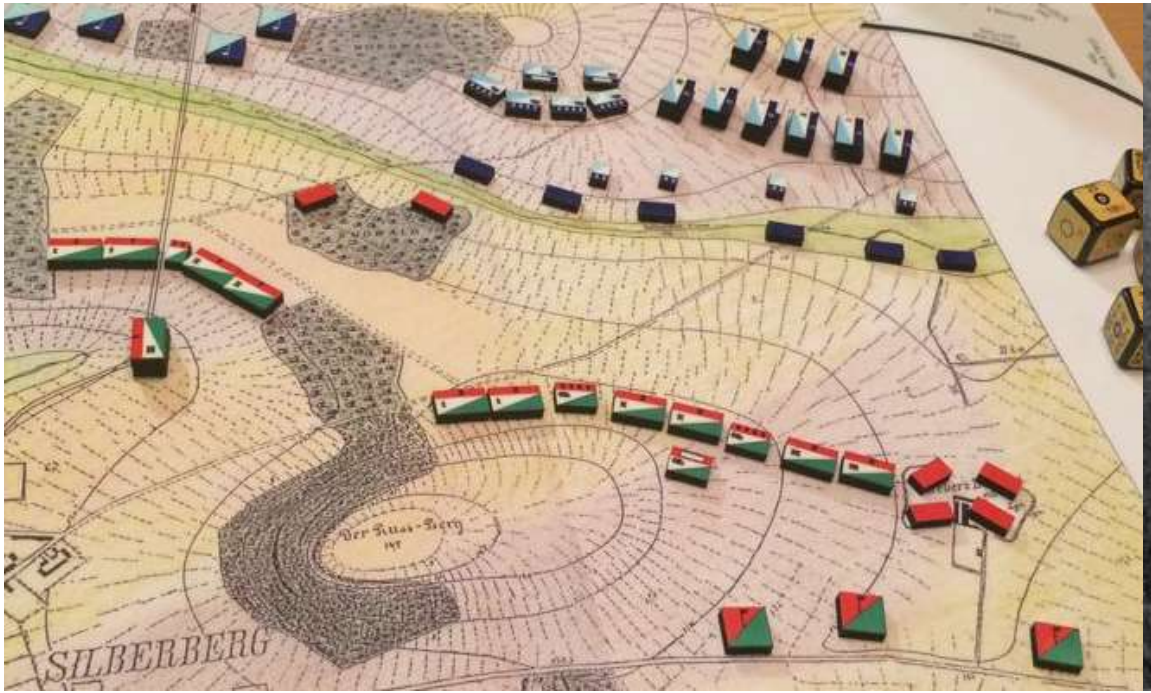
Was ist das eigentlich, und wann braucht man es?

Red Teaming – IT-Security im Stresstest

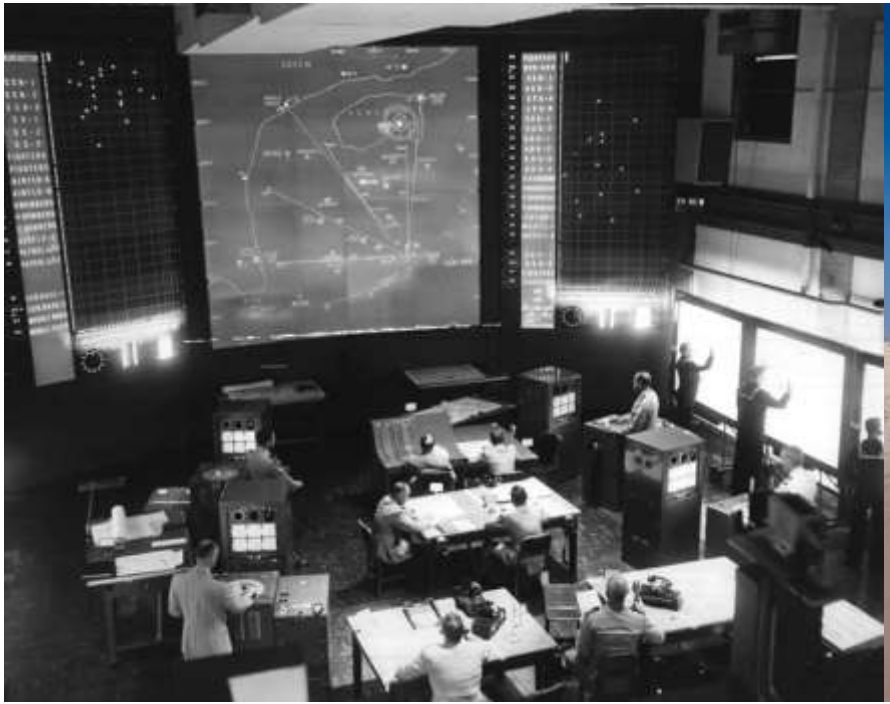
HiSolutions Know-how to go

Dr. Jörg Schneider

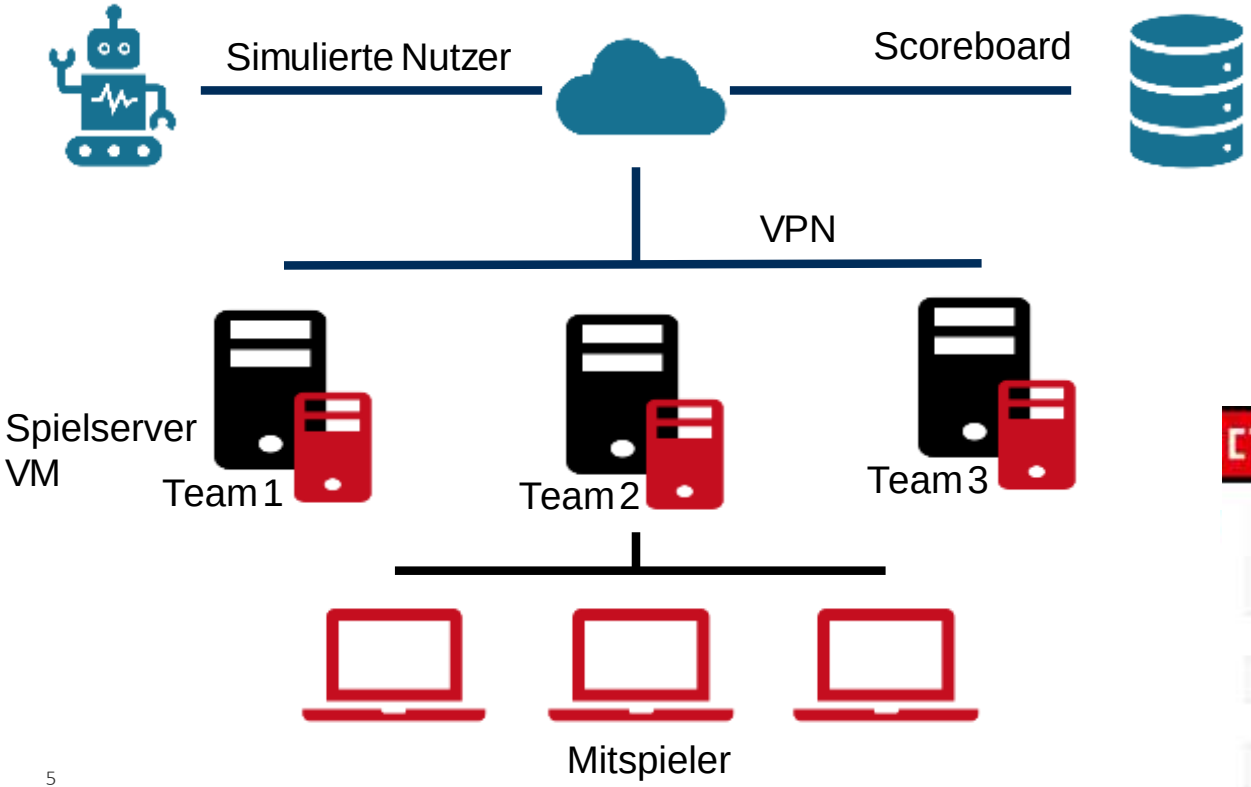
Rot gegen Blau hat eine lange Geschichte



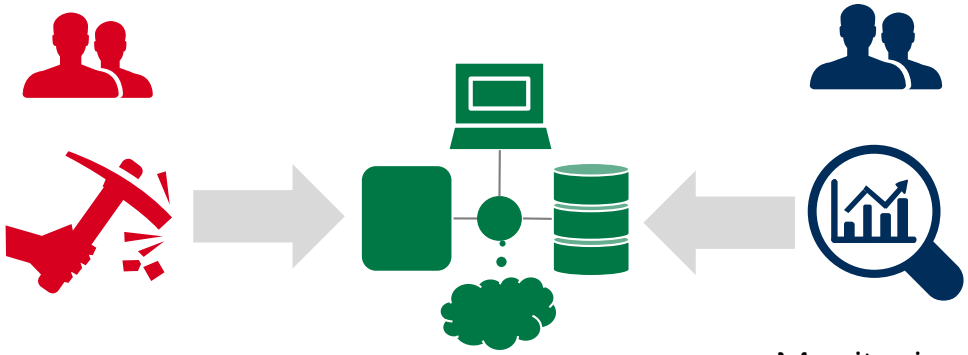
Rot gegen Blau hat eine lange Geschichte



Capture the Flag (CTF)



Und was ist jetzt Red Teaming?



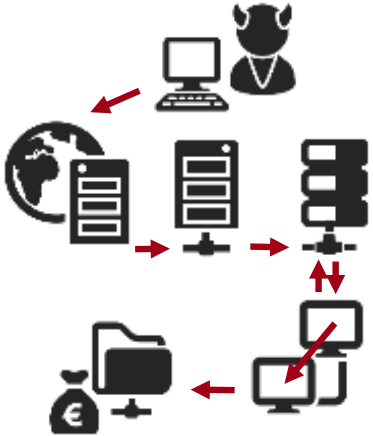
Angriffs-
simulation

Monitoring
SIEM, SOC

Red-Teaming -Szenarien und Komponenten

Physische Angriffe
gegen Standorte oder Bereiche

Social Engineering
Angriffe gegen Nutzer

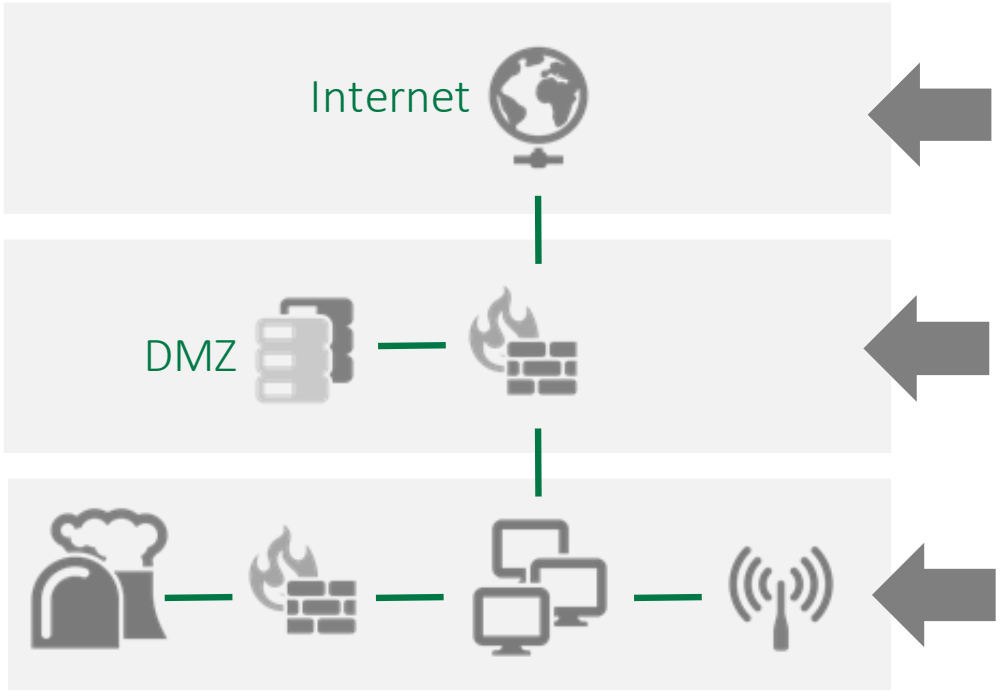


Technische Angriffe
gegen IT-Systeme

Vorgehensweise „Assume Compromise“

- Annahme: irgendwann wird ein System kompromittiert
  (z. B. 0-day-Schwachstelle in externer Anwendung,
  erfolgreicher Phishing-Angriff, schadhaftes Software-Update)
- Schrittweise Simulation des Angriffspfads zur Prüfung auf Folgerisiken
  - Zugriff auf DMS- oder Client-System oder
  - Einbringen eines Systems der Prüfer in das interne Netzwerk
- genauere und kosteneffizientere Defense-in-Depth-Prüfung
  (im Vergleich zur reinen Black-Box-Prüfung)
- Simulation der Risiken bei erfolgreicher Kompromittierung

„Assume Compromise“: Ansatzpunkte und Szenarien



Initial: Angriffe aus dem Internet

- Szenario: externer Angreifer
- Ziel: extern erreichbare Server, Webanwendungen

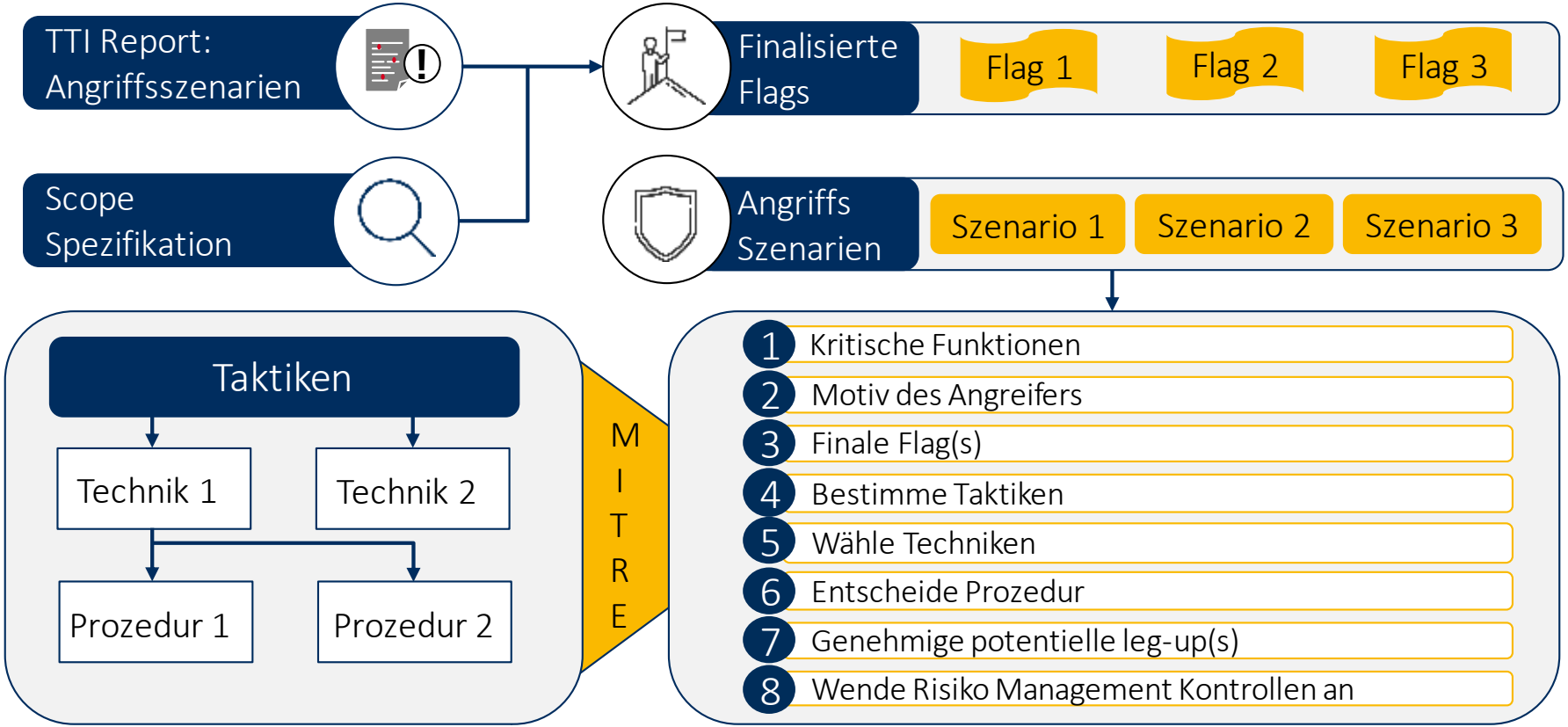
Kompromittiertes DMZ-System

- Szenario: Angreifer hat die Firewall überwunden.
- Ziel: Backend-Systeme, Netztrennung

Angriffe aus dem Intranet

- Szenario: Innentäter oder kompromittiertes Endgerät (z. B. durch Phishing-Angriff)
- Ziel: Gesamt- oder Teilnetz, Netztrennung, interne Anwendungen und Systeme

TIBER – Threat-Intelligence-based Ethical Red Teaming
Ein Standard für die Finanzwirtschaft



Welche Auditform passt wann am besten?

	Security Basis-Check	Penetrationstest	Red Teaming
Reifegrad der Security	Alle	Mittel - Hoch	Hoch
Prüfziele	Lagebestimmung, Risiken identifizieren	Möglichst viele technische Risiken identifizieren	Erkennung und Reaktion prüfen, ggf. Awareness
Aufwand	Niedrig	Mittel	Hoch
Dauer	Kurz (wenige Stunden)	Mittel (einige Tage)	Lang (mehrere Wochen)

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com