



IBM QRadar

Einführung eines SIEM Systems im
BaFin reguliertem Umfeld

Die Macher von:

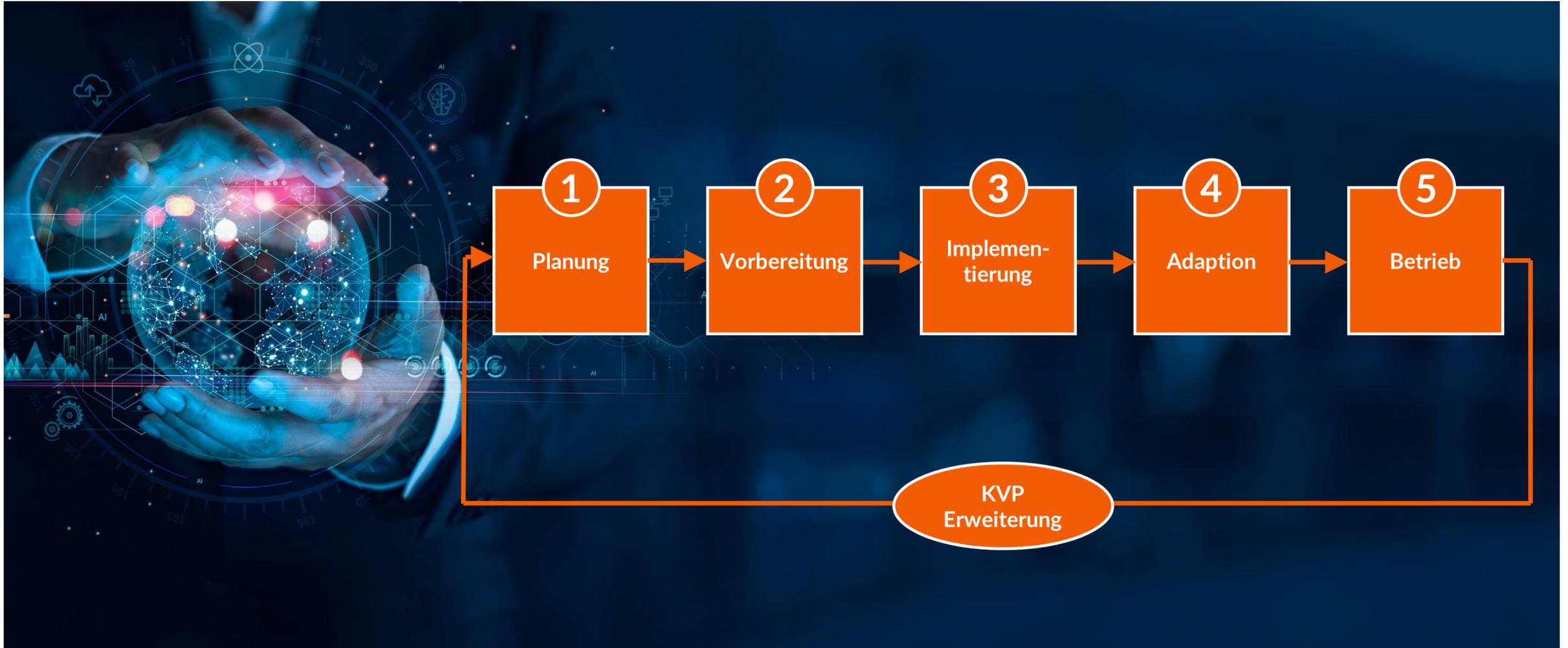
e@sy
Credit

e@sy
Credit
Ratenkauf

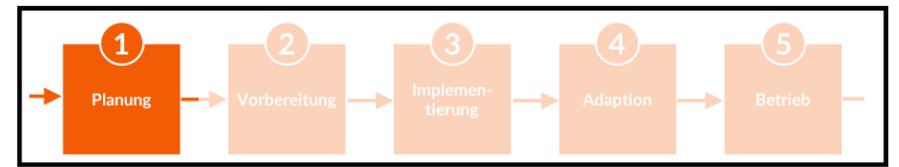
Wolfram Stiasny

TeamBank

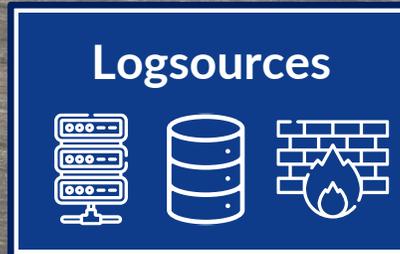
Phasen der Einführung



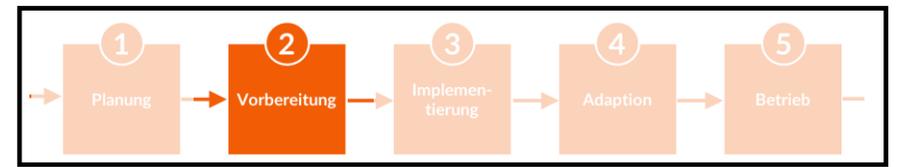
Planung



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



Vorbereitung



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

The screenshots display the 'Use Case Explorer' interface. The top view shows a table of use cases with columns for Title, Platform, and Description. The middle view shows a list of rules with columns for Rule Name, Group, Rule Category, Type, Rule Enabled, Response, and Modification Date. The bottom view shows a circular dependency graph with nodes and connecting lines.



Implementierung



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

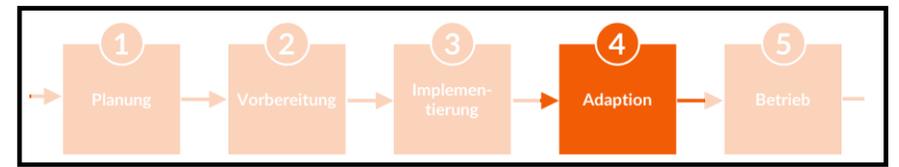


auditd

 Windows Sysinternals

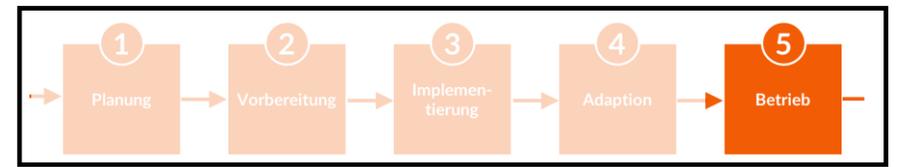
Sysmon

Adaption



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

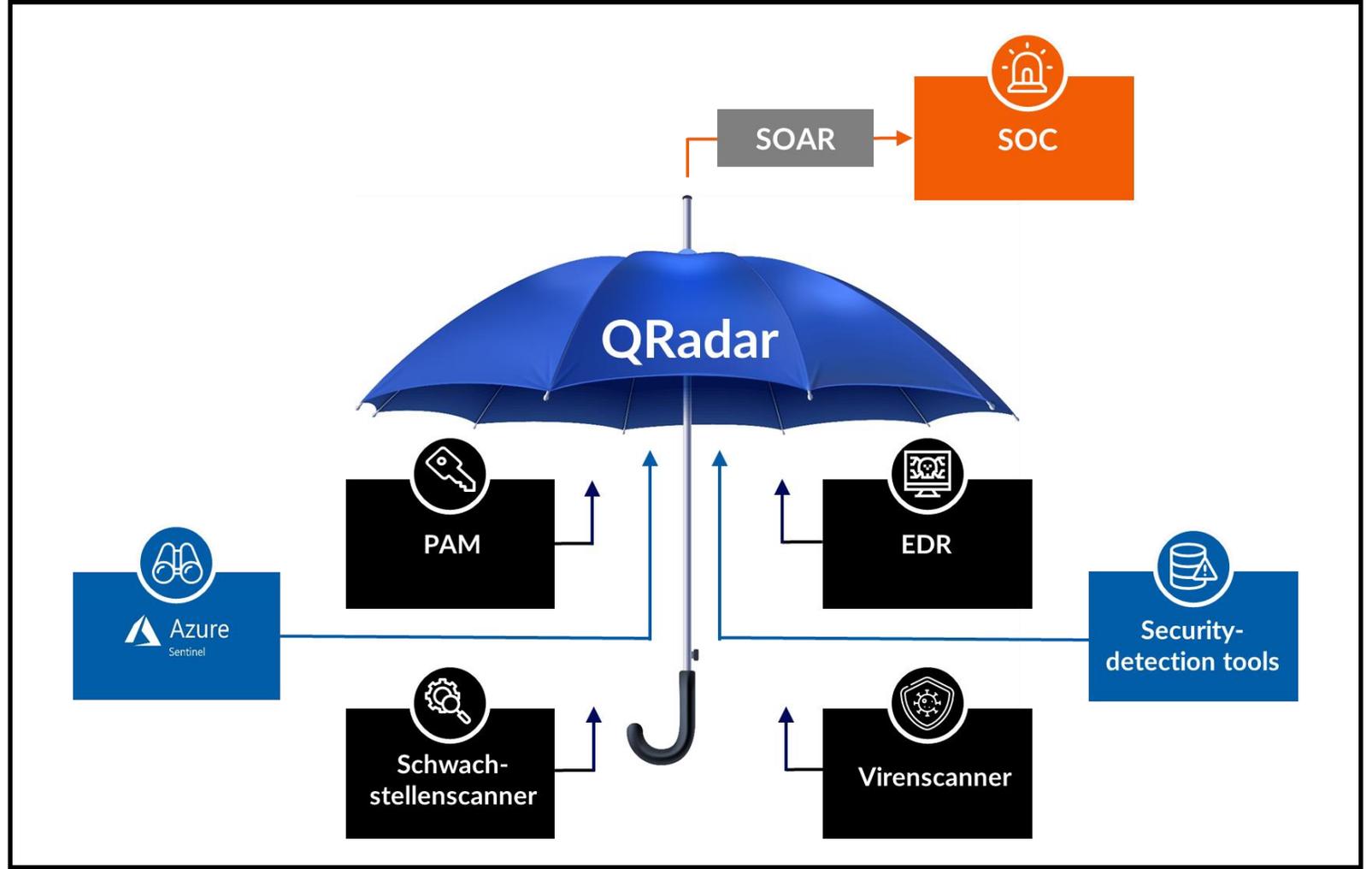




- Regelprozesse
- Tuning
- Anpassung Use Cases
- Lifecycle Management
- Regressionstests
- Back to step 1



QRadar as an umbrella



**Vielen Dank für Ihre
Aufmerksamkeit!**

Wolfram Stiasny