Threat Modeling in der Finanzwelt

Wir geben einen Einblick in die Praxis!

Ihre heutigen Referenten

Cornelius Wilhelm

Assistant Manager

Financial Services | Technology & IT-Compliance

KPMG AG Wirtschaftsprüfungsgesellschaft
Münzgasse 2
04107 Leipzig

M +49 171 8645344
corneliuswilhelm@kpmg.com

Daniel Schulz-Sembten

Assistant Manager

Financial Services | Technology & IT-Compliance

KPMG AG Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

M +49 171 2148827
dschulzsembten@kpmg.com

Marlene Trüby

Senior Associate

Financial Services | Technology & IT-Compliance

KPMG AG Wirtschaftsprüfungsgesellschaft
Münzgasse 2
04107 Leipzig

M +49 151 20990578
marlentrueby@kpmg.com

Agenda

01 Threat Modelling für unsere Kunden

02 Threat Modelling Vorgehen

03 Threat Modelling Beispiel

Threat Modelling für unsere Kunden

Projekte in der Finanzwelt

Regulatorische Vorgaben

- BaFin mit BAIT/VAIT/ZAIT
- BaFin mit MaRisk
- EU Digital Operational Resiliance Act (DORA)
- SWIFT Customer Security Controls Framework (CSCF)

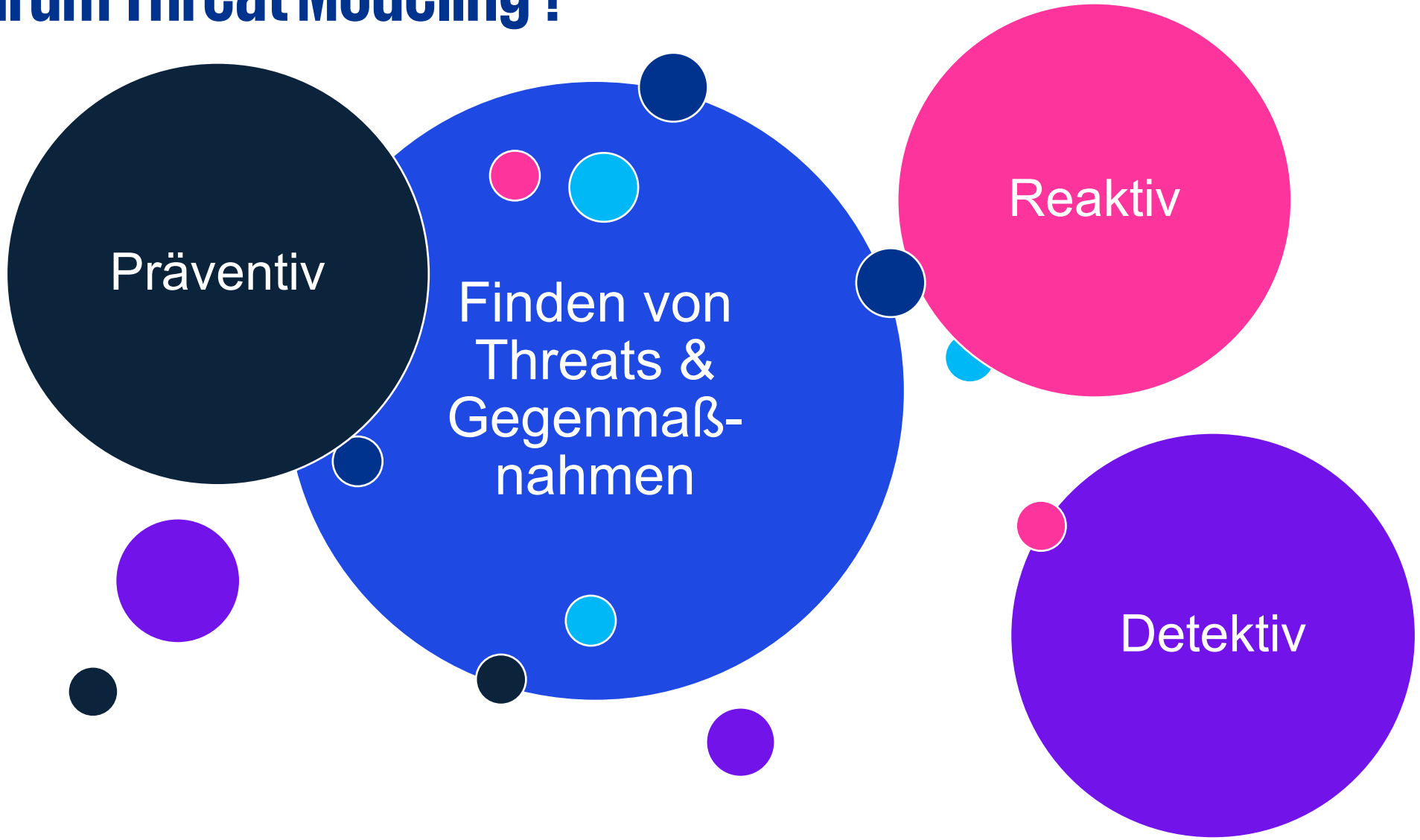
Standards & Frameworks

- ISO27001; ISO27035
- NIST Cybersecurity Framework
- Standard of Good Practice for Information Security
- PCI-DSS
- BSI-Kompendium

Typische Projekte

- Erstellung des SIEM - Frameworks
- Systemauswahl und technische Konzeption
- Risikoorientierte Anbindung von Applikationen
- Prozessintegration für Detection & Response

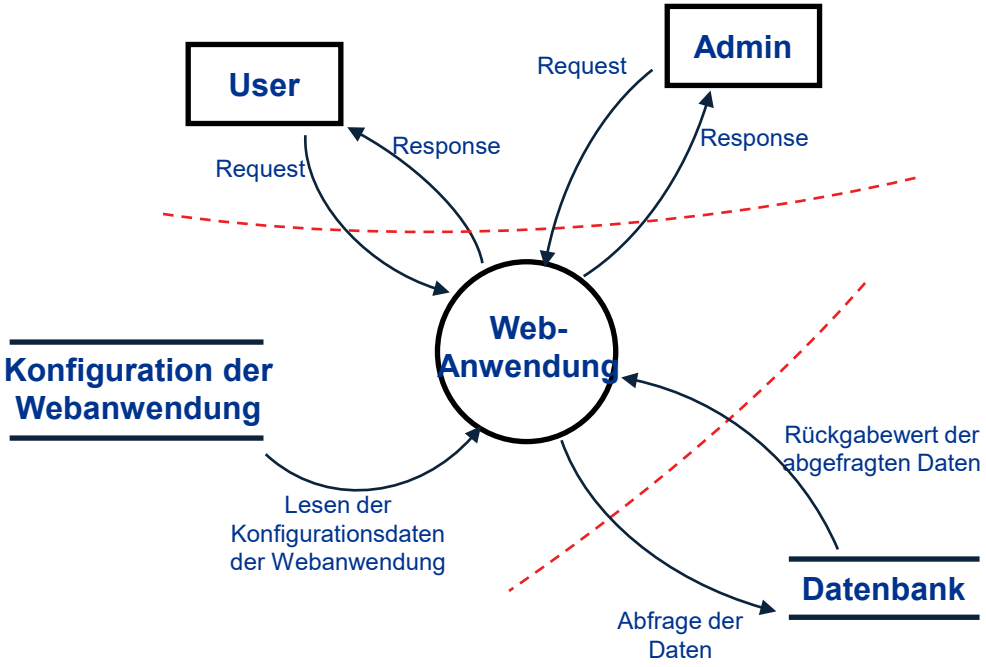
Warum Threat Modeling?



Threat Modeling Vorgehen

Die 2 Blickwinkel zur Threat Findung

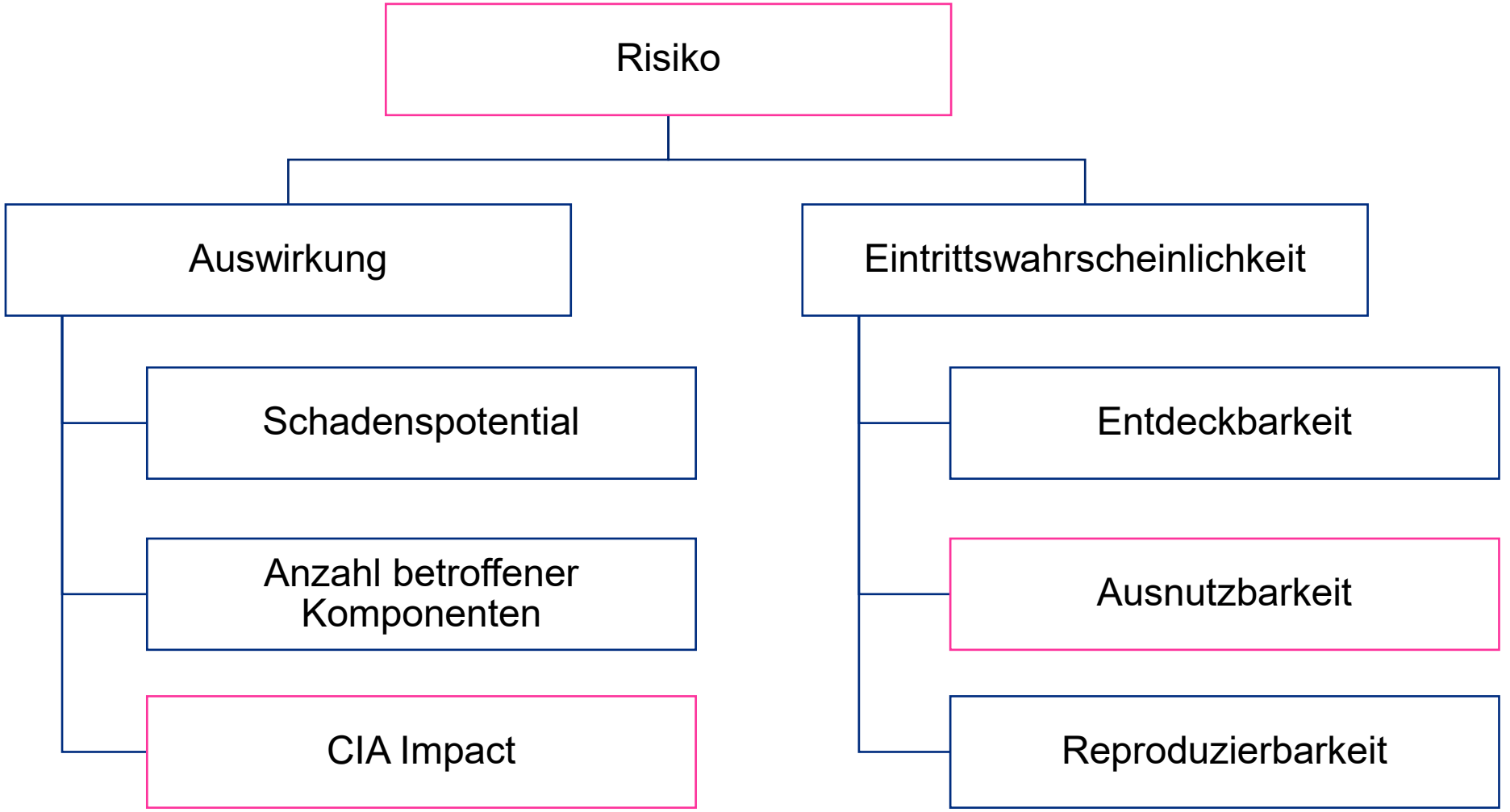
1 Blick auf die Anwendung: Das WIE und das WAS?



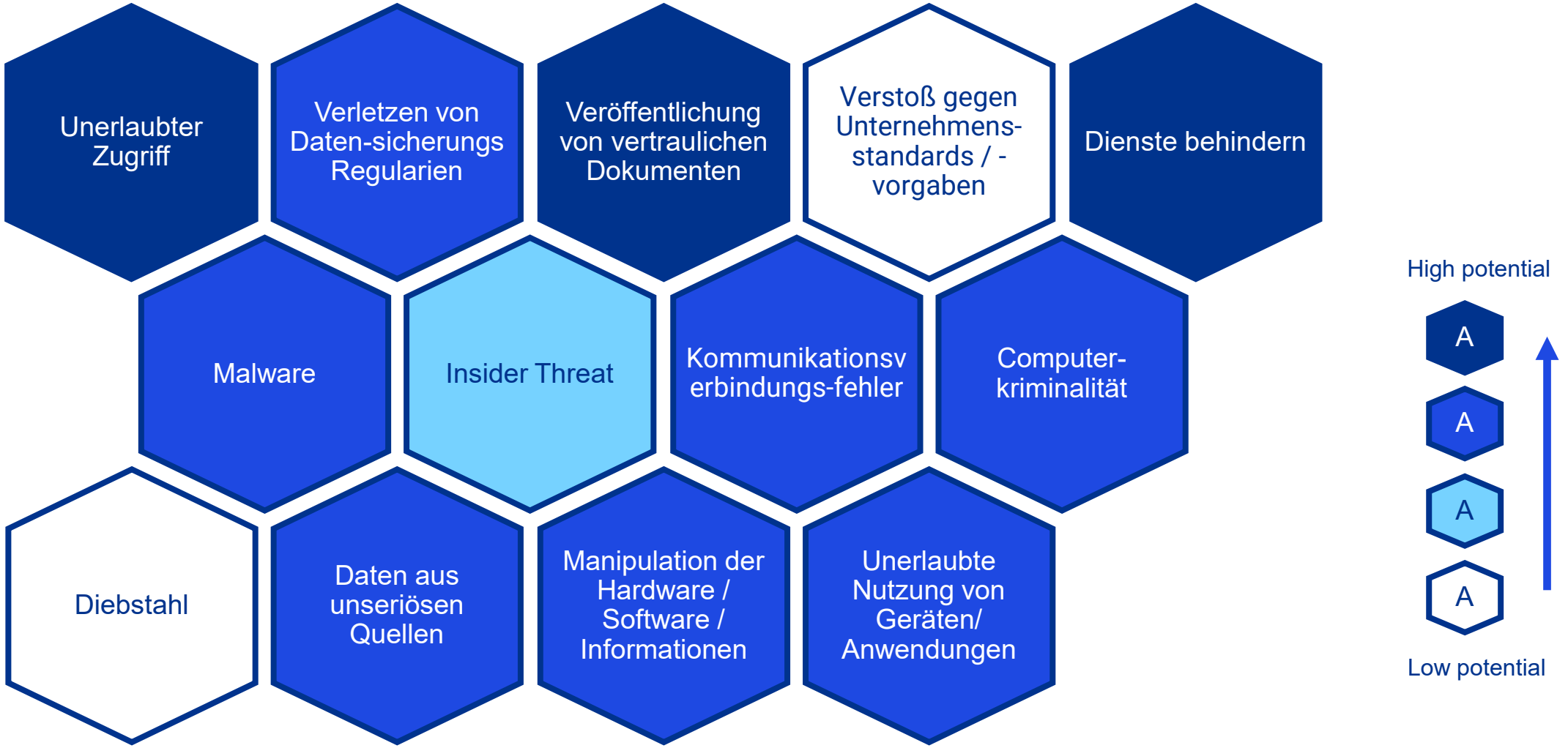
2 Blick des Angreifers: Abgleich mit Threat & Use Case Library

Bedrohungs-szenario	Voraus-setzungen für Anwendbarkeit	Typisch benötigte Log Quellen	Gegenmaßnahme
T2. Bruteforce-Angriffe (**S**poofing)	- Anmeldung via Username – PW	- Logs für fehlgeschlagene Logins mit folgenden Parametern […]	- (Monitoring) - Temporäre IP-Adress-Sperrungen und Alarmierung - Umstellung Authentifikation Methode
T3. Konfigurations-Manipulation (**R**epudiation)	…	…	…
…	…	…	…

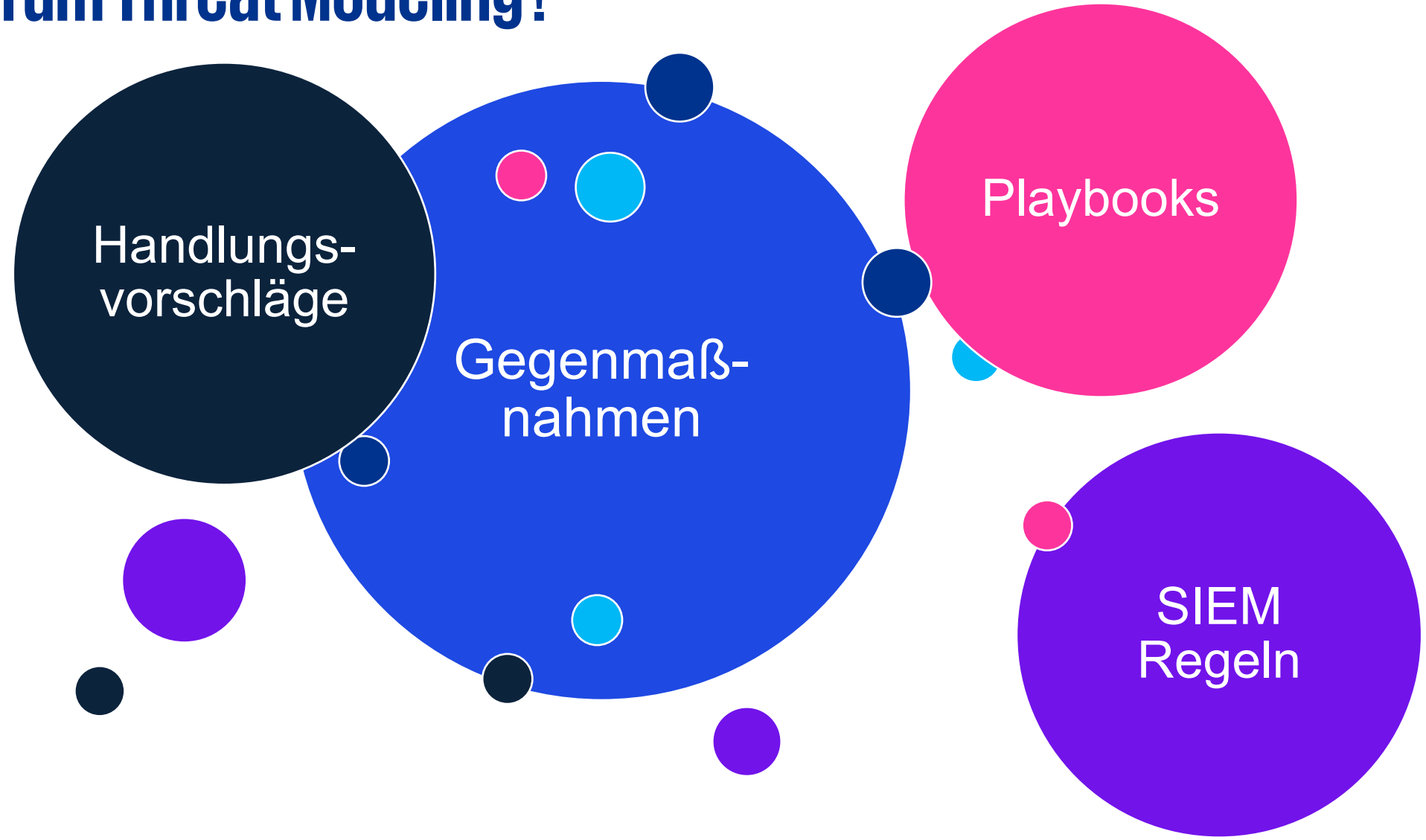
Einschätzung des Risikos



Beurteilung potenzieller Bedrohungen

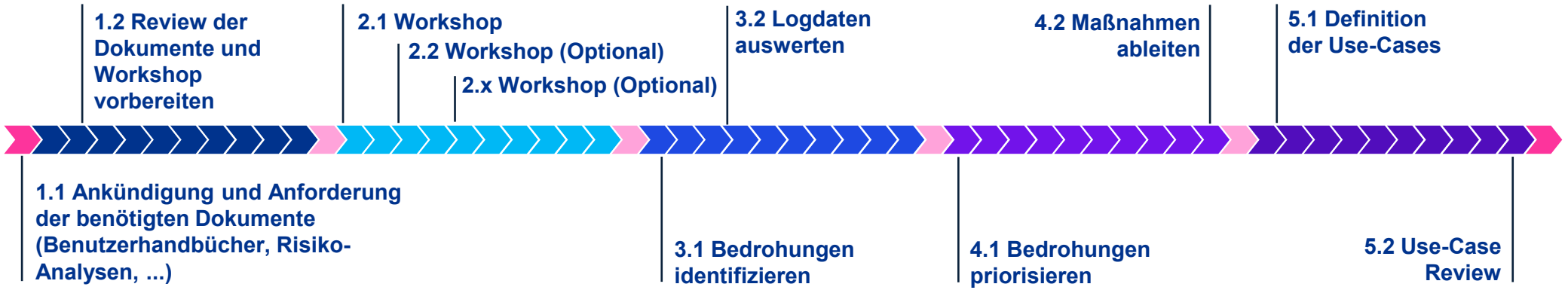


Darum Threat Modeling!



Threat Modelling Beispiel

Wie bindet KPMG Threat Modeling ein?



1 Planung und Organisation

I. Identifikation der Ansprechpartner
II. Workshops planen und vorbereiten
III. Einladungen senden

2 Workshop-Durchführung

I. Review der Anwendungsdokumentation und der Logdaten
II. Durchführen des initialen Workshops
III. Anschlussfragen ableiten
IV. Durchführen der Anschluss-Workshops

3 Threat Modeling

I. Identifikation von applikations-spezifischen Bedrohungen, Einordnung nach STRIDE
II. Sichtung der Logdaten und Bewertung von deren Tauglichkeit

4 Threat Review

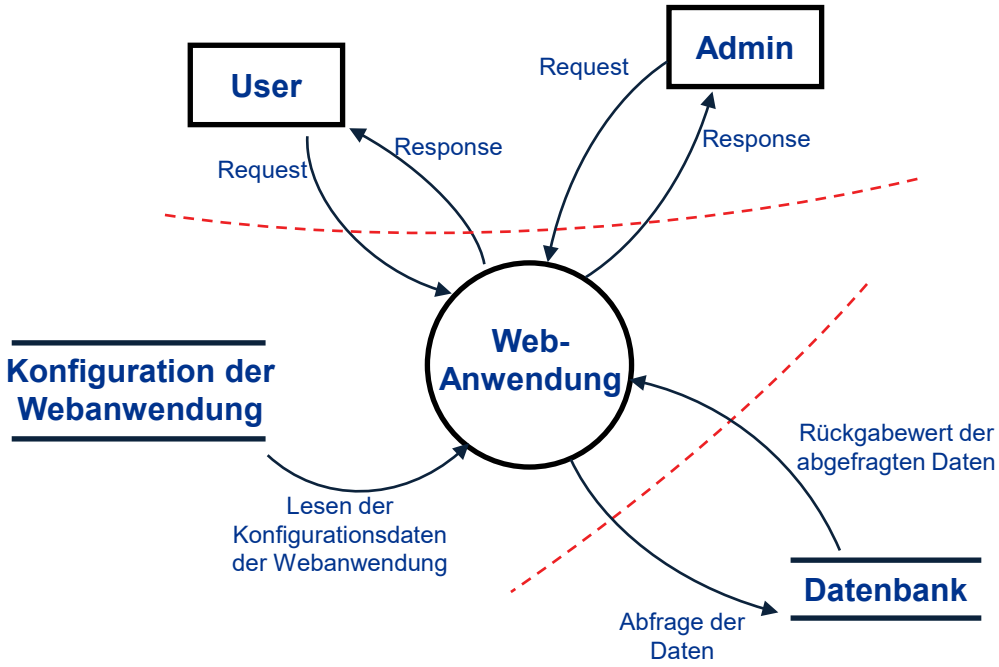
I. Bewertung der Threats nach Schweregrad und Plausibilität
II. Optional: Durchführung von klärenden Workshops nach Bedarf
III. Ableiten von Maßnahmen zur Mitigation (präventiv & Ansätze für SIEM-Use-Cases)

5 Use Case Spezifikation

I. Detaillierte Beschreibung der UC in der UC-Spezifikation
II. Begründung für nicht umzusetzende UC dokumentieren

Beispiel-Ergebnis für das Threat Modeling anhand des DFD

Asset	Bedrohungsszenario	Gegenmaßnahme	Schwere-grad	Aufwand d. Maßnahme
Web-Anwendung	**T1**. (D)DoS Angriffe (**D**enial of Service)	Redundanz für Infrastrukturkomponenten (z.B. Applikation Server) und Load Balancer.	high	high
	T2. Bruteforce-Angriffe (**S**poofing)	Temporäre IP-Adress-Sperrungen und Alarmierung (Monitoring). Siehe **UC1**.	critical	medium
	T3. Konfigurations-Manipulation (**R**epudiation)	Überarbeitung des Rollen- und Rechtekonzepts.	medium	low
		Monitoring: Siehe **UC2**.		medium
Datenbank	**T4**. Nicht-Rekonstruierbarkeit, wer im Fall eines Problems verantwortlich gewesen sein könnte (**R**epudiation)	Überarbeitung des Rollen- und Rechtekonzepts.	medium	low
		Absicherung der administrativen Accounts durch PAM-Lösung.		medium



Wir freuen uns auf Ihre Fragen!

… An unserem Stand

Ihre Ansprechpartner

Cornelius Wilhelm
Assistant Manager
Financial Services | Technology & IT-Compliance
KPMG AG Wirtschaftsprüfungsgesellschaft
Münzgasse 2
04107 Leipzig

M +49 171 8645344
corneliuswilhelm@kpmg.com

Daniel Schulz-Sembten
Assistant Manager
Financial Services | Technology & IT-Compliance
KPMG AG Wirtschaftsprüfungsgesellschaft
Klingelhöferstraße 18
10785 Berlin

M +49 171 2148827
dschulzsembten@kpmg.com

Marlene Trüby
Senior Associate
Financial Services | Technology & IT-Compliance
KPMG AG Wirtschaftsprüfungsgesellschaft
Münzgasse 2
04107 Leipzig

M +49 151 20990578
marlentrueby@kpmg.com

www.kpmg.de/socialmedia

www.kpmg.de