Gelebte IT-Sicherheit

Projekt CONTAIN verbindet Forschung und Praxis

Dr. Steffi Rudel, Universität der Bundeswehr München

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:

Die Ransomware meldet sich – was dann?

Forschungsgegenstand

- **Bewältigung** von **Cybervorfällen**, insbesondere Ransomware-Angriffen
- **Schutz digitaler Währungen**, **Liquidität in der Krise** und Rolle von Cloud- und **Logistikdienstleistungsunternehmen**
- **Zentrale Innovation: CONTAIN-Rahmenwerk** für effektive und effiziente Bewältigung von Cybervorfällen bei **kritischen Infrastrukturen**, **KMUs** und **ganzen Lieferketten**

Universität der Bundeswehr München · SIEMENS · Universität Regensburg · ROLAND · LEW · Giesecke+Devrient · GARTNER THE WORLD OF TRANSPORT · ELVIS · team Technology Management · VICESSE · VDE · ITSECURITY www.it-sicherheitscluster.de · SBCF & Cie. strategy•corporate finance

Bundesministerium Landesverteidigung

BOKU · AIT Austrian Institute of Technology · universität wien

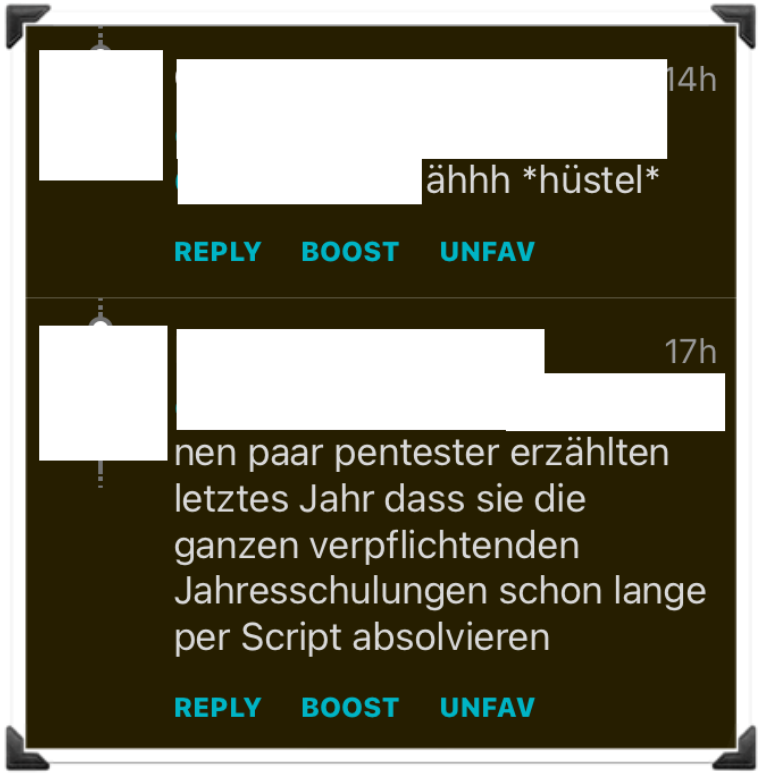
Projektziele und -inhalte

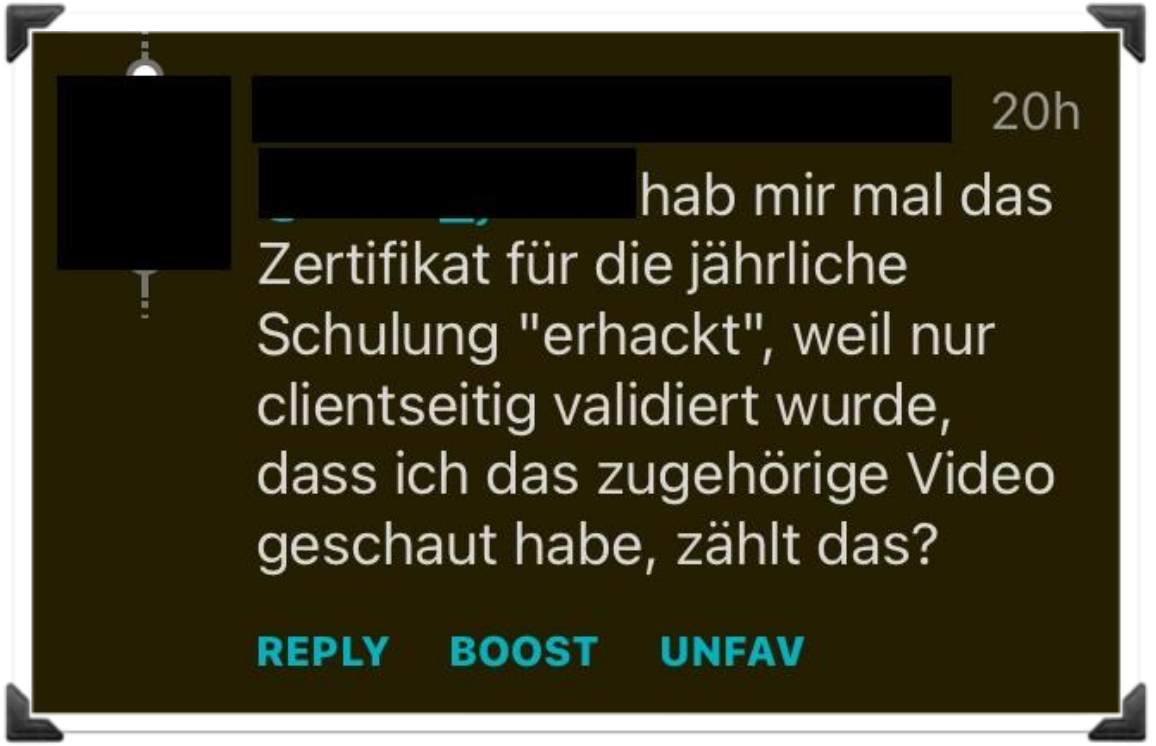
- **Serious Games** als **Methodeninnovationen** des Übens
- Erhöhung **Reifegrade** in der **Bewältigung von Cybervorfällen** durch **Technologiebündel**
- **Auswirkung** von **Cyberangriffen** auf **kritische Infrastrukturen** und **Organisationen**
- **Analysen von Kryptowährungen** als Zahlungsmittel und Schutz von digitalen Währungen gegen Zerstörung, Betrug und Geldwäsche für **Security-by-Design-Lösungen**

contain

Security Awareness, die man wegklickt

„Schulungen zu #Informationssicherheit und #Datenschutz sind ja leider oft zähe und dröge Angelegenheiten. Habt Sie schon mal interessante oder außergewöhnliche Maßnahmen zu diesem Thema gesehen, die Ihnen (positiv) im Gedächtnis geblieben sind?“





Serious Games

Serios Games in der Informationssicherheit

Ziele

- Schulung / Lernen
- Awareness / Sensibilisierung
- Identifikation v. Schwachstellen
- Identifikation v. Bedrohungen
- Strategieentwicklung
- uvm.

Vorteile

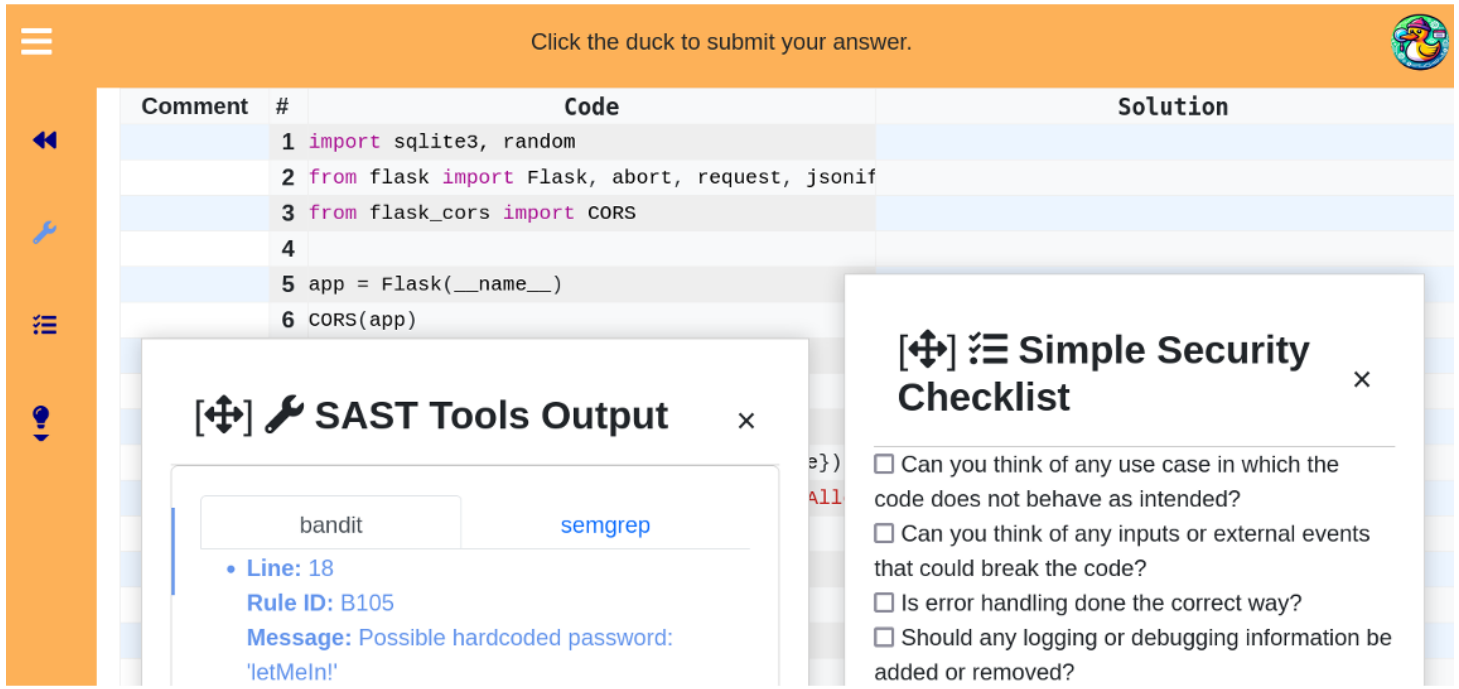
- Motivation, Involvement und Spaß
- Bessere Ergebnisse und Lerneffekte

Nachteile

- Limit der Personenzahl
- Finanzieller und organisatorischer Aufwand
- Vorurteile

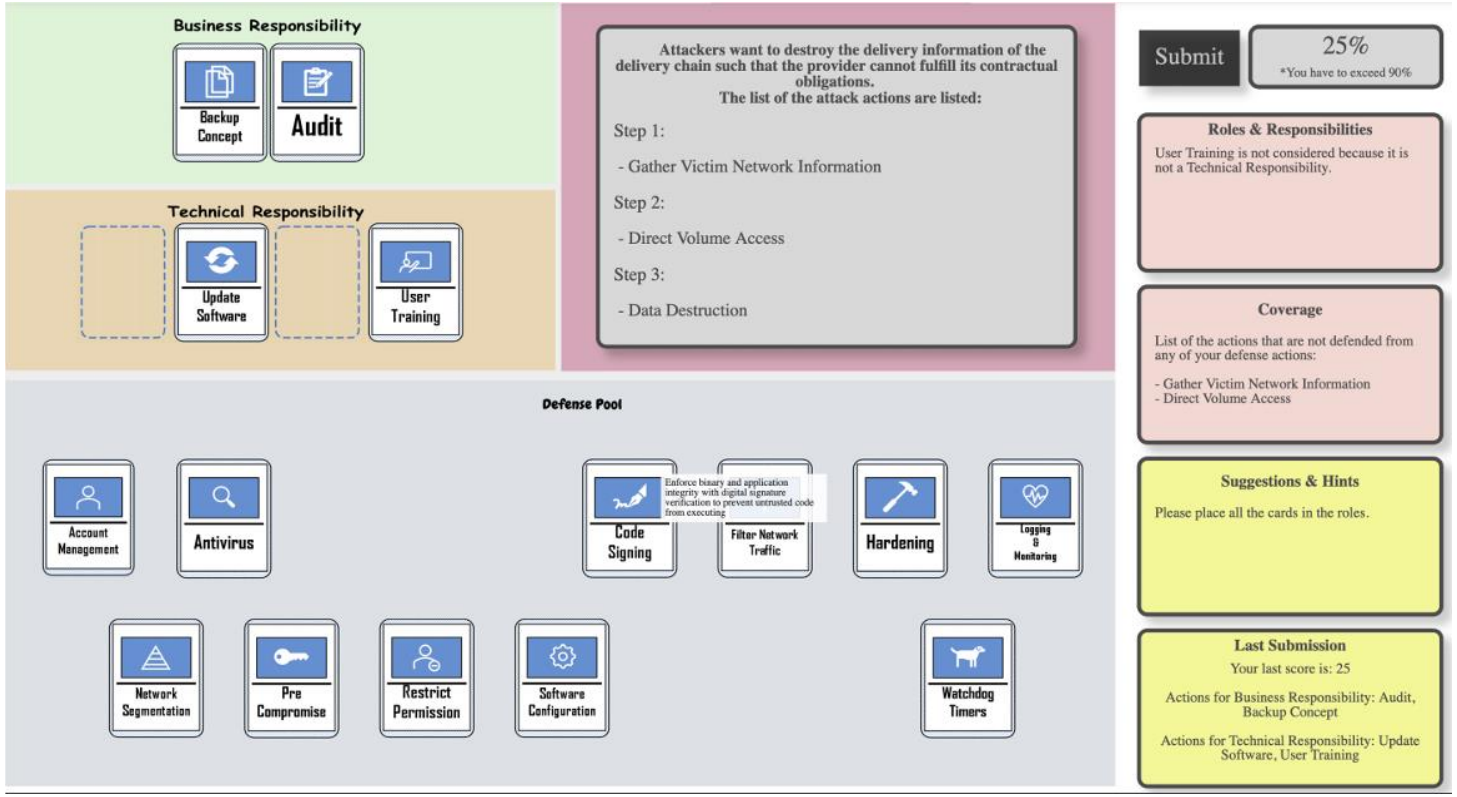
Duck Debugger

- 28 Übungen
- 4 Programmiersprachen
- Codeschnipsel mit versteckten Schwachstellen aus OWASP TOP10, MITRE CWE TOP25
- Checklisten



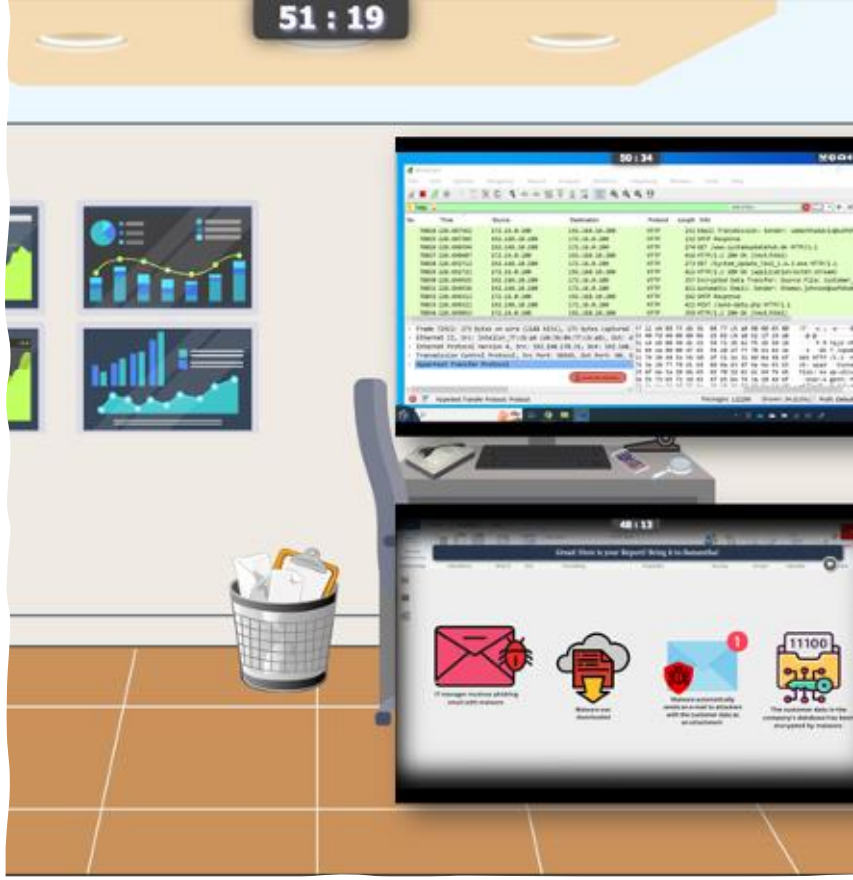
COPYCAT

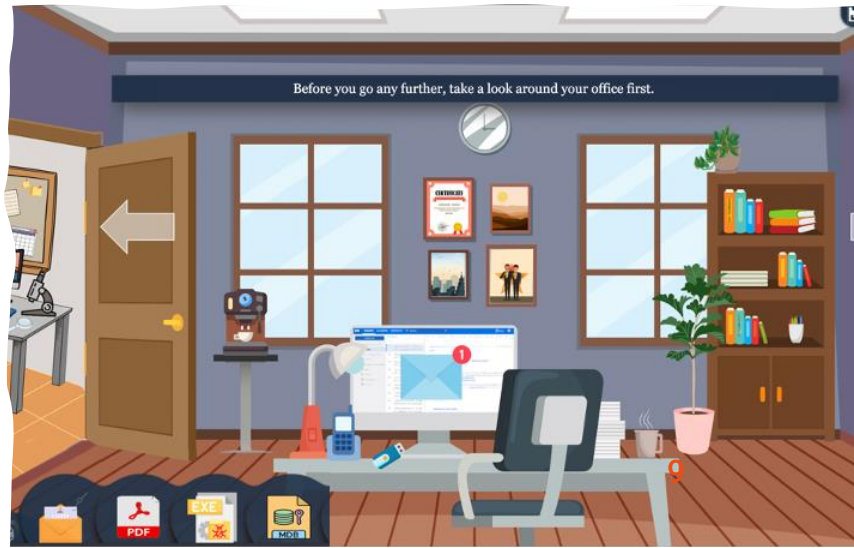
- CONTAIN SupPlY Chain Attack
- 12 x Angriffsszenarien (MITRE ATT&CK)
- Interaktive Spieloberfläche
- Rollen und Verantwortung
- Datenorientierte kill chain



Digital Detectives

- Serious Point-and-Click-Spiel für digitale Forensik
- Interaktive 2D-Spieloberfläche
- Rollen und Verantwortung kennenlernen
- Minispiele lösen, Werkzeuge verwenden und Hinweise sammeln



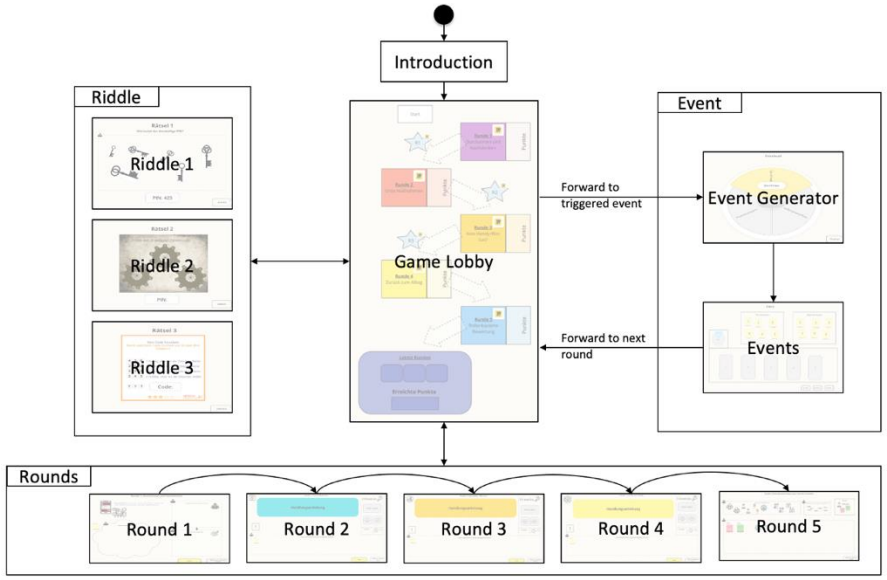


Hack dich nicht

- Spieler übernehmen die Rolle des **Spediteurs** Spediteur wird mit **Cyberangriff** auf sein Unternehmen konfrontiert
- Durch Auswahl verfügbarer Verteidigung- und Ressourcenkarten die Angriffe abzuwehren bzw. Unternehmen und Stakeholder zu schützen (Prävention)
- Interaktives Lernen über Cybersicherheit und deren Gefahren
- •Wissen durch eigene Reaktionsmuster und Strategien der Mitspieler erweitern
- Spontane und bevorzugte Reaktionsmuster erkennen

Eine Frage der Sicherheit

- Ransomware auf dem Handy! Jetzt ist guter Rat teuer. Oder?
- Rundenbasiertes Spiel für 3-8 Spielende
- Ziele:
- Wissen vertiefen
- Notfall durchspielen
- Prozesse überprüfen
- Perspektiven wechseln



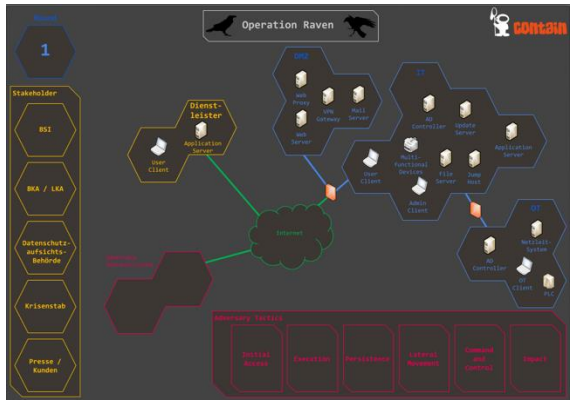
count2zero

- Ein reelles Serious Escape Room Game mit militärischem Kontext

- Methoden: Digitale Assistenzsysteme, IoT, Roboter Technologie, Pentesting
- Ziel: Steigerung des IT- Sicherheitsbewusstseins

Operation Raven

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



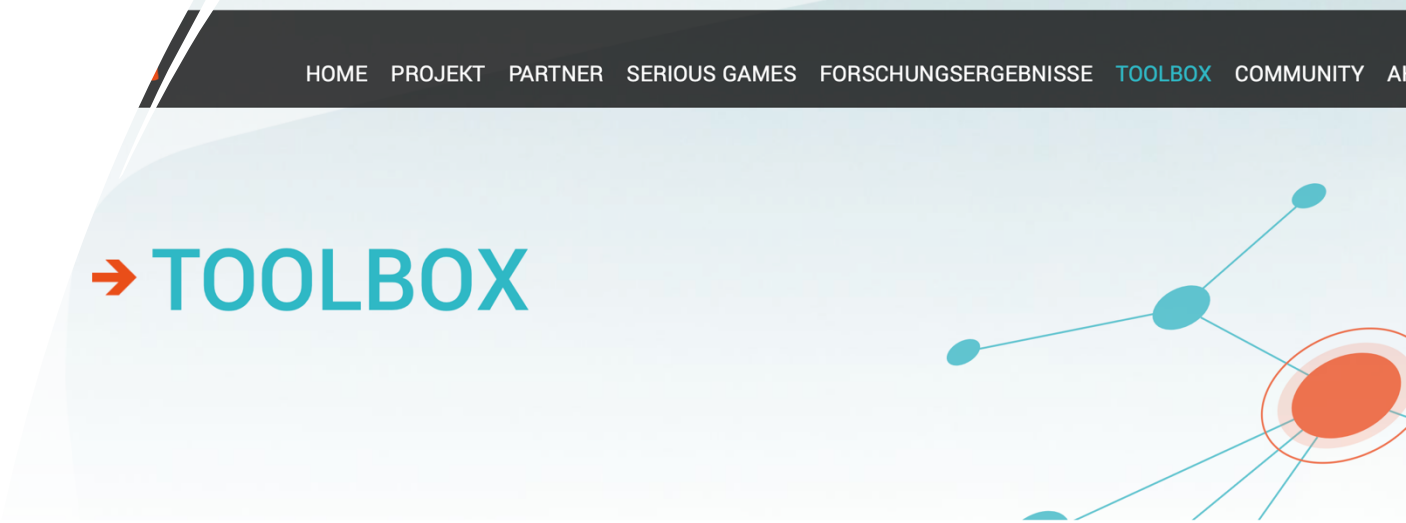
Transfer in die Praxis

Webseite & Toolbox

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

www.contain-projekt.de/

www.contain-projekt.at/



Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?