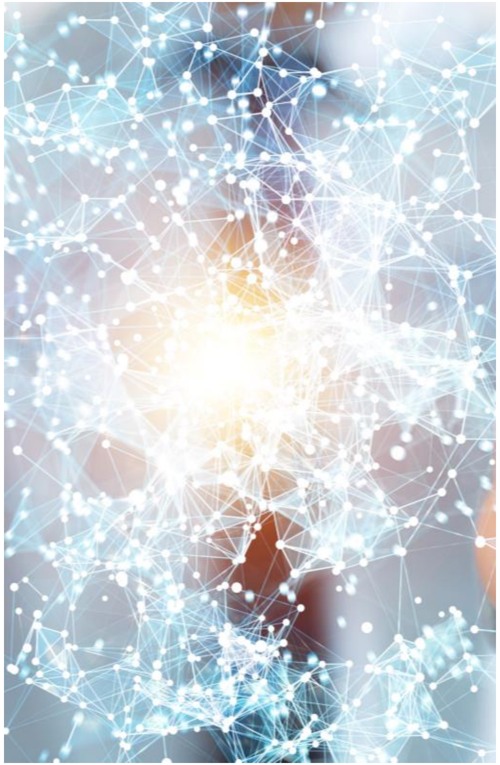
Relevance in the EU context

KRITIS – What is Critical Infrastructure?

- Energy, Water, Finance, Healthcare, IT
- Dependency on digital resilience
- Examples of disruption consequences

Securing Critical Infrastructure in the Era of Sovereign Cloud

Legal & Regulatory Framework



BSI-KritisV (Germany)

Dependency on digital resilience

Examples of disruption consequences

Securing Critical Infrastructure in the Era of Sovereign Cloud

Case Study: DELOS Cloud

German sovereign cloud project

Partnership: Microsoft & Bundesdruckerei

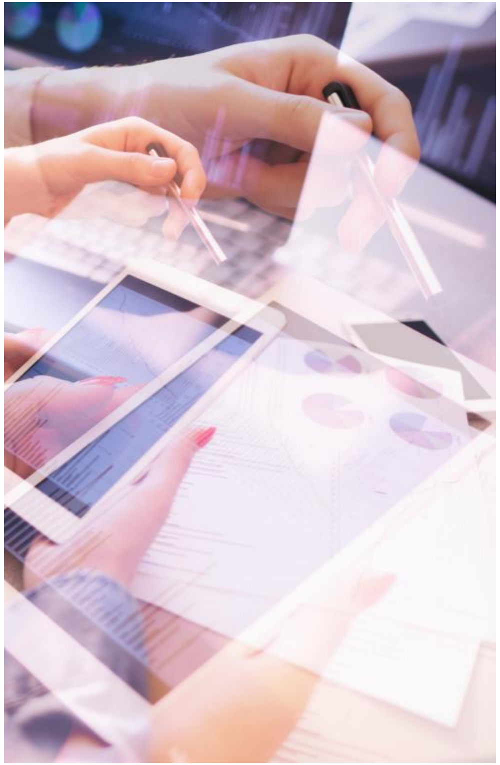
Key features: Isolation, transparency, security

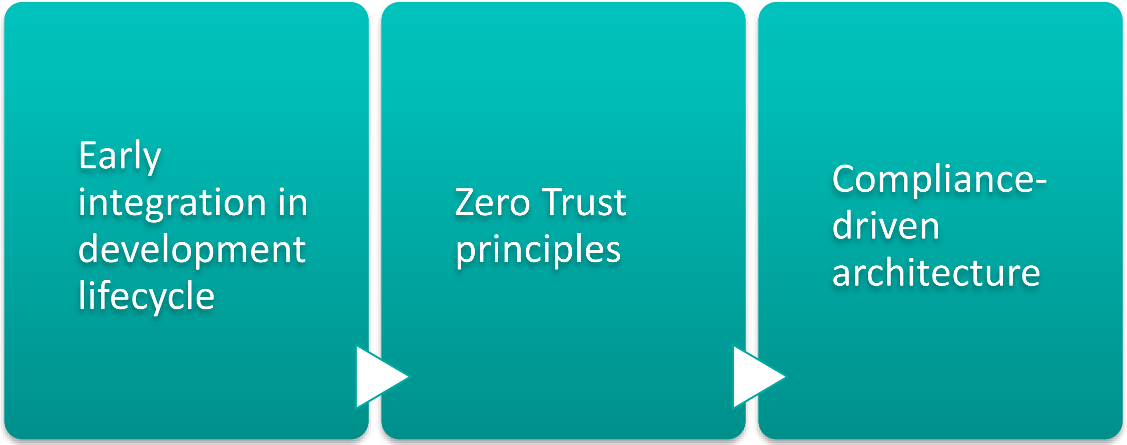
```
at r;
float area;

printf(" Input value of Radius : ");
scanf("%f", &r);

area = (M_PI * ( r * r) ) / 2;

printf("\n Area of the semicircle : %.2f \n\n", area );

return 0;

int hexagonSize;
  int r, s, i;

  printf(" Enter number for Hexagon size : ");
  scanf("%d", &hexagonSize);

  for(r=0; r<hexagonSize; r++)
  {
    for(s=0; s<=hexagonSize-r; s++){
      printf(" ");
```

Key Security Challenges

- Supply chain risks
- Identity & access management
- Logging & monitoring gaps

Security by Design




Early integration in development lifecycle

Zero Trust principles

Compliance-driven architecture

Securing Critical Infrastructure in the Era of Sovereign Cloud

Pentesting KRITIS Environments

Objectives: Identify weaknesses before attackers do

Red teaming vs. classic pentesting

Challenges: Complexity, legal constraints

Real-World Scenarios from Practice

- Simulated attacks on control systems
- Testing emergency response procedures
- Lessons from isolated networks
  - Water
  - Energy

Ethical & Legal Boundaries

- Consent and scope definition
- Handling sensitive data
- Reporting & responsible disclosure

- Regarding to national security all pentesters have to be approved by german goverment (Secuity Check, APT and BSI certified)

Securing Critical Infrastructure in the Era of Sovereign Cloud

Common Attack Vectors

- Misconfigurations
- Insider threats
- Remote access exploits

Mitigation Strategies

- Hardening systems
- Continuous monitoring
- Employee training
- Vulnerability Management

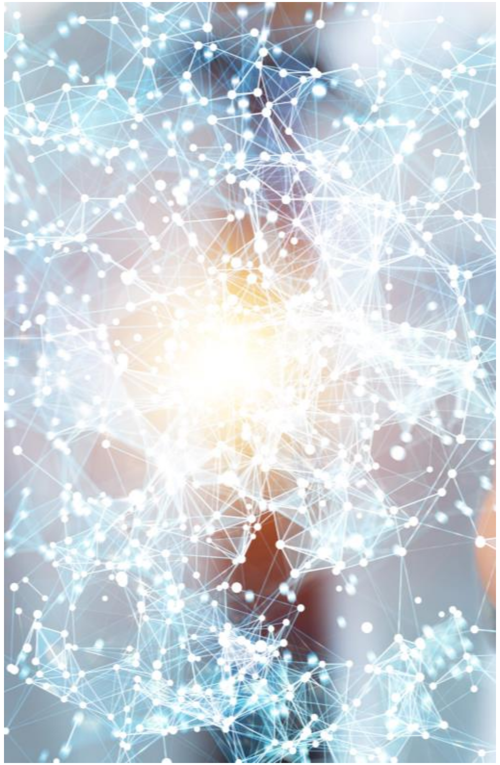
New Threats: Drones

Physical reconnaissance

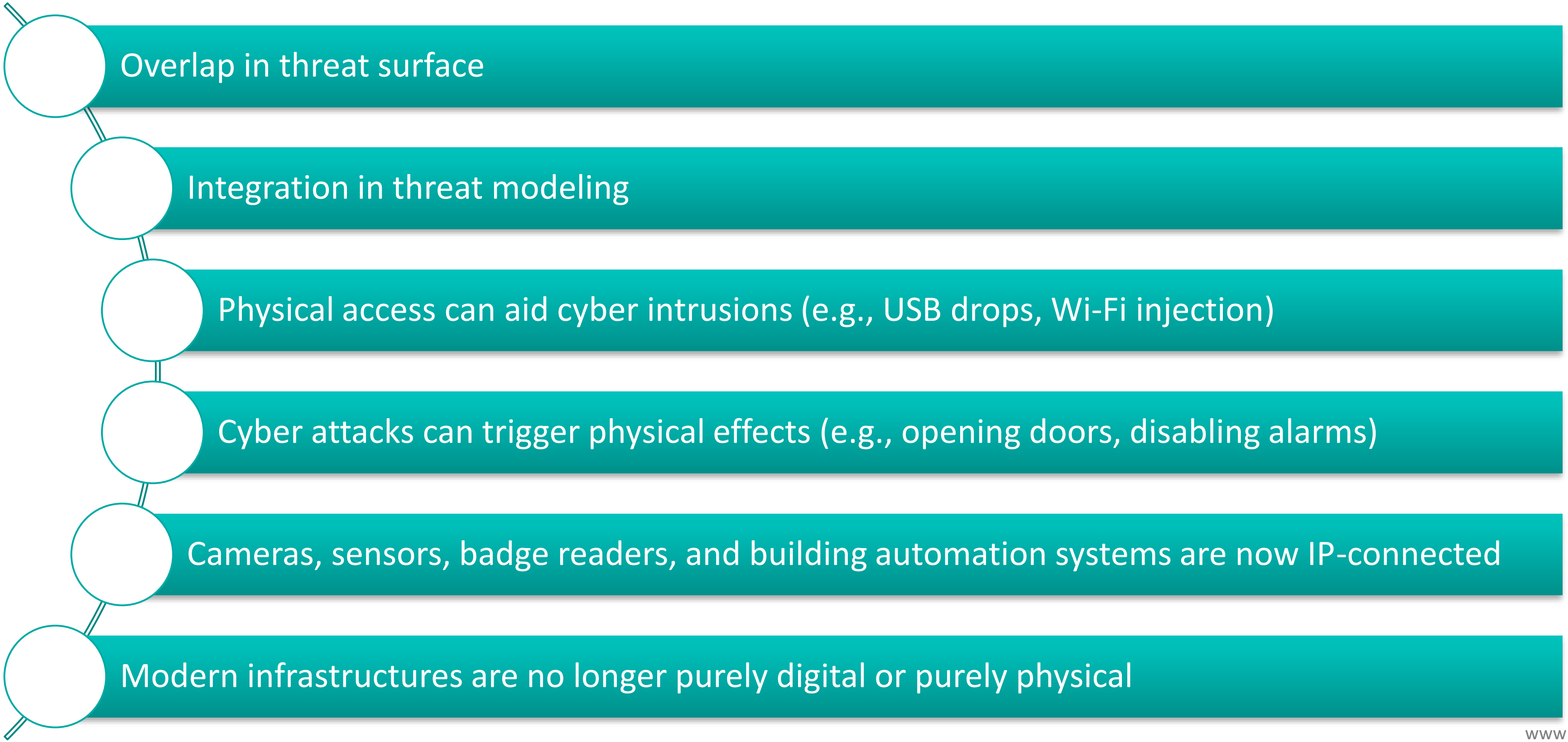
Wireless injection (Wi-Fi, Bluetooth)

Detection & defense techniques

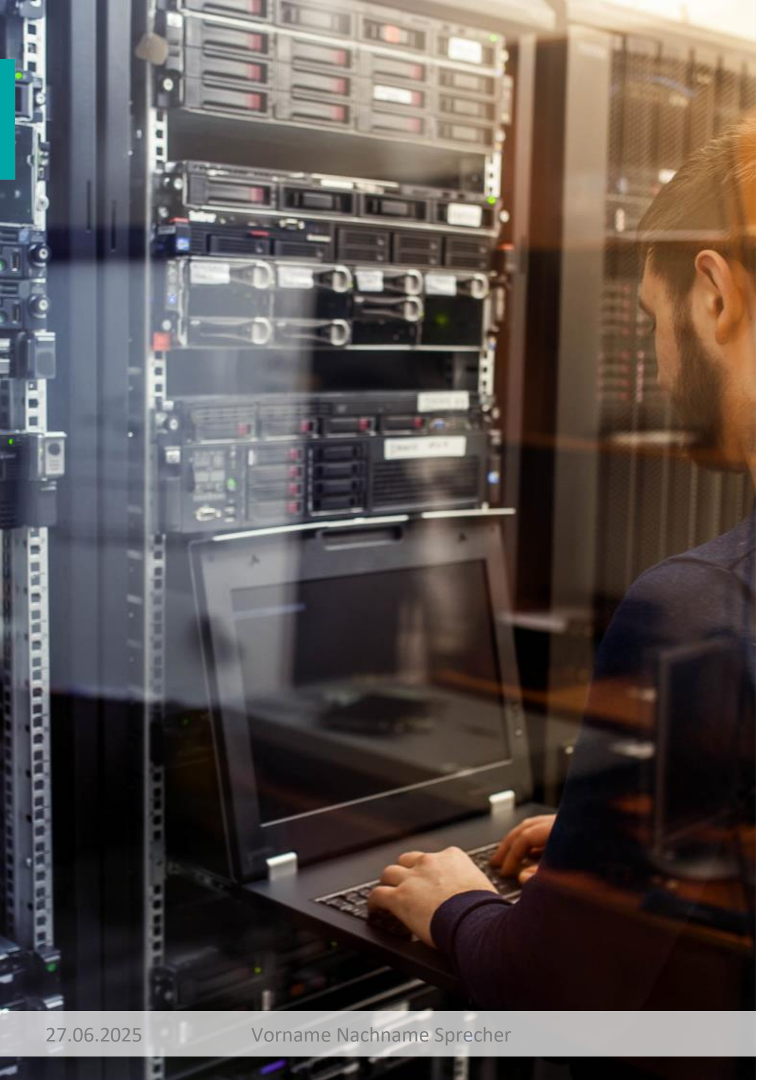
- Open World
- KRITIS Radar / Lida



Physical-Cyber Convergence



- Overlap in threat surface
- Integration in threat modeling
- Physical access can aid cyber intrusions (e.g., USB drops, Wi-Fi injection)
- Cyber attacks can trigger physical effects (e.g., opening doors, disabling alarms)
- Cameras, sensors, badge readers, and building automation systems are now IP-connected
- Modern infrastructures are no longer purely digital or purely physical

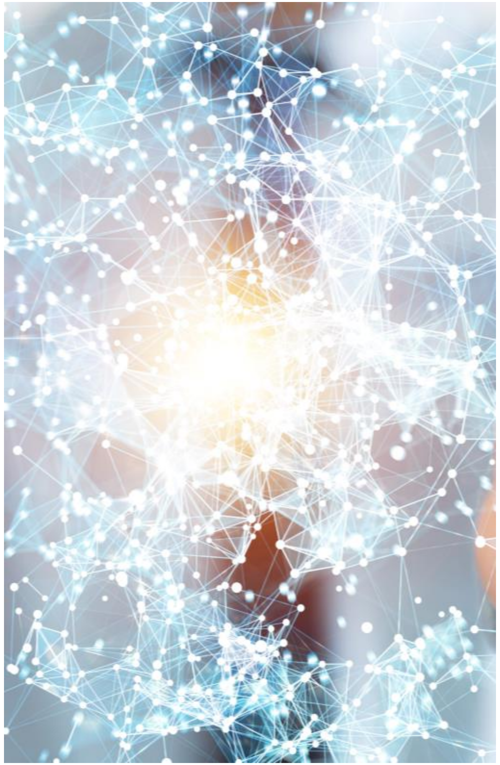


Role of Microsoft in Sovereign Cloud

- Azure under sovereign control
- Governance layer
- Separation of duties
- Other Key Players (Google / AWS)

Summary & Takeaways

- Sovereign cloud enhances resilience
- KRITIS requires special handling
- Pentesting must evolve with new threats



CONET

Thank you for your attention!

Do you have any questions?

- 🌐 www.conet.de
- ☎ +49 228 9714-0
- ✉ info@conet.de

Follow us on: