„Noch sicher oder schon resilient? “

Der CONTAIN-Ansatz für Ransomware Incident Response

Dr. Stefan Schauer (AIT) und Judith Strußenberg M.A. (UniBW München)

17.09.2024 **IKT Sicherheitskonferenz 2024**

Inhalt

Intro & Motivation

Relevanz

The Record.

Cyberattack on telecom giant Frontier claimed by RansomHub

INDEPENDENT

Major cyberattack sees NHS London hospitals declare critical incident with operations cancelled

12 hours ago • Rebecca Thomas

2 days ago • Jonathan Greig

SecurityInfoWatch

Veeam report finds ransomware victims are unable to recover 43% of affected data

14 hours ago

The Register

Here's yet more ransomware using BitLocke against Microsoft's own users

techradar

RansomHub group says it was behind Christie's attack, threatens to release private data of half a million customers

28 May • Sead Fadilpašić

23 May • Jessica Lyons

HIPAA Journal

Ransomware Victim Count Increased by 75% in 2023

16 hours ago

The Register

North Korea building cash reserves using ransomware, video games

National Cyber Security Centre

Global ransomware threat expected to rise with AI, NCSC warns

29 May • Connor Jones

24 Jan

The Record.

Ransomware attack on Seattle Public Library knocks out online systems

28 May • Jonathan Greig

CS CyberScoop

Boeing confirms attempted $200 million ransomware extortion attempt

May 8 • AJ Vicens

Projekt CONTAIN

Funded by:

CONTAIN: Cybersicherheit & Resilienz

- Bilaterales Forschungsprojekt
- CONTAIN untersucht die Bewältigung von Cyber-Vorfällen.

- Resultate:
  - Serious Games
  - Modellierung und Simulation
  - Incident-Response Prozesse

- Ziele: Bessere Bewältigung von Vorfällen

PARTNERS:

FUNDED BY:

Der CONTAIN-Ansatz

CONTAIN Ansatz

Essenzielle Komponenten und deren Vulnerabilitäten

- Erkennen kritischer Systeme, Prozesse und Personen
- Erfassen von Schwachstellen und Bedrohungen
- Austausch mit Expert:innen, Analyse von Dokumenten

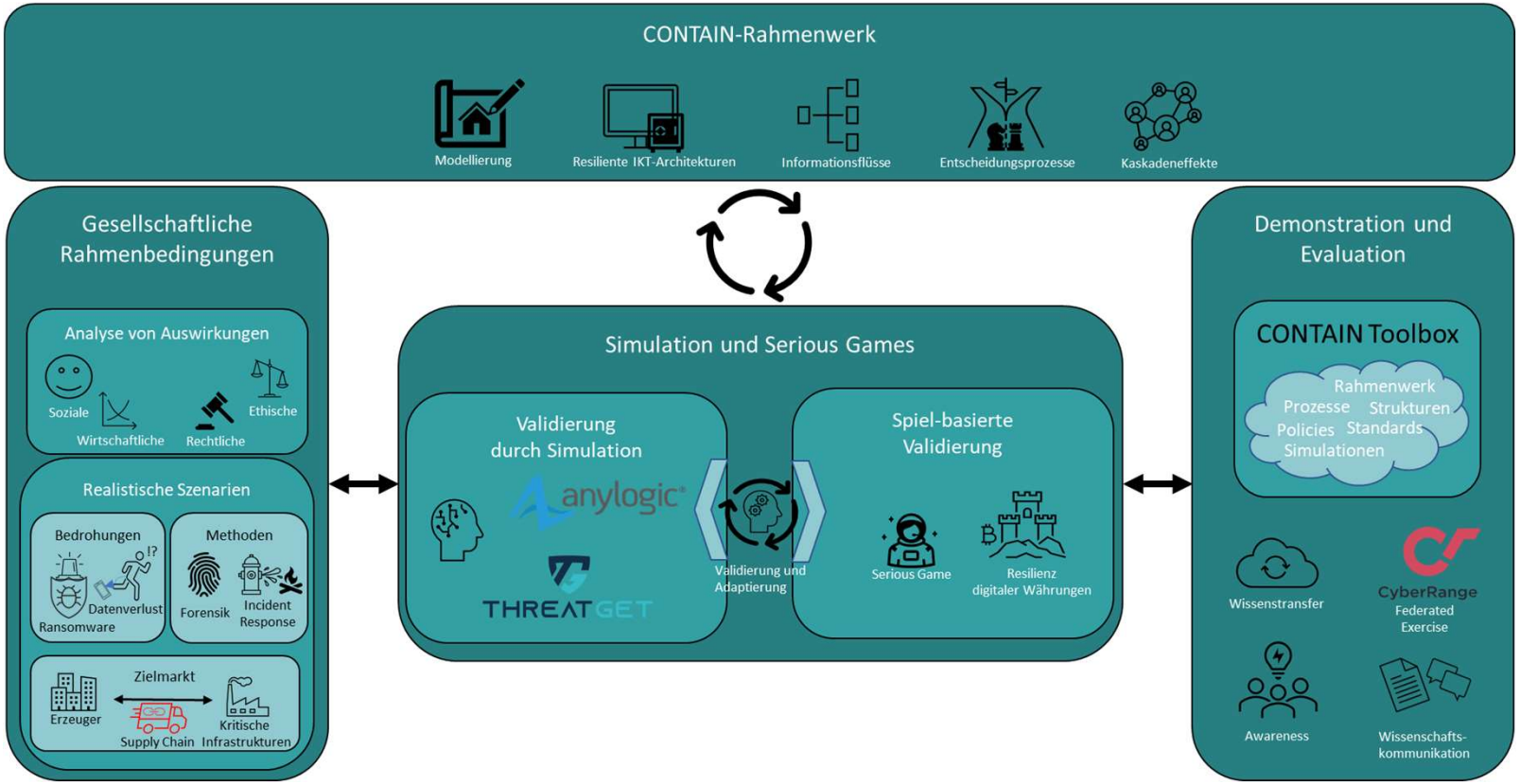
Abhängigkeiten zwischen Systemen und Unternehmen

- Identifikation von zentralen Schnittpunkten und Systemen
- Modellierung der Dynamiken zwischen den Systemen
- Simulation von Kaskaden-effekten und Back-up Mechanismen

Schaffen von Awareness und Preparedness

- Erstellen von realistischen Szenarien in Serious Games
- Üben von Incident Response in einer Cyber Range
- Integration in einen kontinuierlichen Verbesserungsprozess

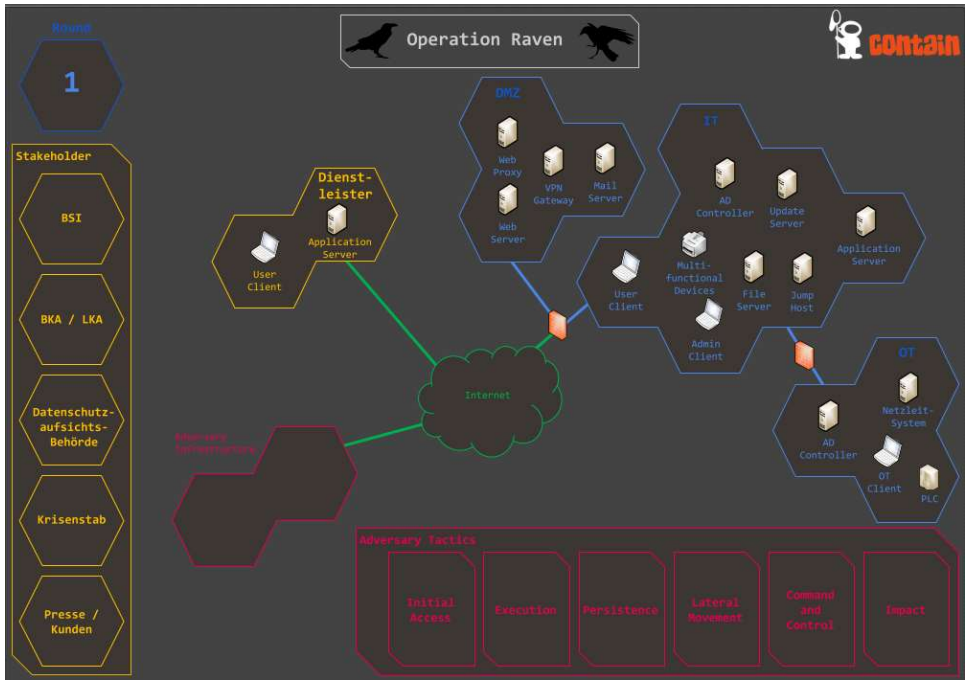
CONTAIN Ansatz



Serious Games

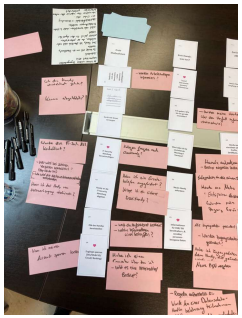
Operation Raven

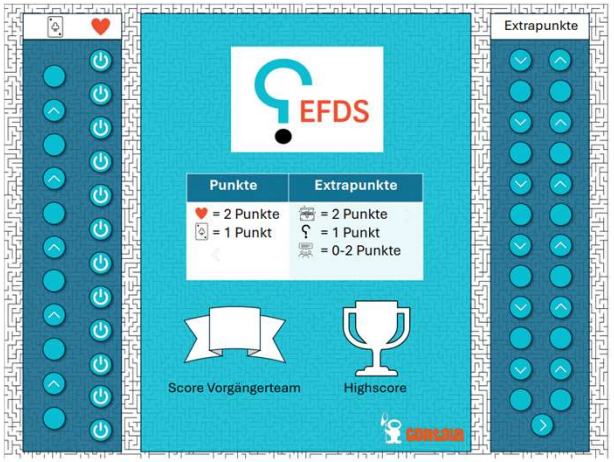
Serious Game zur Vorbereitung und Übung
der Reaktion auf Cybersecurity-Vorfälle



Eine Frage der Sicherheit

Ransomware auf dem Handy!
Jetzt ist guter Rat teuer. Oder?





- Rundenbasiert
- Für 2-8 Spielende
- In Entwicklung

- Ziele:
  - Wissen vertiefen
  - Handhabung üben
  - Perspektiven wechseln

EFDS

Hack dich nicht!

„Ransomware-Angriff in transnationaler Supply-Chain“

Spielmaterial

- Spielbrett, max. 6 Spieler, jeder repräsentiert ein Logistikunternehmen
- 1-4 Spielfiguren pro Spieler, die Spediteure darstellen
- Kartenstapel (verdeckt auf dem Spielfeld)

3 Ebenen:
- ***Cyberangriffskarten:*** verschiedene Cyberangriff-Szenarien
- ***Verteidigungskarten:*** Cybersecurity-Tools, Präventionsmaßnahmen
- ***Ressourcenkarten:*** Finanzmittel, Schulungen, Dienstleistungen

Spielkonzept

- Spieler übernehmen die Rolle des **Spediteurs**
- Spediteur wird mit **Cyberangriff** auf sein Unternehmen konfrontiert (Spieler deckt Angriffskarten auf)
- **Ziel**: Durch Auswahl verfügbarer Verteidigung- und Ressourcenkarten die Angriffe abzuwehren bzw. Unternehmen und Stakeholder zu schützen (Prävention)

Spielziel

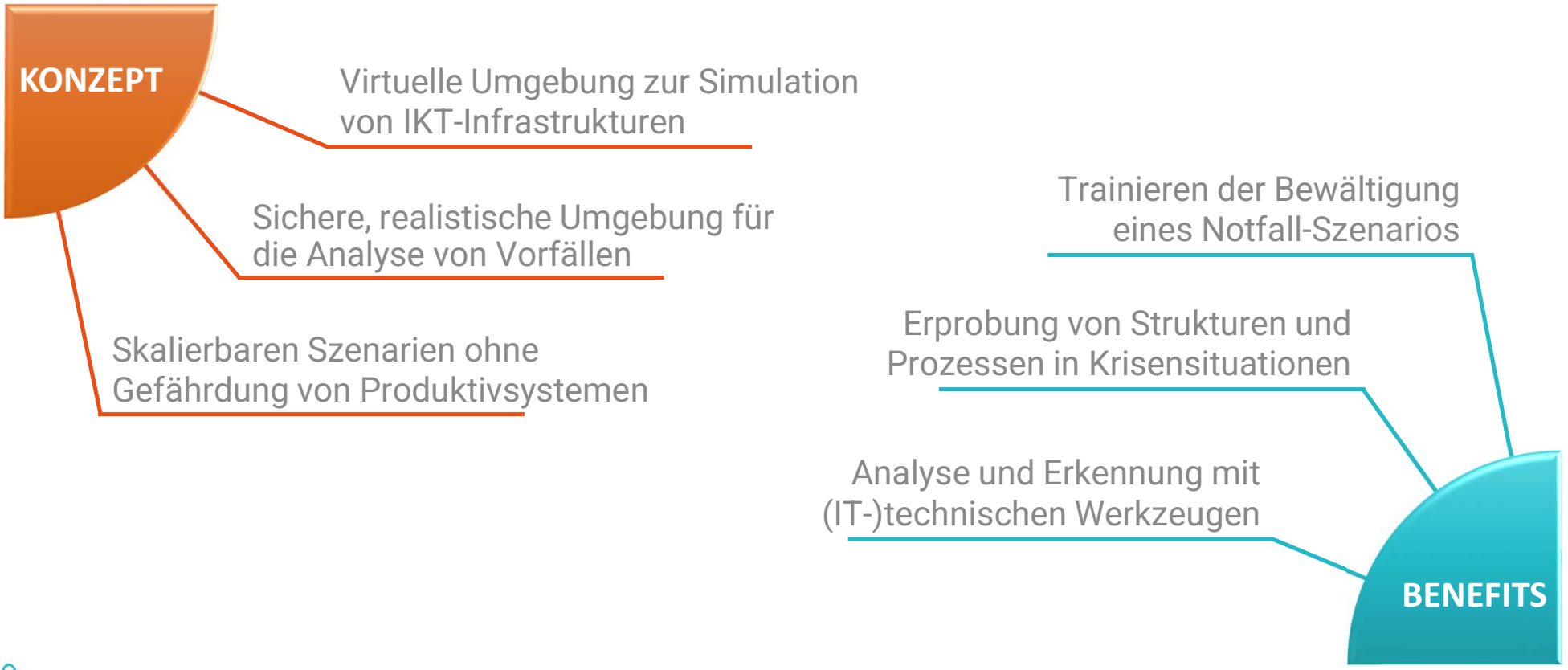
- Die Spielfiguren (Spediteure) sicher ins Ziel (das eigene Logistikunternehmen) zurückzubringen
- Interaktives Lernen über Cybersicherheit und deren Gefahren
- Wissen durch eigene Reaktionsmuster und Strategien der Mitspieler erweitern
- Spontane und bevorzugte Reaktionsmuster erkennen

Digital Detectives

- Serious Point-and-Click-Spiel für digitale Forensik
- Spieler können in einer interaktiven 2D-Umgebung erkunden und lernen
- Sie lösen Minispiele, verwenden Werkzeuge und sammeln Hinweise

Cyber Range

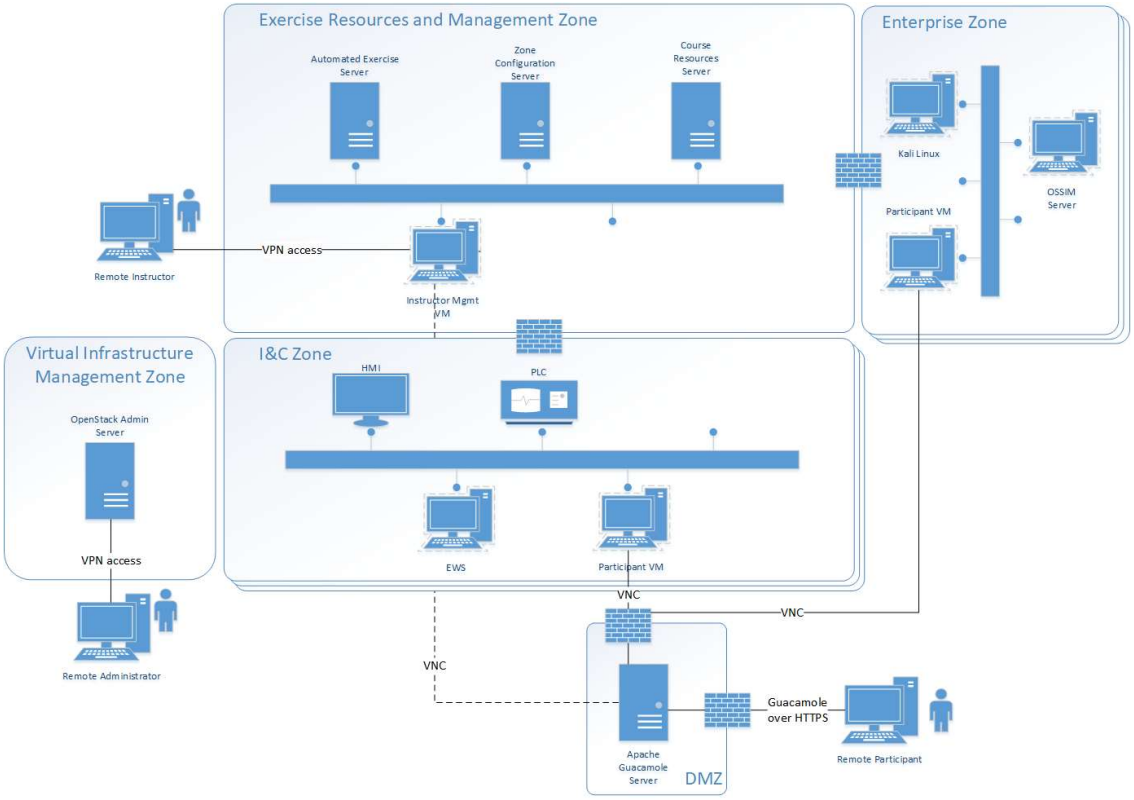
Cyber Range – Konzept



Cyber Range – Technik

- Virtualisierung als zentrale Methode
  - Office-Umgebung (Webserver, Mailserver, etc.)
  - Industrie-Umgebung (PLCs, SCADA & ICS, etc.)

- Zentrales Management für verschiedene Bereiche
  - Management-Bereich für die Systeme in der Übung
  - Management-Bereich für Virtualisierungen, Spielablauf, etc.



Cyber Range – Szenarien

Personen

- Krisenstäbe und Krisenorganisation
- Management, Technik, Spezialbereiche

Prozesse

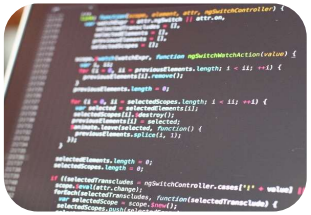
- Notfallpläne und Incident Response
- Kommunikationswege

Technik

- Adaptierte Infrastruktur (SW, HW, …)
- Spezialisierte Systeme und Werkzeuge

Cyber Range – Szenarien

Advanced Persistent Threat (APT)



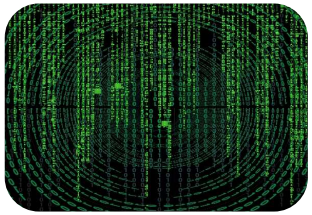
Ransomware

Trojaner / Remote Access Trojaner

Botnets

Data Breach (DSGVO)

Phishing



Vulnerability

DDoS

Fehlkonfiguration

Nachrichten

Regulatorien & Akteure (z.B. CERT, Trust Circle)

Und viele weitere

Fazit & Next Steps

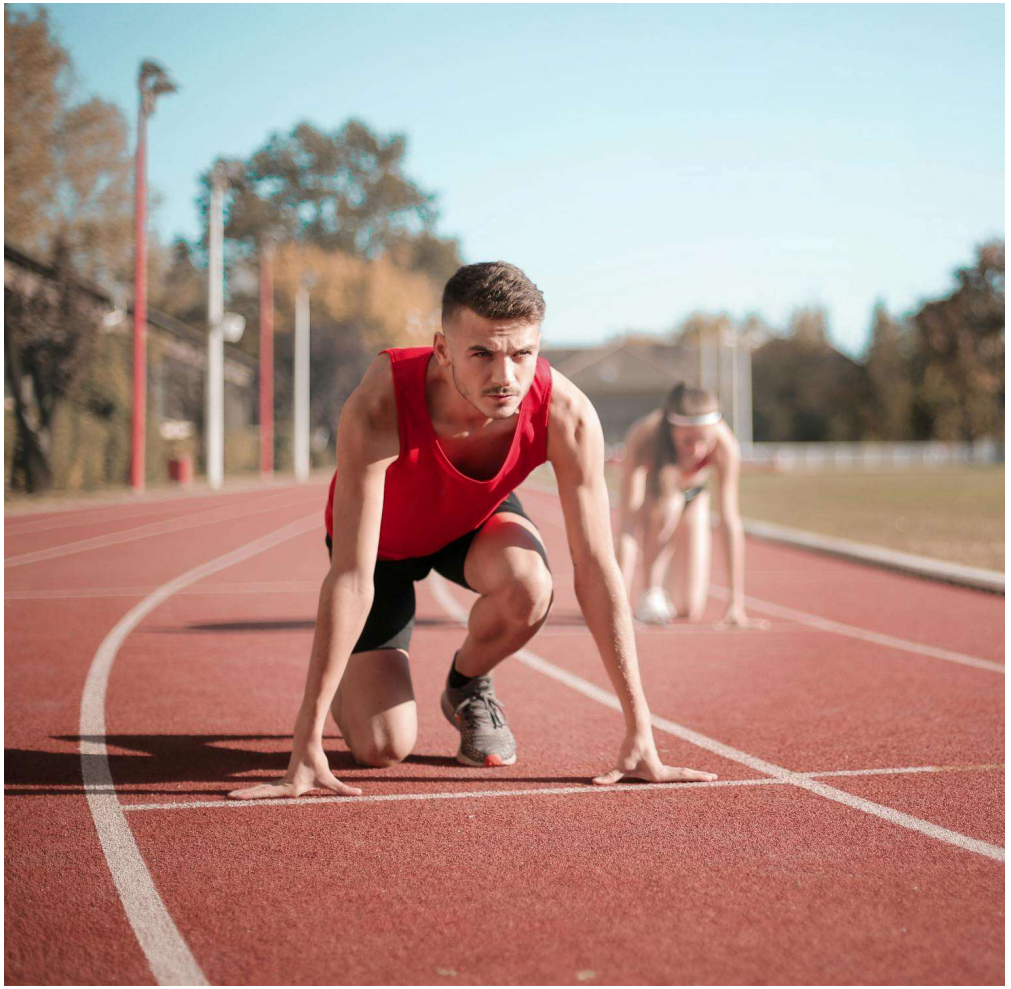
Fazit

Security-Maßnahmen sind wichtig, aber alleine nicht ausreichend

Preparedness und Resilienz sind ebenfalls wichtig

Vorbereitung auf Cyber Incidents kann und soll geübt werden

CONTAIN bietet hier den entsprechenden Rahmen



Hands on: Föderierte Übung 25./26.02.2025

- Bilaterale Übung in Wien und München
- Aktueller Stand aus Wissenschaft und Praxis
- Austausch mit Expert:innen
- Den Ernstfall proben
- Neue Serious Games testen

Bleiben Sie auf dem Laufenden

Folgen Sie uns auf LinkedIN für weitere Informationen:

„CONTAIN - Research Project CONTAIN“

https://www.linkedin.com/groups/9549256/

contain

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?

IKT-Sicherheitskonferenz 2024