# KubeArmor

Internal Design

# Agenda

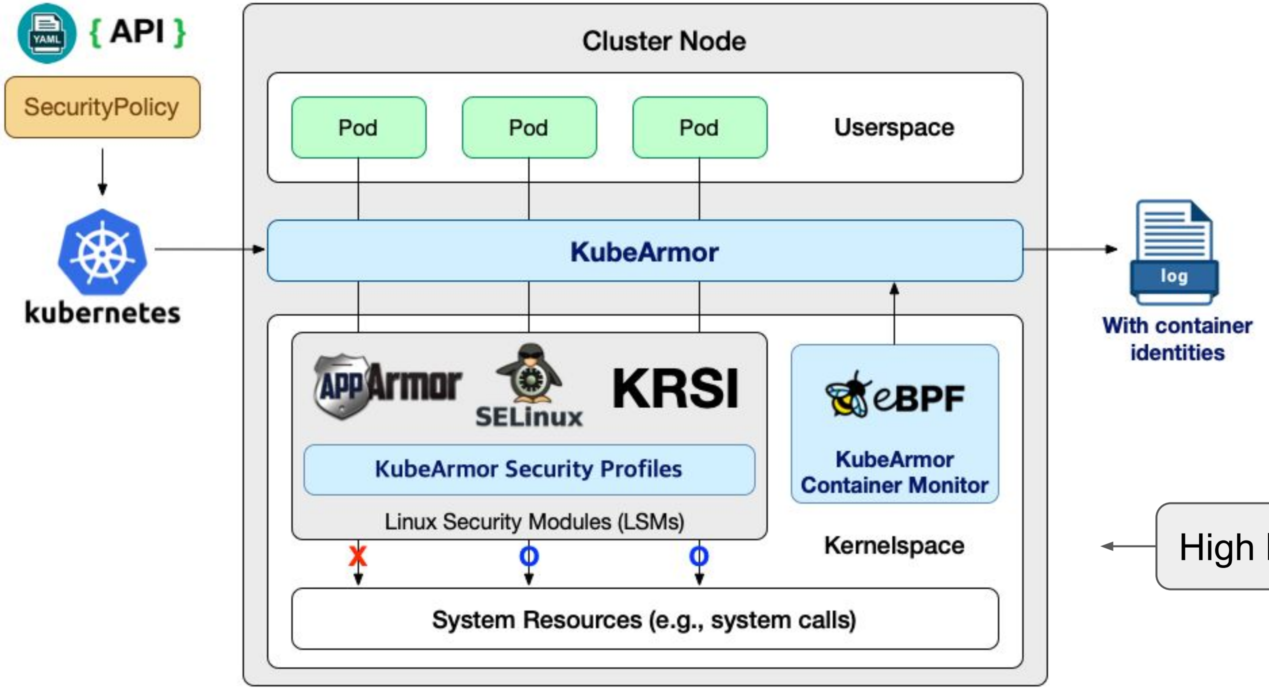
1. Architectural Overview of KubeArmor

2. Components in KubeArmor
   a. KubeArmor Core Engine
   b. Platform Handler
   c. LSM Enforcer
      i. AppArmor Enforcer
      ii. SELinux Enforcer
   d. System Monitor
   e. Logger

# Architectural Overview of KubeArmor

# KubeArmor

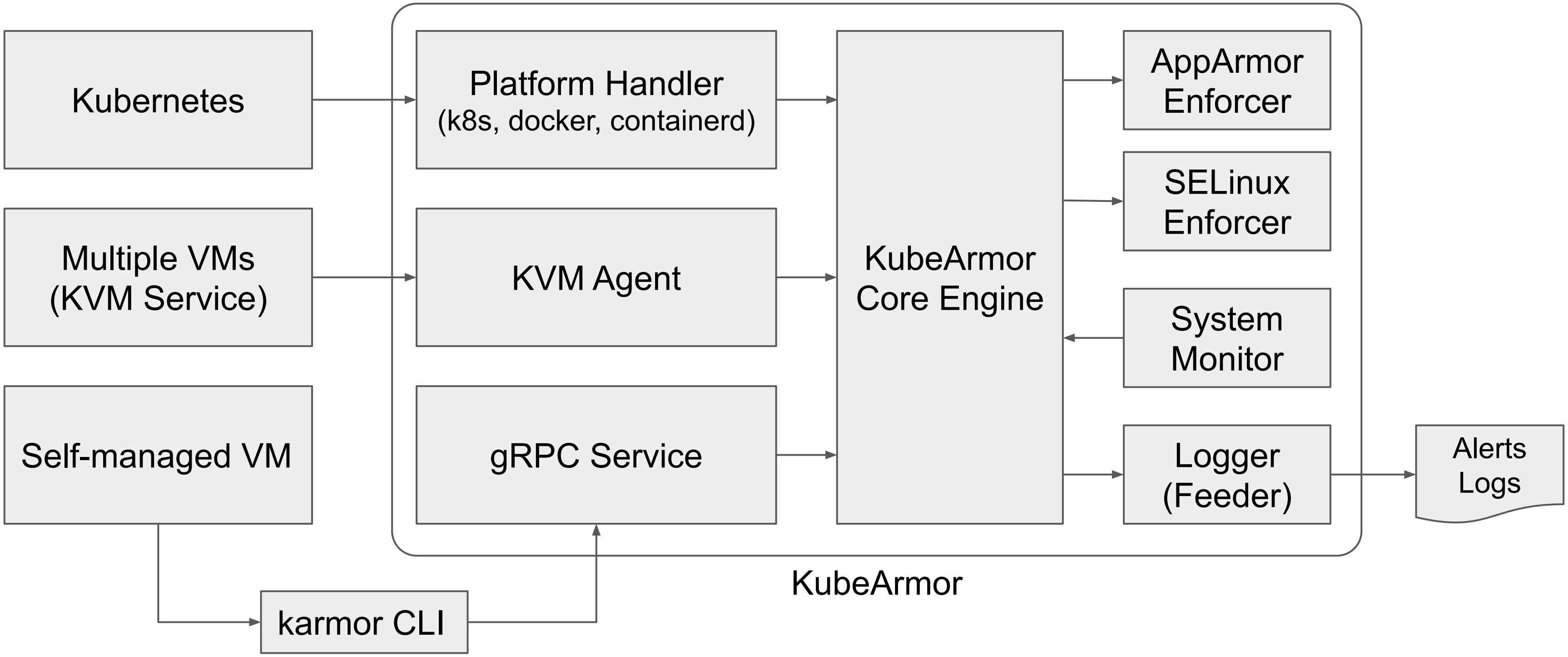
High-level definition ⇒ Runtime security enforcement system for containers and VMs



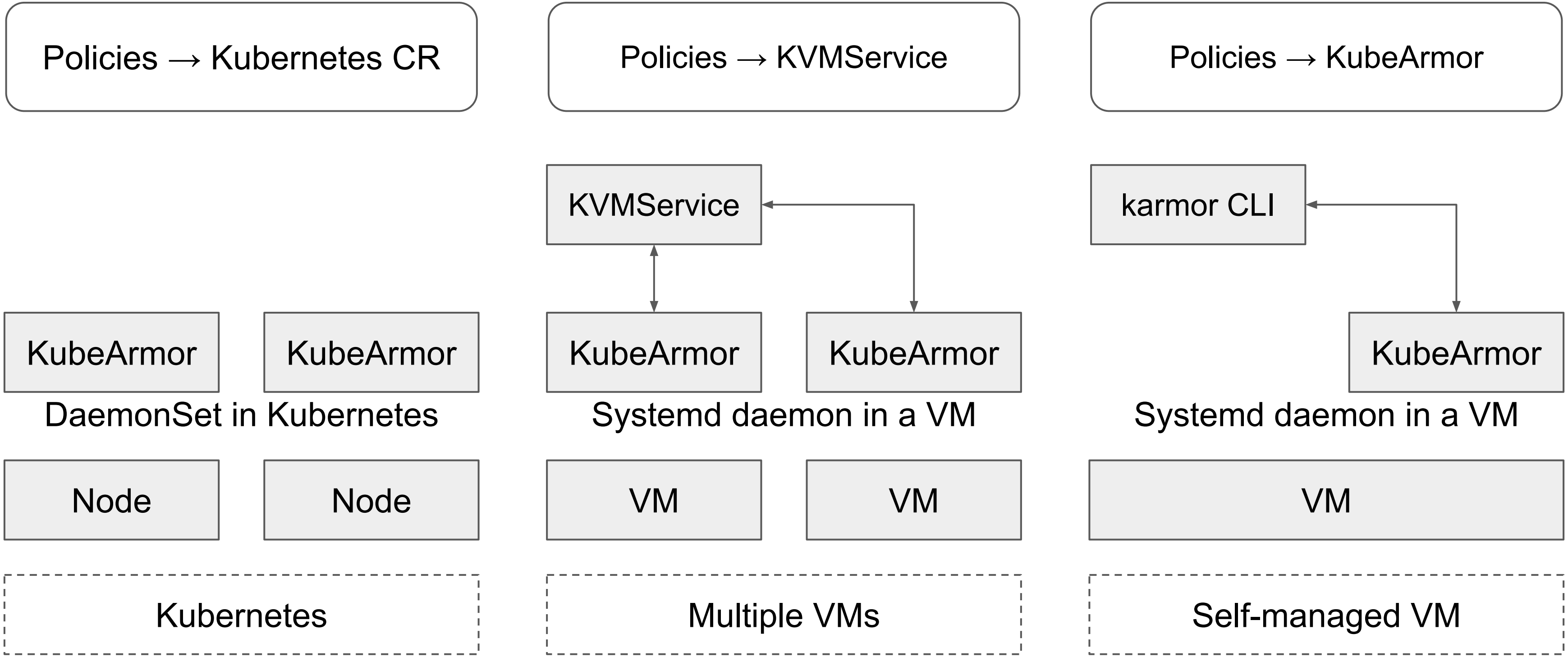
{ API }
YAML
SecurityPolicy
kubernetes
Cluster Node
Pod
Pod
Pod
Userspace
KubeArmor
AppArmor
SELinux
KRSI
KubeArmor Security Profiles
Linux Security Modules (LSMs)
eBPF
KubeArmor Container Monitor
Kernelspace
X
O
O
System Resources (e.g., system calls)
log
With container identities

High level point of view

# Architectural Overview of KubeArmor



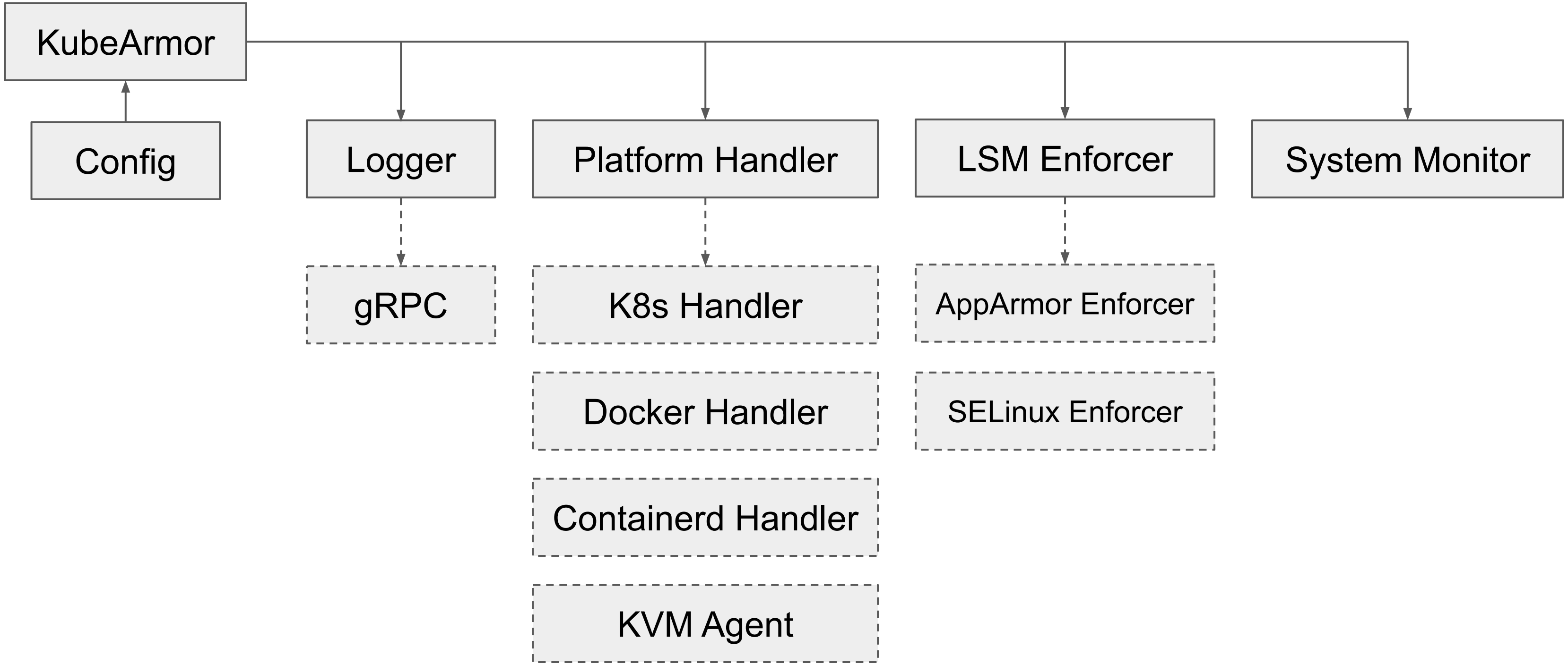
# Where KubeArmor is?



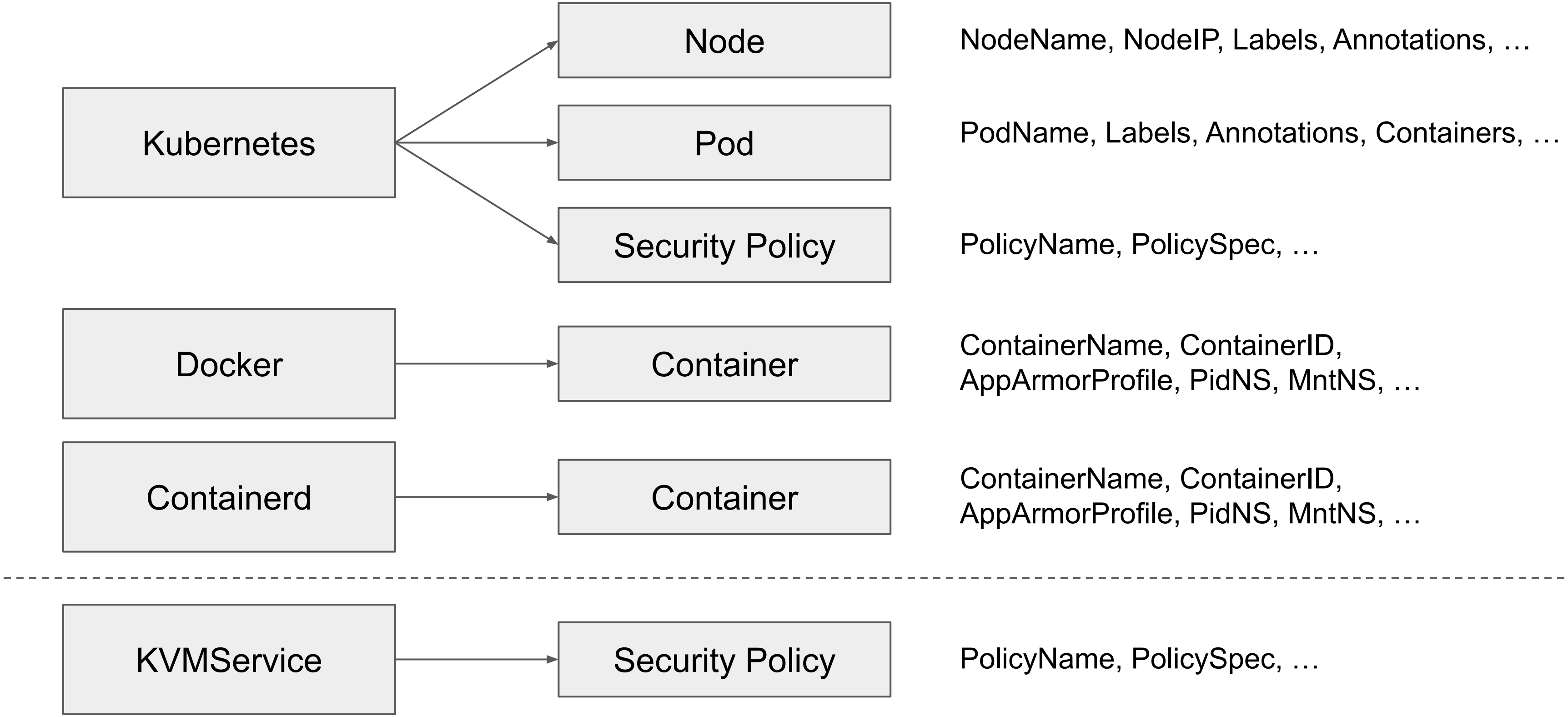
# KubeArmor Components

# KubeArmor Core Engine

## Component initialization



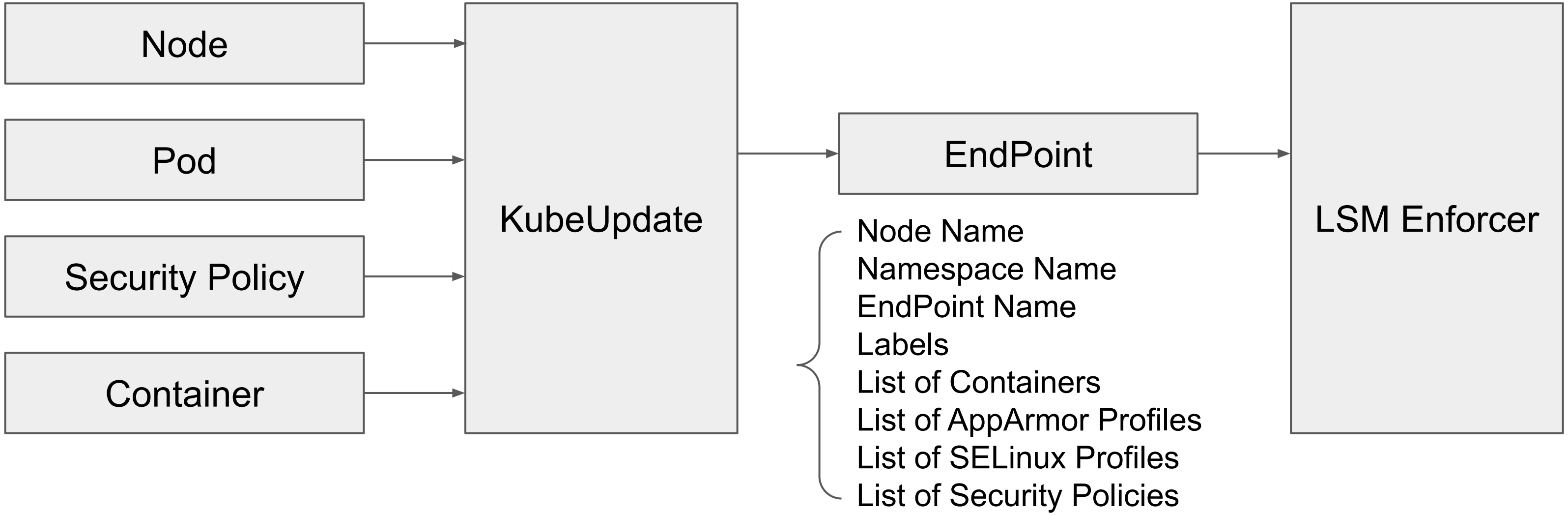
# Platform Handler



| | | |
|---|---|---|
| Kubernetes | Node | NodeName, NodeIP, Labels, Annotations, … |
| | Pod | PodName, Labels, Annotations, Containers, … |
| | Security Policy | PolicyName, PolicySpec, … |
| Docker | Container | ContainerName, ContainerID,<br>AppArmorProfile, PidNS, MntNS, … |
| Containerd | Container | ContainerName, ContainerID,<br>AppArmorProfile, PidNS, MntNS, … |
| KVMService | Security Policy | PolicyName, PolicySpec, … |

< Event-driven watcher >

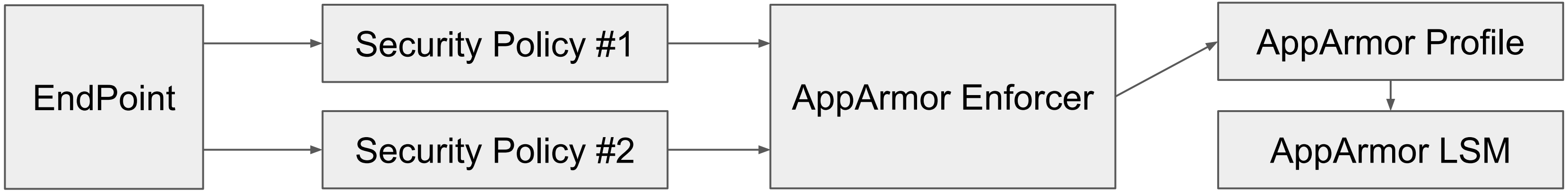
# KubeArmor Core Engine

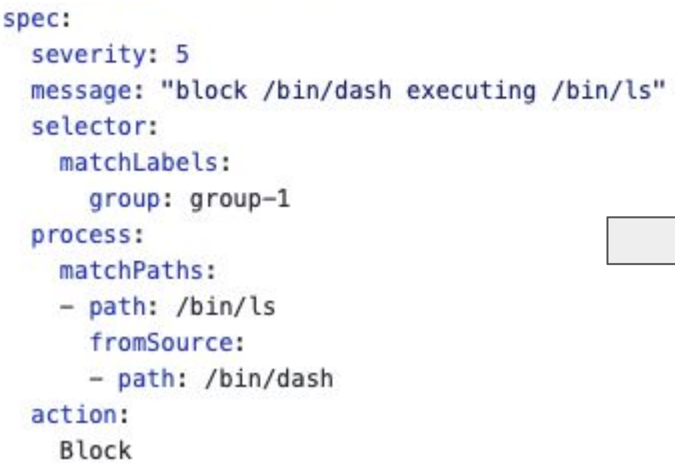


Node Name
Namespace Name
EndPoint Name
Labels
List of Containers
List of AppArmor Profiles
List of SELinux Profiles
List of Security Policies

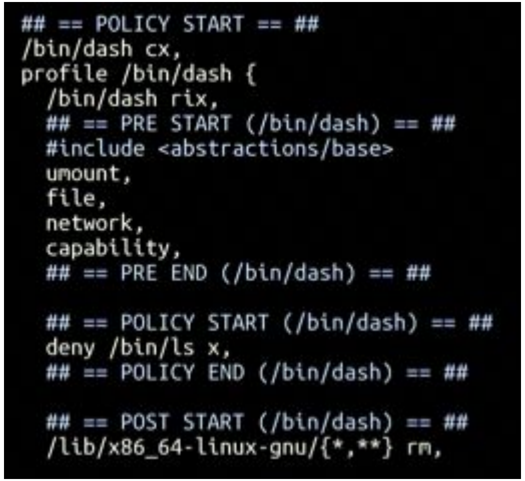
# LSM Enforcer: AppArmor

AppArmor → File-based security enforcement





```
spec:
  severity: 5
  message: "block /bin/dash executing /bin/ls"
  selector:
    matchLabels:
      group: group-1
  process:
    matchPaths:
    - path: /bin/ls
      fromSource:
      - path: /bin/dash
  action:
    Block
```



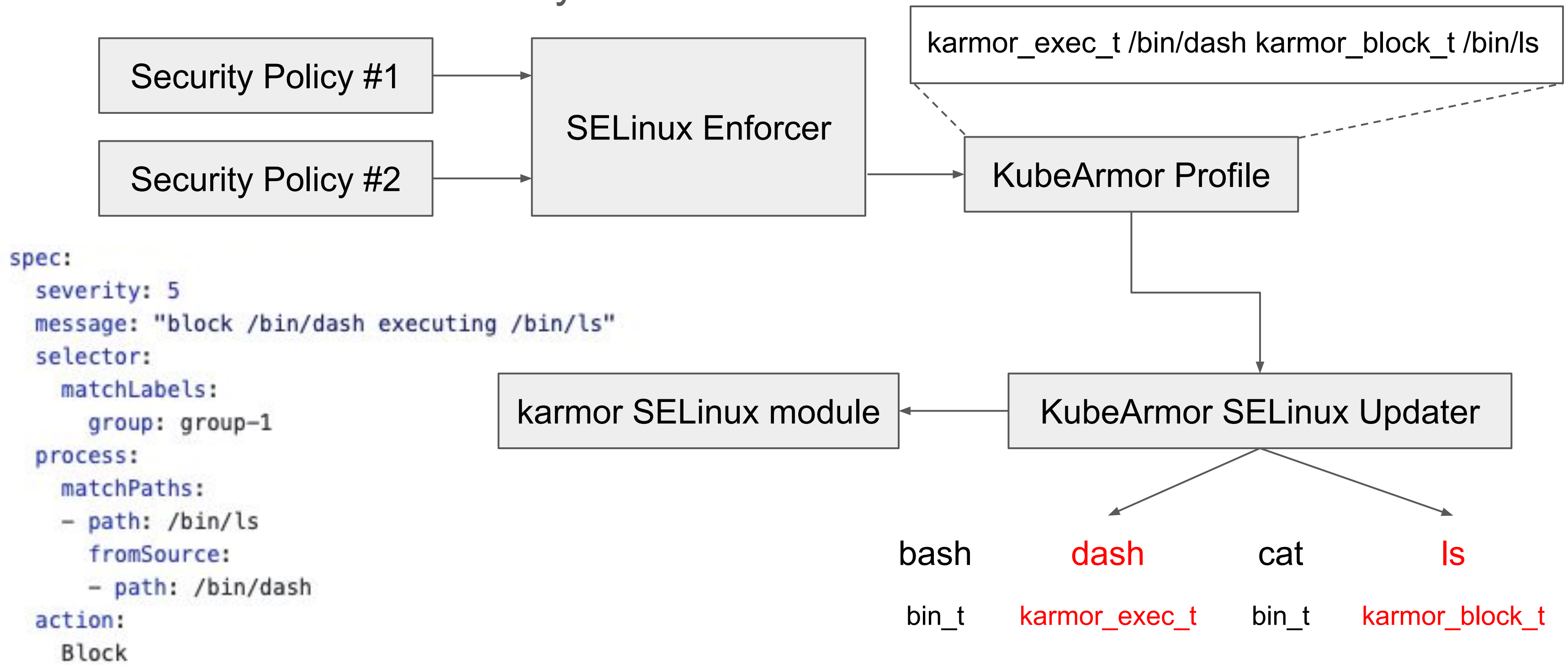
```
## == POLICY START == ##
/bin/dash cx,
profile /bin/dash {
  /bin/dash rix,
  ## == PRE START (/bin/dash) == ##
  #include <abstractions/base>
  umount,
  file,
  network,
  capability,
  ## == PRE END (/bin/dash) == ##

  ## == POLICY START (/bin/dash) == ##
  deny /bin/ls x,
  ## == POLICY END (/bin/dash) == ##

  ## == POST START (/bin/dash) == ##
  /lib/x86_64-linux-gnu/{*,**} rm,
```

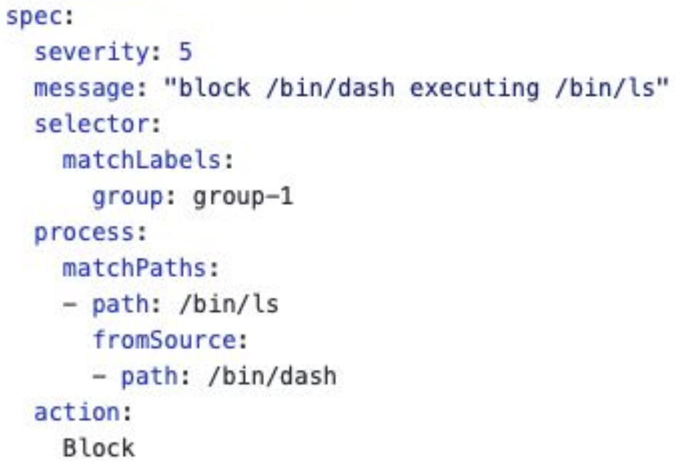
# LSM Enforcer: SELinux

SELinux → Label-based security enforcement



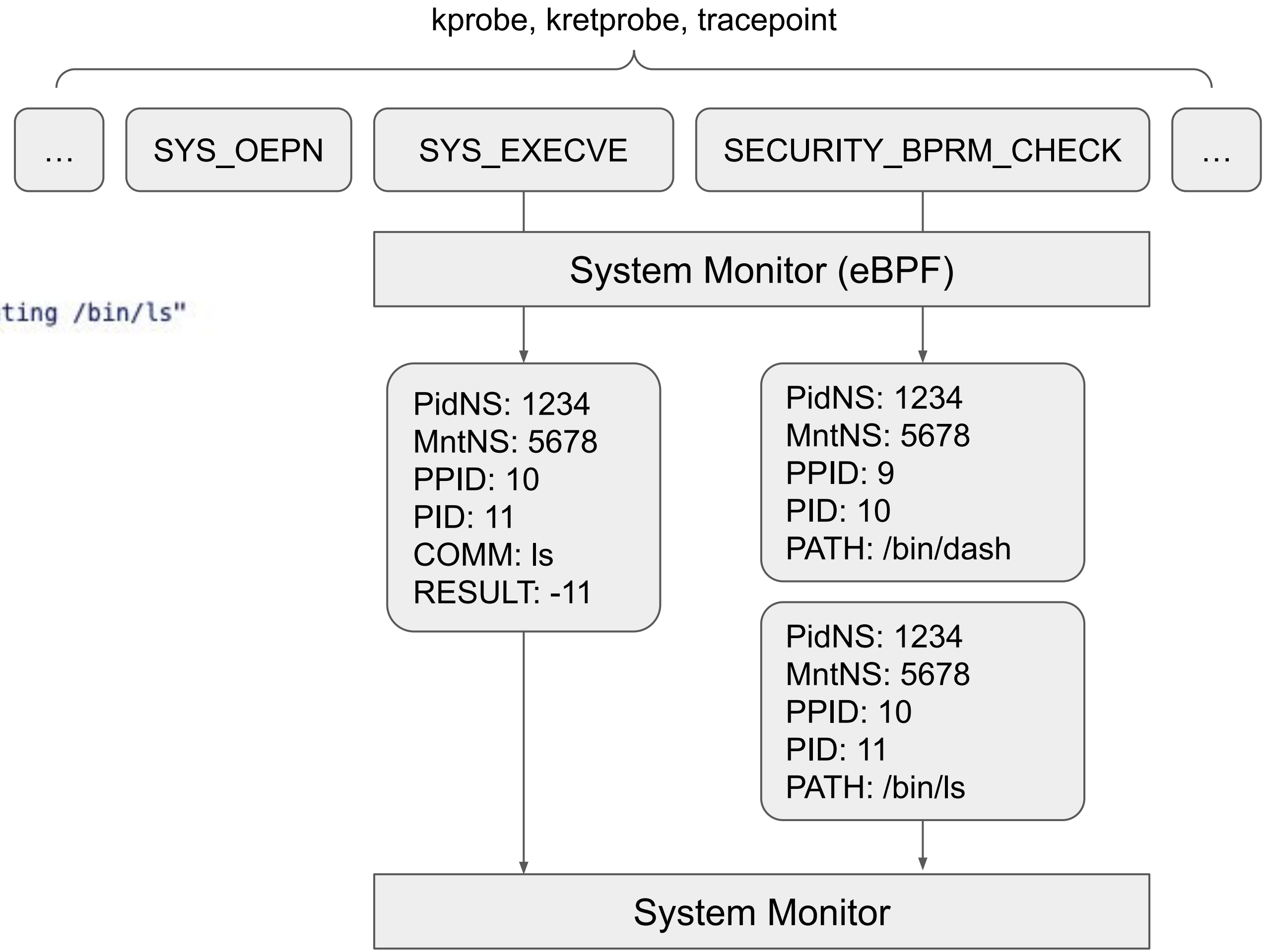
```
spec:
  severity: 5
  message: "block /bin/dash executing /bin/ls"
  selector:
    matchLabels:
      group: group-1
  process:
    matchPaths:
    - path: /bin/ls
      fromSource:
      - path: /bin/dash
  action:
    Block
```

# System Monitor



```
spec:
  severity: 5
  message: "block /bin/dash executing /bin/ls"
  selector:
    matchLabels:
      group: group-1
  process:
    matchPaths:
    - path: /bin/ls
      fromSource:
      - path: /bin/dash
  action:
    Block
```

```
(dash) $ ls
Permission Denied
```



kprobe, kretprobe, tracepoint

…

SYS_OEPN

SYS_EXECVE

SECURITY_BPRM_CHECK

…

System Monitor (eBPF)

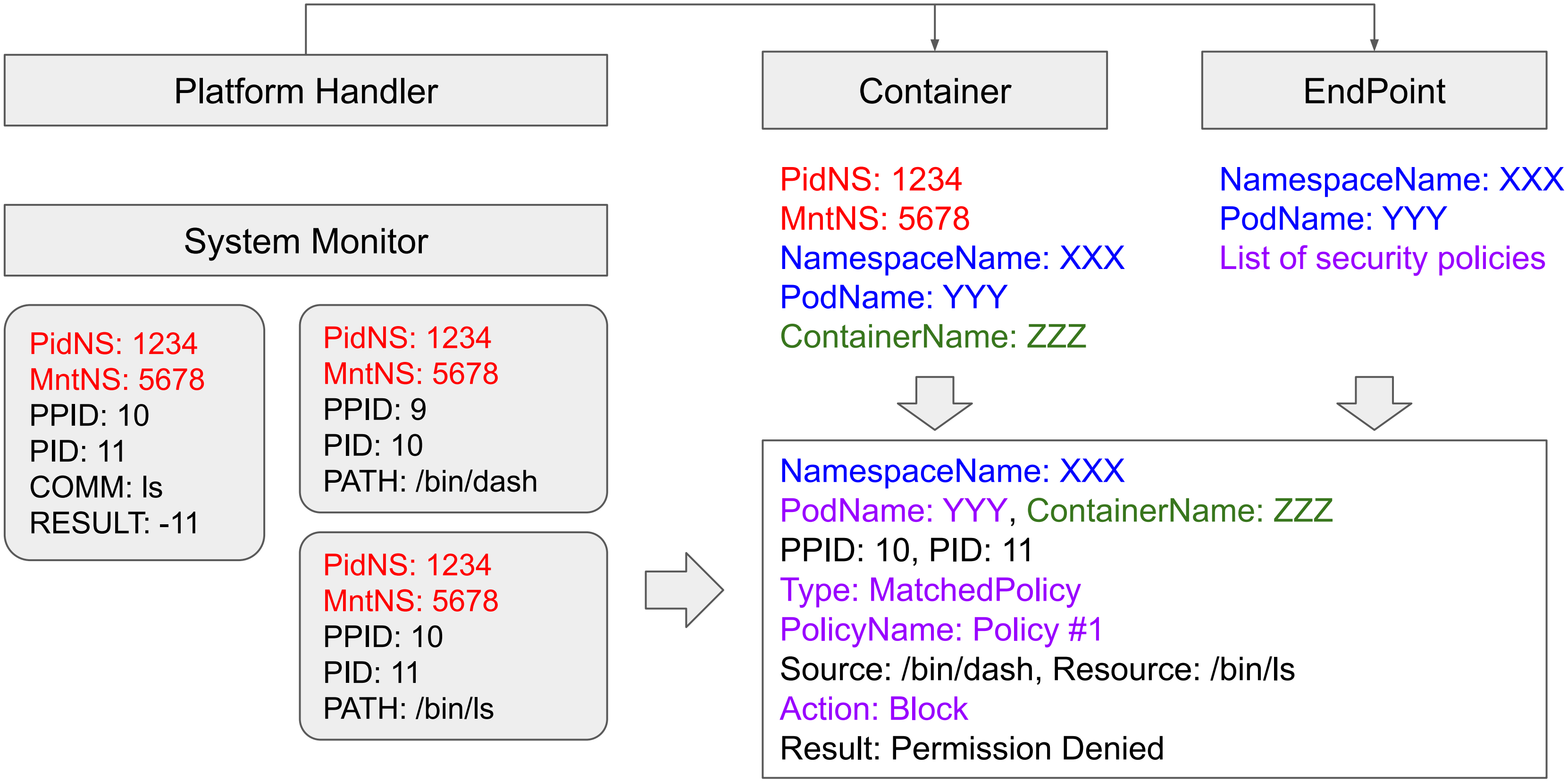
PidNS: 1234
MntNS: 5678
PPID: 10
PID: 11
COMM: ls
RESULT: -11

PidNS: 1234
MntNS: 5678
PPID: 9
PID: 10
PATH: /bin/dash

PidNS: 1234
MntNS: 5678
PPID: 10
PID: 11
PATH: /bin/ls

System Monitor

# Logger (Feeder)



Platform Handler

Container

EndPoint

System Monitor

PidNS: 1234
MntNS: 5678
PPID: 10
PID: 11
COMM: ls
RESULT: -11

PidNS: 1234
MntNS: 5678
PPID: 9
PID: 10
PATH: /bin/dash

PidNS: 1234
MntNS: 5678
PPID: 10
PID: 11
PATH: /bin/ls

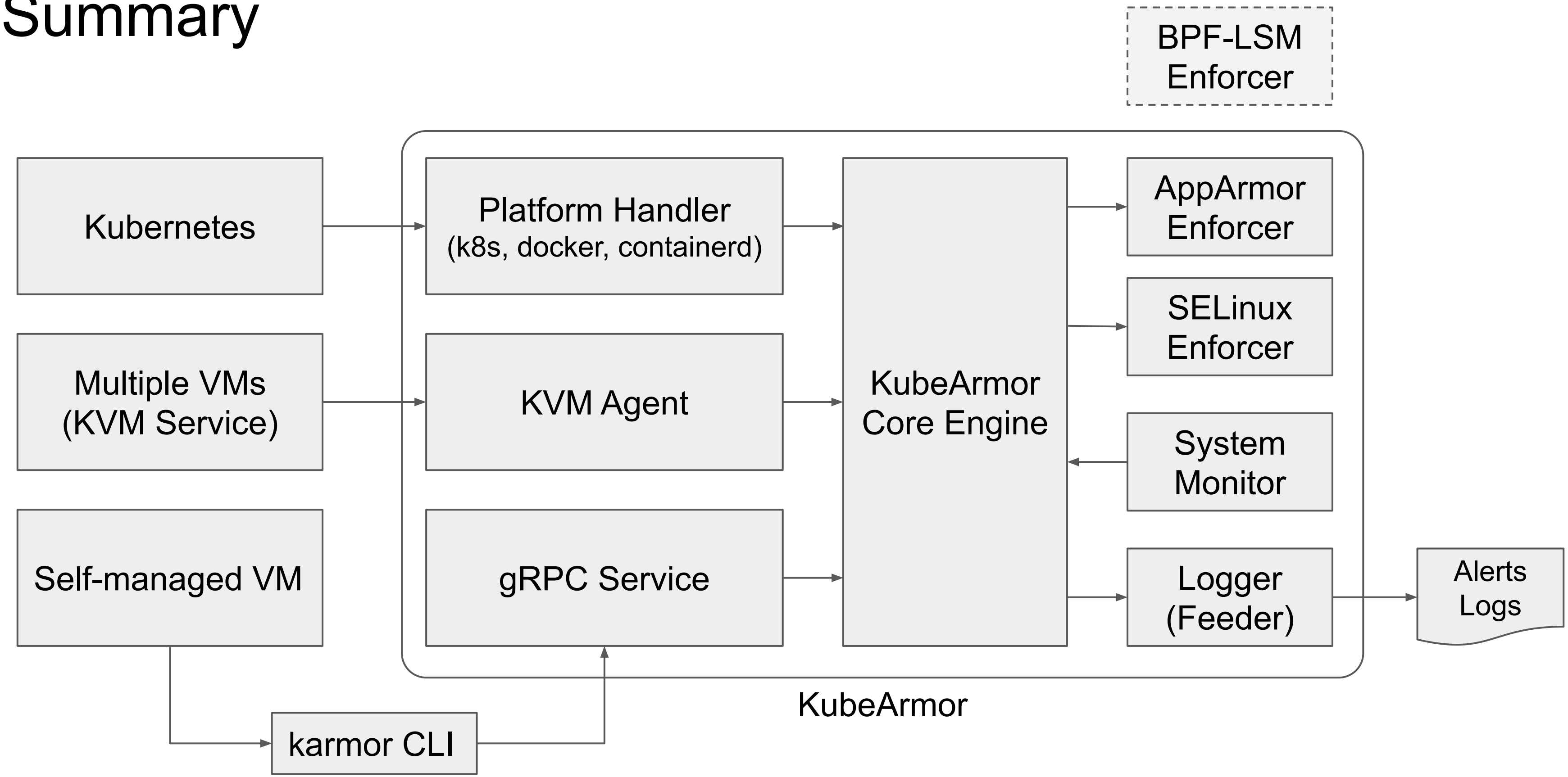
PidNS: 1234
MntNS: 5678
NamespaceName: XXX
PodName: YYY
ContainerName: ZZZ

NamespaceName: XXX
PodName: YYY
List of security policies

NamespaceName: XXX
PodName: YYY, ContainerName: ZZZ
PPID: 10, PID: 11
Type: MatchedPolicy
PolicyName: Policy #1
Source: /bin/dash, Resource: /bin/ls
Action: Block
Result: Permission Denied

# Summary

# Summary


BPF-LSM Enforcer
Kubernetes
Platform Handler (k8s, docker, containerd)
Multiple VMs (KVM Service)
KVM Agent
Self-managed VM
gRPC Service
KubeArmor Core Engine
AppArmor Enforcer
SELinux Enforcer
System Monitor
Logger (Feeder)
Alerts Logs
KubeArmor
karmor CLI