Bundesamt
für Sicherheit in der
Informationstechnik

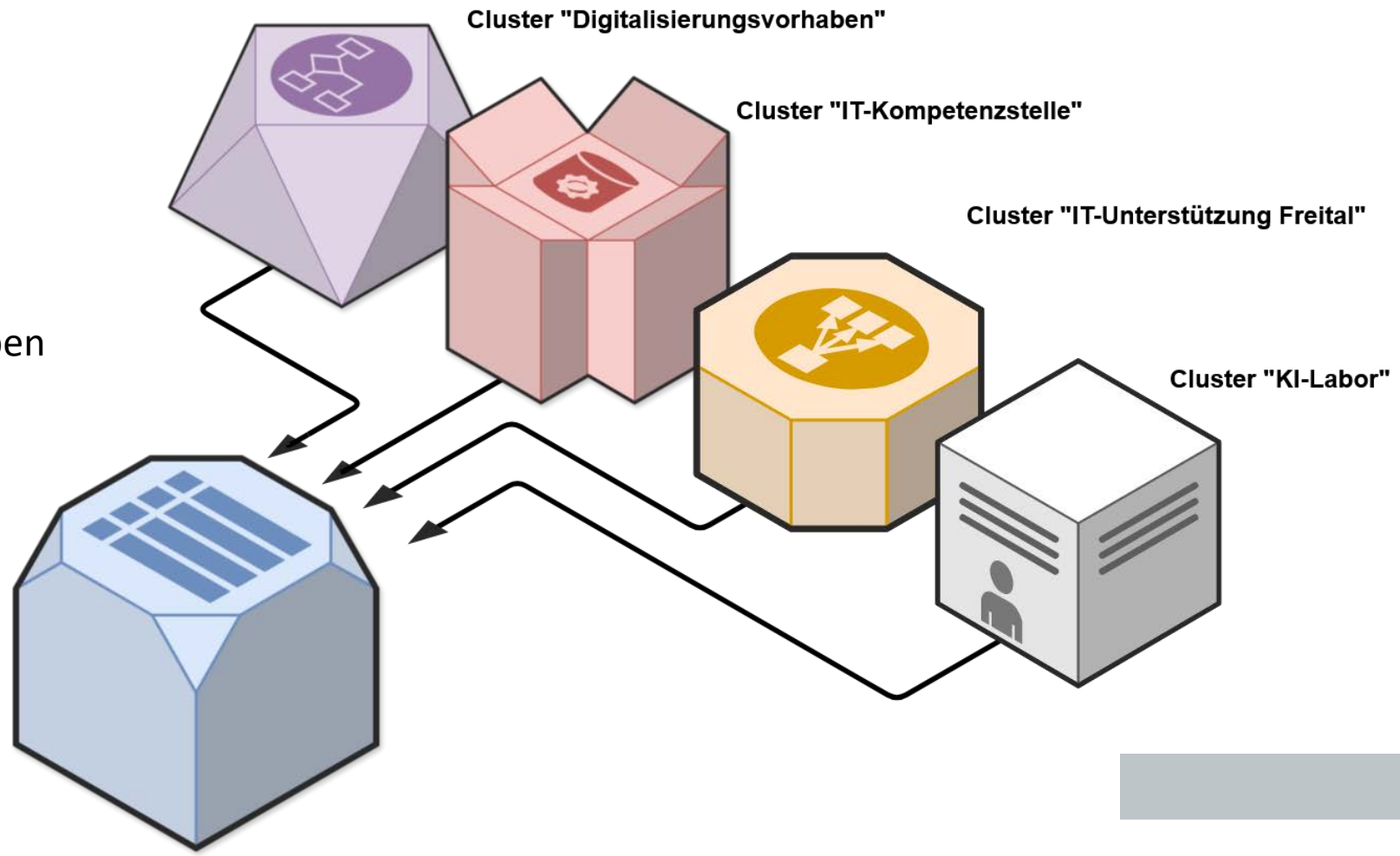
Deutschland
Digital•Sicher•BSI•

KI in der Verwaltung für den Dienstgebrauch

Inhaltsübersicht

Einleitung

Paul Köhler
BSI Standort Freital
Referent, T 36
Cluster Digitalisierungsaufgaben



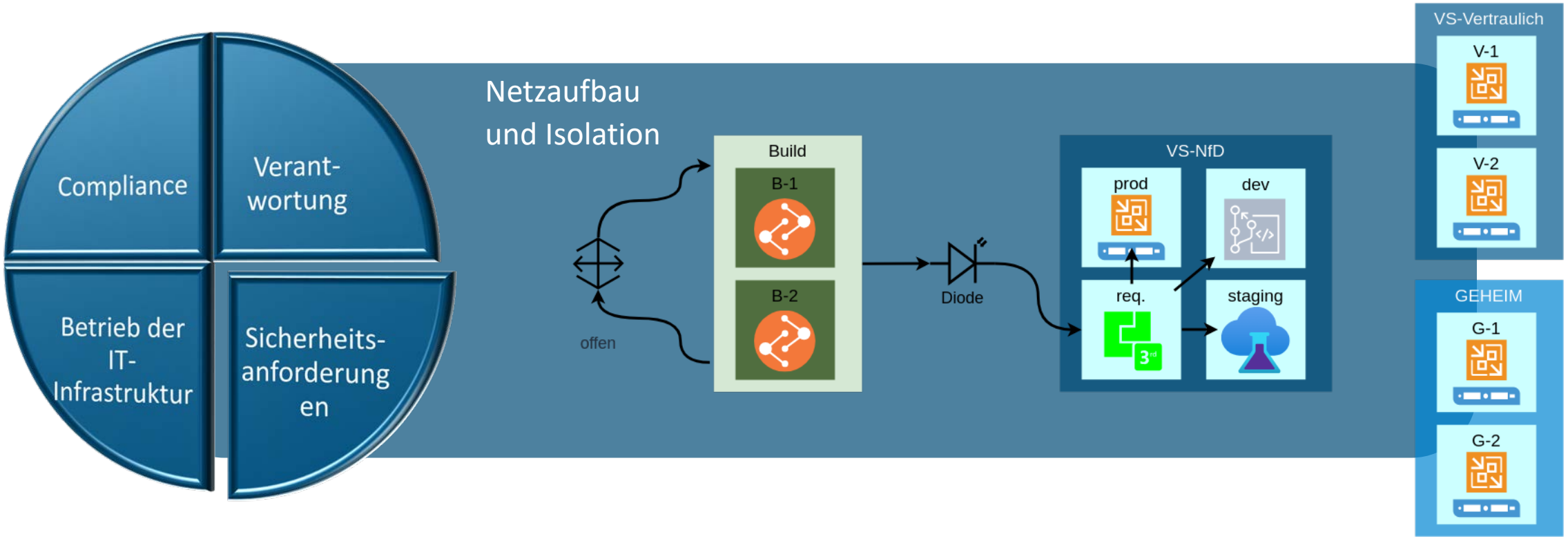
Herausforderungen bei KI-Integration in der Verwaltung

Herausforderungen bei KI-Integration in der Verwaltung

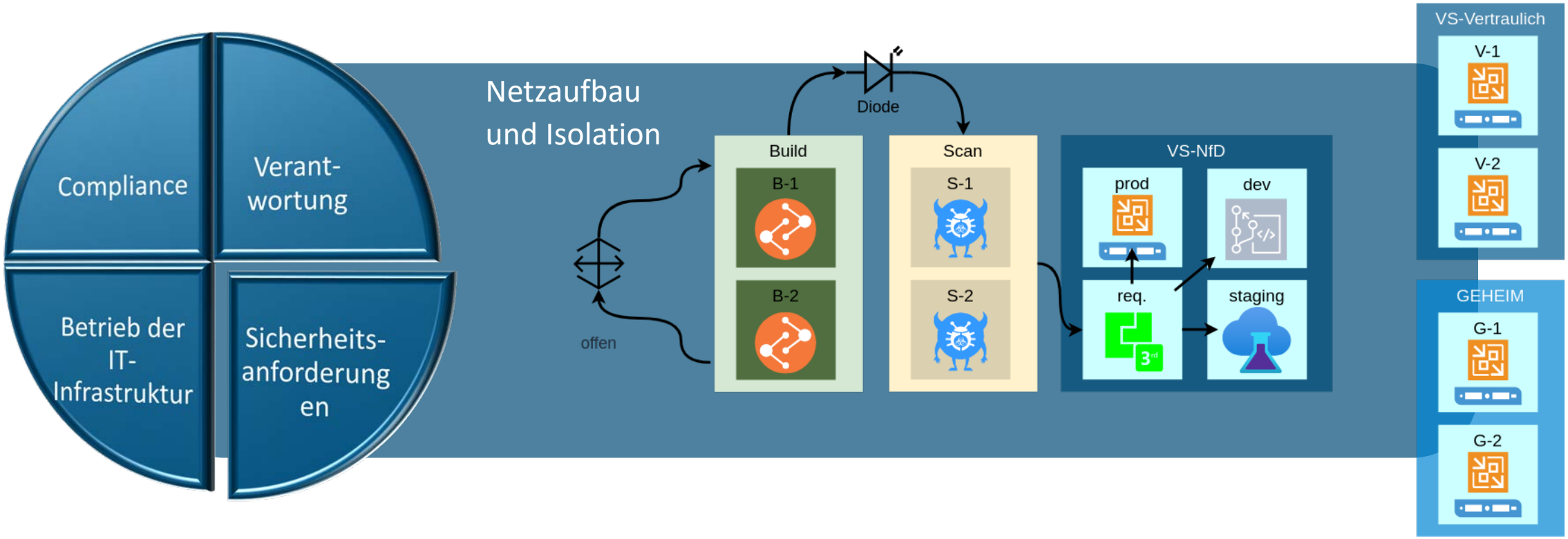
Herausforderungen bei KI-Integration in der Verwaltung

- Schulung der Nutzer für die bereitgestellten Tools
- Servicevereinbarung mit Nutzern
- Zugangs- und Ressourcen-Beantragung
- Datenpools (öffentliche sowie spezifische Fachdaten für UseCase)
- Einstufung der Daten

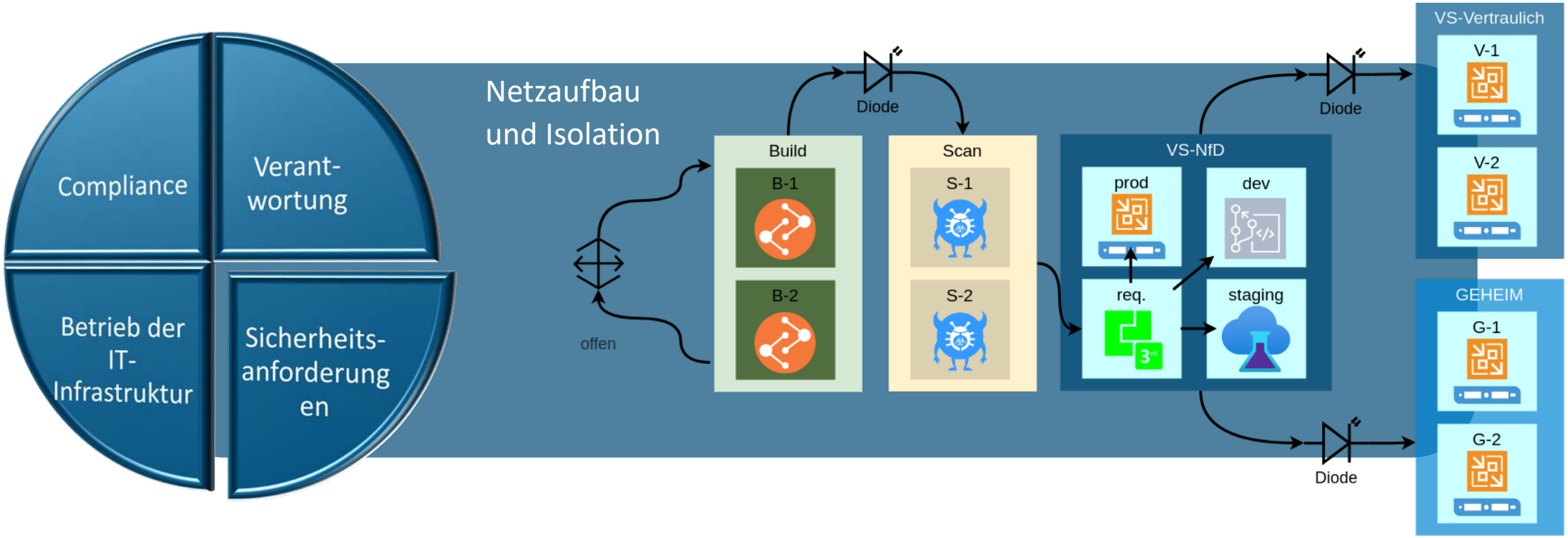
Sicherheitsaspekte bei KI-Diensten mit VS-Daten



Sicherheitsaspekte bei KI-Diensten mit VS-Daten



Sicherheitsaspekte bei KI-Diensten mit VS-Daten

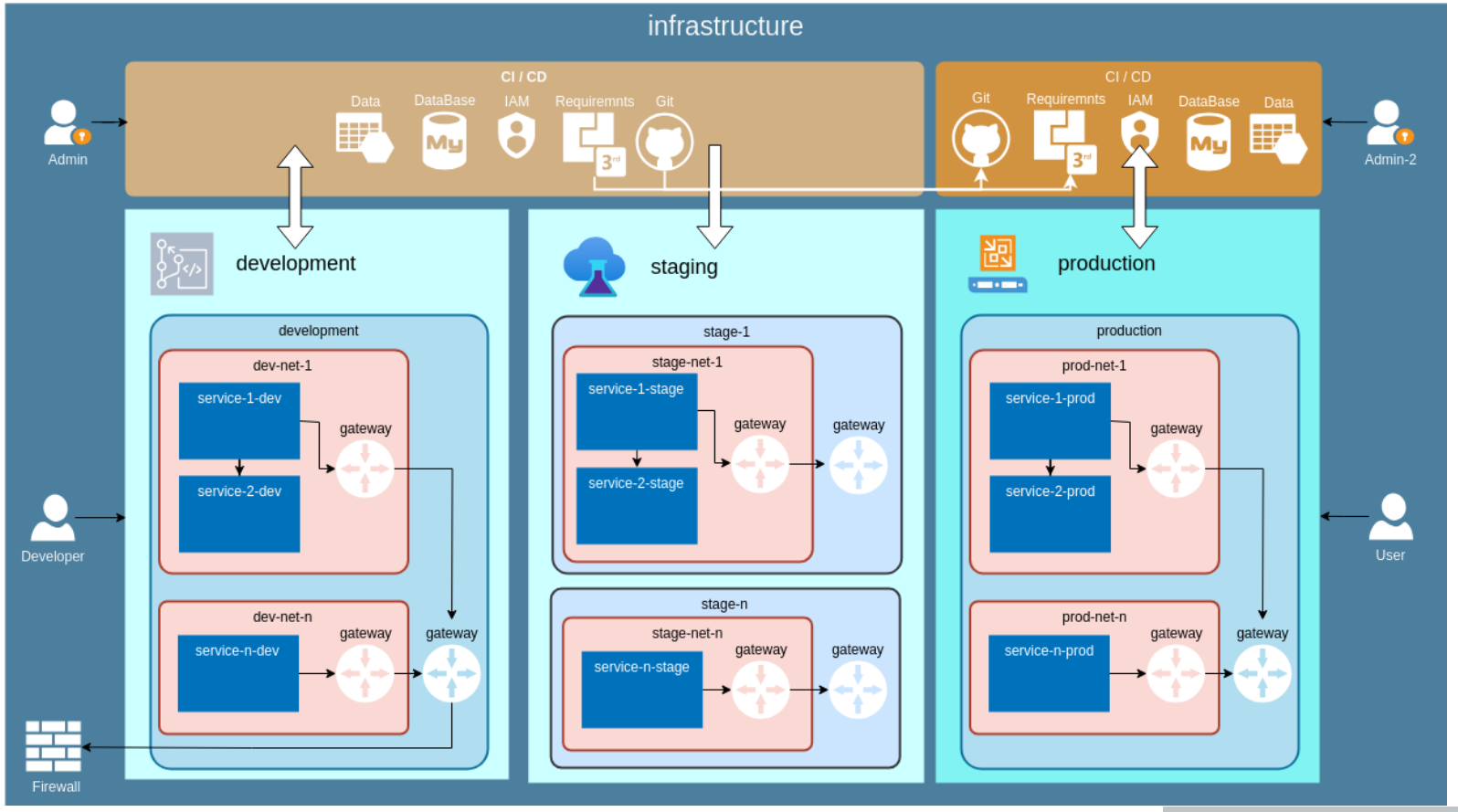


Sicherheitsaspekte bei KI-Diensten mit VS-Daten

Weitere Themenschwerpunkte:

- Absicherung der angebundener Datenpools (extern / intern)
- Datenverschlüsselung
- IAM für Schlüsselmanagement ~ Need2Know Prinzip
- Prüfungen der Funktionalitäten und deren Implementierungen
- Management für Härtung und regelmäßige Prüfungen

Infrastrukturanforderungen für KI-Dienste



Infrastrukturanforderungen für KI-Dienste

Weitere Themenschwerpunkte:

- Paketverwaltung und Updatemethoden
- IaC, Backupmanagement, Ausfallmanagement
- Load Balancing der Hardware für die Services / Instanzen
- Servicelandschaft (Entwicklung / Training / Produktion)

Nächste Schritte

Aufbau einer Arbeitsgruppe aus weiteren Bundesbehörden für den Austausch der bisherigen Ergebnisse

z.B.: ZITis arbeitet an Entwürfen der rechtlichen Rahmenbedingungen und Nutzersensibilisierung

Vergleich durch Benchmark der geplanten Deployment-Prozesse an Hand der aktuellen Anforderungen

z.B.: vGPU Partitionierung, Kubernetes VS Docker

Härtung der ersten Services wie OpenWebUI und Ollama als API Access für RollOut der BSI Bedarfsträger

weiterer Ausbau: ComfyUI, anonyme Websuche, RAG Funktionalitäten, Whisper ASR

Vielen Dank für ihre Aufmerksamkeit

Bei Fragen schreiben Sie uns: