MindBytes

Pentesting vs. Red Teaming

Schwachstellen gezielt aufspüren – Einblicke aus der Praxis

3 Dinge, die ich euch mitgeben möchte

Sprecht über Inhalte und
verlasst euch *nicht* auf Begriffe.

Überlegt, welche **Ziele** ihr mit
dem Projekt verfolgen möchtet.

Gestaltet das Projekt
passend zu euren Zielen.

MindBytes & ich

3 Gründer & Geschäftsführer

Jeweils 6-8 Jahre Erfahrung in der IT-Sicherheitsbranche

Gegründet 2023

Spezialisiert auf das Aufdecken von Schwachstellen und Angriffssimulationen (Pentesting & Red Teaming)

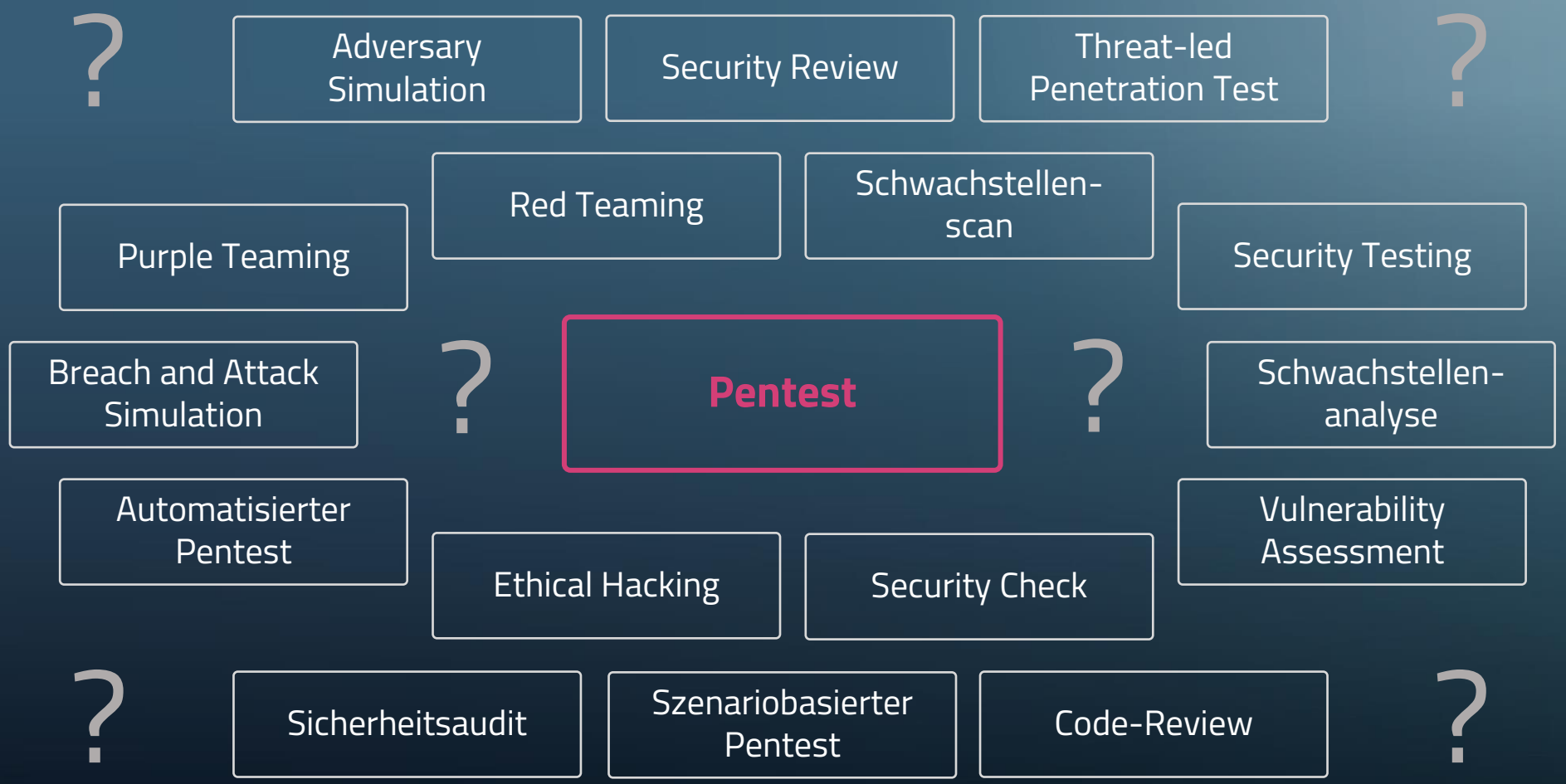
Christian Stehle
Stuttgart
(OSCP, CRTO, OSEP, OSWE, CRTP, ...)

Nina Wagner
Augsburg
(OSCP, CRTO, CARTP, CSP)

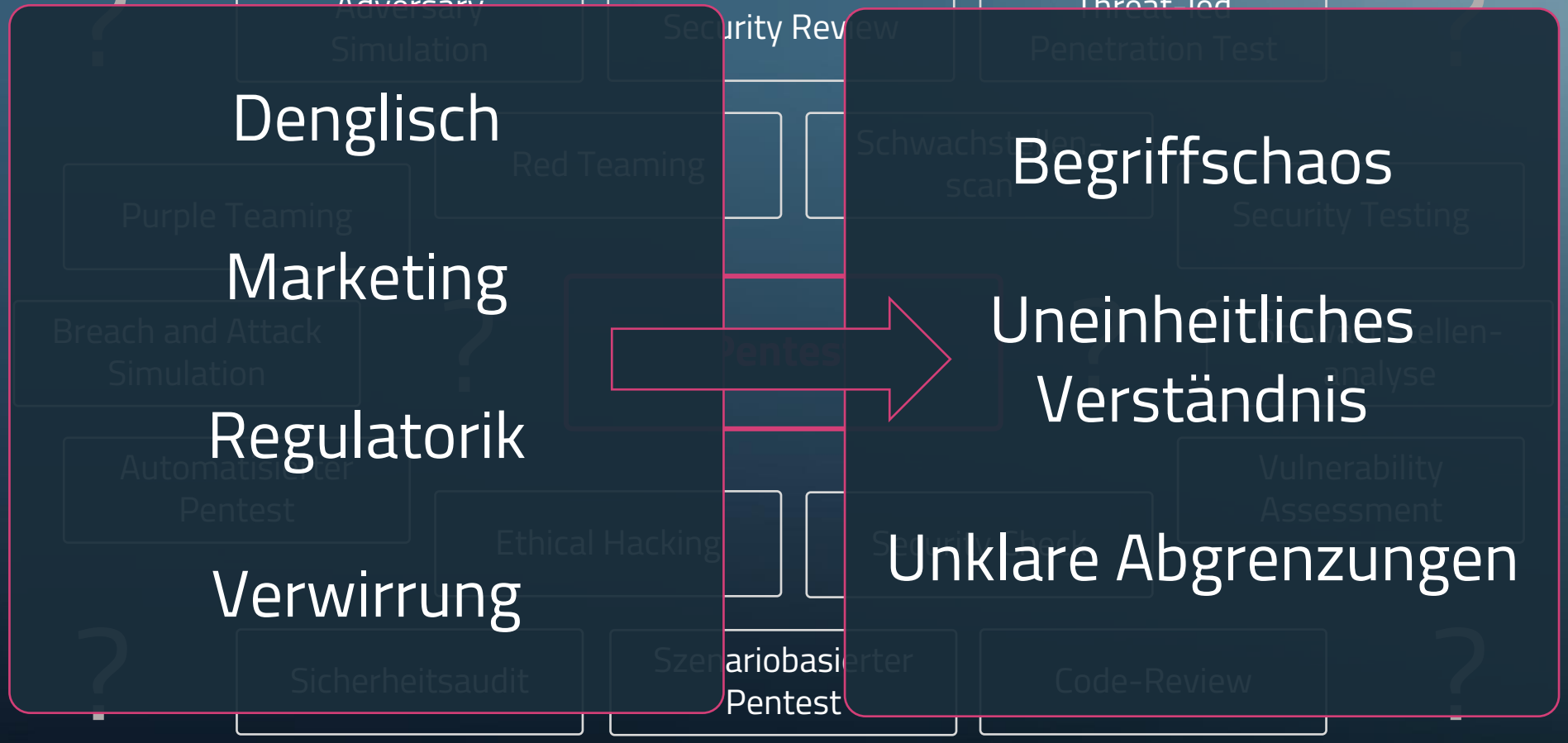
Simon Holl
Hamburg
(OSCP, OSEP, BSCP)

Begrifflichkeiten: Willkommen im Chaos

Pentest: Buzzword-Bingo



Pentest: Buzzword-Bingo



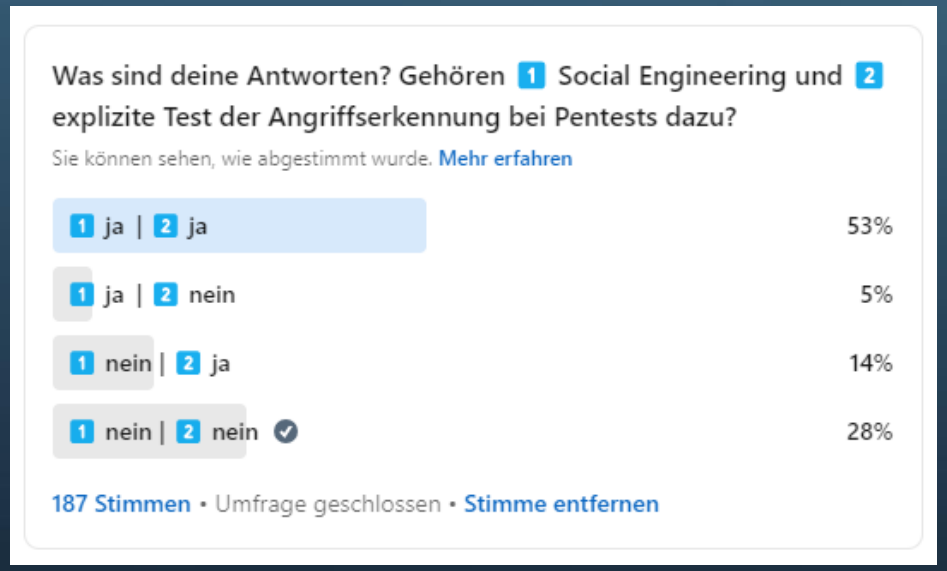
Kurze Umfrage

Gehören **Social Engineering** und **explizite Tests zur Angriffserkennung** bei Pentests dazu?

Antwortmöglichkeiten:

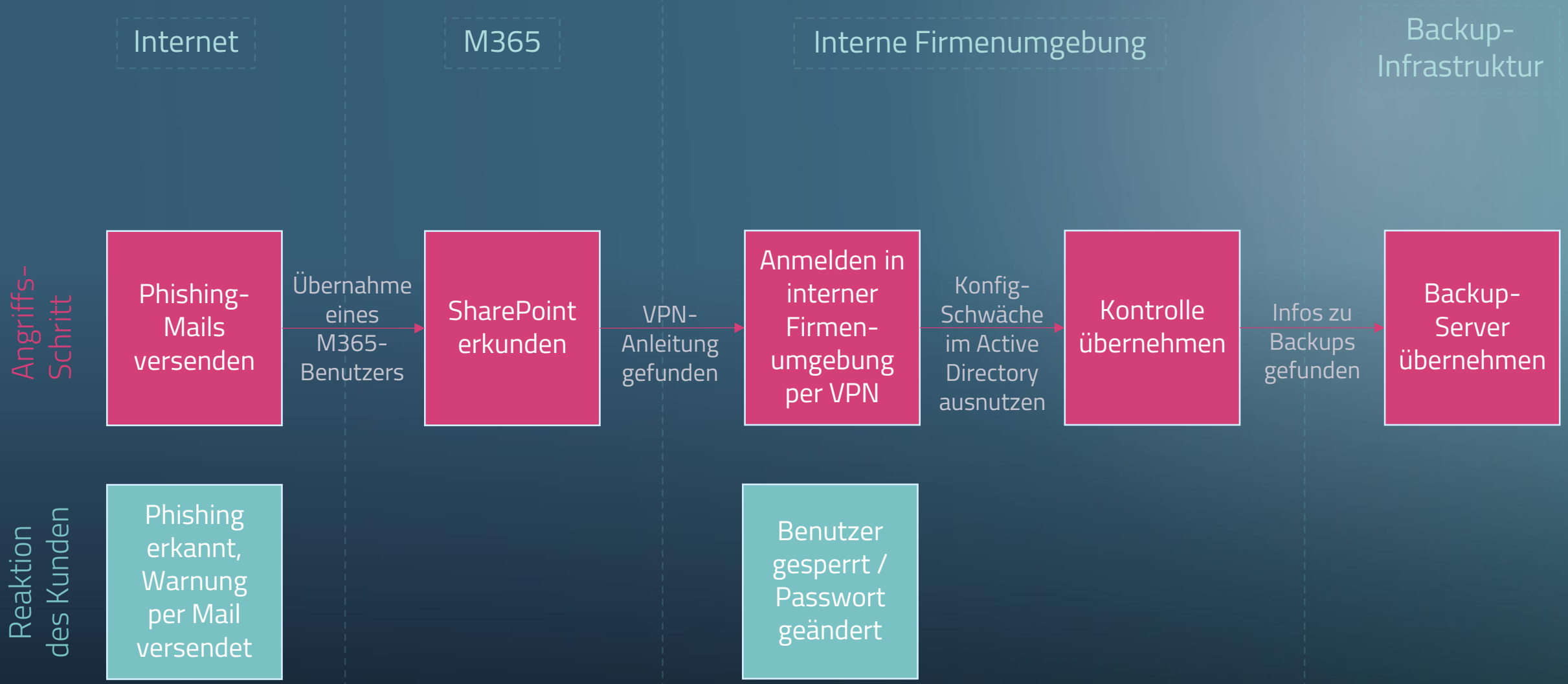
1: Ja, Ja
2: Ja, Nein
3: Nein, Ja
4: Nein, Nein

Ergebnisse der LinkedIn-Umfrage…



Quellen: Umfrage | Auswertung Gruppe Pentesting | Auswertung Gruppe CISOs

Dann machen wir‘s einfach konkret


Internet
M365
Interne Firmenumgebung
Backup-Infrastruktur
Angriffs-Schritt
Phishing-Mails versenden
Übernahme eines M365-Benutzers
SharePoint erkunden
VPN-Anleitung gefunden
Anmelden in interner Firmen-umgebung per VPN
Konfig-Schwäche im Active Directory ausnutzen
Kontrolle übernehmen
Infos zu Backups gefunden
Backup-Server übernehmen
Reaktion des Kunden
Phishing erkannt, Warnung per Mail versendet
Benutzer gesperrt / Passwort geändert

If *das wäre ein Pentest gewesen* **then**…

keine Mühe gegeben, unentdeckt zu bleiben

keine Reaktionen auf der Verteidigungsseite erfolgt, da Pentest angekündigt

Lücken in Reaktionsprozessen *nicht* aufgedeckt

externe und interne Infrastruktur getrennt angeschaut, Phishing

vielleicht weitere Schwachstellen aufgedeckt

Gestaltungsmöglichkeiten

Rezept

Projektziele x Testgegenstand

Designentscheidungen treffen

Pentest / Red Teaming / Artverwandtes

Typische Ziele & Tests

	„Pentest“		„Red Teaming“
Ziel	Effizientes Aufdecken von (techn.) Schwachstellen	Tests zur Angriffserkennung und -abwehr	Simulation realer Angriffe

Reifegrad im Unternehmen →

Tests			
	Externe Infrastruktur, Cloud		
	Interne Infrastruktur	Alarmtests, Purple Teaming	
	Wichtige Anwendungen		Gesamtes Unternehmen
	Eigene Produkte	Social Engineering	

Was kann man testen?

Externe Infrastruktur

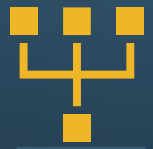
Extern gehostete Systeme
Firmenpräsenz, Webshop, Kundenportal

IT-Schnittstellen nach außen
Mail, VPN, Citrix, Firmenpräsenz, Webshop, Kundenportal, (vergessene) Server

Cloud-Dienste, Software-as-a-Service
(M365, AWS, Azure, GCP, ...)

eher (Konfig-)Audit als klassischer Pentest

Anwendungen
Web, Mobile, Desktop



OT / Hardware

Prozesse, SIEM / SOC

Interne IT
Server, Firewalls, Clients, Active Directory, SAP, Mainframe, selbstentwickelte Apps, Schatten-IT

Produktion

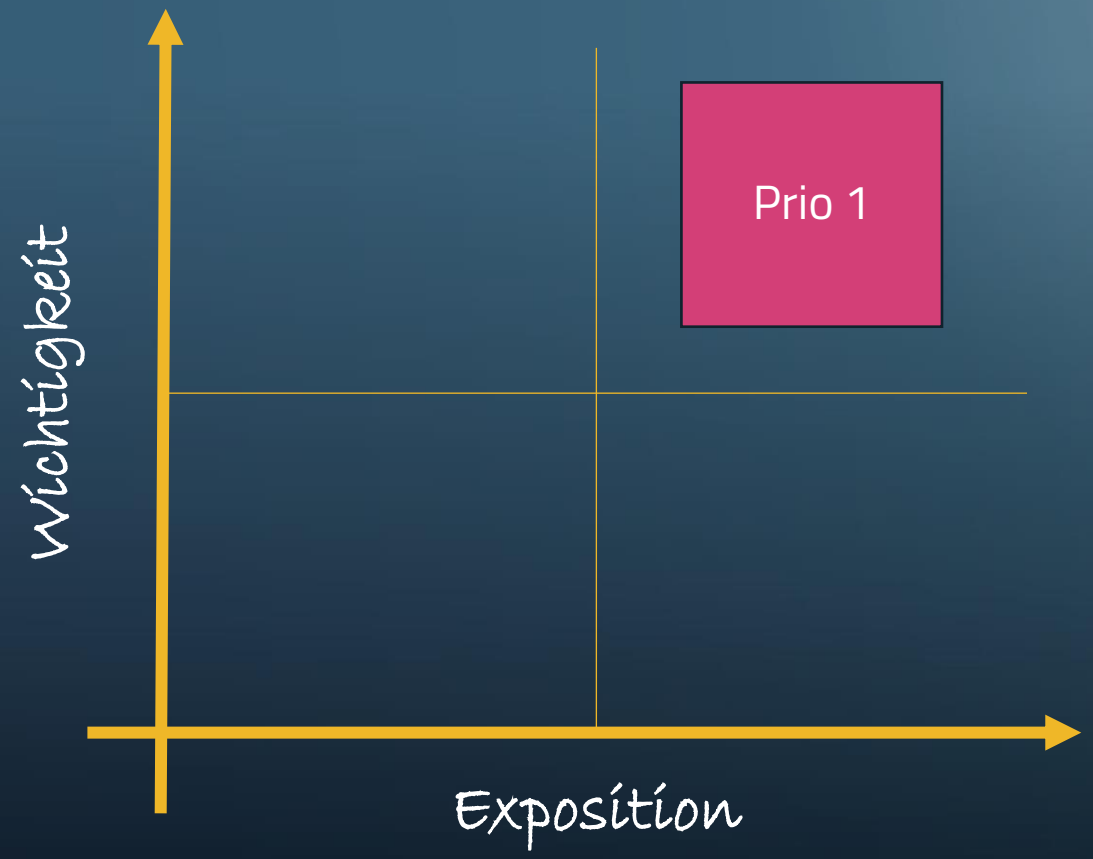
Mitarbeitende

Bürogebäude

Interne Infrastruktur
meist mit AD; einzelne Systeme

Social Engineering / Physical Pentest

Priorisieren von Tests



Gestaltung eines Projekts

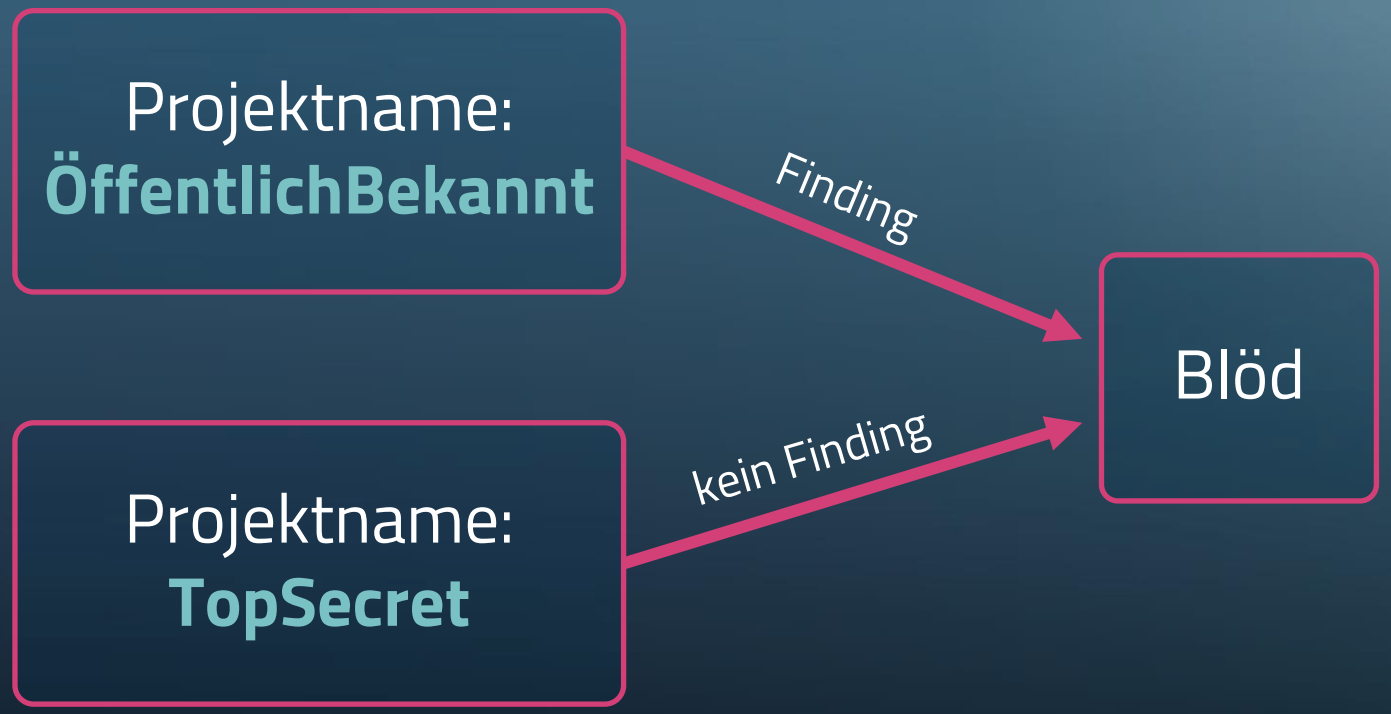
abhängig von Testgegenstand & Projektziel

Kernfrage

Designentscheidungen

Testtiefe	Wie tiefgehend soll der Testgegenstand geprüft werden?
Perspektive	Welche Perspektive sollen Pentester im Pentest einnehmen?
Vorgehensweise	Sollen Pentester versuchen, unerkannt zu bleiben?
Kommunikation	Wer soll über den Pentest informiert werden?
Erlaubte Mittel	Welche Methoden und Techniken dürfen/sollen Pentester einsetzen?

Worst-Case-Szenarien

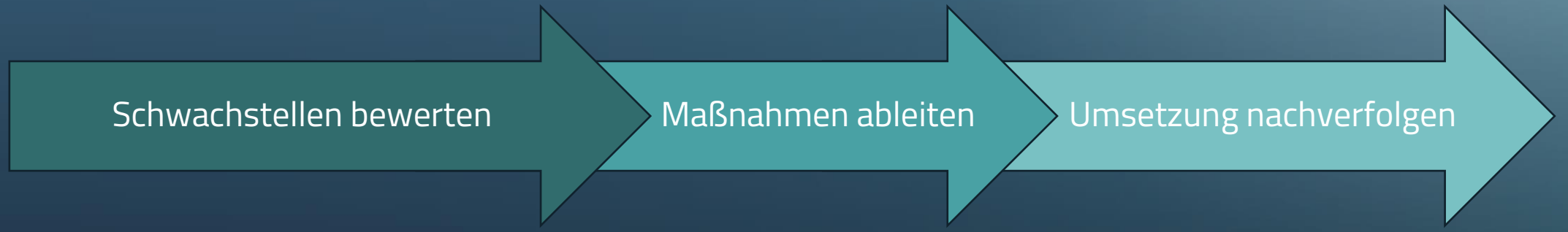


Ergebnisse

Der **Bericht** ist das, was nach einem Pentest bleibt.

Abschluss-besprechung zur Vorstellung der Ergebnisse und Fragenklärung.

Ergebnisse in Risikomanagement übernehmen



3 Dinge, die ich euch mitgeben möchte

Sprecht über den Inhalt und
verlasst euch *nicht* auf Begriffe.

Überlegt, welche **Ziele** ihr mit
dem Projekt verfolgen möchtet.

Gestaltet das Projekt
passend zu euren Zielen.

Danke für’s Zuhören!

nina.wagner@mind-bytes.de | +49 711 49064186 | https://mind-bytes.de

LinkedIn LinkedIn Nina YouTube