Container-Plattform - aber sicher!

PUZZLE ITC
changing IT for the better

Ein Kurztrip durch die Landschaft der Cloud-Nativen Security-Produkte

Lukas Kallies

Nice to meet you

Lukas Kallies
@lubeka@mastodon.social

Organisatorisches

- Bei Fragen, fragen!

Agenda

1. Allgemeine Sicherheitsanforderungen
2. Klassische IT-Landschaften
3. Containerbasierte Umgebungen
4. Herausforderungen / Unterschiede dieser Umgebungen
5. Red Hat Advanced Cluster Security und SUSE Security
6. Fazit

Allgemeine Sicherheitsanforderungen

Vertraulichkeit

Integrität

Verfügbarkeit

Sicherheit in klassischen IT-Landschaften

Prozesskommunikation systemintern

Identifizierung von Bedrohungen anhand von Signaturen

Relativ statischer Aufbau

Sicherheit in containerbasierten Umgebungen

Prozesskommunikation über das Netzwerk

Dynamischer Aufbau

Herausforderungen / Unterschiede dieser Umgebungen

Traditionelle Werkzeuge funktionieren nicht effektiv genug

Neue Angriffsflächen

Abstraktion

Notwendigkeit der Automation

Komplexität von Richtlinien

Red Hat Advanced Cluster Security (RHACS)

Sieht alle Images, welche verwendet werden und gleicht (CVE) Datenbanken ab

Prüfung bereits in CI/CD-Pipelines möglich

Prüft auch auf Host-Level (CoreOS)

Visualisiert den Datenverkehr

SUSE Security (NeuVector)

Ebenfalls: CVE-Abgleich, CI/CD-Pipeline-Integration, Host-Level-Security

Build- und Runtime Security-Lösung

Registry-Scanning

Data Loss Prevention ("Regex für Traffic")

Fazit

Ähnlicher Funktionsumfang

Integrationen in SIEM, Registries, CI/CD

Visualisierung ausbaufähig

Dankeschön!

@lubeka@mastodon.social

m.puzzle-itc.de/lkallies