IBM QRadar

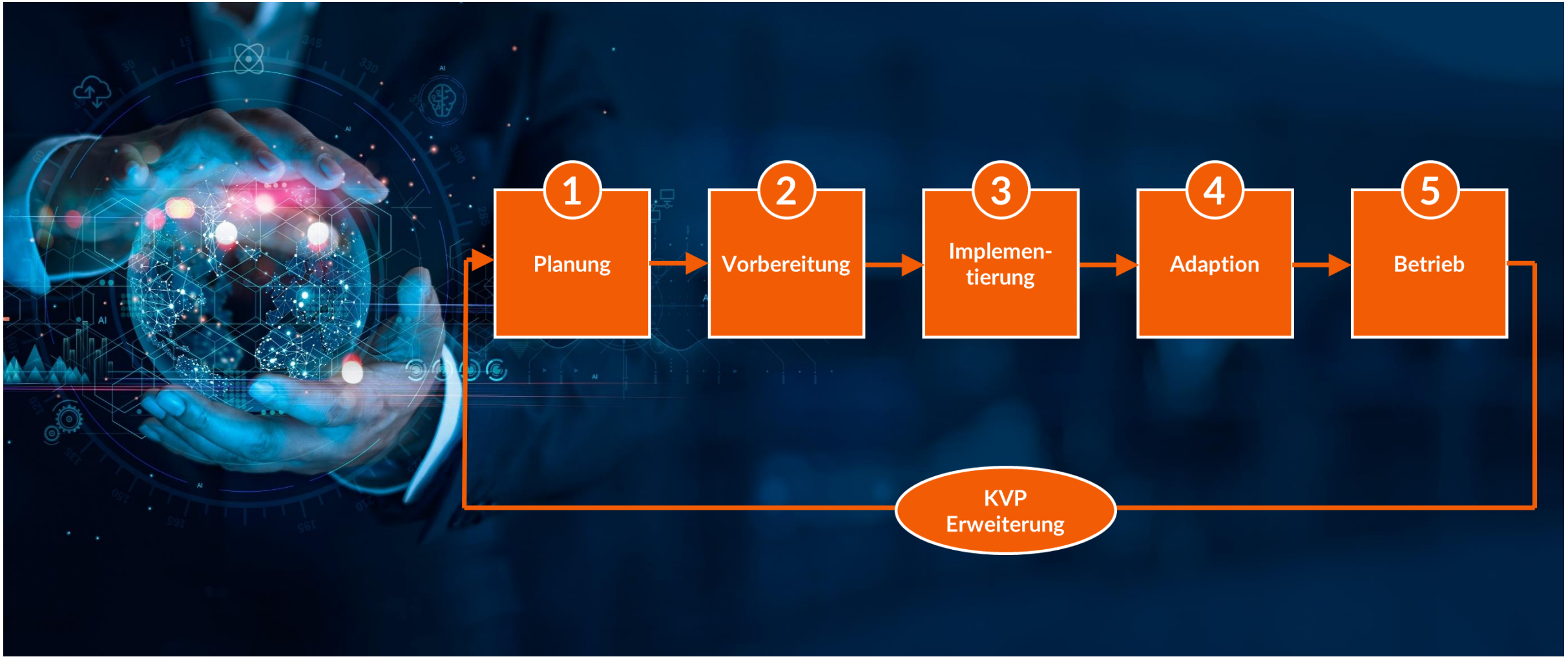
Einführung eines SIEM Systems im BaFin reguliertem Umfeld

Wolfram Stiasny

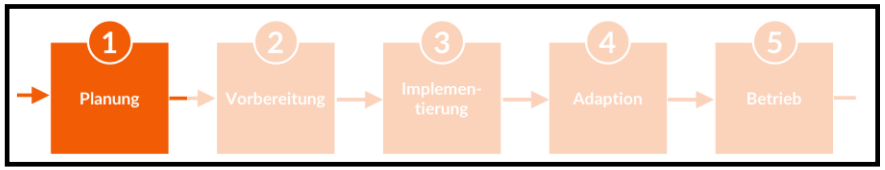
TeamBank

Die Macher von: easyCredit easyCredit Ratenkauf

Phasen der Einführung



Planung



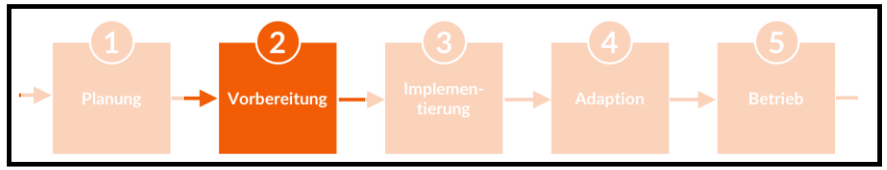
- Strategie
- Regulatorik
- Toolauswahl
- Dienstleister
- Integrator
- Logquellenauswahl
- Use Case Definition

IBM

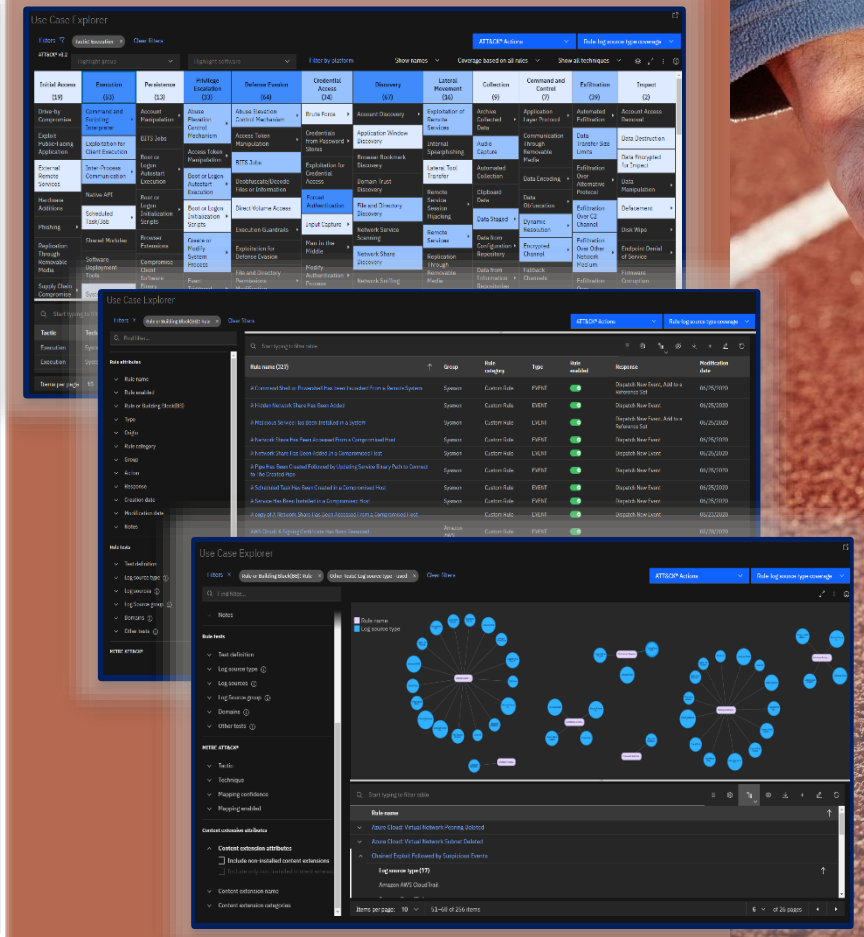
Logsources

MITRE ATT&CK™

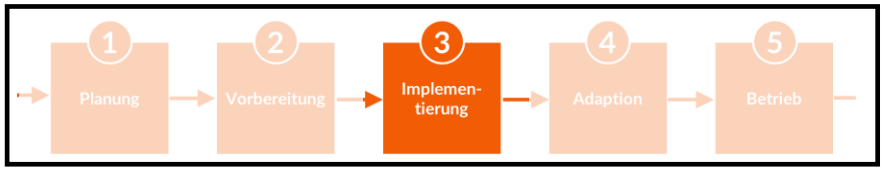
Vorbereitung



- Konzeption
- Dimensionierung
- Systemdesign
- Logsourcekonfiguration
- Use Case Entwicklung
- Training



Implementierung



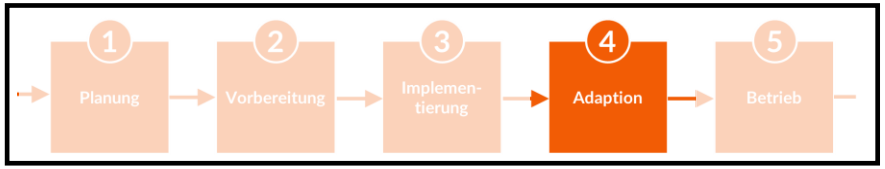
- Aufbau QRadar System
- Technischer Durchstich
- Logsourceanbindung
- Rollout Logsourcekonfig
- Use Case Implementierung
- Tests

auditd

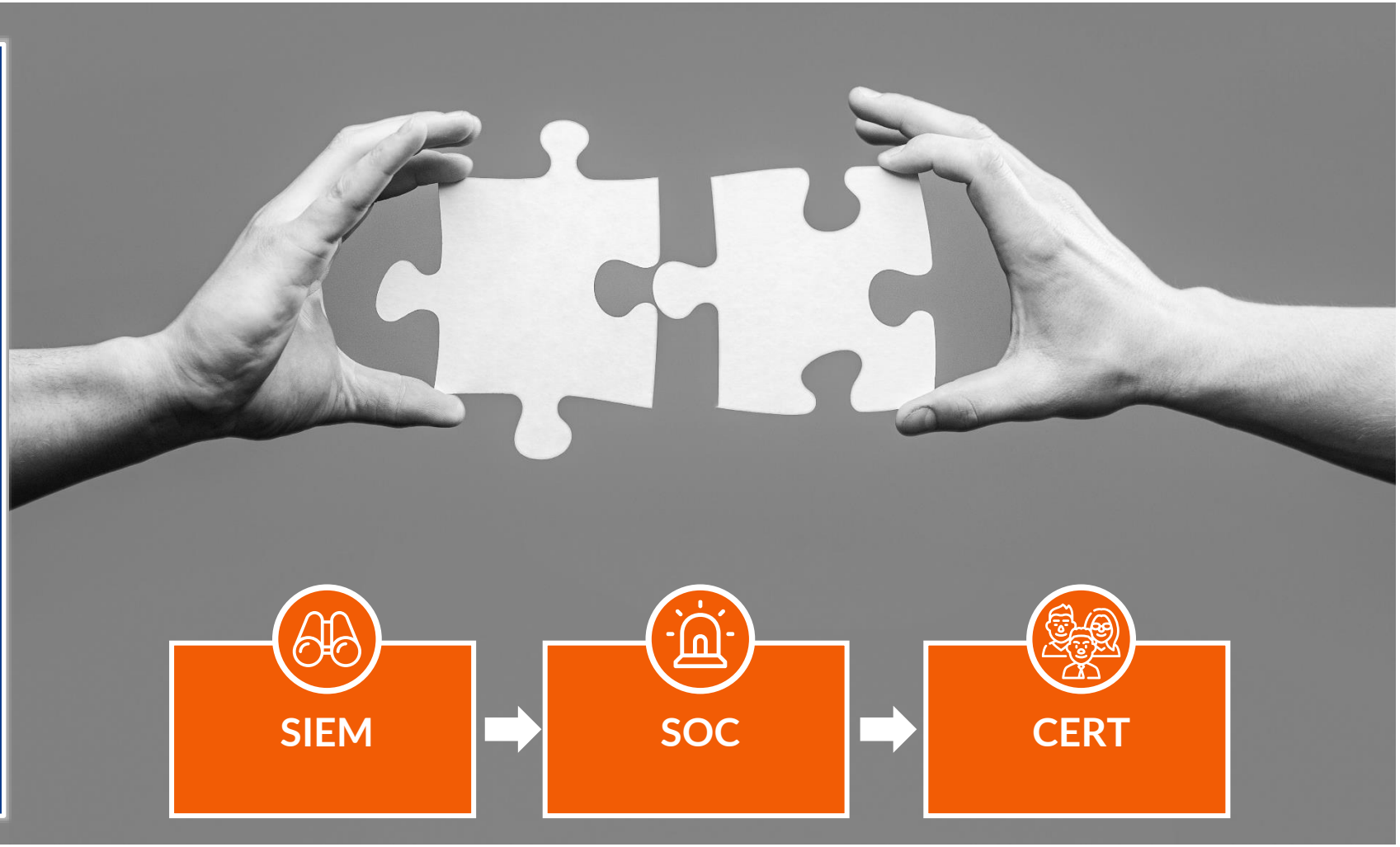
Windows Sysinternals

Sysmon

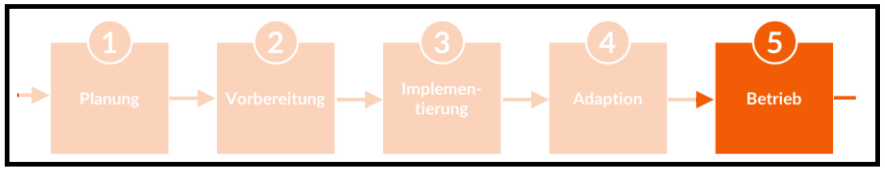
Adaption



- Tuning
- Runbook Erstellung
- SOC Integration
- Training SOC
- 3rd Level Team (CERT)

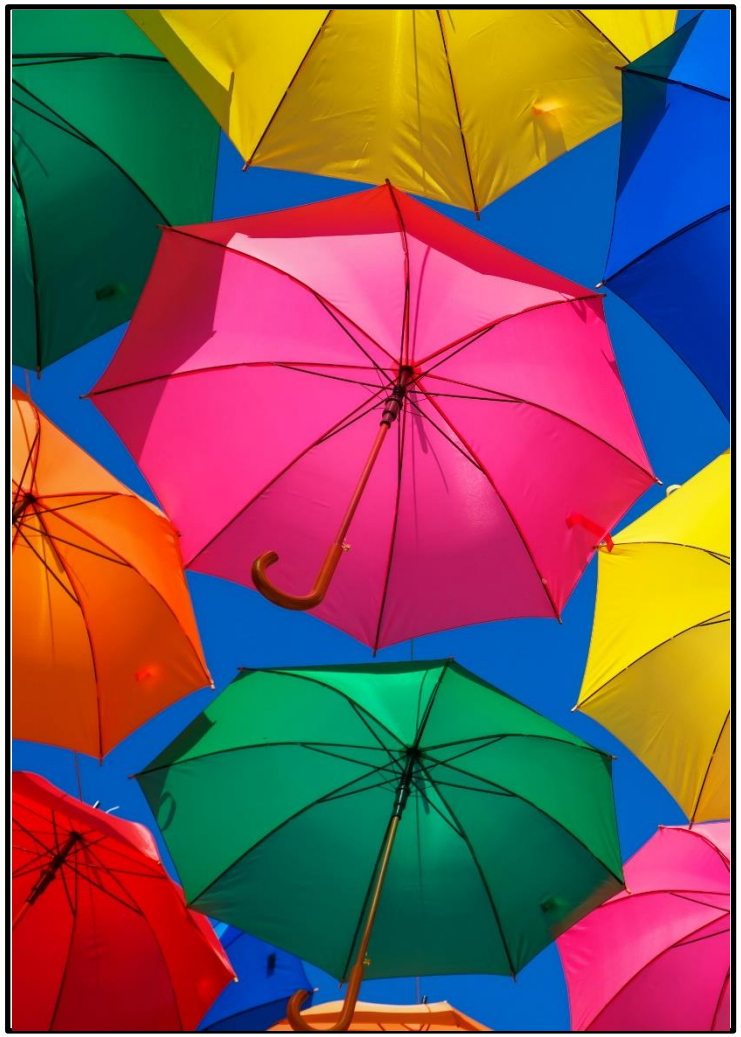


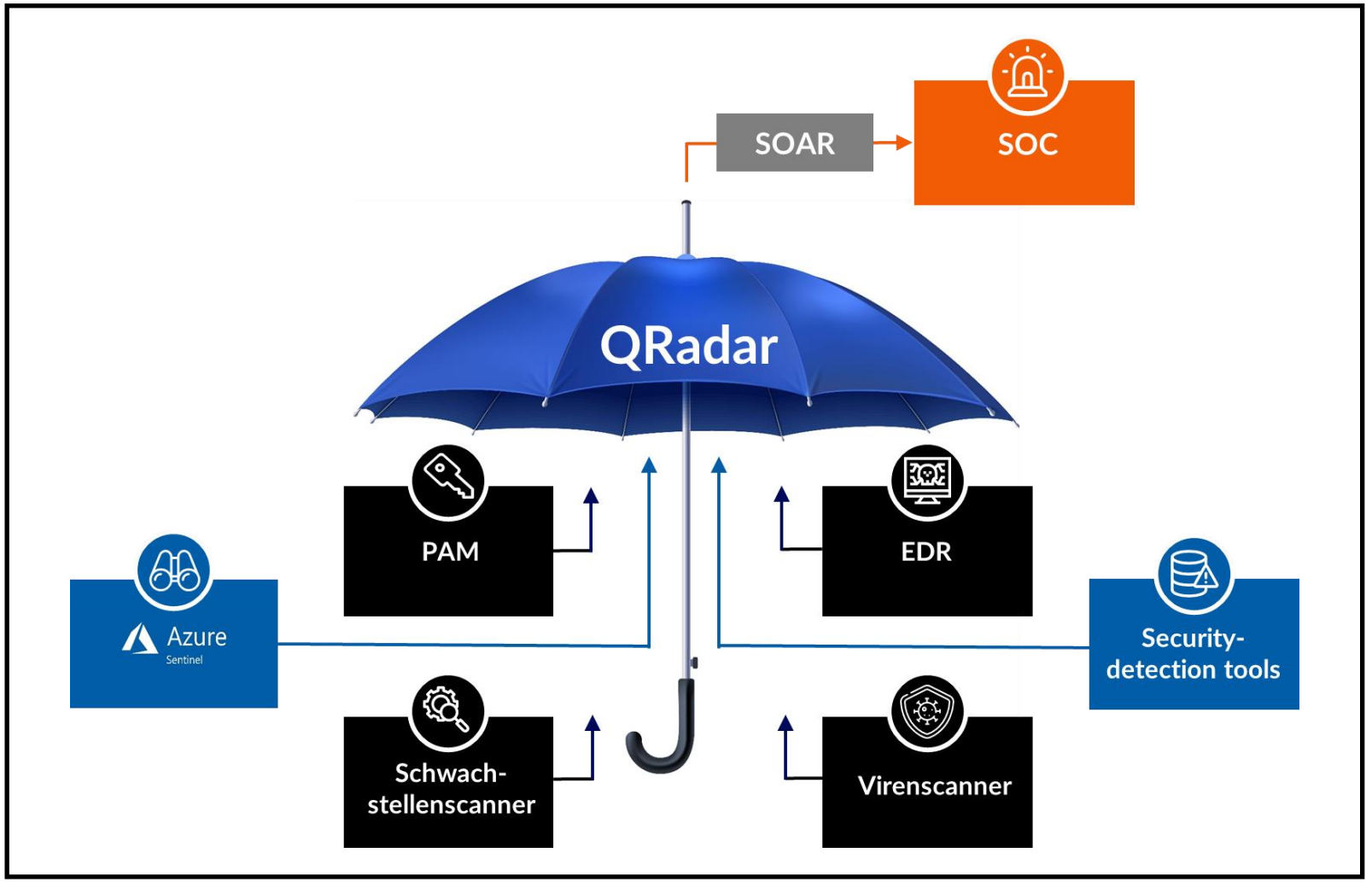
Betrieb



- Regelprozesse
- Tuning
- Anpassung Use Cases
- Lifecycle Management
- Regressionstests
- Back to step 1

QRadar as an umbrella





Vielen Dank für Ihre Aufmerksamkeit!

Wolfram Stiasny