**Monitoratge i detecció de comportaments sospitosos.
Introducció a Falco i cAdvisor**

Objectiu

* Configurar eines de monitoratge i detecció dins d’un clúster Kubernetes.
* Detectar activitats anòmales o potencialment malicioses executades dins dels pods.
* Entendre com es poden identificar comportaments que poden indicar un atac en curs.

Eines utilitzades

* Falco: eina de detecció d’activitat sospitosa basada en syscalls del sistema.

*(Quan un programa vol fer una acció com llegir un fitxer, obrir una connexió de xarxa, executar un procés o accedir a la memòria, no pot fer-ho directament. En lloc d’això, fa una* ***syscall*** *que el nucli del sistema s’encarrega d’executar de manera segura i controlada.)*

* cAdvisor: eina de monitoratge de rendiment de contenidors (CPU, memòria, etc.).

**Fase 1: Desplegament de cAdvisor**

1. Crear un pod amb cAdvisor

**Requisit important:** assegurar-se que no hi hagi cap altre servei exposat al port 8080 (com nginx de la primera pràctica

* + Si cal, aturar el port-forward o eliminar el servei anterior.

**Opcions:**

* Aturar el port-forward actiu amb Ctrl+C
* Fer servir un port local diferent, per exemple: 8081
* Eliminar el servei web-nginx amb:

kubectl delete service web-nginx

kubectl delete deployment web-nginx

kubectl run cadvisor --image=gcr.io/cadvisor/cadvisor:v0.45.0 --port=8080

feu

 kubectl get pods

i espereu fins que veieu que el cAdvisor està corrent.

**Fase 2: Exposar el servei de cAdvisor al navegador**

Si el port 8080 està lliure:

kubectl port-forward pod/cadvisor 8080:8080

Si el port 8080 ja està ocupat, utilitzar un altre, per exemple:

kubectl port-forward pod/cadvisor 8081:8080

Obrir el navegador i accedir a

<http://localhost:8080>

per veure les estadístiques d’ús de recursos dels contenidors actius.

**Fase 3: Desplegament de Falco**

1. Afegir el repositori de Helm.

Primer hem d’instal·lar Helm, que és el gestor de paquets per a Kubernetes, es poden utilitzar dues opcions:

curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash

Un cop instal·lat, comprovar que funciona correctament:

helm version

Helm és necessari per desplegar Falco fàcilment.

helm repo add falcosecurity <https://falcosecurity.github.io/charts>
helm repo update

1. Desplegar Falco amb Helm

helm install falco falcosecurity/falco

1. Comprovar l’estat del pod Falco

kubectl get pods

 trigarà una mica de temps en estar en estat “running”

****

**Fase 3: Simulació d’activitat sospitosa**

Simularem accions típiques d’un atacant dins del clúster per veure si Falco les detecta.

Primer arranquem falco perquè comenci a monitoritzar

kubectl logs -l app=falco

Si ens dona un error hem de mirar quina etiqueta te el pod que volem monitoritzar:

kubectl get pods --show-labels

1. En una finestra nova de terminal (sense tancar l’altra), crear un pod temporal per simular una acció sospitosa

kubectl run attacker --image=alpine -it --restart=Never -- sh

1. Dins del pod, executar una d’aquestes comandes sospitoses:

touch /etc/passwd
cat /etc/shadow
sh

1. Sortir del pod

exit

1. Tornar a comprovar els logs de Falco per veure si s’ha detectat l’activitat sospitosa.

kubectl logs -l app=falco

**Fase 4: Neteja**

Eliminar els recursos creats:

kubectl delete pod attacker
helm uninstall falco
kubectl delete -f <https://raw.githubusercontent.com/google/cadvisor/master/deploy/kubernetes/base.yaml>

Fase 5: Reflexió

* Quines activitats del pod **attacker** ha detectat Falco?