AYI NEDJIMI Consultants

Falco : Detection Runtime Cloud-Native (CNCF 2026

10 mai 2026 • Mis à jour le 17 mai 2026 • 19 min de lecture • 4003 mots • 65 vue

Falco est le moteur de detection runtime cloud-native de reference, projet CNCF graduated (fevrier 2024) qui observe en temps reel les syscalls Linu via eBPF moderne et les audit logs Kubernetes pour declencher des alerte lorsqu'un comportement suspect correspond a une regle YAML. Cree par Sysdig en 2016 puis donne a la CNCF en 2018, Falco instrumente plus de 120 syscalls sensibles, embarque un langage de regles declaratives et expose les alertes via Falcosidekick vers 30+ destinations (Slack, PagerDuty, Elastic, Sentinel). Version 0.41 sous licence Apache 2.0, c'est l brique standard de runtime threat detection en Kubernetes.

Falco est le moteur de **detection runtime cloud-native** de reference, projet **CNCF graduated** (graduation prononcee en fevrier 2024) qui observe en temps reel les **syscalls Linux** via une sonde eBPF moderne ou un m que les **au logs Kubernetes**, pour declencher des alertes lorsqu suspect

correspond a une regle declarative en YAML. Cree initialement par **Sysdig Inc.** en 2016 puis donne a la **Cloud Native Computing Foundation** en octobre 2018, Falco devenu en huit ans la brique standard de runtime threat detection deployee dans l architectures Kubernetes de production : il instrumente plus de **120 syscalls sensibles**, embarque un langage de regles compose de conditions booleennes su des champs typees (`proc.name` , `fd.name` , `k8s.pod.label` , `container.image`) expose les alertes via stdout, syslog, fichier, gRPC ou les 30+ destinations de **Falcosidekick** (Slack, PagerDuty, Elastic, Loki, OpenSearch, AWS Lambda, Pub/Su La version stable courante est **Falco 0.41.0** (avril 2026), distribuee sous **licence Apache 2.0**, avec un driver eBPF moderne (CO-RE) qui supprime la dependance a headers noyau et permet le deploiement immutable sur les distributions minimales (Bottlerocket, Talos Linux, Flatcar). Falco occupe une niche distincte de Wazuh ou Sentinel : ce n'est ni un SIEM, ni un EDR, mais un detecteur runtime pur dont la val reside dans la finesse d'observation kernel et la capacite a couvrir des scenarios **container escape**, **cryptomining**, **reverse shell** ou **exec dans un pod sensible** que outils superieurs (CSPM, KSPM, SIEM) ne voient pas.

À RETENIR

A retenir

Falco est le moteur runtime threat detection cloud-native de reference, projet CNCF graduated depuis fevrier 2024, distribue sous licence Apache 2.0.

Trois drivers de capture syscalls : module noyau classique, eBPF probe legacy, eBPF moderne CO-RE (recommande

Réponse sous 24h

Devis gratuit →