



DEVSECOPS

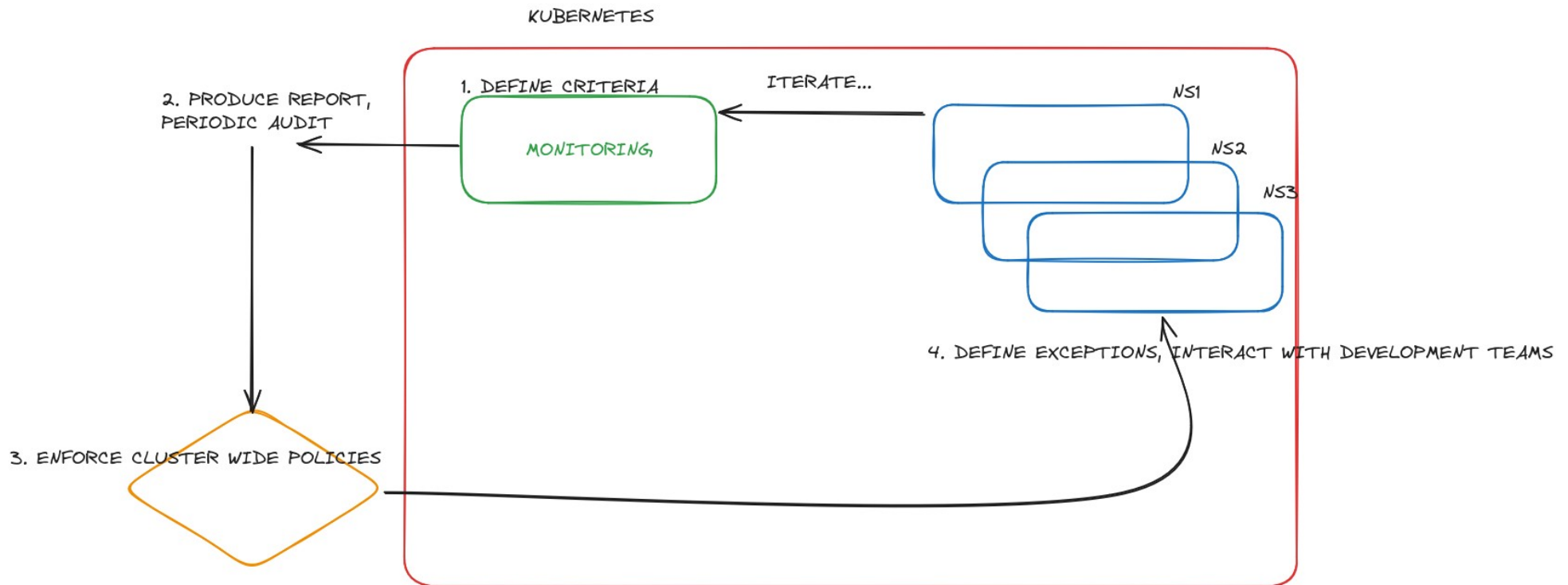


SECURITY HARDENING

Three common sources of compromise in Kubernetes are supply chain risks, malicious threat actors, and insider threats.

Supply chain risks are often challenging to mitigate and can arise in the container build cycle or infrastructure acquisition. **Malicious threat actors** can exploit vulnerabilities and misconfigurations in components of the Kubernetes architecture, such as the control plane, worker nodes, or containerized applications. **Insider threats** can be administrators, users, or cloud service providers. Insiders with special access to an organization's Kubernetes infrastructure may be able to abuse these privileges.

MITIGATION STRATEGY



AUDIT POLARIS

Cluster Overview: <https://10.245.0.1:443>

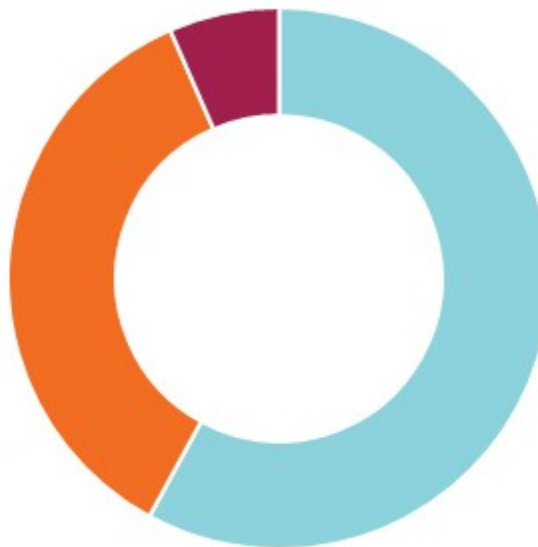


Smooth sailing within sight

Grade: **C-**

Score: **70%**

Score is the percentage of passing checks. Warnings get half the weight of dangerous checks.



1270
passing checks



778
warning checks



144
dangerous checks

! Some checks were skipped based on configured exemptions. [Click here](#) to view the report with these checks included.

Kubernetes Version: 1.28

Nodes: 3

Namespaces: 25

Controllers: 57

Pods: 0

CLOUD SECURITY SCORING

2023/24

Conteneurisation et Orchestration
de conteneurs - Aureliano Sinatra

4 / 9

AUDIT POLARIS

Namespace: **mjust**

▶ ConfigMap:	kube-root-ca.crt	<div></div>
▶ Ingress:	cm-acme-http-solver-lcvhs	<div></div>
▶ Ingress:	example-webapp-test	<div></div>
▶ Ingress:	example-webapp-test	<div></div>
▼ Pod:	debug	<div></div>

Spec:

! Label app.kubernetes.io/instance must match metadata.name ?

Pod Spec:

- ✗ Host network should not be configured ?
- ! A NetworkPolicy should match pod labels and contain applied egress and ingress rules ?
- ! Priority class should be set ?
- ! Pod should be configured with a valid topology spread constraint ?
- ! The ServiceAccount will be automounted ?
- ✓ Host IPC is not configured ?
- ✓ Host PID is not configured ?

Container debug:

- ✗ Privilege escalation should not be allowed ?
- ✗ Should not be allowed to run as root ?
- ! Readiness probe should be configured ?
- ! CPU limits should be set ?
- ! Use one of AppArmor, Seccomp, SELinux, or dropping Linux Capabilities to restrict containers using unwanted privileges ?

AUDIT FALCO

Kubernetes Client Tool Launched in Container

sandbox

WARNING

enabled

Container Drift Detected (chmod)

sandbox

ERROR

disabled

Description:

Detect new executables created within a container as a result of chmod. While this detection can generate significant noise, chmod usage is frequently linked to dropping and executing malicious implants. The newer rule "Drop and execute new binary in container" provides more precise detection of this TTP using unambiguous kernel signals. It is recommended to use the new rule. However, this rule might be more relevant for auditing if applicable in your environment, such as when chmod is used on files within the /tmp folder.

Condition:

```
chmod and container and evt.rawres>=0 and ((evt.arg.mode contains "S_IXUSR") or
(evt.arg.mode contains "S_IXGRP") or
(evt.arg.mode contains "S_IXOTH"))
and not runc_writing_exec_fifo and not runc_writing_var_lib_docker and not
user_known_container_drift_activities
```

☒ Highlight All ☐ Match Case ☐ Match Diacritics ☐ Whole Words

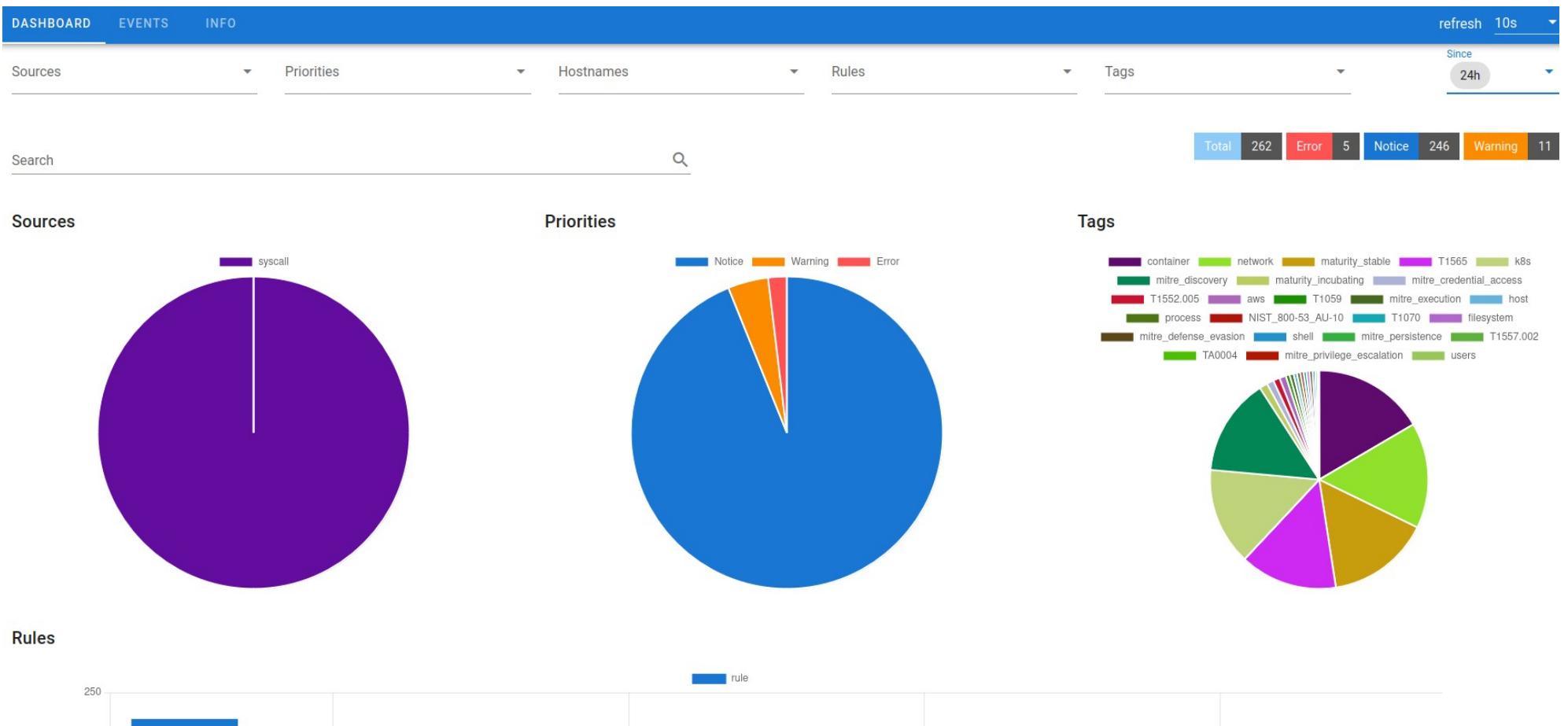
CUSTOMIZABLE THREATS DEFINITION AND PRIORITIZATION

2023/24

Conteneurisation et Orchestration
de conteneurs - Aureliano Sinatra

6 / 9

AUDIT FALCO



THREATS DASHBOARD AND REPORTING

2023/24

Conteneurisation et Orchestration
de conteneurs - Aureliano Sinatra

7 / 9

100

DASHBOARD

EVENTS

INFO

Sources

Priorities

Hostnames

Rules

Tags

refresh

10s

Since

1h

Search

EXPORT

Total

83

Notice

76

Warning

7

Timestamp	Source	Hostname	Priority	Rule	Output
2024/01/09 12:09:47:346	syscall	falco-hmqvs	Warning	Launch Suspicious Network Tool in Container	<div> <div>11:09:47.346408226: Warning Network tool launched in container (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=nmap proc_exepath=/usr/bin/nmap parent=bash command=nmap terminal=34816 exe_flags=EXE_WRITABLE container_id=3f56b7a34f4c container_image=docker.io/asinatra/arpscan container_image_tag=v1.0.3 container_name=debug k8s_ns=asinatra k8s_pod_name=debug)</div> <div> <div>container.id</div> <div>3f56b7a34f4c</div> <div>container.image.repository</div> <div>docker.io/asinatra/arpscan</div> <div>container.image.tag</div> <div>v1.0.3</div> <div>container.name</div> <div>debug</div> <div>evt.arg.flags</div> <div>EXE_WRITABLE</div> <div>evt.time</div> </div> <div> <div>1704798587346408200</div> <div>evt.type</div> <div>execve</div> <div>k8s.ns.name</div> <div>asinatra</div> <div>k8s.pod.name</div> <div>debug</div> <div>proc.cmdline</div> <div>nmap</div> <div>proc.exepath</div> <div>/usr/bin/nmap</div> <div>proc.name</div> <div>nmap</div> <div>proc.pname</div> <div>bash</div> </div> <div> <div>proc.tty</div> <div>34816</div> <div>user.loginuid</div> <div>-1</div> <div>user.name</div> <div>root</div> <div>user.uid</div> <div>0</div> </div> </div>
2024/01/09 12:08:59:055	syscall	falco-hmqvs	Warning	A shell was used as the endpoint/exec point into a container with an attached terminal. Parent process may have legitimately already exited and be null (read container_entrypoint macro). Common when using "kubect exec" in Kubernetes. Correlate with k8saudit exec logs if possible to find user or serviceaccount	<div> <div>11:08:59.055193293: Warning A shell was spawned in a container with an attached terminal (evt_type=execve user=root user_uid=0 user_loginuid=-1 process=bash proc_exepath=/bin/bash parent=bash command=bash terminal=34816 exe_flags=EXE_WRITABLE container_id=3f56b7a34f4c container_image=docker.io/asinatra/arpscan container_image_tag=v1.0.3 container_name=debug k8s_ns=asinatra k8s_pod_name=debug)</div> <div> <div>container.id</div> <div>3f56b7a34f4c</div> <div>container.image.repository</div> <div>docker.io/asinatra/arpscan</div> <div>container.image.tag</div> <div>v1.0.3</div> <div>container.name</div> <div>debug</div> <div>evt.arg.flags</div> <div>EXE_WRITABLE</div> <div>evt.time</div> </div> <div> <div>1704798539055193300</div> <div>evt.type</div> <div>execve</div> <div>k8s.ns.name</div> <div>asinatra</div> <div>k8s.pod.name</div> <div>debug</div> <div>proc.cmdline</div> <div>bash</div> <div>proc.exepath</div> <div>/bin/bash</div> <div>proc.name</div> <div>bash</div> <div>proc.pname</div> <div>runc</div> <div>p</div> </div> <div> <div>34816</div> <div>user.loginuid</div> <div>-1</div> <div>user.name</div> <div>root</div> <div>user.uid</div> <div>0</div> </div> </div>

REALTIME SCAN OF THREATS



ATELIER

- Using threats definitions from FALCO define a set of malicious scripts in order to trigger the alerts
- Build and deploy images
- Run them in cluster