



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

# Third-Party Audit Update

## KubeCon Europe 2026





KubeCon



CloudNativeCon

Europe 2026

# whoami





KubeCon



CloudNativeCon

Europe 2026

# SIG-Security Third Party Audit



# Iain - Prior Audits & Context

- Both were performed against Kubernetes, meaning the core components
- 2019 - Security-Audit Working Group Atredis & Trail of Bits
- 2022 - NCC Group



<https://github.com/kubernetes/sig-security/tree/main/sig-security-external-audit>

# Iain - Prior Audits & Context

|        | 2019 Audit | 2022 Audit | Total |
|--------|------------|------------|-------|
| Open   | 13         | 9          | 22    |
| Closed | 24         | 10         | 34    |

# Rey - Defining Scope



2.5 million lines of code!



Asked SIGs



Alternate audit scope  
core and non-core



External Audit Roadmap  
k/sig-security



65 stable features graduated  
between v1.24 and v1.31



93 features / areas  
initially identified



<https://github.com/kubernetes/sig-security/blob/main/sig-security-external-audit/security-audit-2025/RFP.md>



# Rey - Defining Scope



## Graduated Stable Features

- Pod Security Admission (v1.25)
- Cgroups v2 (v1.25)
- Ephemeral Containers (v1.25)
- CEL for Admission Control / ValidatingAdmissionPolicy (v1.30)
- CRD Validation Expression (v1.29)
- Seccomp By Default (v1.27)
- Node Topology Manager (v1.27)
- Third Party Device Monitoring Plugins (v1.28)
- AppArmor Support (v1.31)
- Local Ephemeral Storage Capacity Isolation (v1.25)
- Cleaning Up iptables Chain Ownership (v1.28)



## External Audit Roadmap

- Cluster API
- Windows
  - CSI Proxy
- Konnectivity
- Shared public cloud library
- Shared cloud provider library
- Credential provider plugin
- Image Builder
- Kops

## Scope of Non-Core Audit

# Open Source Technology Improvement Fund, Inc – Third Party Audit Champion



Third Party Security Audits are Complex.

Worked with Kubernetes Community for 6+ months scoping and information gathering.

Interest from security firms and audit teams.

Prioritize needs and scope accordingly.

Communicate expectations in RfP process.

Diligently assess proposals.





KubeCon



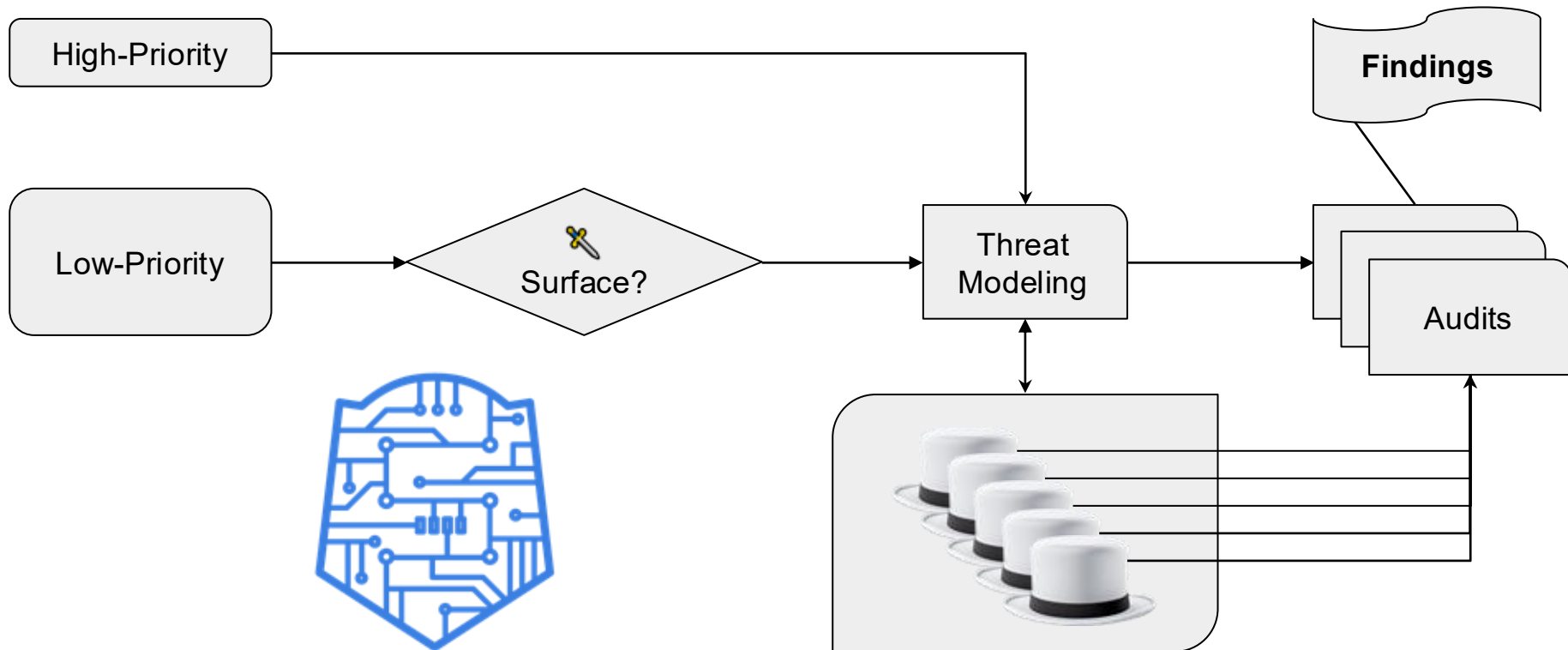
CloudNativeCon

Europe 2026

# Security Response Committee Perspective



# Audit - Methodology



# Audit - Summary

20 findings, plus hardening  
recommendations

**Fuzzing** contributions

**Trust issues** in supply  
chains

Threat Modeling in  
Kubernetes is **complex**

Hard to provide **secure  
defaults**

Assumption for an OS do  
not stand for another





KubeCon



CloudNativeCon

Europe 2026

# Proof Of Concept - Image Builder Hardcoded Credentials



# PoC - ImageBuilder Hardcoded Credentials

**You can deploy a Kubernetes cluster  
pretty much everywhere.**

...but should you?

# PoC - ImageBuilder Hardcoded Credentials

Image  Builder is a tool to produce Kubernetes VM Images

Ideally used in tandem with the **Cluster API**

Ensures **consistency** across different cloud providers

But should support any setup based on kubeadm

Essentially, a collection of **packer** and **ansible** scripts!

# PoC - ImageBuilder Hardcoded Credentials



KubeCon



CloudNativeCon

Europe 2026

```
# images/capi/packer/ova/packer-windows.json
{
  "builders": [
    {
      "content": "{\n \"unattend_timezone\" : \"{{user `unattend_timezone`}}\"\n,\n \"admin_password\" : \"{{user `windows_admin_password`}}\"\n}\n",
      "target": "../packer_cache/unattend.json",
      "type": "file"
    },
    {
      // ... SNIP ...
      "winrm_password": "{{user `windows_admin_password`}}",
      "winrm_timeout": "4h",
      "winrm_username": "Administrator"
    },
    {
      // ... SNIP ...
      "winrm_insecure": true,
      "winrm_password": "{{user `windows_admin_password`}}",
      "winrm_timeout": "4h",
      "winrm_username": "Administrator"
    }
  ],
  "post-processors": [
    // ... SNIP ...
  ],
  "provisioners": [
    // ... SNIP ...
  ],
  "variables": {
    // ... SNIP ...
    "prepull": null,
    "unattend_timezone": "Pacific Standard Time",
    "windows_admin_password": "S3cr3t0!",
    "windows_service_manager": null,
    "windows_updates_categories": null,
    "windows_updates_kbs": null
  }
}
```

# PoC - ImageBuilder Hardcoded Credentials



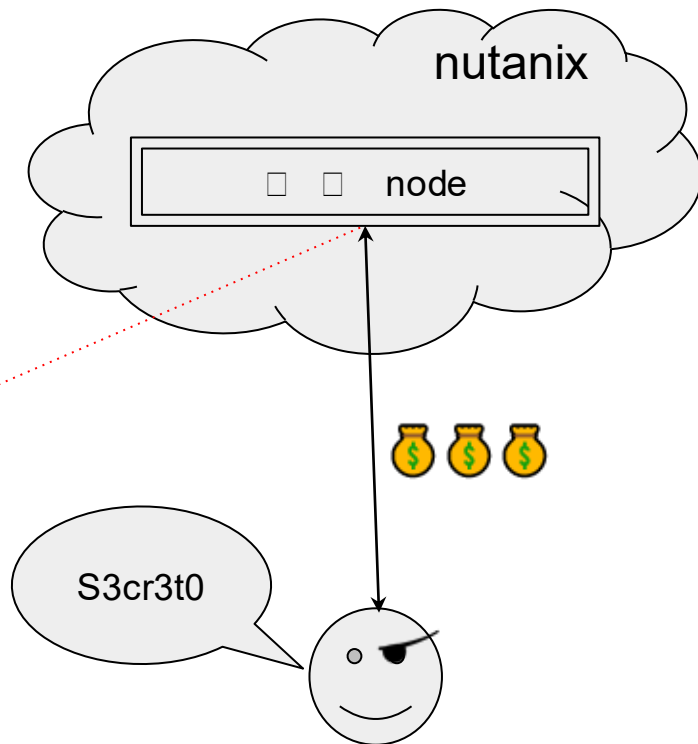
KubeCon



CloudNativeCon

Europe 2026

```
# images/capi/packer/ova/packer-windows.json
{
  "builders": [
    {
      "content": "{\\n \\\"unattend_timezone\\\" : \\\"{{user `unattend_timezone`}\\\"}\\n, \\\"admin_password\\\" : \\\"{{user `windows_admin_password`}\\\"}\\n}\\n\"",
      "windows_admin_password": "{{user `windows_admin_password'}}",
      "target": "../packer_cache/unattend.json",
      "type": "file"
    },
    {
      // ... SNIP ...
      "winrm_password": "{{user `windows_admin_password'}}",
      "winrm_timeout": "4h",
      "winrm_username": "Administrator"
    },
    {
      // ... SNIP ...
      "winrm_insecure": true,
      "winrm_password": "{{user `windows_admin_password'}}",
      "winrm_timeout": "4h",
      "winrm_username": "Administrator"
    }
  ],
  "post-processors": [
    // ... SNIP ...
  ],
  "provisioners": [
    // ... SNIP ...
  ],
  "variables": {
    // ... SNIP ...
    "prepull": null,
    "unattend_timezone": "Pacific Standard Time",
    "windows_admin_password": "S3cr3t0!",
    "windows_service_manager": null,
    "windows_updates_categories": null,
    "windows_updates_kbs": null
  }
}
```



# PoC - ImageBuilder Hardcoded Credentials

CVE-2025-7342: VM images built with Kubernetes Image Builder Nutanix or OVA providers use default credentials for Windows images if user did not override #133115

🔒 Closed

**FIXED**



KubeCon



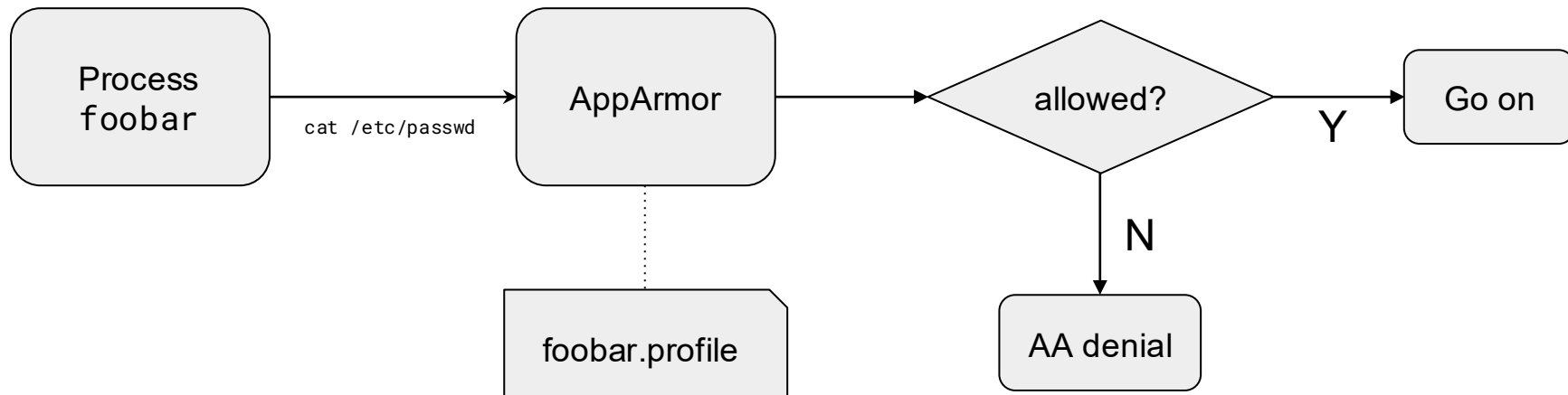
CloudNativeCon

Europe 2026

# Proof Of Concept - Bypass of PSS AppArmor Policy



# PoC - Bypass of PSS AppArmor Policy



# PoC - Bypass of PSS AppArmor Policy



KubeCon



CloudNativeCon

Europe 2026

```
#include <tunables/global>

profile k8s-apparmor-example-deny-
write flags=(attach_disconnected) {
    #include <abstractions/base>

    file,

    # Deny all file writes.
    deny /** w,
}
```

```
apiVersion: v1
kind: Pod
metadata:
  name: hello-apparmor
spec:
  securityContext:
    appArmorProfile:
      type: Localhost
      localhostProfile: k8s-apparmor-example-deny-write
  containers:
    - name: hello
      image: busybox:1.28
      command: [ "sh", "-c", "echo 'Hello AppArmor!' && sleep 1h" ]
```

# PoC - Bypass of PSS AppArmor Policy



KubeCon



CloudNativeCon

Europe 2026

## Pod Security Standards

- Defines three security *policies*
  - **privileged**: unrestricted policy
  - **baseline**: prevents known privilege escalations
  - **restricted**: heavily hardened Pods
- It “touches” AppArmor configuration, too!

# PoC - Bypass of PSS AppArmor Policy



KubeCon



CloudNativeCon

Europe 2026

## AppArmor

On supported hosts, the `RuntimeDefault` AppArmor profile is applied by default. The baseline policy should prevent overriding or disabling the default AppArmor profile, or restrict overrides to an allowed set of profiles.

### Restricted Fields

- `spec.securityContext.appArmorProfile.type`
- `spec.containers[*].securityContext.appArmorProfile.type`
- `spec.initContainers[*].securityContext.appArmorProfile.type`
- `spec.ephemeralContainers[*].securityContext.appArmorProfile.type`

### Allowed Values

- `Undefined/nil`
- `RuntimeDefault`
- `Localhost`

# PoC - Bypass of PSS AppArmor Policy



KubeCon



CloudNativeCon

Europe 2026

master apparmor / profiles / apparmor.d

Find file Code

profiles/apparmor.d/abstractions/transmission-common: LP: #2137395  
Alex Murray authored 3 days ago

Unverified aed0a3b3

Code owners Assign users and groups as approvers for specific file changes. Learn more.

| Name               | Last commit                                                 | Last commit  |
|--------------------|-------------------------------------------------------------|--------------|
| -                  |                                                             |              |
| abi                | Merge policy: Add a wip 5.0 abi file and update policy t... | 5 mont       |
| abstractions       | profiles/apparmor.d/abstractions/transmission-commo...      | 3 da         |
| apache2.d          | policy: Add a wip 5.0 abi file and update policy to use it  | 5 mont       |
| local              | local/README: instructions for overriding deny rules        | 4 mont       |
| tunables           | profiles: make /sys/devices PCI paths hex-aware             | 7 mont       |
| 1password          | policy: Add a wip 5.0 abi file and update policy to use it  | 5 mont       |
| Discord            | policy: Add a wip 5.0 abi file and update policy to use it  | 5 mont       |
| MongoDB_Compass    | policy: Add a wip 5.0 abi file and update policy to use it  | 5 months ago |
| QtWebEngineProcess | policy: Add a wip 5.0 abi file and update policy to use it  | 5 months ago |

policy: Add a wip 5.0 abi file and update policy to use it  
John Johansen authored 5 months ago

aecf7801 History

Code owners Assign users and groups as approvers for specific file changes. Learn more.

runc 359 B

```
1 # This profile allows everything and only exists to give the
2 # application a name instead of having the label "unconfined"
3
4 abi <abi/5.0>,
5 include <tunables/global>
6
7 profile runc /usr/{bin,sbin}/runc flags=(unconfined) {
8     userns,
9     @{exec_path} mr,
10
11     # Site-specific additions and overrides. See local/README for details.
12     include if exists <local/runc>
13 }
14
```

# PoC - Bypass of PSS AppArmor Policy



KubeCon



CloudNativeCon

Europe 2026

```
apiVersion: v1
kind: Pod
metadata:
  name: evades-apparmor
spec:
  securityContext:
    appArmorProfile:
      type: Localhost
      localhostProfile: runc # THIS WILL RUN UNCONFINED!
  containers:
    - name: hello
      image: busybox:1.28
      command: [ "sh", "-c", "<privileged command>" ]
```



KubeCon



CloudNativeCon

Europe 2026

# Proof Of Concept - Cluster API Provider Supply Chain



# PoC - Cluster API Provider Supply Chain

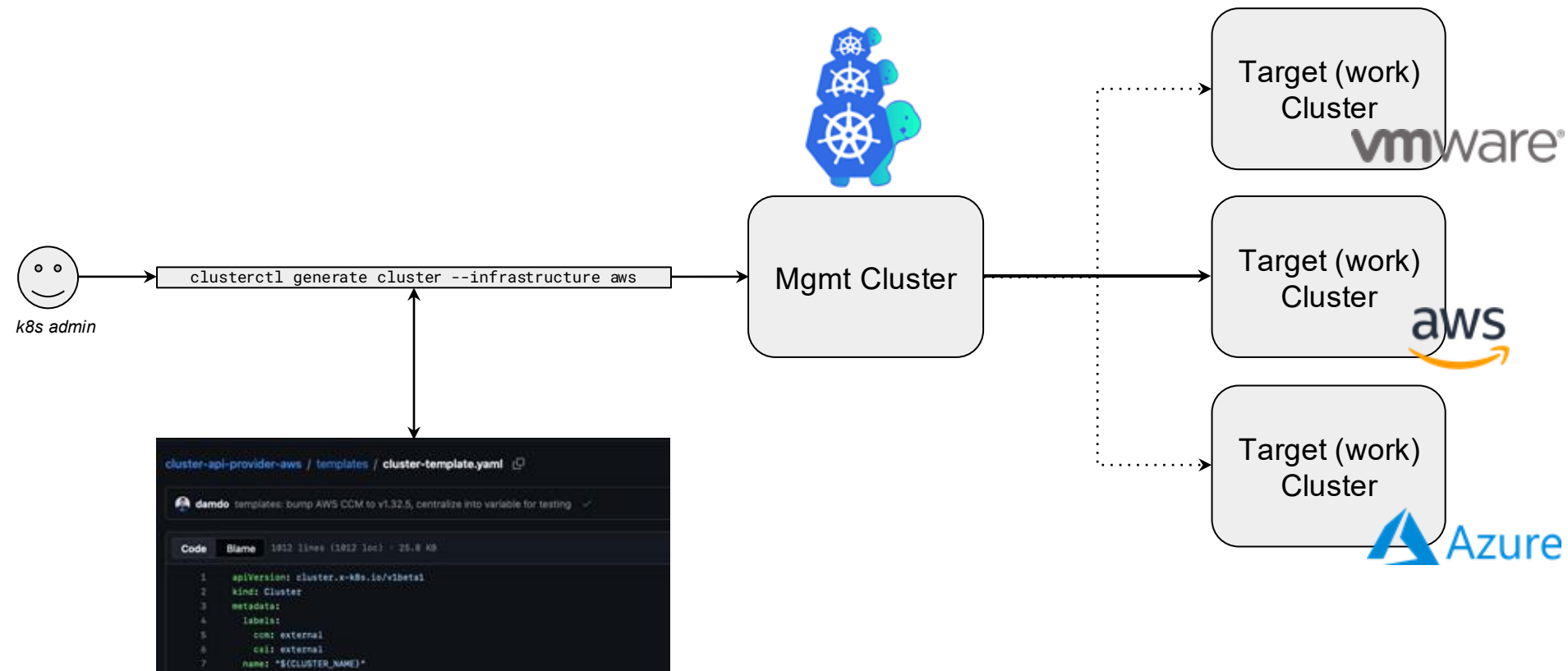


KubeCon



CloudNativeCon

Europe 2026



# PoC - Cluster API Provider Supply Chain

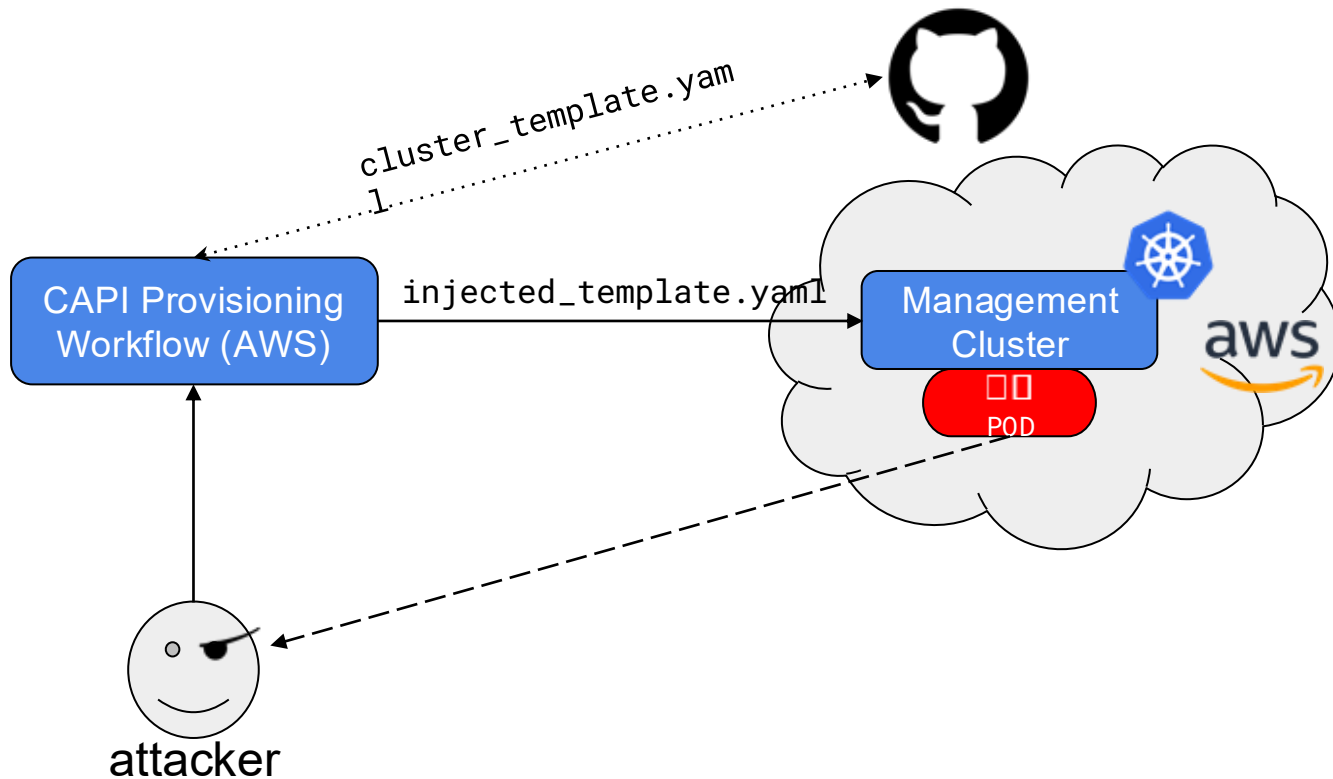


KubeCon



CloudNativeCon

Europe 2026



# Audit - Summary

20 findings, plus hardening  
recommendations

**Fuzzing** contributions

**Trust issues** in supply  
chains

Threat Modeling in  
Kubernetes is **complex**

Hard to provide **secure  
defaults**

Assumption for an OS do  
not stand for another



KubeCon



CloudNativeCon

Europe 2026

# Questions?





KubeCon



CloudNativeCon

Europe 2026

