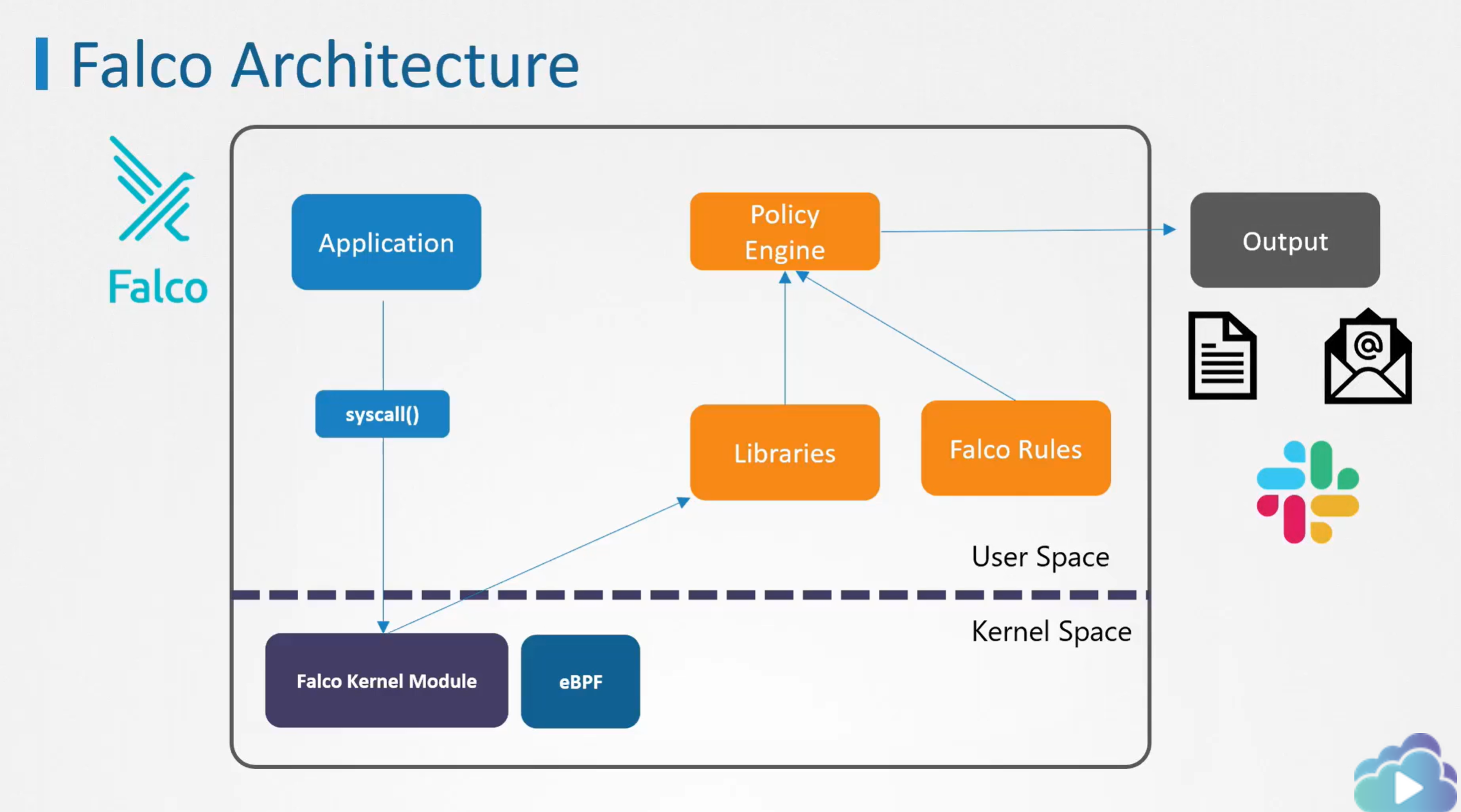
**K8S Monitoring Logging and Runtime Security**

### K8S Monitoring

1. Falco overview and installation



Falcon needs to see what system calls are coming through from the applications in the user space into the linux kernel. This means that somehow, it has to insert itself into the kernel to sit in the middle and see what’s coming in.

Falcom Kernel Module & eBPF:

One way to do this is by making use of a kernel module. However, it basically means that we insert additional code right inside the linux kernel. Some manage Kubernetes service providers do not allow us to do this. Falco can also interact with the kernel through what is called eBPF

Libraries:

System calls are then analyzed by libraries in the user space

Policy Engine:

The events are then filtered by the Falco policy engine by making use of the predefined rules that can detect whether the event was suspicious or not.

1. Falco Installation

Out of k8s cluster: <https://falco.org/docs/getting-started/installation/>

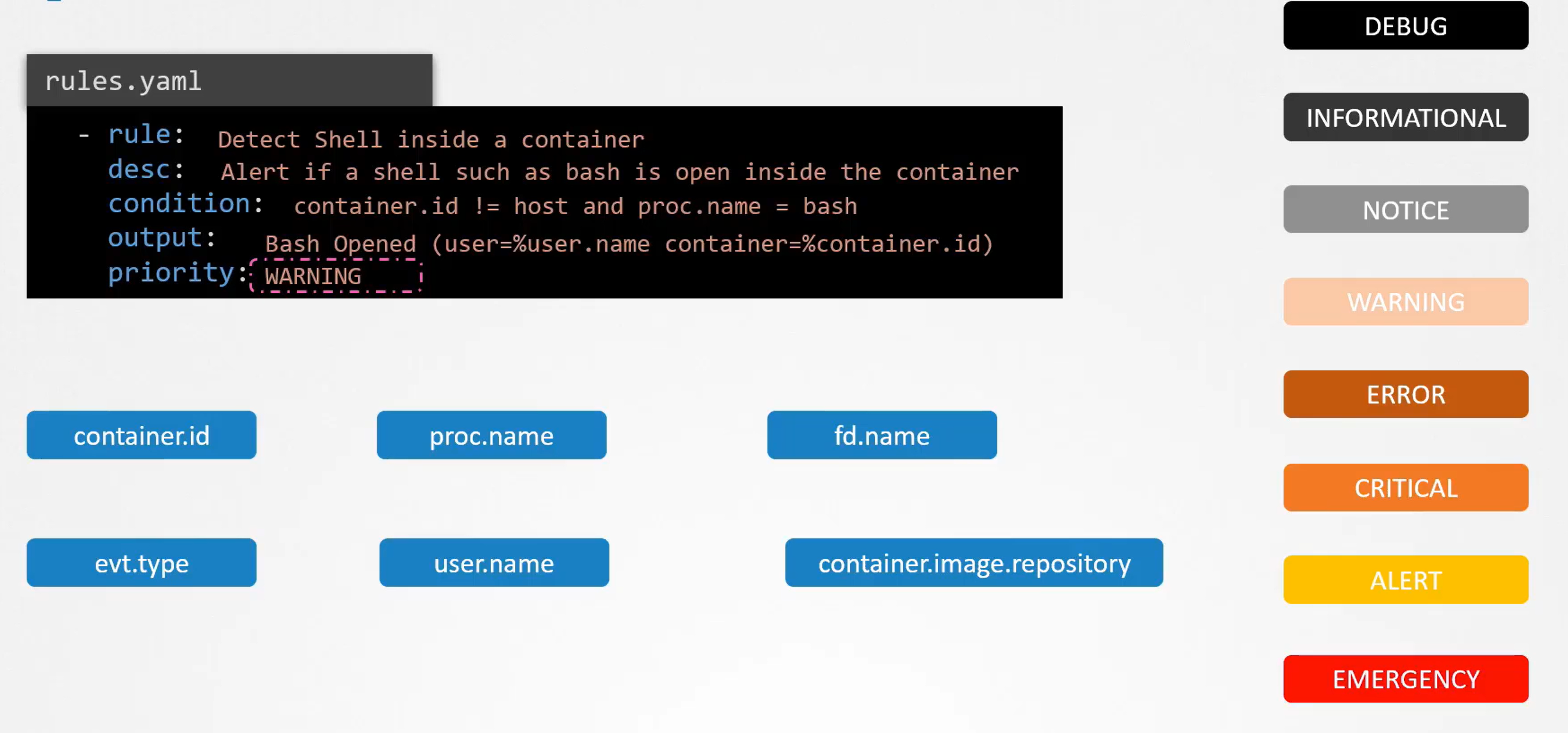
Inside of k8s cluster:

<https://github.com/falcosecurity/charts/tree/master/falco#adding-falcosecurity-repository>

1. Falco outpus when matching rules



1. Falco Rules



container.id != host and proc.name = bash: The event will be record if the BASH process was run inside the container.

container.id: filters the name of a container

proc.id: filters the name of the process

fd.name: match events against a specific file, such reading or writing inside a file

evt.type: filters system calls by name such as execve, open, accept, connect, etc

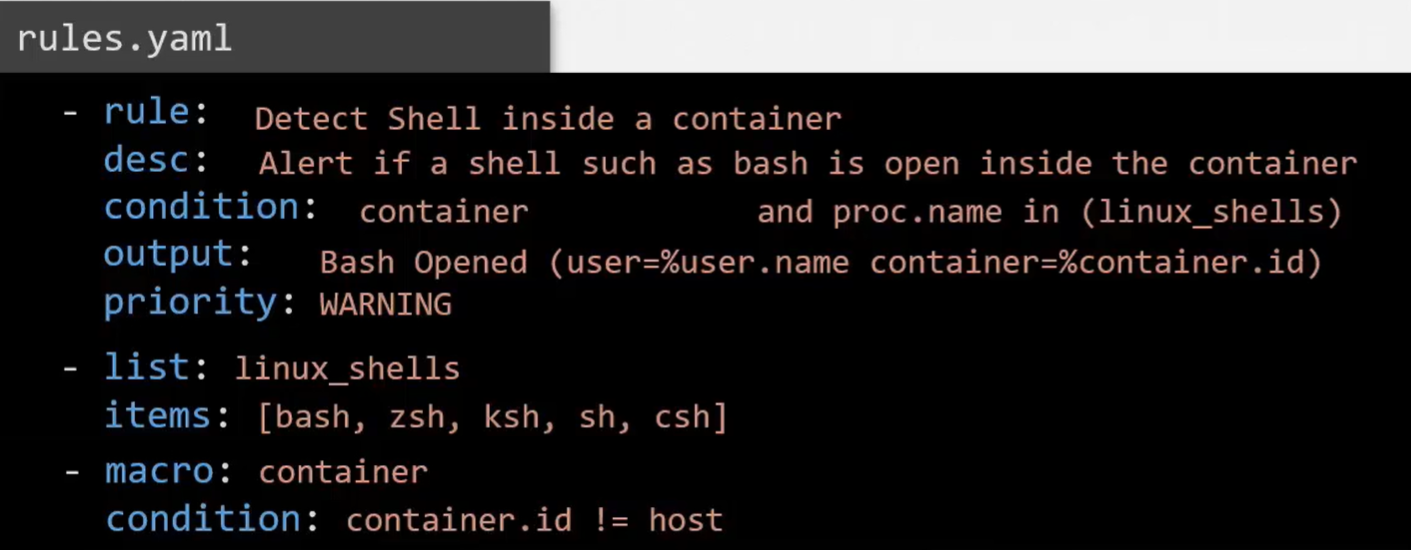
user.name: filter the user whose actions generated the event.

container.image.repository: filters the specific images by name.

<https://falco.org/docs/rules/supported-fields/>

Condition

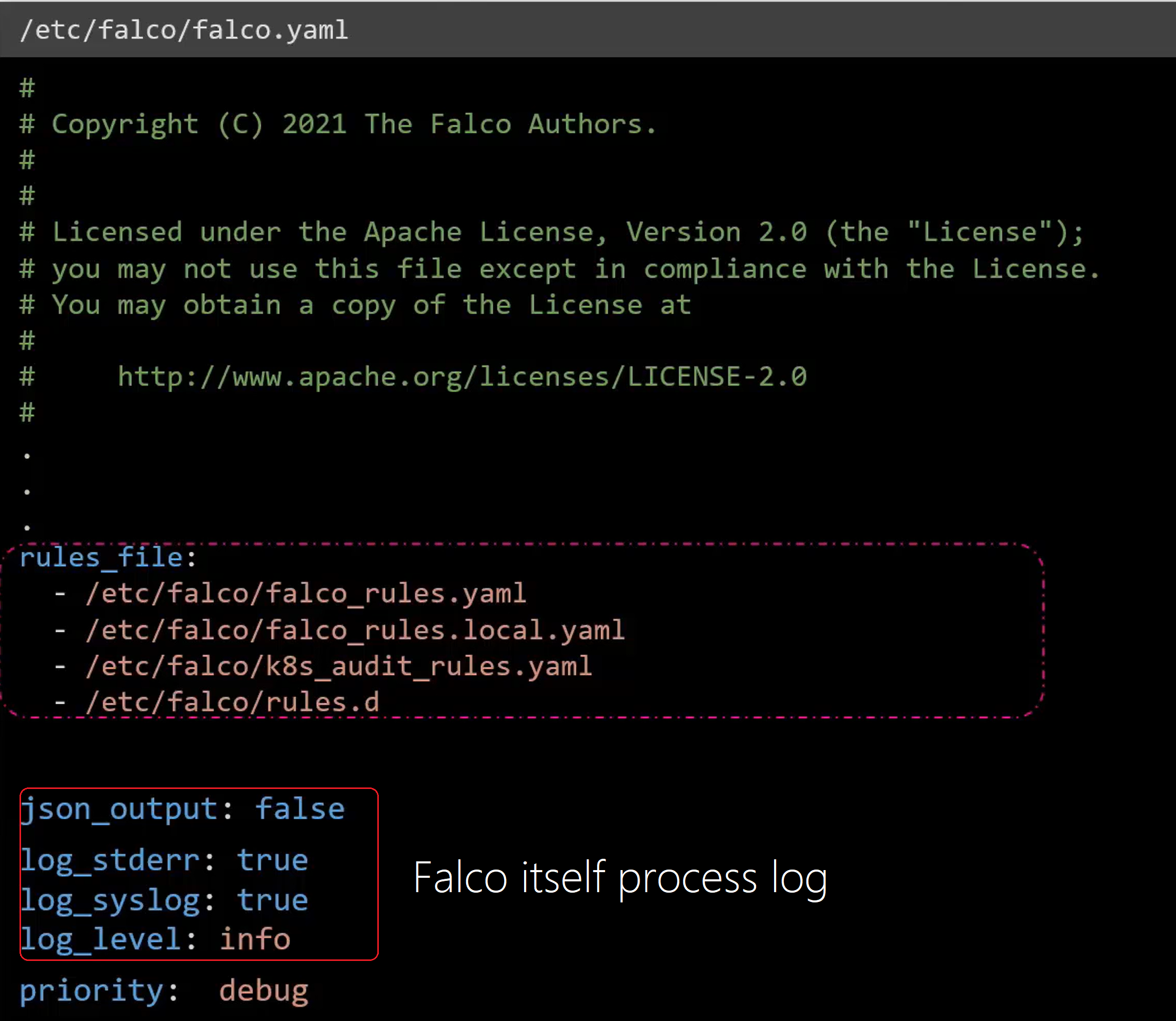
For multiple conditions, can use list



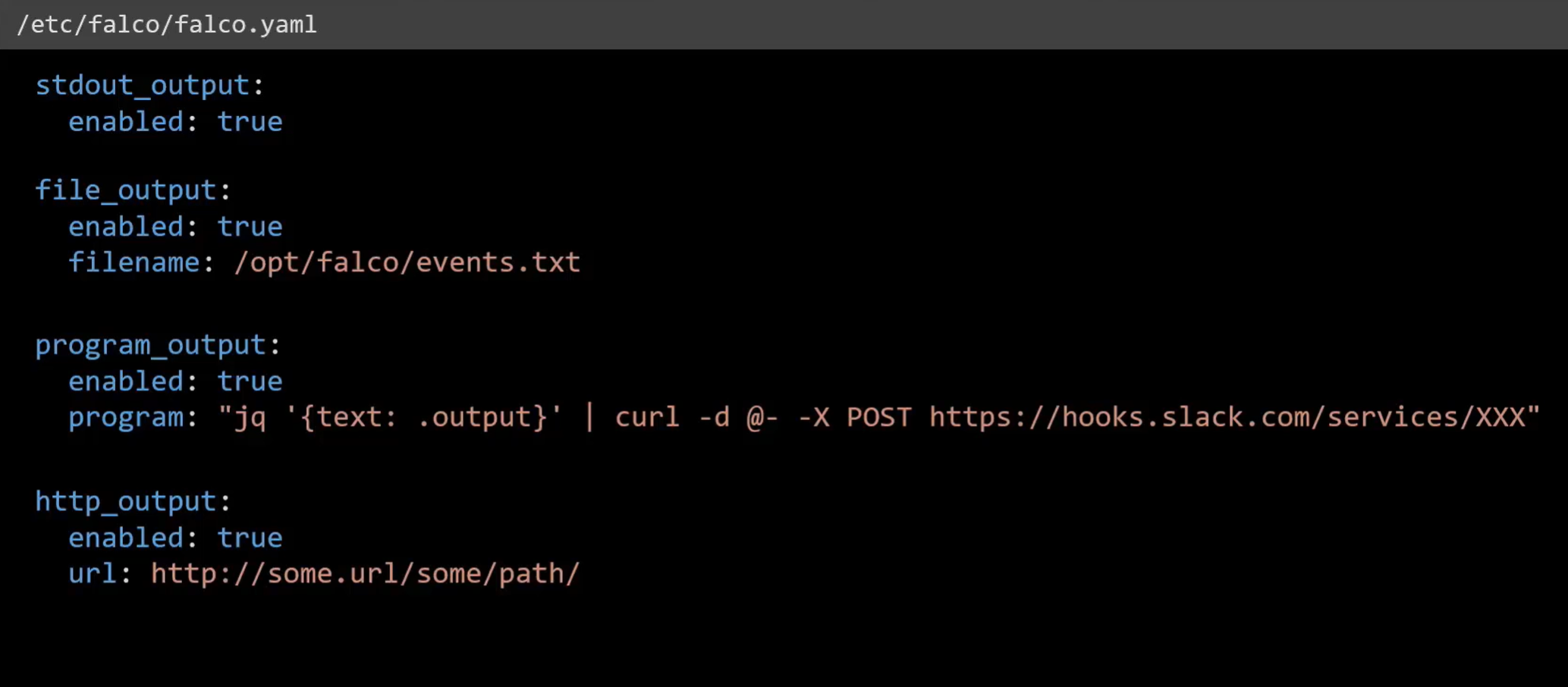
<https://falco.org/docs/rules/default-macros/>

1. Falco Configuration Files

/etc/falco/falco.yaml



Output channels that can be configured



Every time change the falco.yaml configuration, we need reload falco configuration and restart the engine

Hot Reload:

Find falco process ID: cat /var/run/falco.pid

Signal SIGHUP: kill -1 $(cat /var/run/falco.pid)

Reference:

<https://falco.org/docs/configuration/>

Falco Rules configuration

Default rule: /etc/falco/falco\_rules.yaml contains all built-in rules, lists and micros

\* Any changes made to the falco\_rules.yaml file will be overwritten when falco package is updated. While the change can be made to the falco\_rules.local.yaml