DIFFERENCE BETWEEN FALCO AND KUBEARMOR

INTRODUCTION TO KUBERNETES RUNTIME SECURITY

- Containers need runtime security beyond initial deployment.
- Falco and KubeArmor provide security at different levels.
- Importance of proactive and reactive security measures.
- Overview of key differences between the two tools.

FALCO OVERVIEW

- Open-source runtime security tool by Sysdig.
- Detects threats based on kernel system calls.
- Uses rule-based security monitoring.
- Sends alerts when suspicious activities occur.

KUBEARMOR OVERVIEW

- Cloud-native runtime security solution.
- Enforces security policies at the system call level.
- Uses Linux security modules (AppArmor, SELinux, BPF-LSM).
- Provides policy enforcement rather than just detection.

COMPARISON TABLE - FALCO VS KUBEARMOR

Feature	Falco	KubeArmor
Detection Method	Monitors syscalls via eBPF	Enforces security policies
Policy Type	Rule-based alerts	Policy enforcement
Integration	Works with SIEM tools	Works with AppArmor/SELinux
Use Case	Threat detection & alerts	Access control & policy enforcement

THANK YOU

Aravind Shilam