

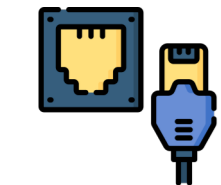


Telemetrie-Daten

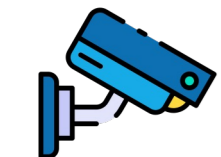
(siehe Pillar „Operational Excellence“)



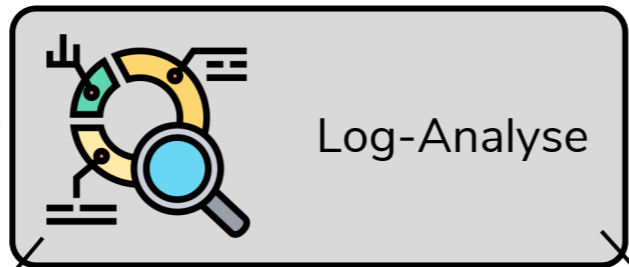
Metriken und Logs



Netzwerk-Logs

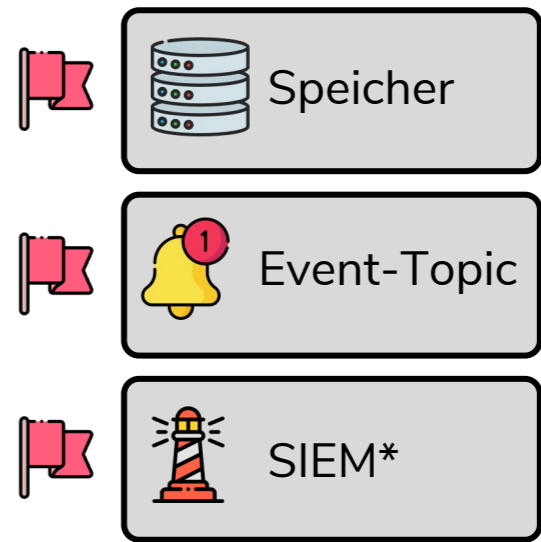


Audit-Logs



Security-Event

- Existieren Crypto Mining Pools?
- Sind Hosts auffällig und mit Malware infiziert?
- Wurden Hosts mittels SSH brute force attackiert?
- Führt ein Host Portscans durch?
- Existieren auffällige Anfragen gegen Cloud-Service-APIs?
- Sind Datenspeicher öffentlich zugänglich?
- ...



Automatische Behebung des Zwischenfalls

Benachrichtigung relevanter Personen

Ticketing-System

