Tagebuch eines Red Teamers – Kapitel 1

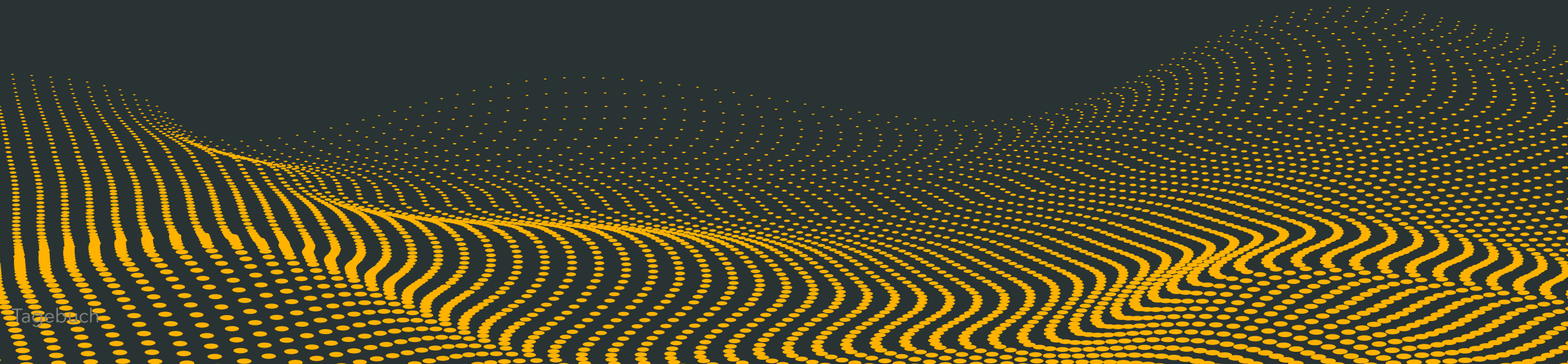
K-Businesscom

MEMBER OF CANCOM GROUP

h4ck

// we ~~transform~~ for the better

Die Angebotsphase:
Wie reden wir erfolgreich aneinander vorbei?



Why do we test a pen?!

Der Unterschied zwischen Vulnerability Scan, Penetration Test und Red Teaming

Vulnerability Scan (Inventarisierung)	**Penetration Test (Detailanalyse)**	**Red Teaming (Simulation)**
• Bekannte Schwachstellen • Automatisiert • Ausführung durch IT-Personal	• Unbekannte/komplexe Schwachstellen • Kombination aus manueller und automatisierter Analyse • Hilfestellung durch IT-Personal	• Bewertung der Effektivität der Sicherheitsstruktur • Überwiegend manuell gesteuerte Angriffe • Minimale Hilfestellung durch IT-Personal

REDuziertes Teaming

Red Nessing

- Einmaliger automatisierter Schwachstellenscan mit Nessus inkl. automatisiertem Bericht
- Kostet zwar mehr, dafür bekommst du aber auch weniger ☺

Red Exing / Red Inting

- Klassischer externer oder interner Penetration Test …
- … klingt jedoch cooler, wenn das Wort „Red“ drin vorkommt!

Red Singling

- Red **TEAM**ing mal anders
- **T**oll, **E**iner **A**llein **M**acht‘s

Und “richtiges” Red Teaming!??

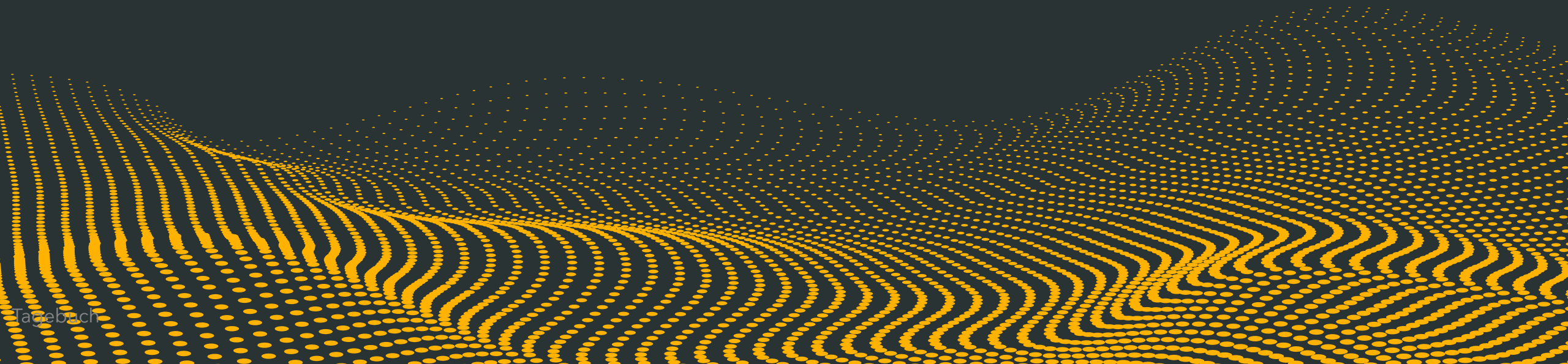
Stichwort: TIBER-EU

- Möglichkeit zur Erkennung und Reaktion auf Angriffe
  - Idealerweise eigenes Blue Team

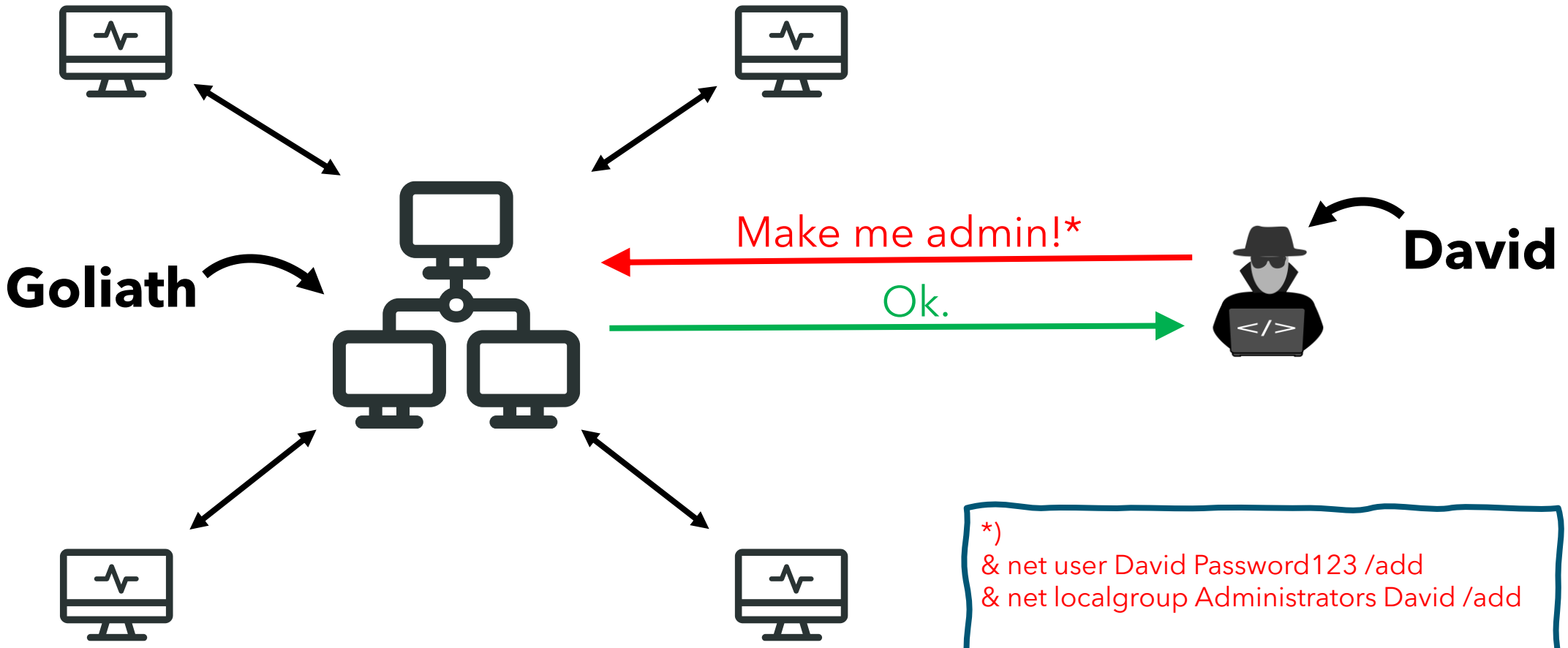
- Breite Ausrichtung
  - Finden von Schwachstellen ist idR nicht das Hauptziel

- Ständiger Kontakt zwischen Red Team und dem Kunden (White Team)
  - White Team: Organisation und Überwachung des Red Teamings

Die Auftragsdurchführung: Solides Fundament oder doch nur Sandburg?



David gegen Goliath

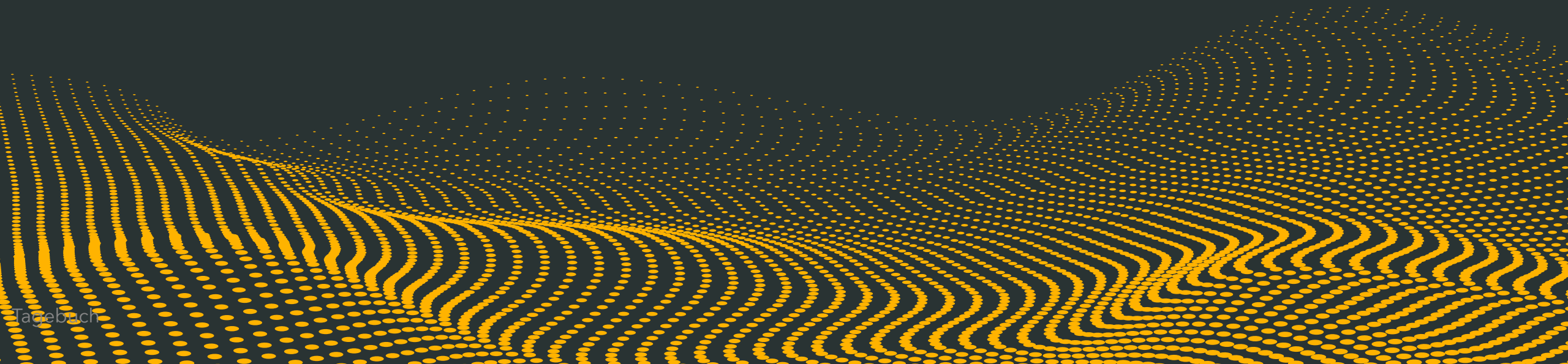


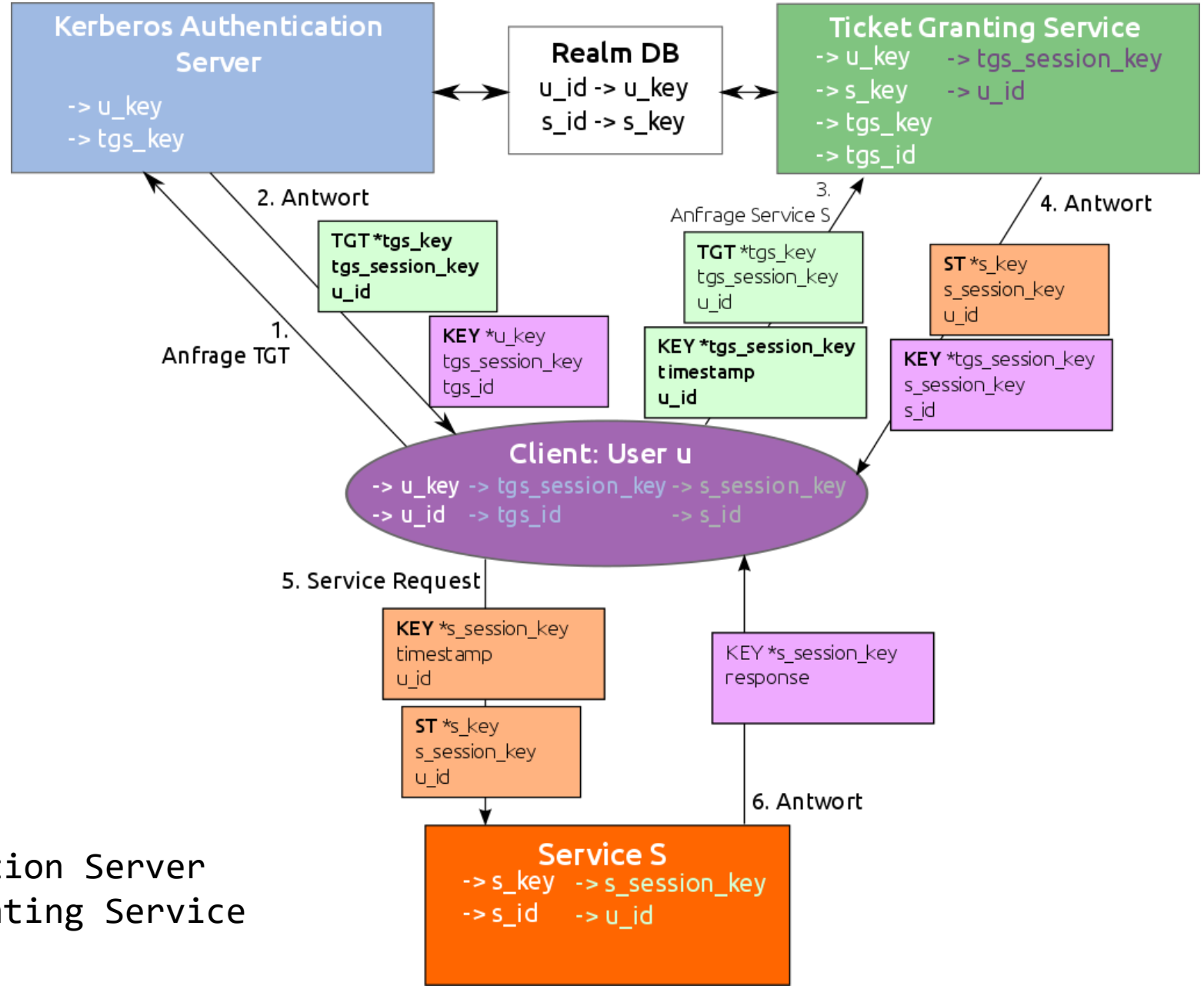
Kaffeemaschinen-Effekt

Ihr so

Ich so

Die Auftragsdurchführung:
Wie war das gleich nochmal?

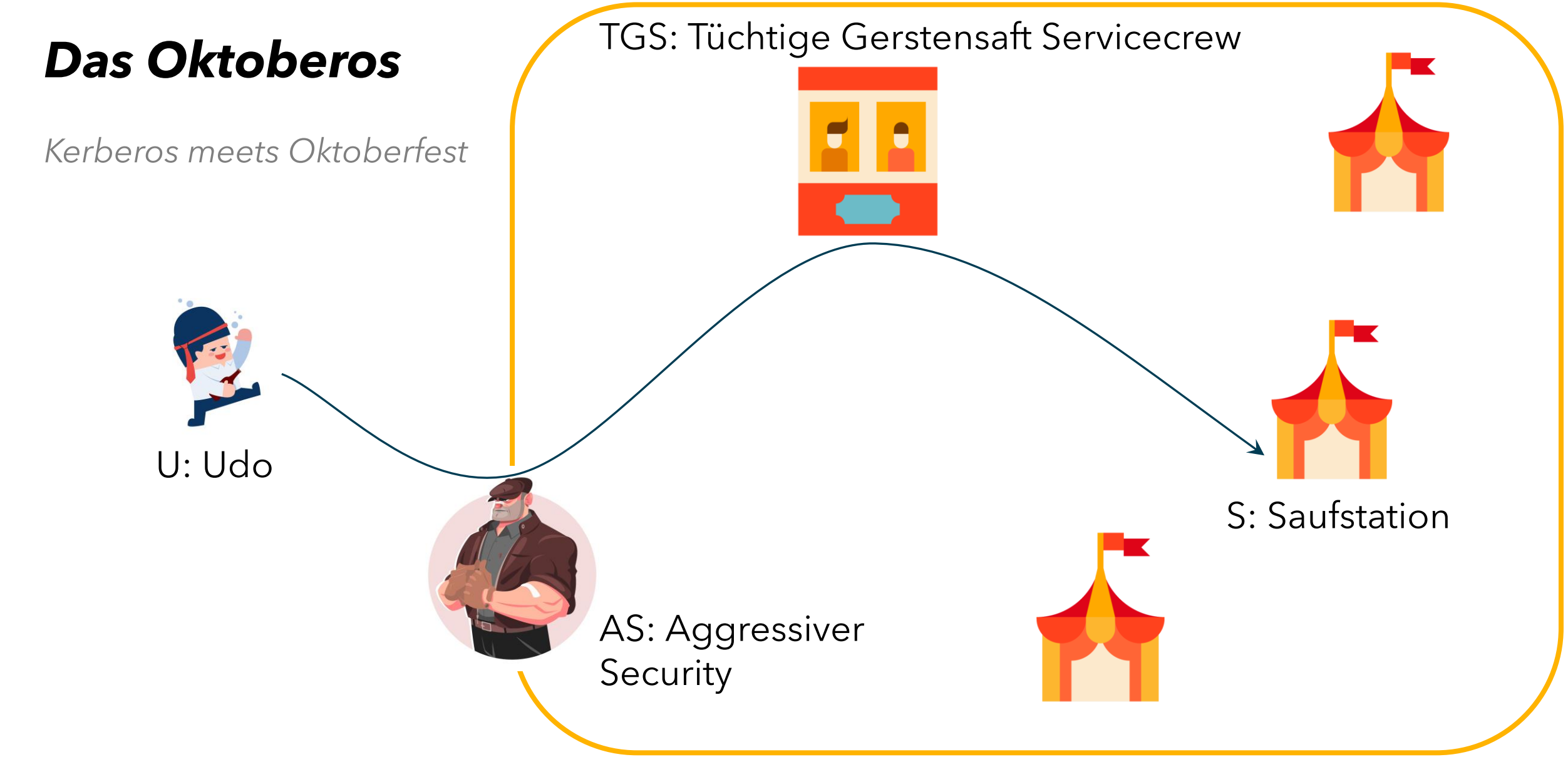




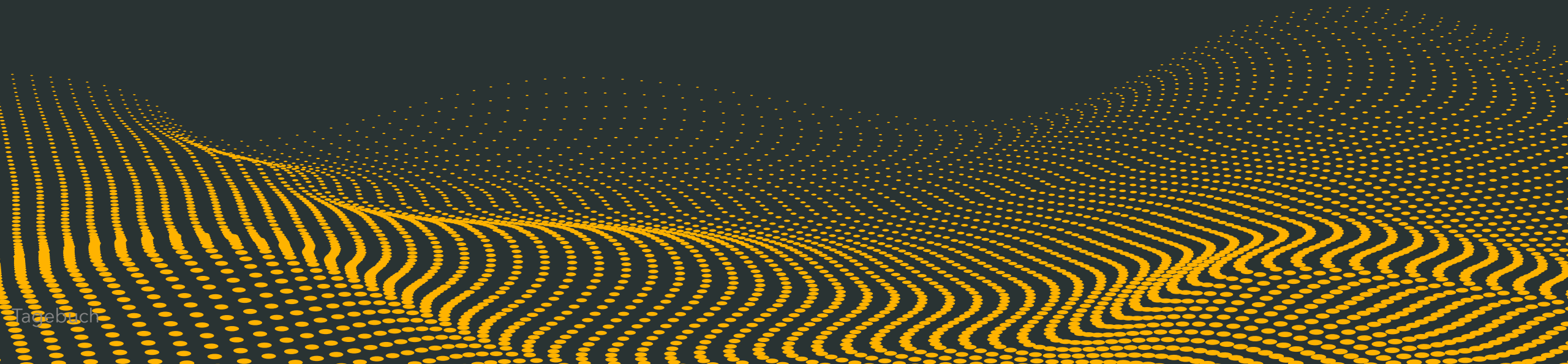
U: User
AS: Authentication Server
TGS: Ticket Granting Service
S: Service

Das Oktoberos

Kerberos meets Oktoberfest

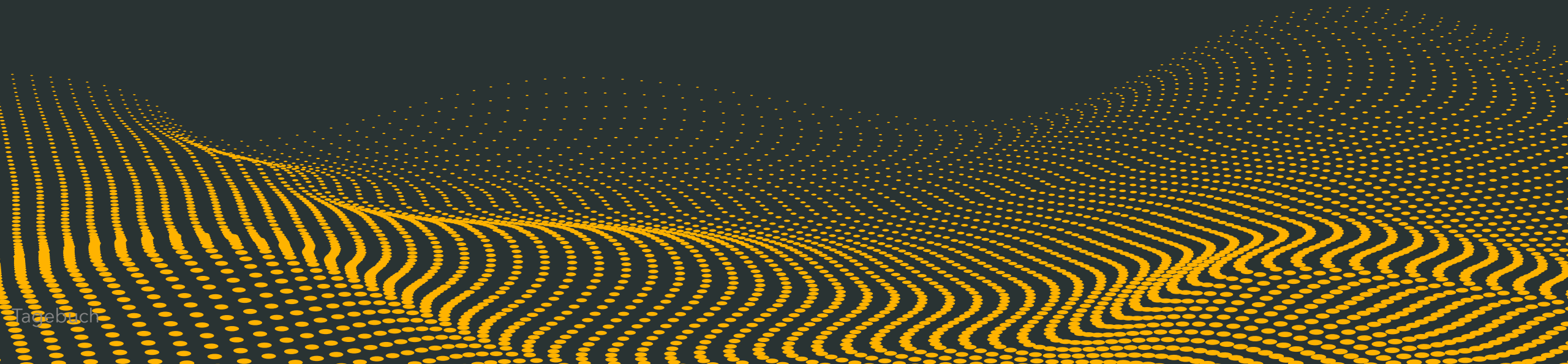


Der Projektabschluss:
Das Beste kommt zum Schluss!




Hannes
Manfred
(Teamlead)

War da jetzt irgendwas Wichtiges dabei?



Takeaways

- Vulnerability Scan ≠ Penetration Test ≠ Red Teaming
  - Vulnerability Scan → Inventarisierung
  - Penetration Test → Detailanalyse
  - Red Teaming → Simulation

- Gemeinsames Verständnis des Projektziels sowie des Weges dorthin ist enorm wichtig!

- In allen Fällen arbeiten wir **zusammen**! Alle Beteiligten sollten sich abgeholt fühlen!

MEMBER OF
CANCOM GROUP

Hannes Trunde

#gerneperdu

Information Security Auditor
Erfinder des Kaffeemaschinen-Effekts
Gründer des Oktoberos

hannes.trunde@k-business.com
redteam@k-business.com

https://linkedin.com/in/hannestrunde/

https://twitter.com/hannestrunde

https://youtube.com/@hannestrunde