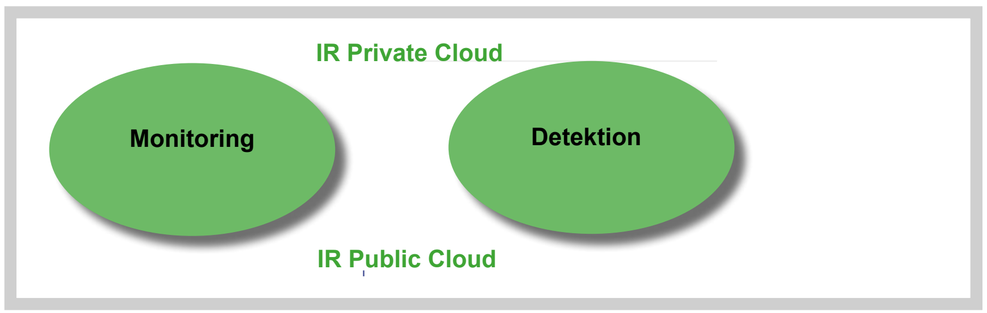
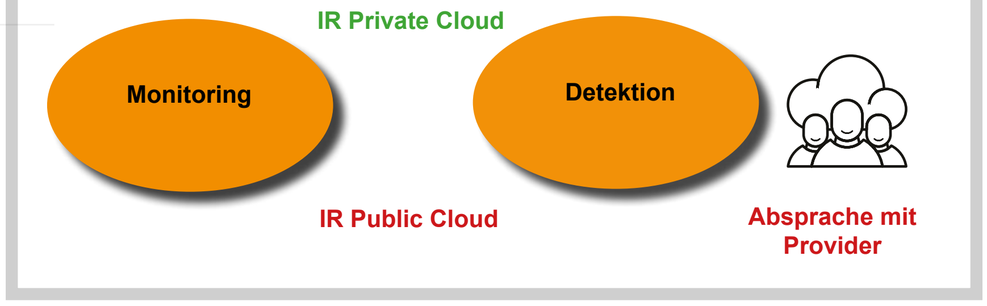
Monitoring und Detektion von Sicherheitsvorfällen in der Hybrid Cloud

IaaS



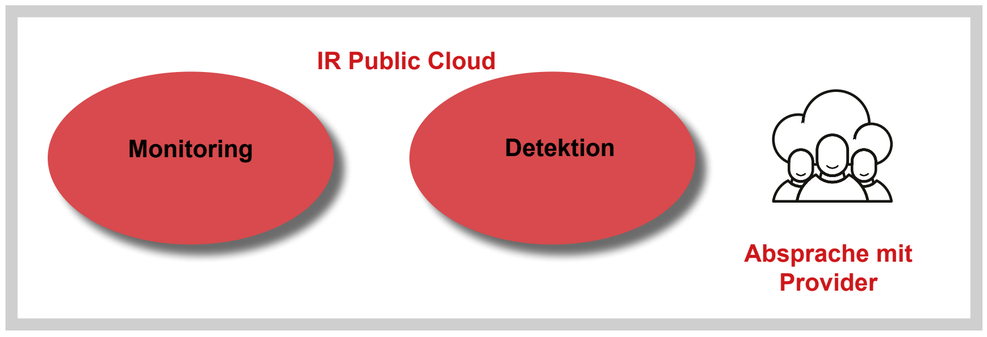
- Ob Public oder Private: User behält die Hoheit über die komplette hybride Cloud und entscheidet eigeninitiativ über den Sensoren-Einsatz zu den Betriebssystemen
- Anbindung auf Systemebene an das eigene SIEM oder die APT-Sensoren für alle Systeme möglich
- Zugriff auf alle erforderlichen Informationen
- kein Zugriff auf die physische Netzwerkinfrastruktur des Providers

PaaS



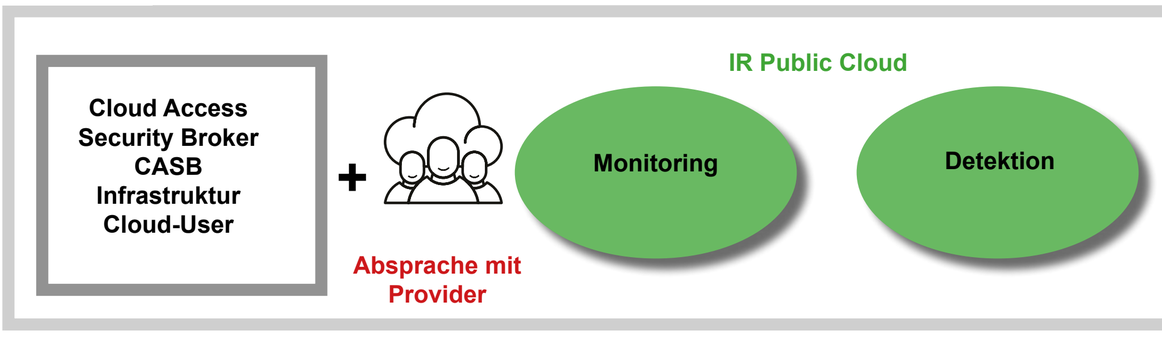
- Private-Cloud: User entscheidet über den Sensoren-Einsatz
- Anbindung auf Systemebene an das eigene SIEM oder die APT-Sensoren eingeschränkt möglich
- im Public-Cloud-Anteil kein Zugriff auf Systeminfrastruktur, für IR Abstimmung mit Provider erforderlich

SaaS



- Kein Zugriff auf auf die darunterliegenden Netzwerkstrukturen, daher kein Monitoring und keine Detektion von Security Incidents durch den User
- hohe Abhängigkeit von IR-Strategie des Providers

SaaS



- Mittels Zugriffs-Überwachung durch den CASB kann der Cloud-Nutzer das Monitoring auf Netzwerkebene auf den SaaS-Service erweitern und in seine eigenen Systeme integrieren.
- CASB ermöglichen die transparente Überwachung des Zugriffs auf Cloud Services sowie die Einsteuerung technischer Richtlinien in den Bereichen Malware Prevention, Authentifizierung, Verschlüsselung und DLP.

TÜVRheinland®
Genau. Richtig.