CORPORATE INNOVATION CHALLENGE

REUTLINGEN UNIVERSITY CENTER FOR ENTREPRENEURSHIP

Corporate Innovation Challenge – AI-Z Group GmbH

Titel: Brane Breakers – Könnt ihr unsere KI-Firewall knacken?

AI-Z Group entwickelt Brane AIF — einen On-Premise KI-Server für Unternehmen, der automatisch erkennt, wenn sensible Daten das System verlassen wollen. Eure Mission: Red Team + Business Risk Assessment — interdisziplinäre Teams willkommen.

Challenge:

Szenario: Ihr seid das externe Security-Audit-Team für MedTech Solutions GmbH

Technisch — Red Team:
- Encoding & Obfuskation (Base64, Leetspeak, Unicode)
- Sprach-Manipulation (Code-Switching, Multi-Sprache)
- Kontext-Täuschung („In meinem Roman…“)
- Fragmentierung über mehrere Nachrichten
- Prompt Injection (System-Override, Rollen-Wechsel)

Betriebswirtschaftlich — Risk Assessment:
- Schadensbewertung je Bypass (DSGVO, MDR, Betrieb)
- DSGVO Art. 83: bis 20 Mio. € oder 4% Umsatz
- Risiko-Matrix: Eintrittswahrsch. × Schadenshöhe
- Priorisierte Maßnahmen-Roadmap
- Executive Summary für Geschäftsführung

Phase 1 — Reconnaissance
System kennenlernen. Welche Kategorien erkannt? Namen, IBANs, Gesundheitsdaten…

Phase 2 — Attack
Bypasses entwickeln: Encoding, Sprach-Mixing, Kontext-Täuschung, Prompt Injection.

Phase 3 — Risk Assessment & Defense
Risiko-Klassifizierung, Schadensbewertung MedTech, priorisierte Maßnahmen-Roadmap.

Bewertung & Achievement Levels:

25% Kreativität & Tiefe der Angriffe
25% Business Impact Assessment
20% Dokumentationsqualität
15% Gegenmaßnahmen
15% Pitch & Präsentation

Corporate Innovation Challenge – AI-Z Group GmbH

Titel: Brane Breakers – Can you crack our AI firewall?

AI-Z Group is developing Brane AIF — an on-premise AI server for enterprises that automatically detects when sensitive data is about to leave the system. Your mission: Red Team + Business Risk Assessment — interdisciplinary teams are welcome.

Challenge:

Scenario: You are the external security audit team for MedTech Solutions GmbH

Technical — Red Team:
- Encoding & obfuscation (Base64, Leetspeak, Unicode)
- Language manipulation (code-switching, multilingual approaches)
- Context deception ("In my novel...")
- Fragmentation across multiple messages
- Prompt injection (system override, role switching)

Business — Risk Assessment:
- Damage assessment per bypass (GDPR, MDR, operations)
- GDPR Art. 83: up to €20 million or 4% of revenue
- Risk matrix:
  Probability of occurrence × impact severity
- Prioritized measures roadmap
- Executive summary for management

Phase 1 — Reconnaissance
Get to know the system. Which categories are detected? Names, IBANs, health data...

Phase 2 — Attack
Develop bypasses: encoding, language mixing, context deception, prompt injection.

Phase 3 — Risk Assessment & Defense
Risk classification, damage assessment for MedTech, prioritized mitigation roadmap.

Evaluation & Achievement Levels:

25% creativity & depth of attacks
25% business impact assessment
20% documentation quality
15% countermeasures
15% pitch & presentation