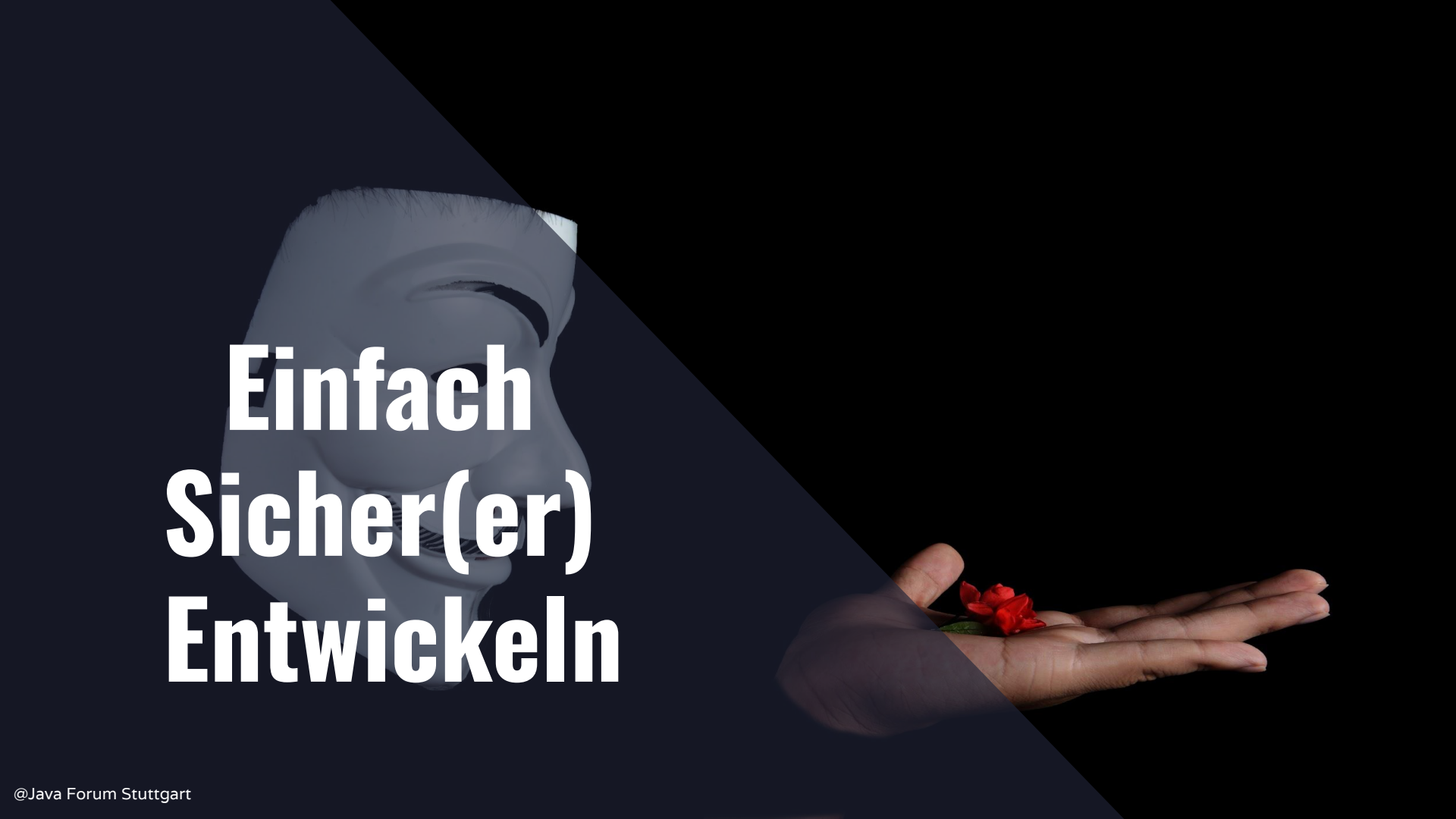

Einfach
Sicher(er)
Entwickeln

About me

Steve Gerstner

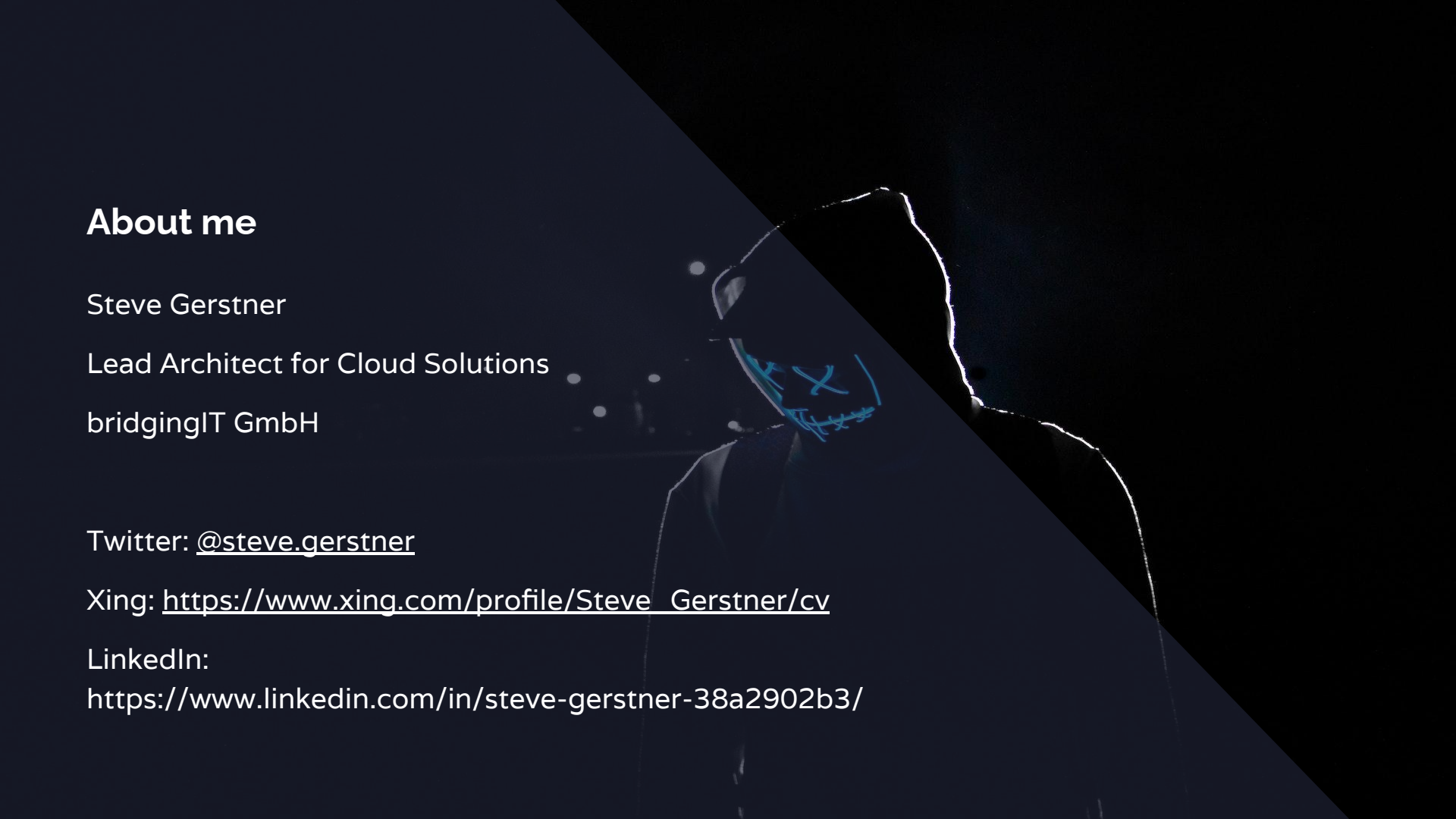
Lead Architect for Cloud Solutions

bridgingIT GmbH

Twitter: @steve.gerstner

Xing: https://www.xing.com/profile/Steve_Gerstner/cv

LinkedIn:
https://www.linkedin.com/in/steve-gerstner-38a2902b3/



Disclaimer

Agenda

- Motivation
- Security für Architekten
- Security in der Entwicklung

Nach globalem IT-Ausfall

BSI-Chefin will stärker auf Qualität von Produkten achten

Ein fehlerhaftes Update führte weltweit zu Chaos. Die Chefin des Bundesamts für Sicherheit in der Informationstechnik, Claudia Plattner, kündigt Maßnahmen an. Ganz werde man derartige Ausfälle aber nicht verhindern können.

20.07.2024, 05.28 Uhr

Artikel zum Hören • 2 Min Anhören

https://www.spiegel.de/netzwelt/crowdstrike-und-microsoft-bsi-chefin-plattner-will-staerkere-kontrollen-a-3374dc42-71c4-4592-b831-829ddc05b7ef

Entwickelt IHR sicher?

Habt ihr schon einmal eine Sicherheitslücke gefunden?

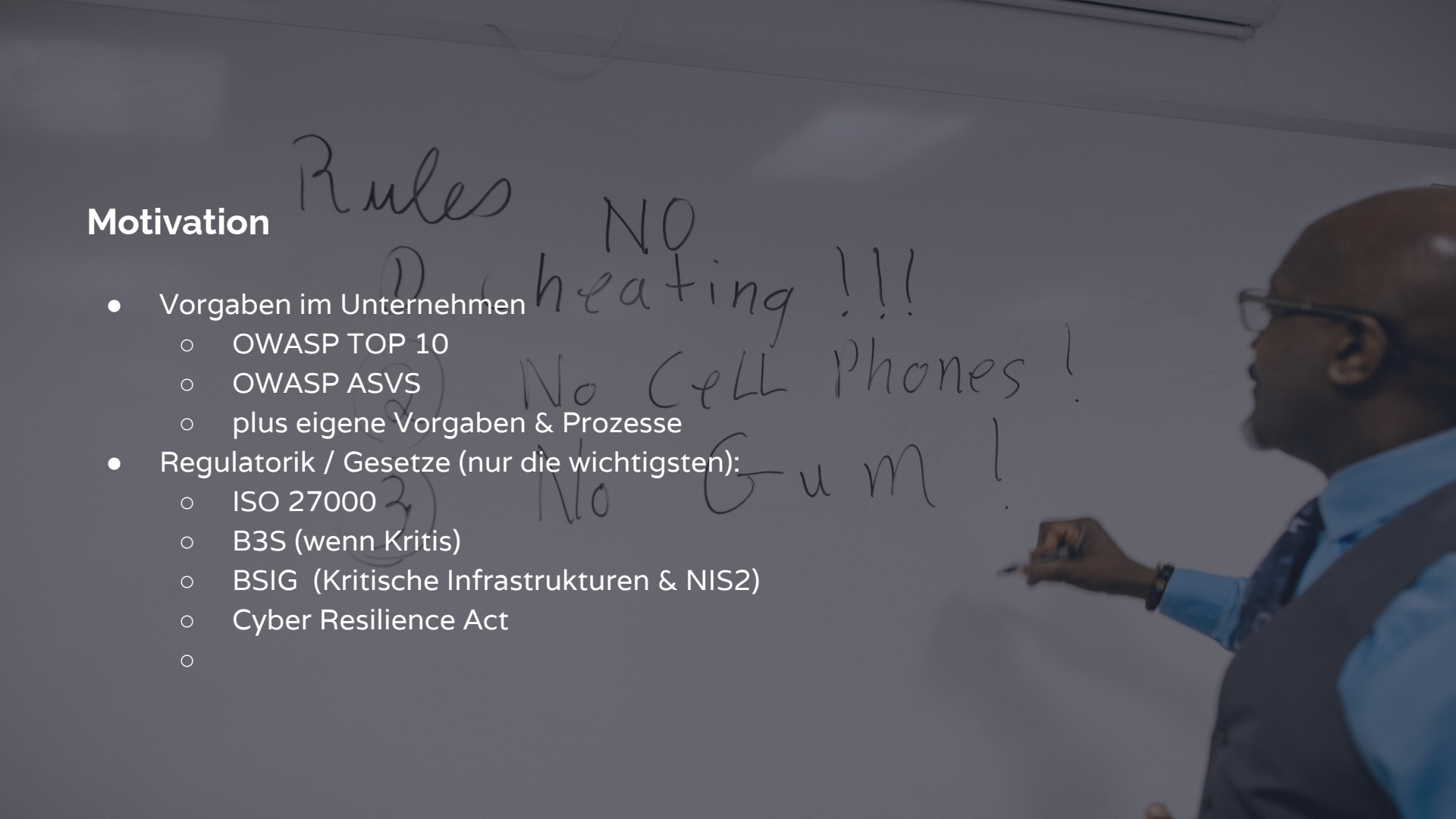
Habt ihr schon einmal eine Sicherheitslücke verursacht?

Motivation

Softwarecraftsmanshift

Motivation

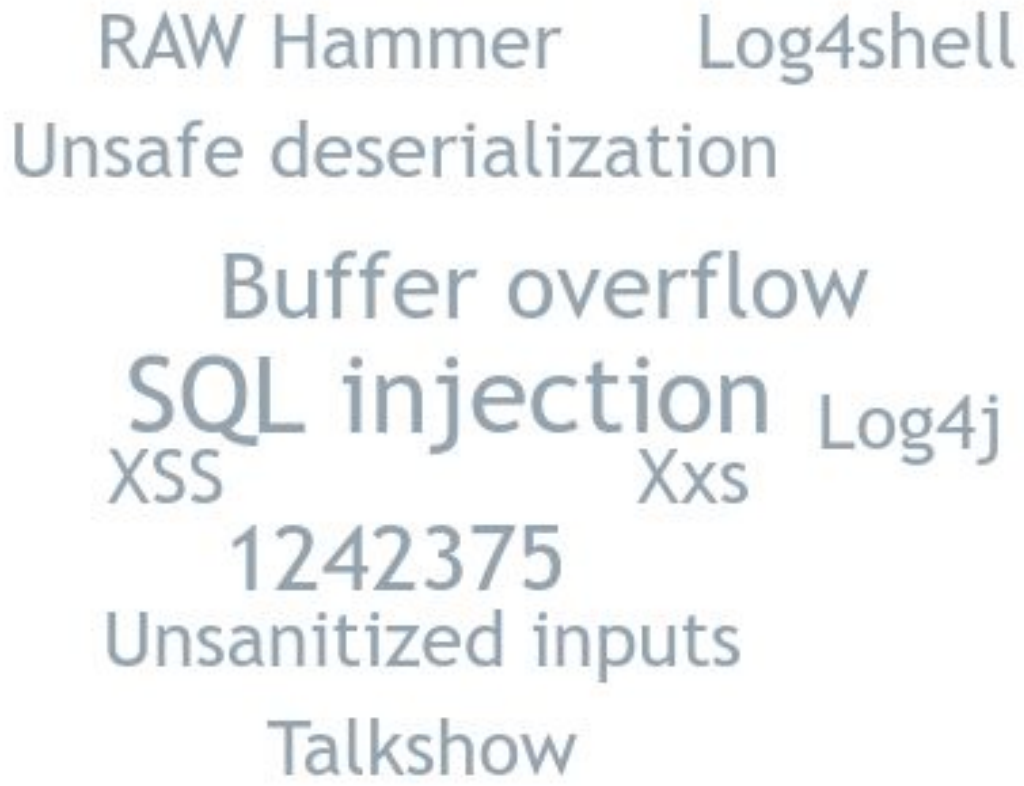
- Vorgaben im Unternehmen
  - OWASP TOP 10
  - OWASP ASVS
  - plus eigene Vorgaben & Prozesse
- Regulatorik / Gesetze (nur die wichtigsten):
  - ISO 27000
  - B3S (wenn Kritis)
  - BSIG (Kritische Infrastrukturen & NIS2)
  - Cyber Resilience Act
  -



ISO 27001 A8.25

Rules for the secure development of software and systems should be established and applied.

Welche Security Bugs kennt ihr?



OWASP Top 10

1. Injection
2. Authentication-Fehler
3. Verlust der Vertraulichkeit sensibler Daten
4. XML External Entities (XXE)
5. Fehler in der Zugriffskontrolle
6. sicherheitsrelevante Fehlkonfiguration
7. XSS
8. unsichere Deserialisierung
9. Nutzung von Komponenten mit bekannten Schwachstellen
10. Unzureichendes Logging und Monitoring

OWASP Application Security Verification Standard

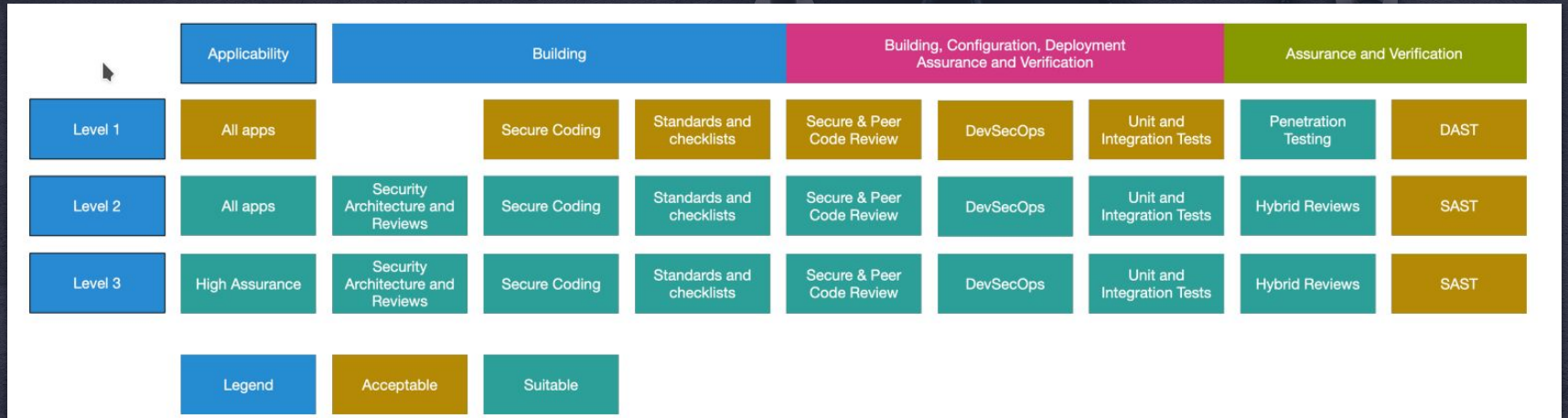


Figure 1 - OWASP Application Security Verification Standard 4.0 Levels

https://www.owasp.org/images/d/d4/OWASP_Application_Security_Verification_Standard_4.0-en.pdf


Security für
Architekten

Welche Security-Themen berücksichtigt ihr in der Entwicklung?

Least privilege

Security Header (CORS etc)

Zugriff auf Endpunkte

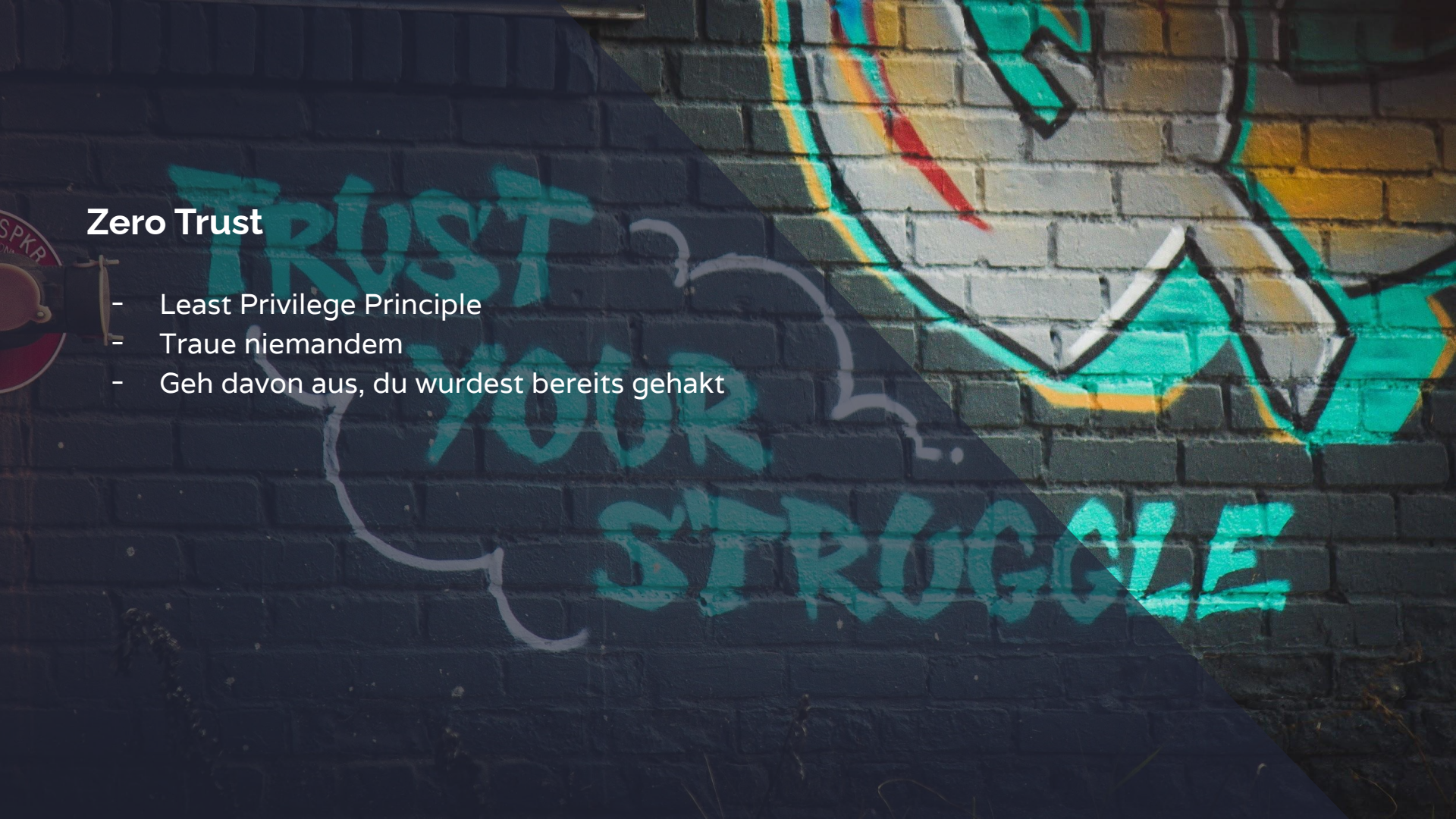
Talahon Rbac XXE

Escaping Input sanitizing

Valid inputs

Penetration Testing

Input validation



Zero Trust

- Least Privilege Principle
- Traue niemandem
- Geh davon aus, du wurdest bereits gehakt

Verteidigung in der Tiefe

Checkliste Architektur

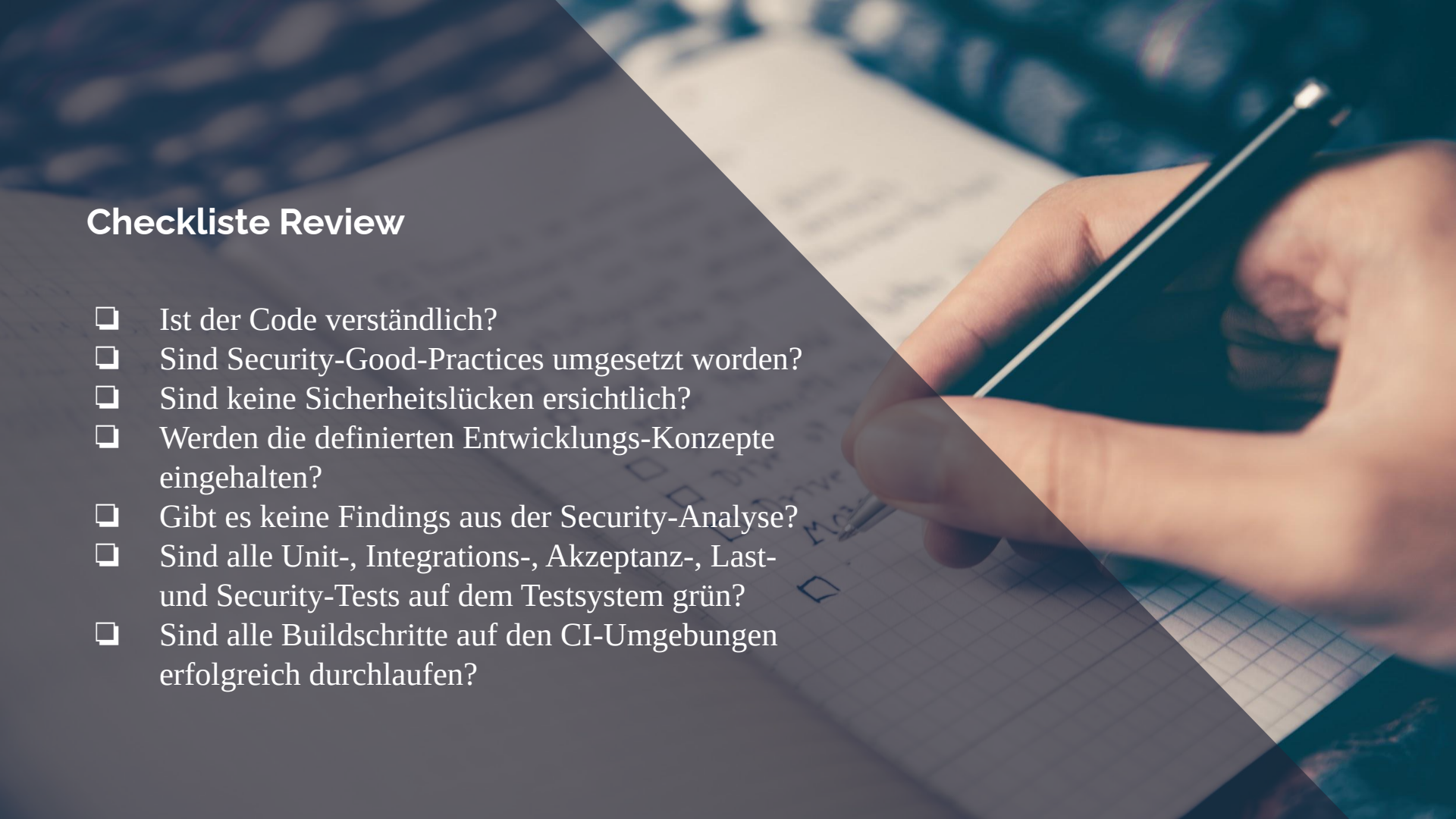
- ❑ Architekturdokumentation
- ❑ Infrastruktur
- ❑ Qualitative Anforderungen
  - ❑ ISO 25000
  - ❑ Arc42 Quality Model
- ❑ sicherer Entwicklungsprozess
  - ❑ Reviews
  - ❑ Code sicher halten
  - ❑ Umgang mit Sicherheitslücken
  - ❑ Security-Infrastruktur für die Entwicklung
  - ❑ Threat Model
  - ❑ SAST/DAST

Sichere Datenübertagung

- ❏ Daten im Transfer sind verschlüsselt
- ❏ vertrauliche und/oder persönliche Daten im Storage sind verschlüsselt
- ❏ nicht genutzte Methoden und Content-Types sind blockiert
- ❏ alle relevanten HTTP-Header sind gesetzt (OWASP ASVS)
- ❏ Sessions im Webserver sind sicher konfiguriert

Schreibt ihr für eure Security-Funktionen Tests inkl. aller Fehlerfälle?

Security für Entwickler



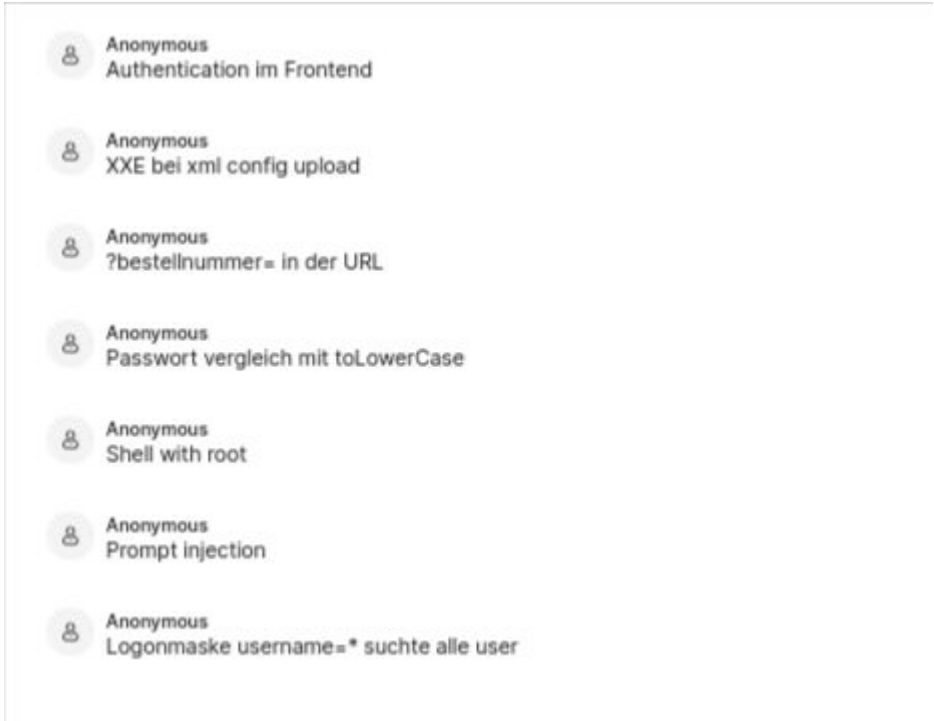
Checkliste Review

- ❑ Ist der Code verständlich?
- ❑ Sind Security-Good-Practices umgesetzt worden?
- ❑ Sind keine Sicherheitslücken ersichtlich?
- ❑ Werden die definierten Entwicklungs-Konzepte eingehalten?
- ❑ Gibt es keine Findings aus der Security-Analyse?
- ❑ Sind alle Unit-, Integrations-, Akzeptanz-, Last- und Security-Tests auf dem Testsystem grün?
- ❑ Sind alle Buildschritte auf den CI-Umgebungen erfolgreich durchlaufen?

Verteidigung im Code

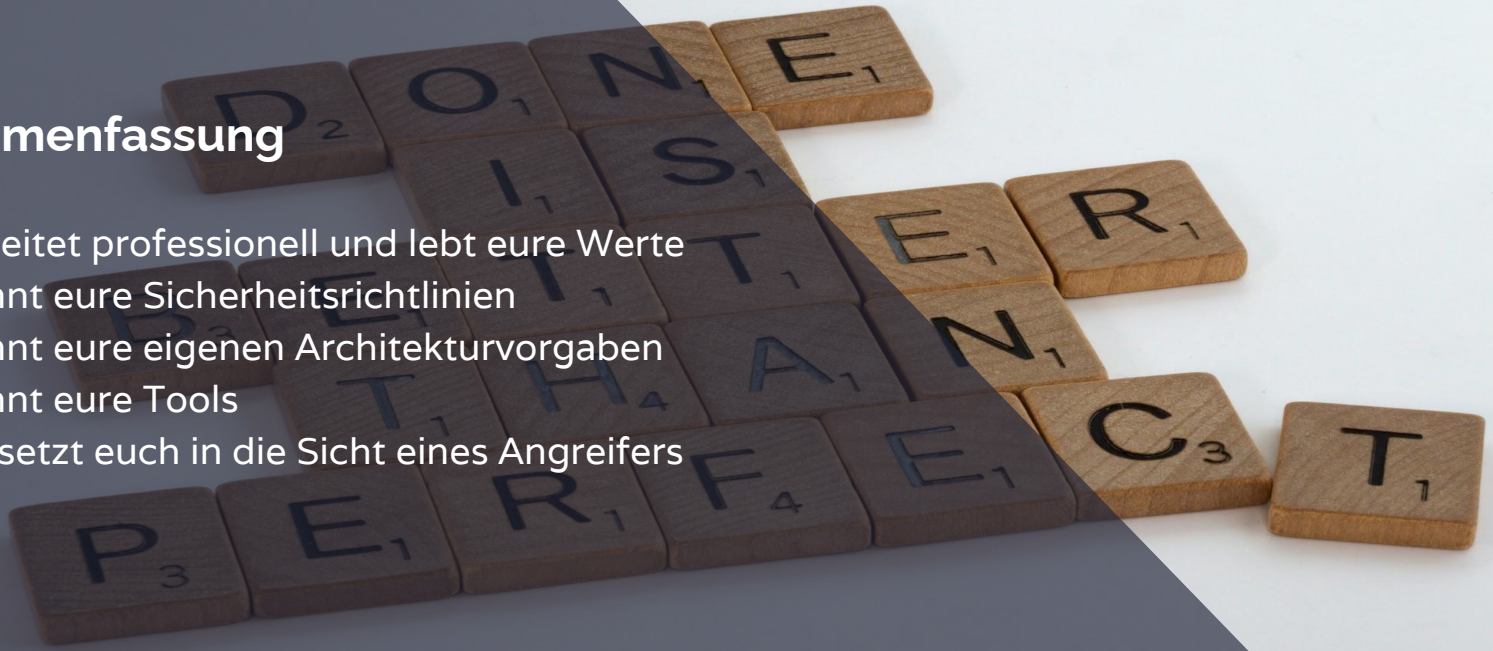
- ❏ Authentication
- ❏ Authorization am Endpoint
- ❏ Input Validation
- ❏ Authorization auf dem Objekt
- ❏ Persistenz
- ❏ Output Encoding
- ❏ keine Informationen über den Code an Nutzer

Was war die spannendeste Lücke, die ihr schon selbst gefunden habt?



Zusammenfassung

- ✓ arbeitet professionell und lebt eure Werte
- ✓ kennt eure Sicherheitsrichtlinien
- ✓ kennt eure eigenen Architekturvorgaben
- ✓ kennt eure Tools
- ✓ versetzt euch in die Sicht eines Angreifers

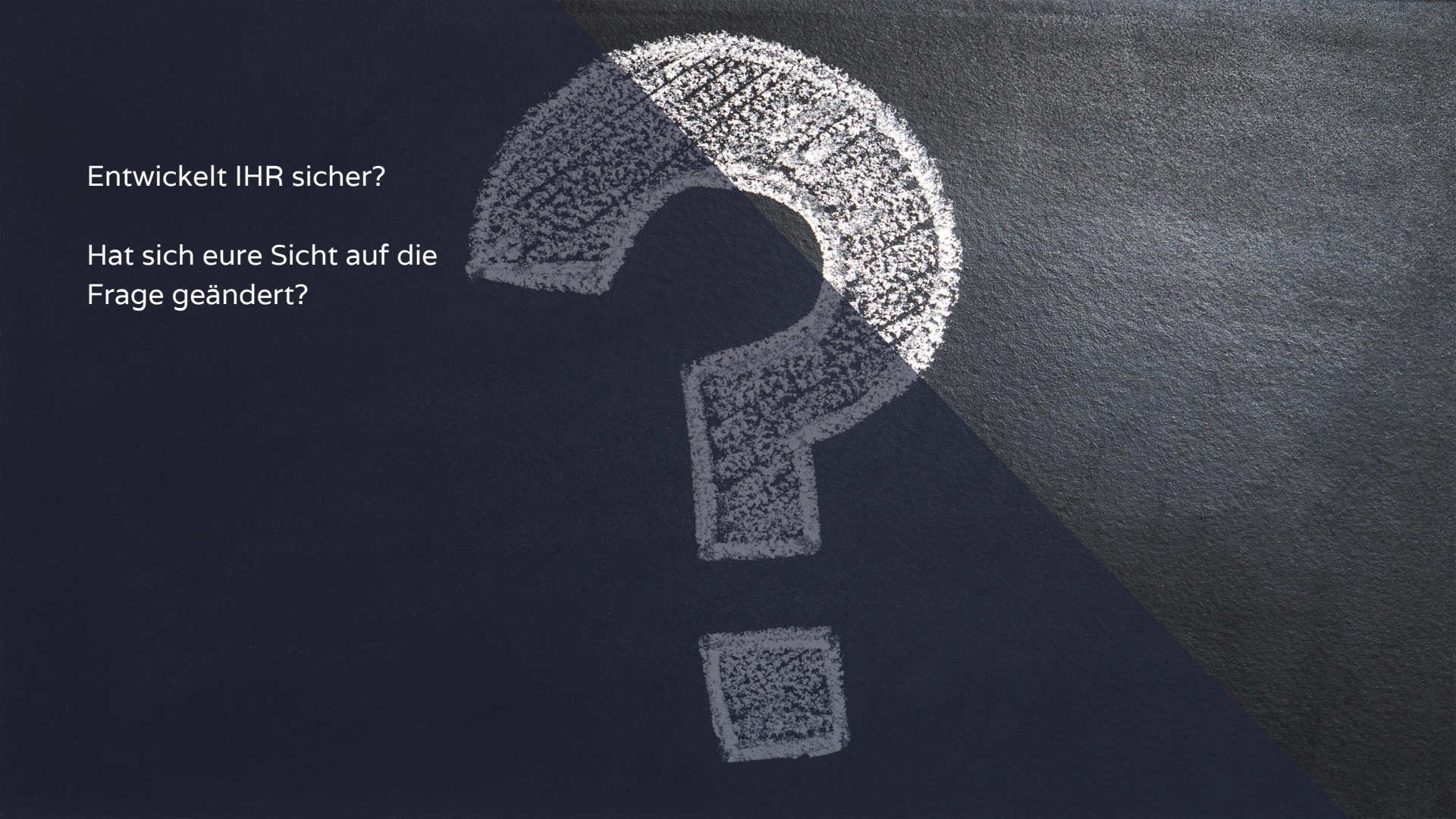


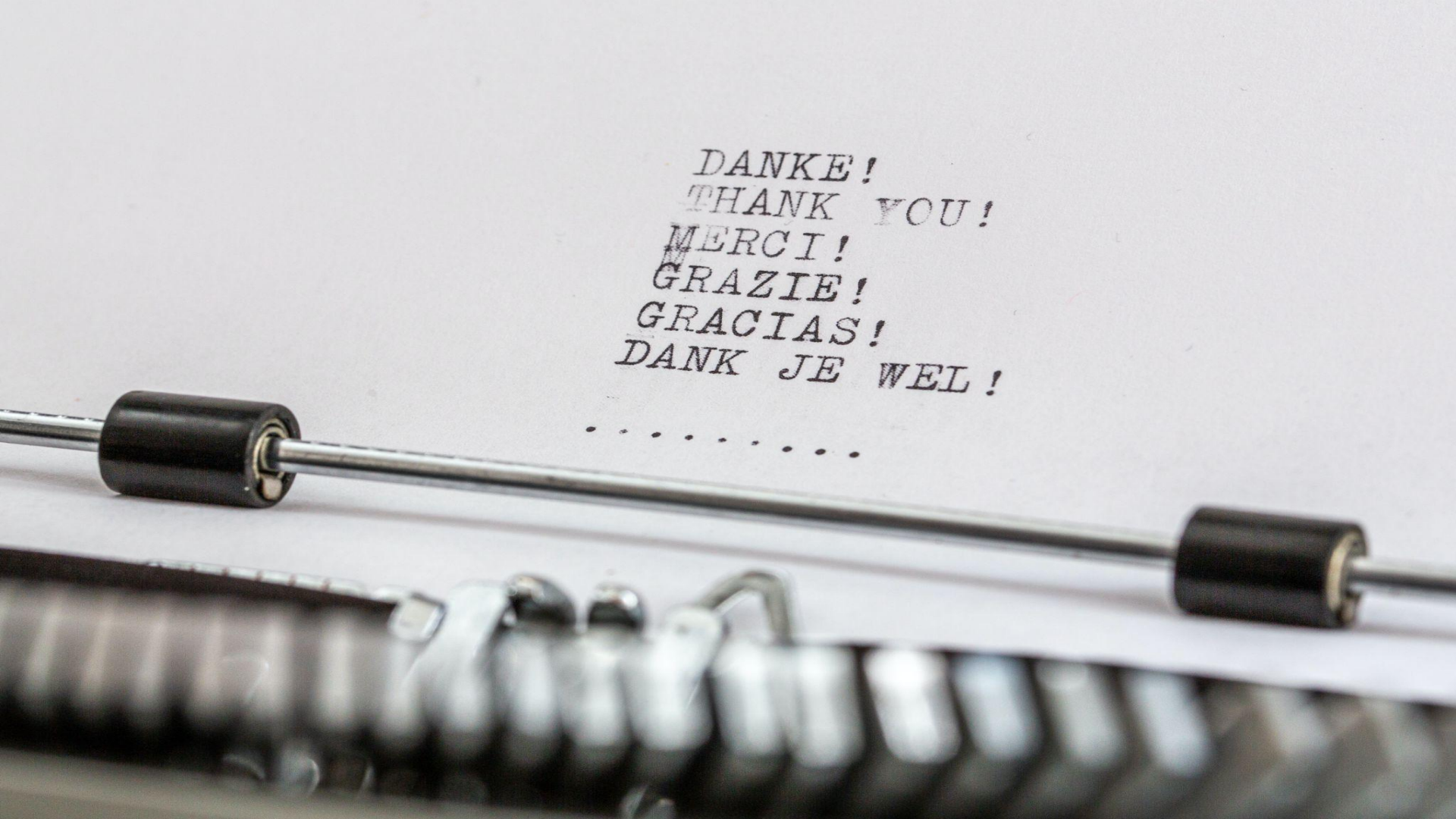
What's next

- Kryptografie
- AI
- Pentesting
- ...

Entwickelt IHR sicher?

Hat sich eure Sicht auf die Frage geändert?




DANKE!
THANK YOU!
MERCI!
GRAZIE!
GRACIAS!
DANK JE WEL!