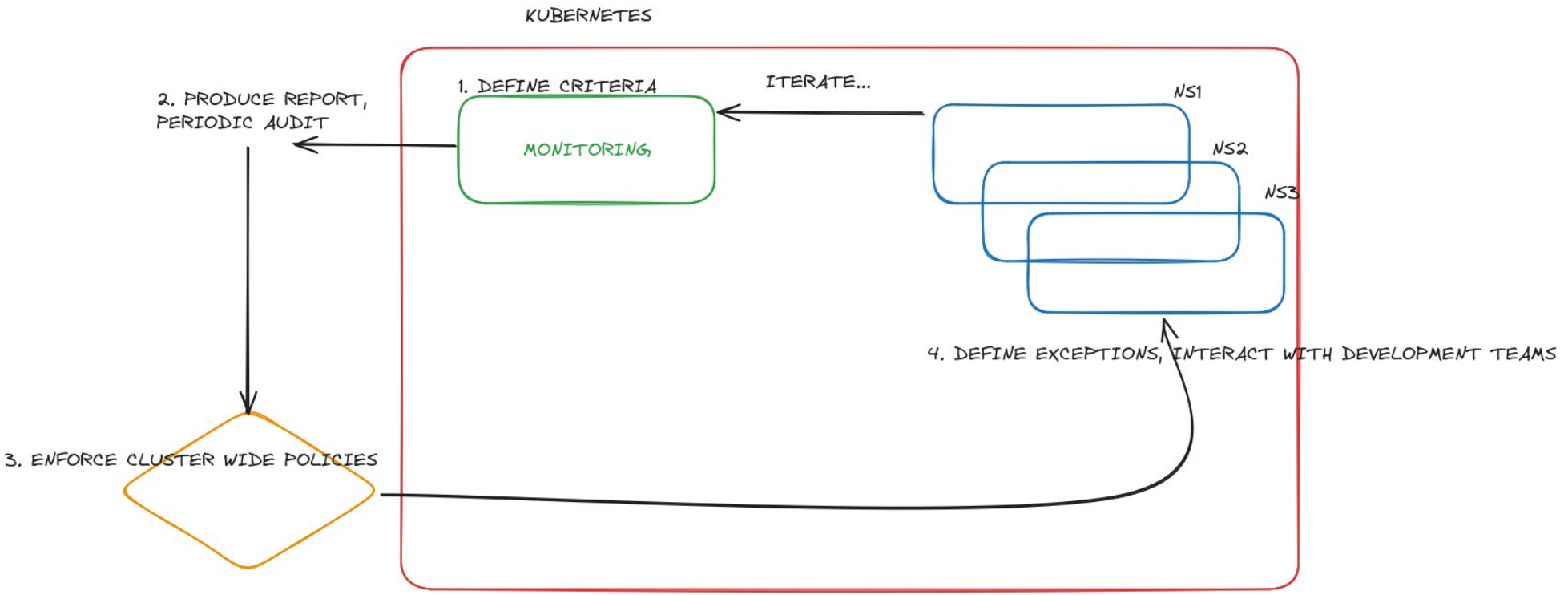
DEVSECOPS

SECURITY HARDENING

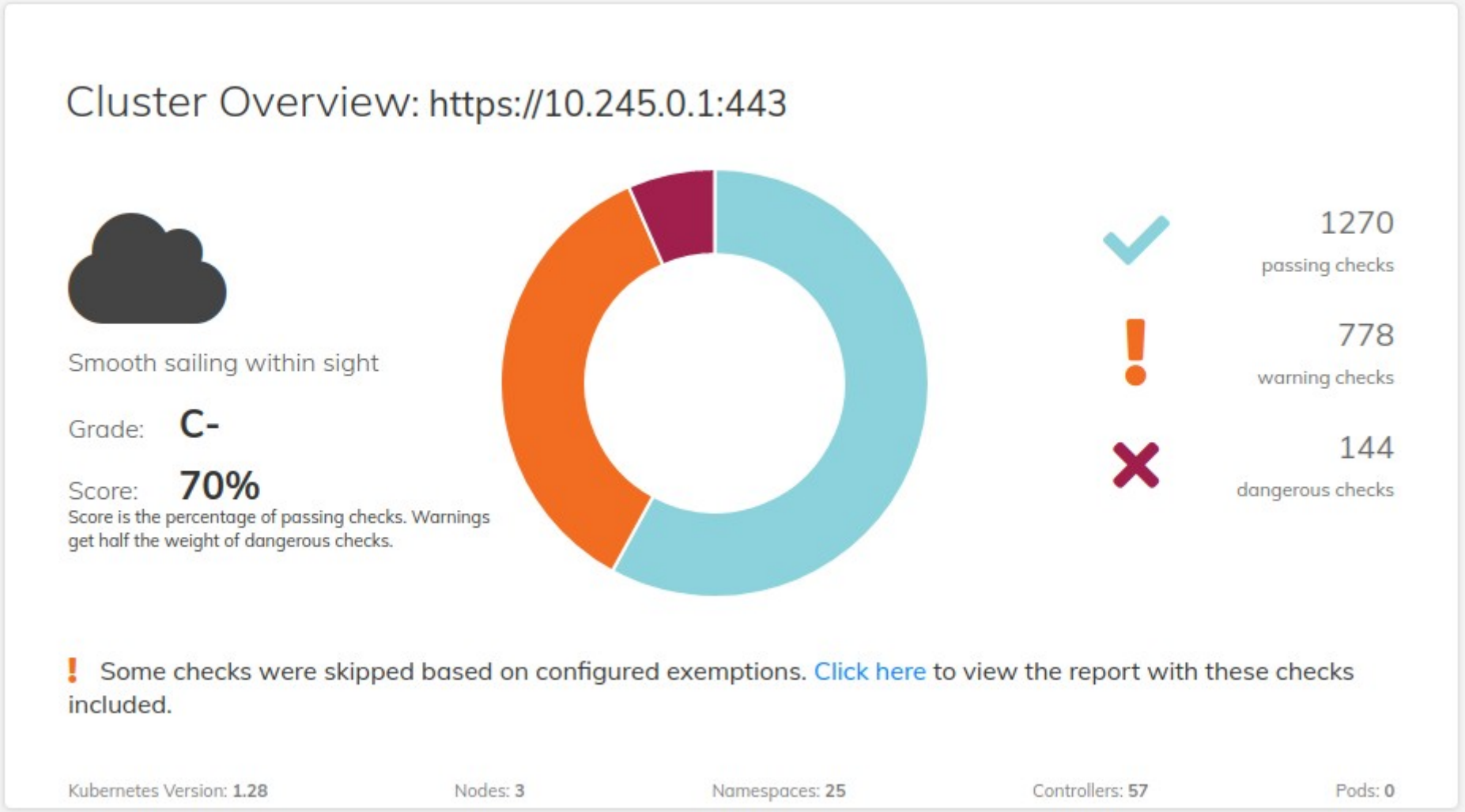
Three common sources of compromise in Kubernetes are supply chain risks, malicious threat actors, and insider threats.

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

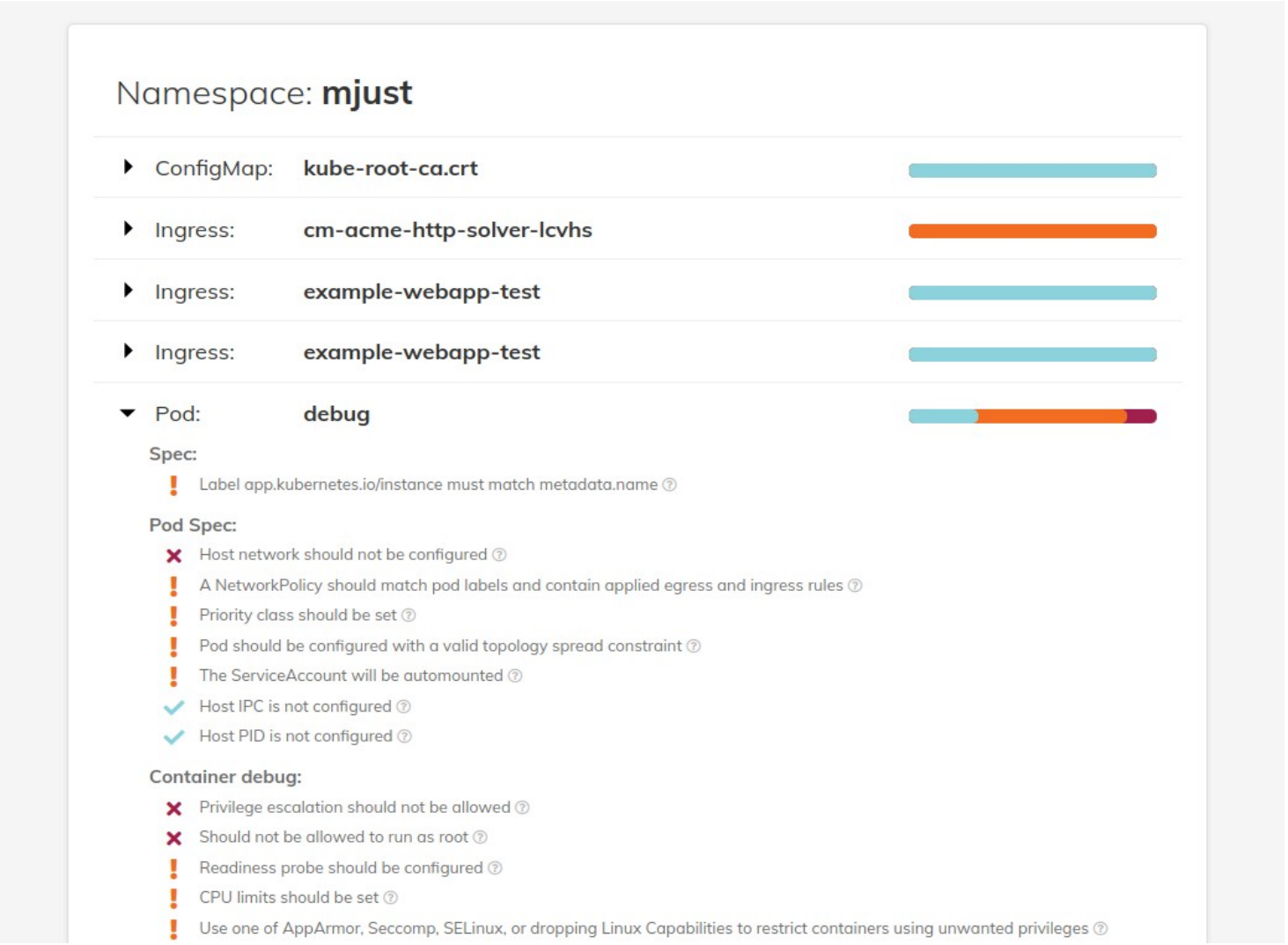


AUDIT POLARIS



CLOUD SECURITY SCORING

AUDIT POLARIS



AUDIT FALCO

Kubernetes Client Tool Launched in Container sandbox WARNING enabled

Container Drift Detected (chmod) sandbox ERROR disabled

Description:

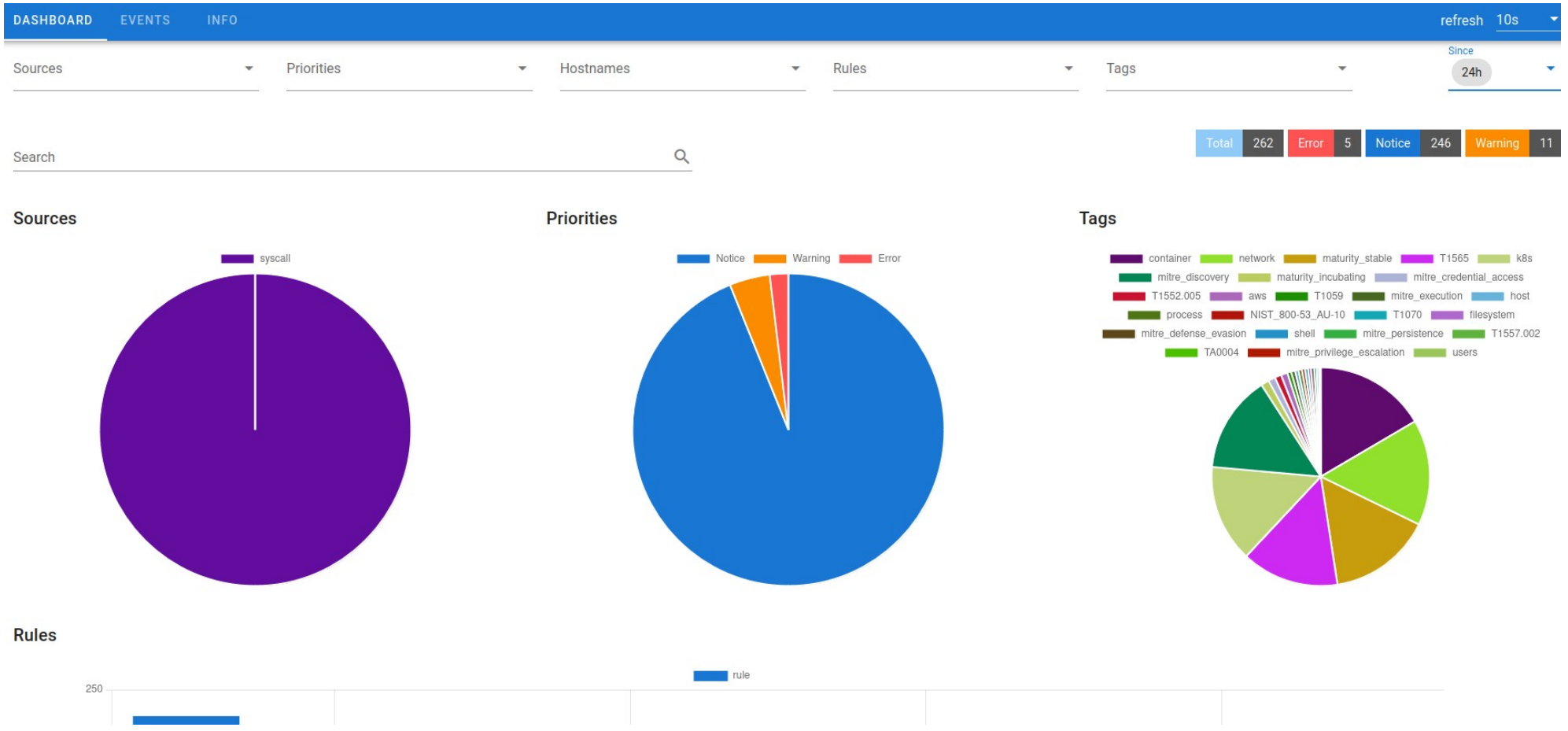
Detect new executables created within a container as a result of chmod. While this detection can generate significant noise, chmod usage is frequently linked to dropping and executing malicious implants. The newer rule "Drop and execute new binary in container" provides more precise detection of this 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
```

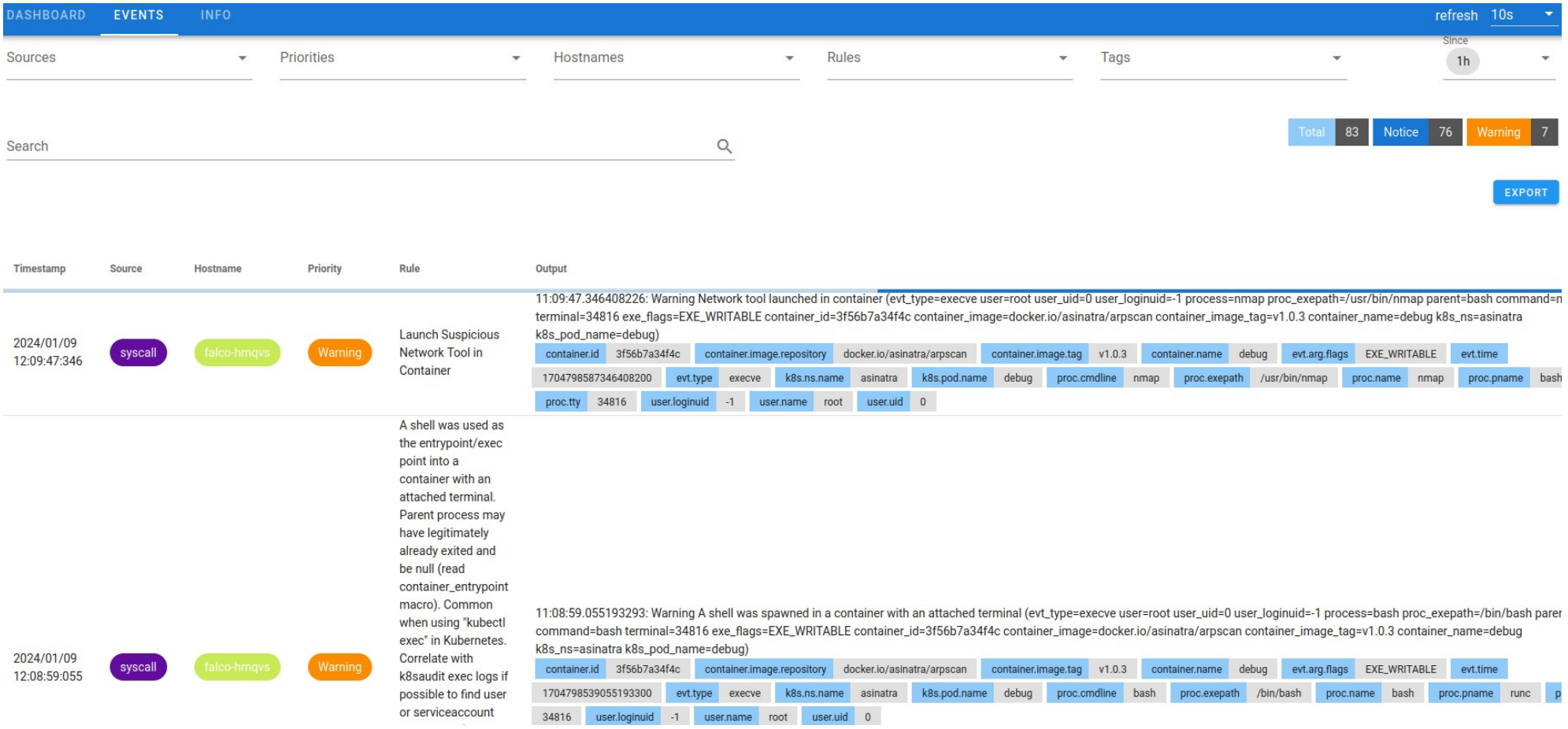
CUSTOMIZABLE THREATS DEFINITION AND PRIORITIZATION

AUDIT FALCO



THREATS DASHBOARD AND REPORTING

AUDIT FALCO



REALTIME SCAN OF THREATS

ATELIER

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