Kubernetes Privilege Escalation: Container Escape == Cluster Admin?

Yuval Avrahami & Shaul Ben Hai, Palo Alto Networks

whoami

- Cloud security researchers @PANW
- Vulnerability research in the cloud
  - Azurescape
- Threat hunting in the cloud
  - Slioscape

Kubernetes Privilege Escalation: Container Escape == Cluster Admin?

Agenda

- Container Escapes
- Kubernetes 101
- Malicious Node
- Attack Classes
- Escape == Admin?
- Recommendations & Takeaways

Container Escapes

A Compendium of Container Escapes

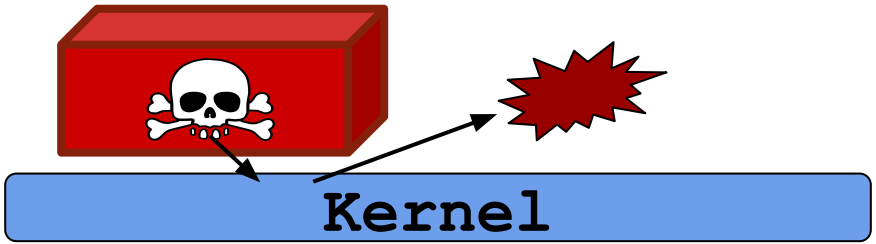
Brandon Edwards & Nick Freeman

BLACK HAT USA 2019

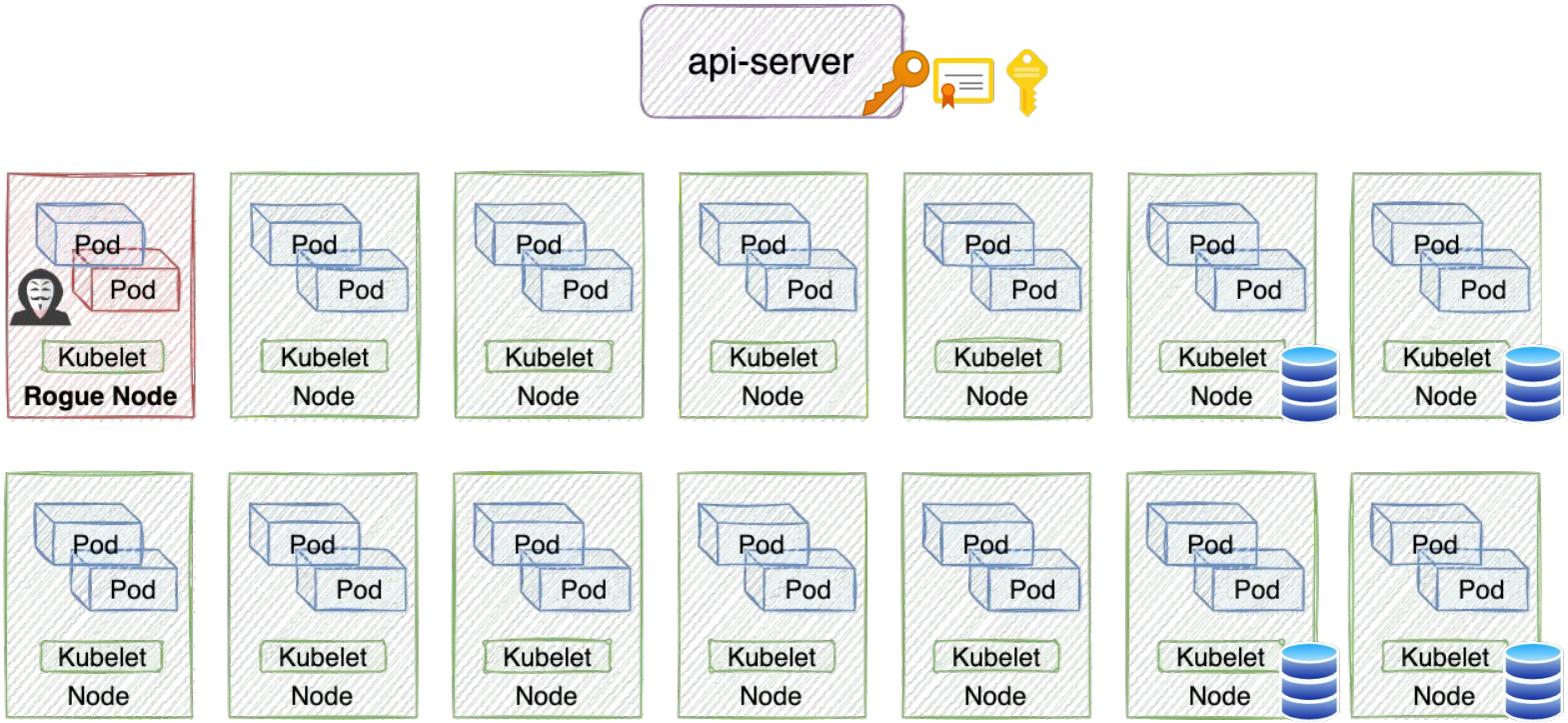
CAPSULE8

Do containers contain?

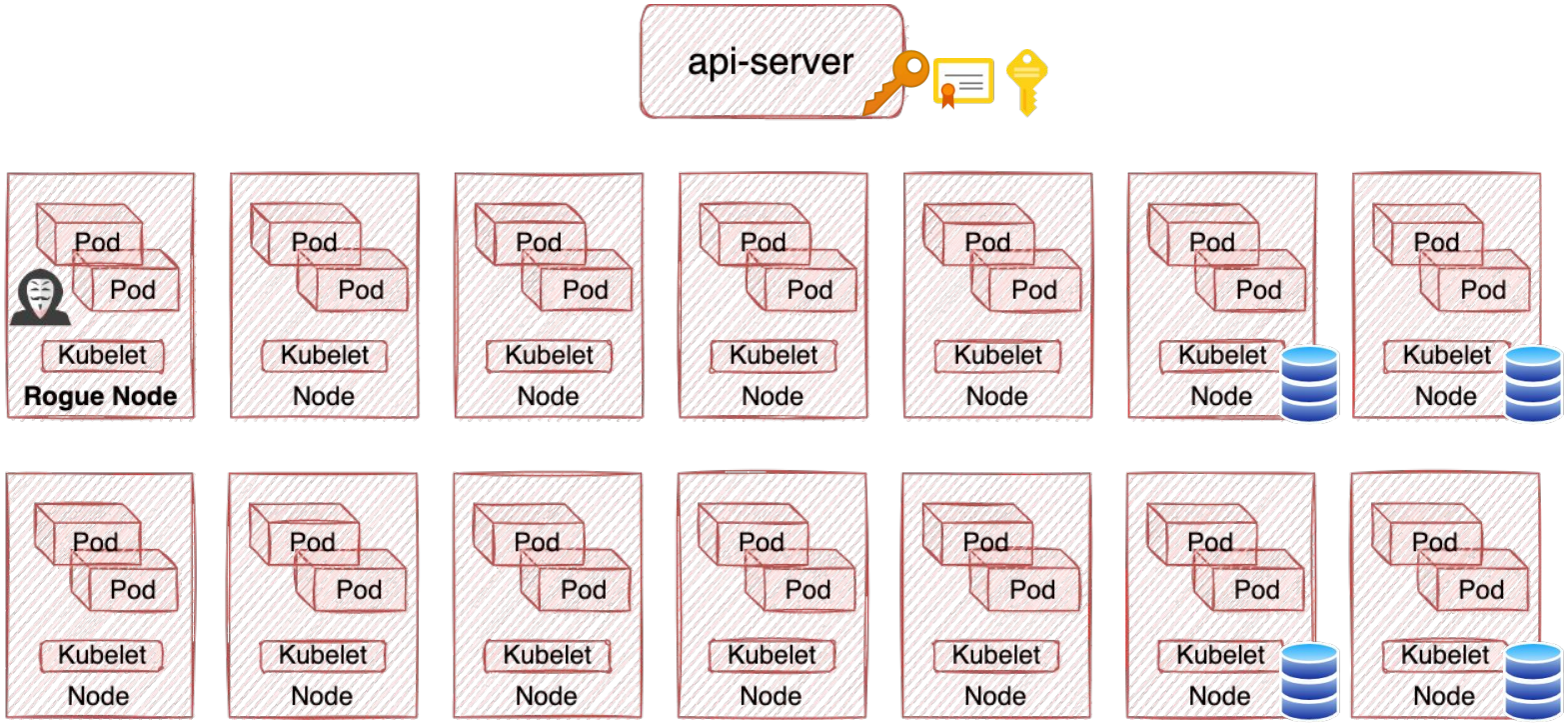
- Containers are great for packaging & deploying software
- Weak security boundary
- Escapes will inevitably occur
  - **Vulns in 2022 alone**: DirtyPipe, containerd CVE-2022-23648, multiple kernel vulns @Google's kctf, cri-o CVE-2022-0811
  - **Misconfigurations**: privileged containers, host mounts, etc
  - **In-the-wild malware**: Siloscape, TeamTNT
- **What's the impact?**



Obvious Impact: Compromised Node



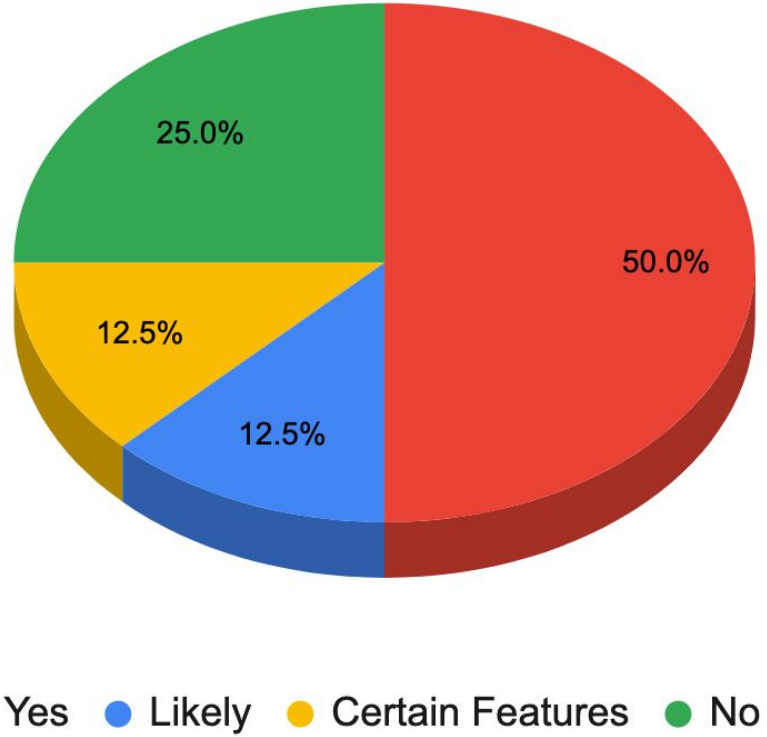
Container Escape == Cluster Admin?




SPOILER
ALERT!

Container Escape == Cluster Admin? (Feb)

- We looked into the most popular platforms
- In half, **by default escape == admin**



Terminology

- Admin

```
ya@demo:~$ kctl auth can-i "*" "*" --all-namespaces
yes
```

- Admin-equivalent

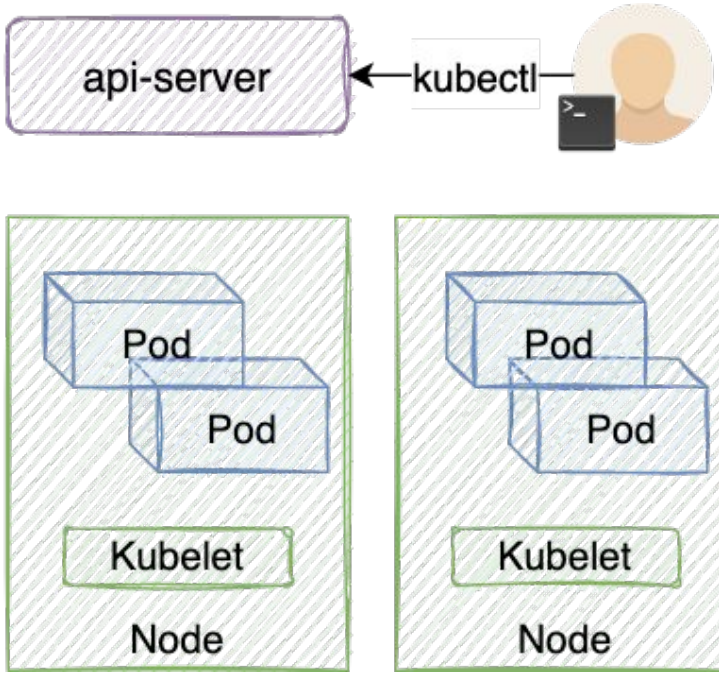
Few trivial steps

```
ya@demo:~$ kctl auth can-i list secrets -n kube-system
yes
```

Kubernetes 101

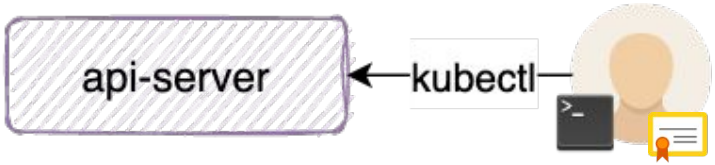
Kubernetes 101

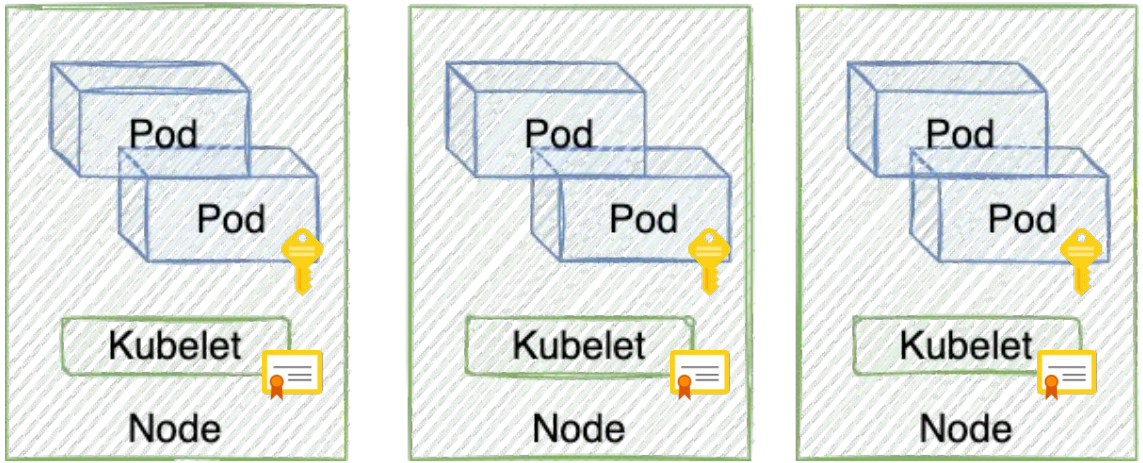
- Orchestrates pods (containers) on nodes (VMs)
- **It's everywhere**



Kubernetes 101 - Authentication

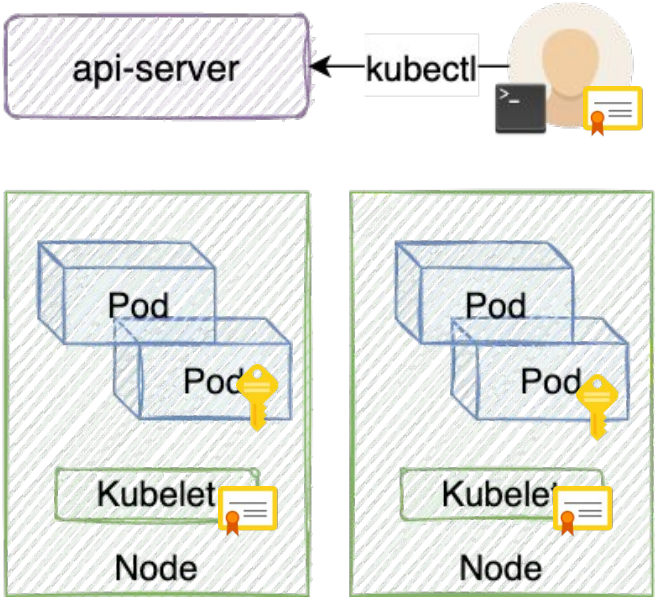
- Certificates: users & nodes
- ServiceAccount tokens: pods



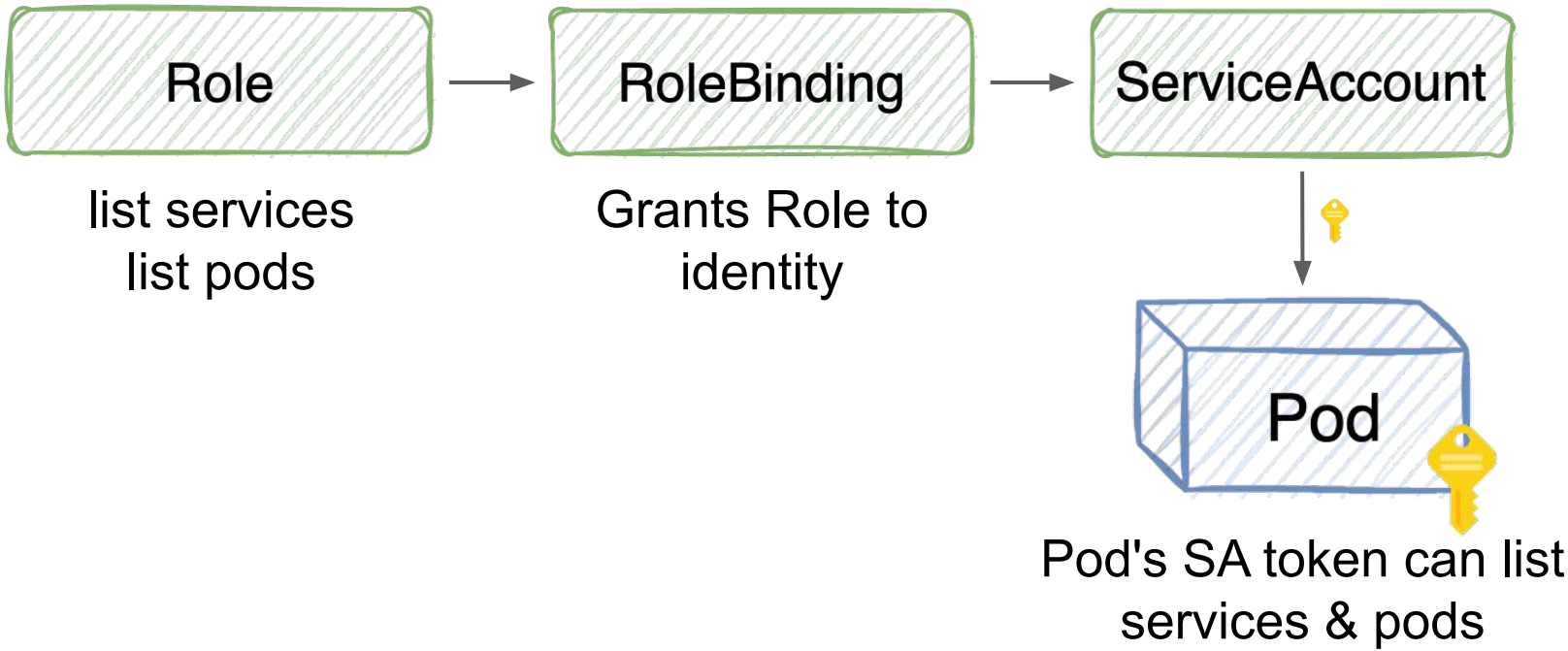


Kubernetes 101 - Authorization (RBAC)

- **Perms** expressed <verb> <resource>
  - list secrets, create pods
- Perms grouped into **Roles**
- **Bindings** grant Roles
  - ns-scoped
  - cluster-wide



Permission grant to Pod



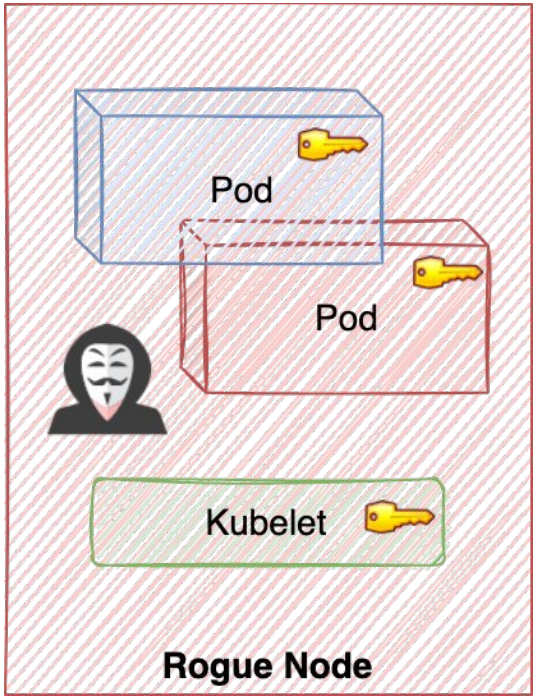
</101>

Post Container Escape

Credentials on a Rogue Node

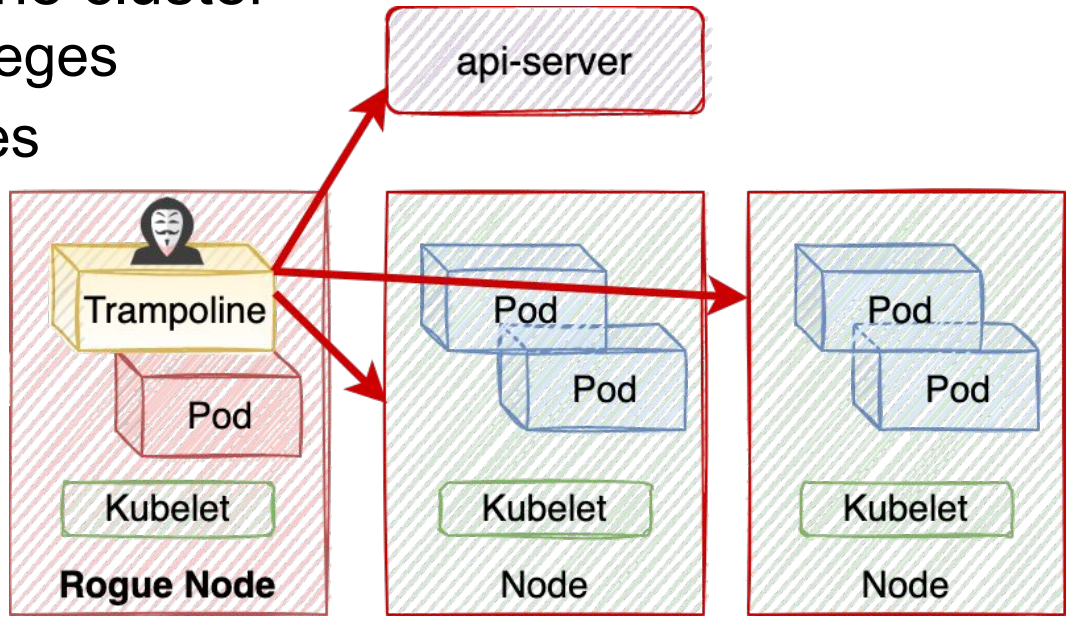
- Kubelet credentials
  - Restricted: NodeAuthorizer & NodeRestriction
  - Node perms != admin
- Neighboring pods' service accounts
  - Permissions vary

Node's interesting permissions are largely its pods' permissions!



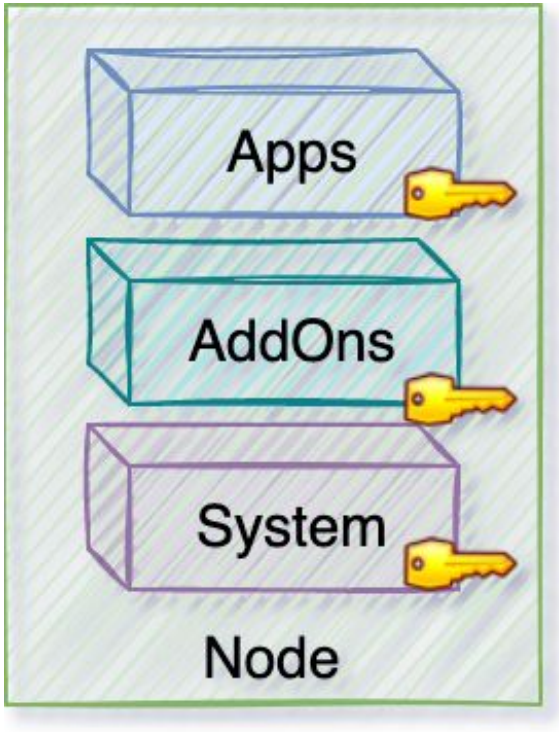
Trampoline Pods

- Powerful pods with enough permissions to bounce you around the cluster
  - Reach higher privileges
  - Jump to other nodes
  - Feel young again



Know Your Nodes

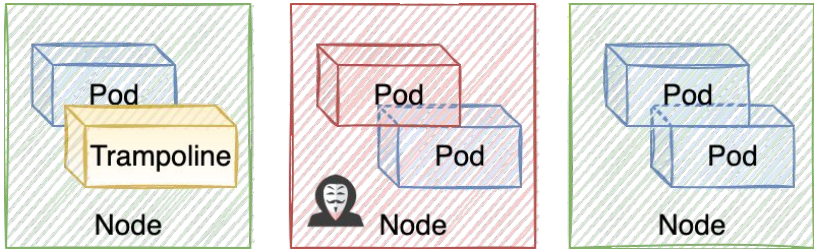
- What pods run on your nodes?
  - Applications
  - Add-on (Prometheus, Istio)
  - System (kube-proxy, coredns)
- Permissions blind spot: system & add-on pods
  - Often as DaemonSets on all nodes



DaemonSets VS Pods

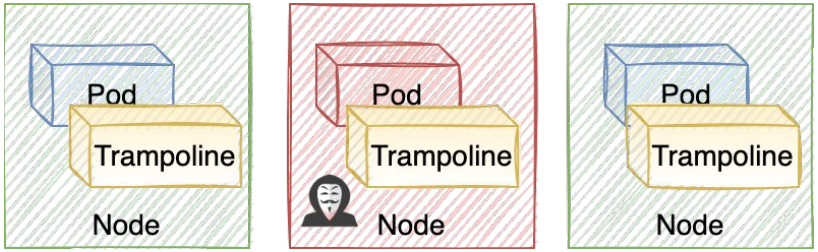
Trampolines Pods

- Attacker might hit jackpot



Trampoline DaemonSets

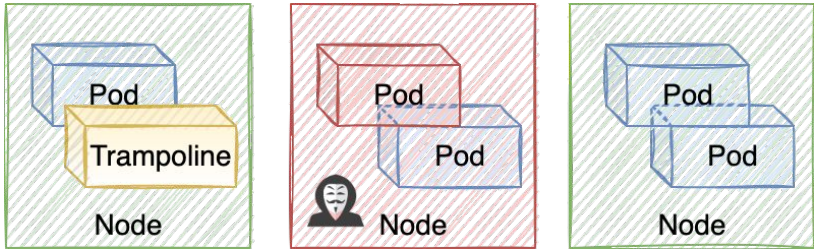
- Attacker **guaranteed** to hit jackpot



DaemonSets VS Pods

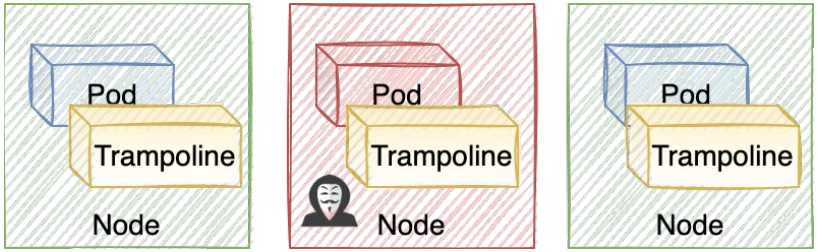
Trampolines Pods

- Attacker might hit jackpot



Trampoline DaemonSets

- Attacker **guaranteed** to hit jackpot



Real impact on escape == admin

Spotting Trampolines: What Makes a Pod Bouncy?

Example Infra Pod

- list services
- delete pods
- create configmaps
- update nodes/status

Is this pod powerful?

Powerful Permissions?

- No public list
  - "Is this add-on asking for risky permissions?"
  - "Can I abuse this pod's perms for privEsc?"
- Seemingly restricted perms surprisingly powerful
- **Define interesting attacks & classify perms**

Kubernetes Attack Classes

Manipulate AuthN / AuthZ

- Impersonate other identities / alter permissions

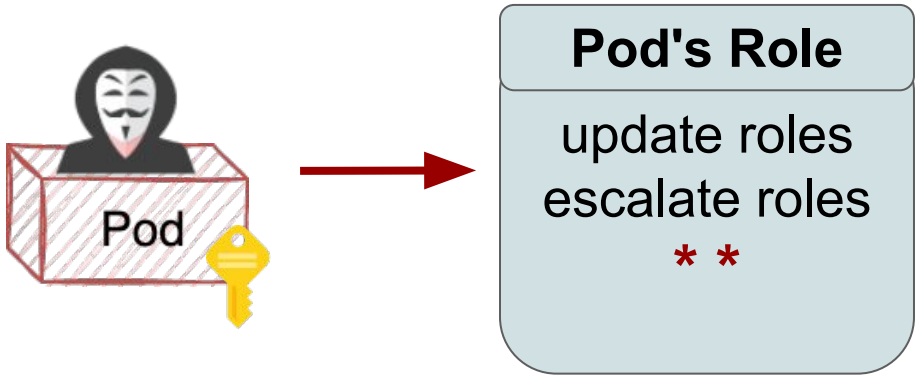
Manipulate AuthN / AuthZ

- Impersonate other identities / alter permissions
- **escalate roles**

Pod's Role
update roles escalate roles

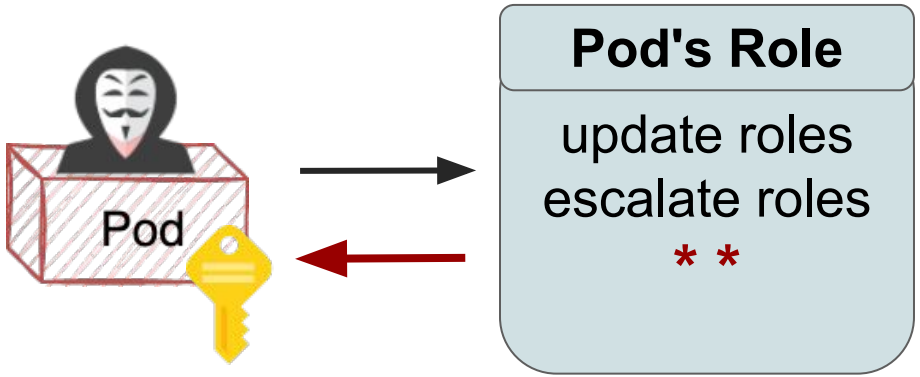
Manipulate AuthN / AuthZ

- Impersonate other identities / alter permissions
- **escalate roles**



Manipulate AuthN / AuthZ

- Impersonate other identities / alter permissions
- **escalate roles**

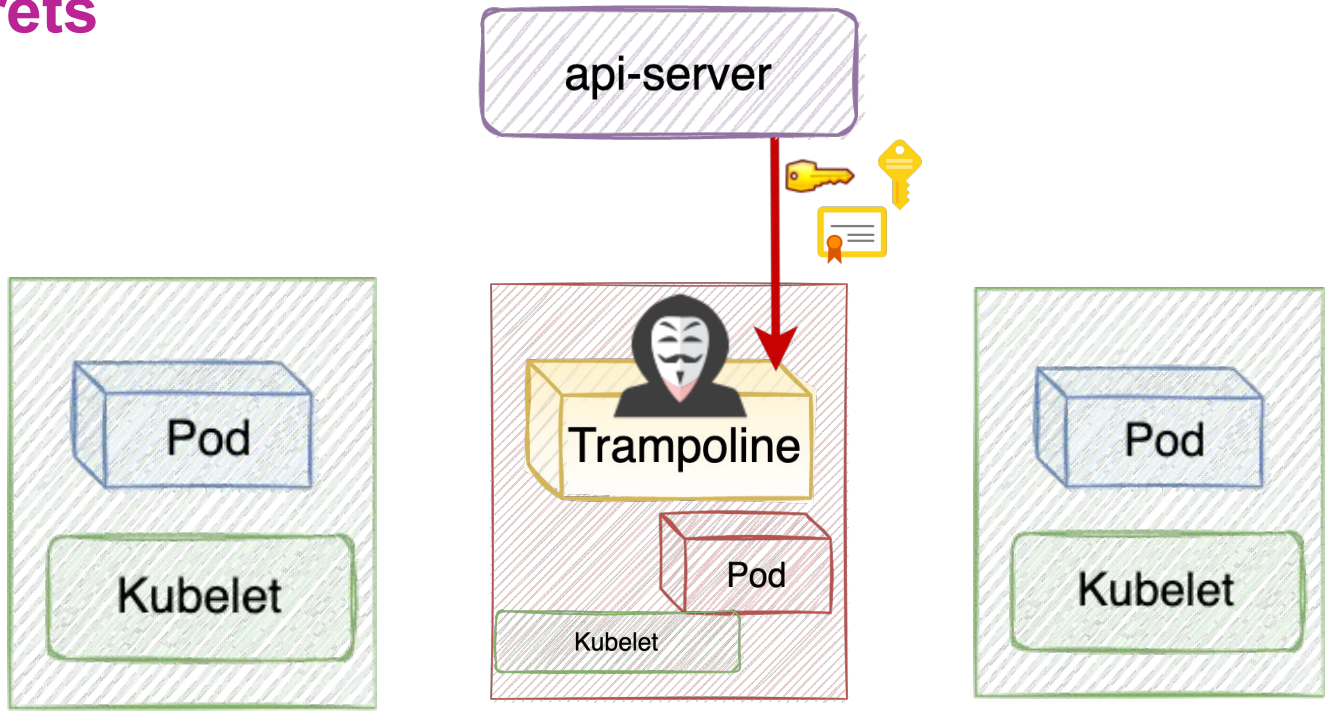


Acquire Tokens

- Retrieve or create SA tokens
- Impact: does namespace host powerful SAs?
  - kube-system ns

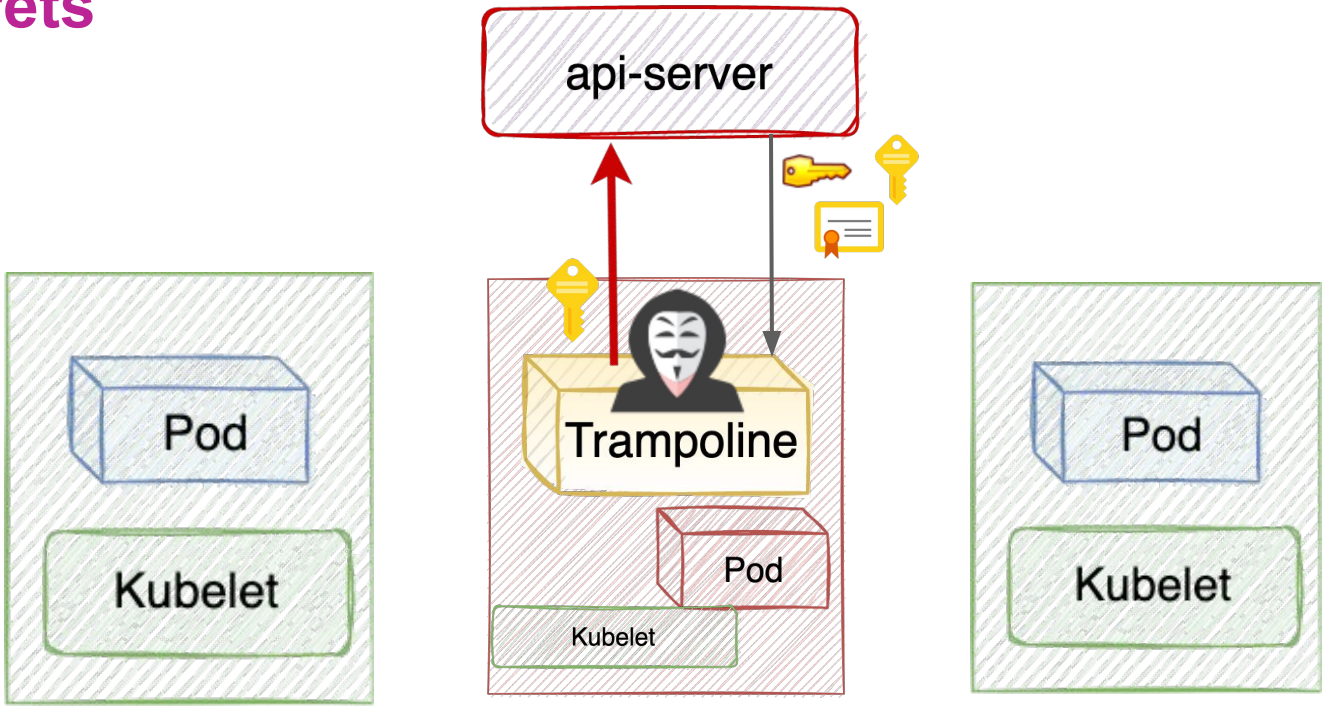
Acquire Tokens

- list secrets



Acquire Tokens

- list secrets

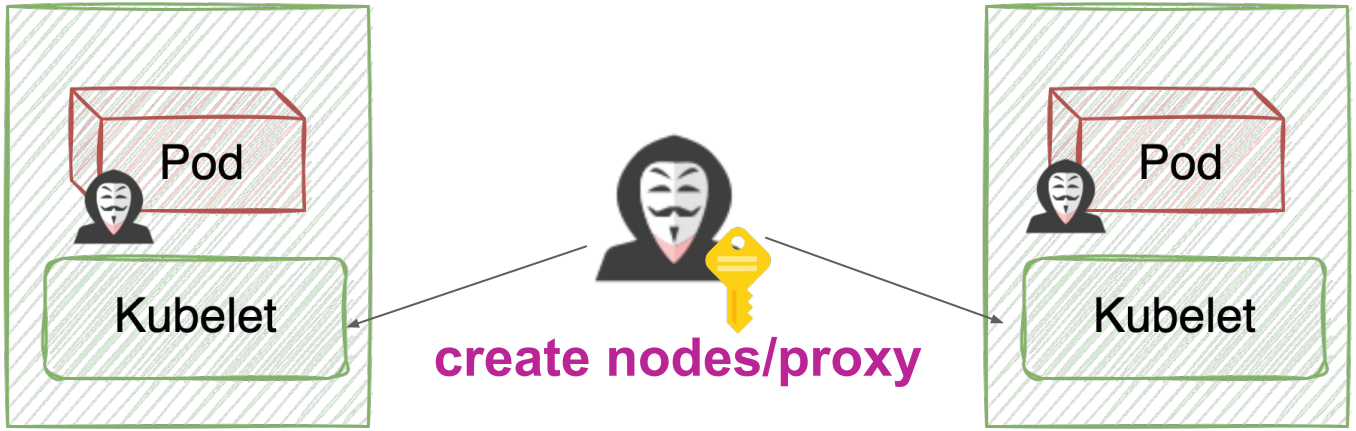


Remote Code Execution

- Execute code on pods / nodes

Remote Code Execution

- Execute code on pods / nodes

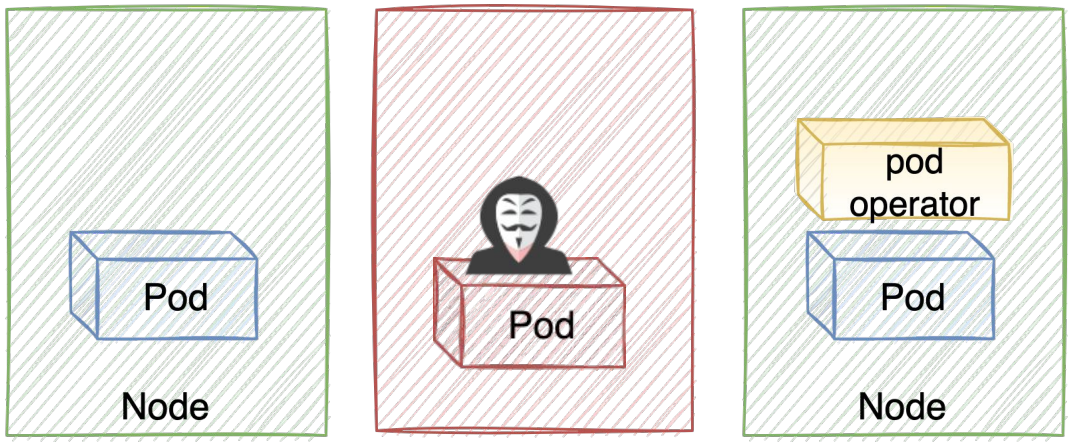


Steal Pods

- Move pods from one node to another
  - Interesting business logic
  - Pods with powerful SAs!

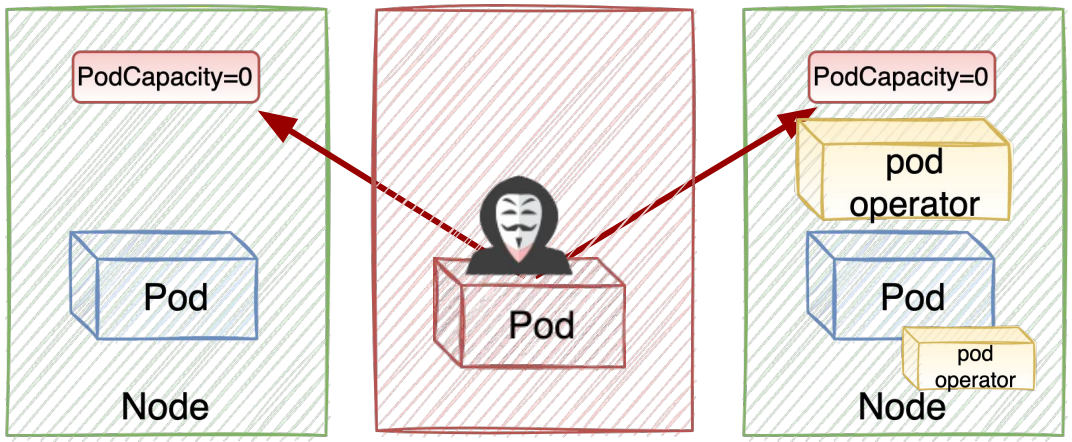
Steal Pods

- update nodes/status
- delete pods



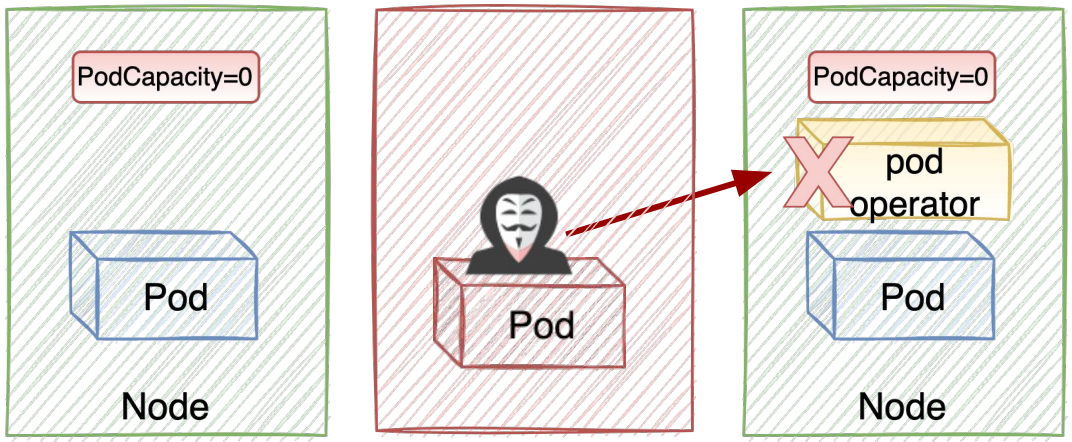
Steal Pods

- update nodes/status
- delete pods



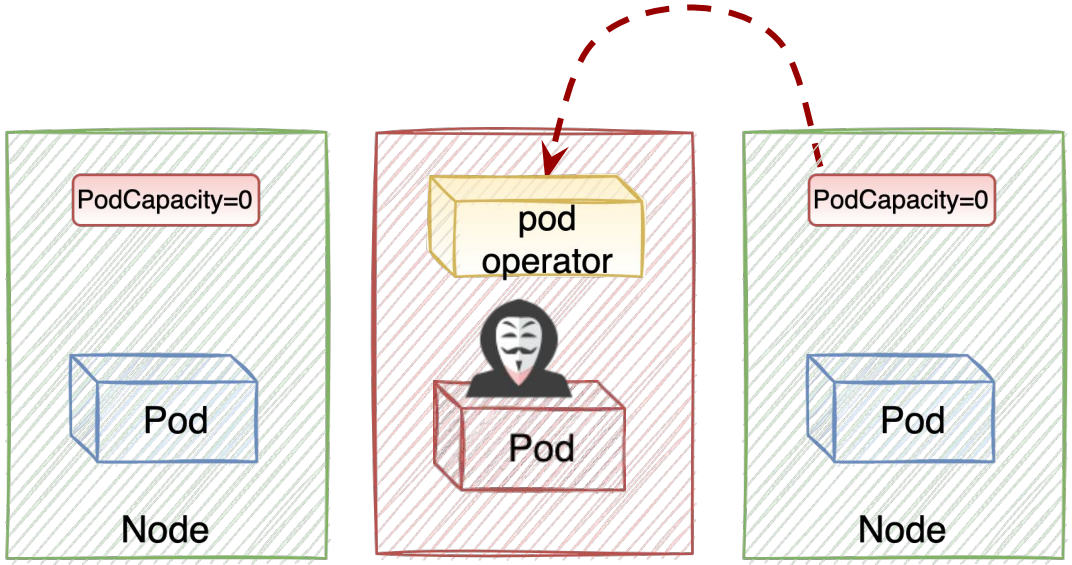
Steal Pods

- update nodes/status
- delete pods



Steal Pods

- update nodes/status
- delete pods



Powerful Permissions By Attack Class

Manipulate AuthN \ AuthZ

- impersonate
- escalate
- bind
- approve signers
- update csr/approval
- control mutating webhooks

Remote Code Execution

- create pods/exec
- update pods/ephemeralcontainers
- create nodes/proxy
- control pods
- control pod controllers
- control mutating webhooks

Acquire Tokens

- list secrets
- create secrets
- create serviceaccounts/token
- create pods
- control pod controllers
- control validating webhooks
- control mutating webhooks

Steal Pods

- modify nodes
- modify nodes/status
- create pods/eviction
- delete pods
- delete nodes
- modify pods/status
- modify pods

Trampolines:

- Pods with permissions to:
  - Manipulate AuthN/AuthZ
  - Acquire Tokens
  - Remote Code Execution
  - Steal Pods
- Real shot at getting cluster admin

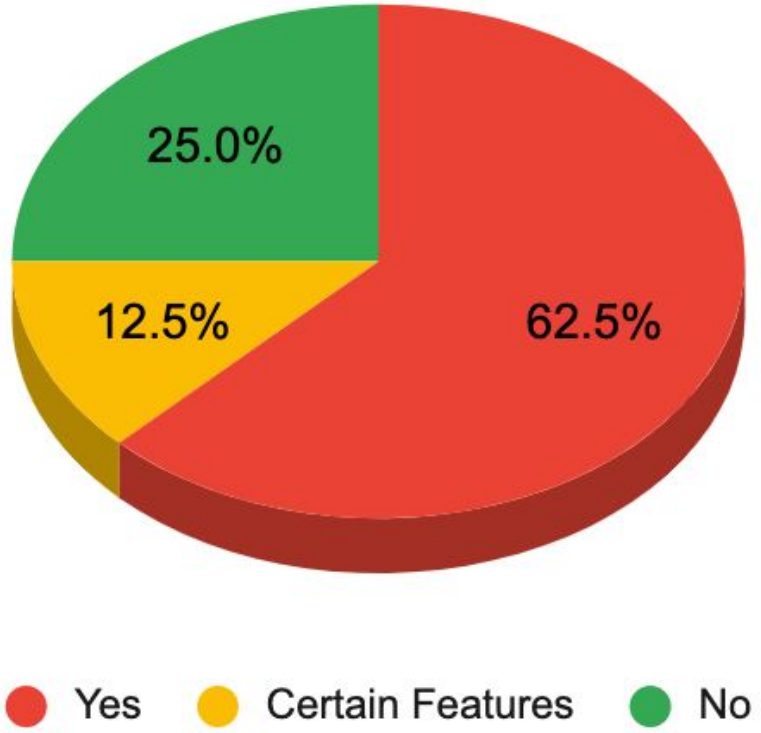
Escape == Admin?
Trampolines Across Popular Platforms

Analyzed Platforms

- Focused on common infra components
- Managed K8s Services & K8s Distributions
  - AKS, EKS, GKE, OpenShift
- Container Network Interfaces (CNIs)
  - Antrea, Calico, Cilium, WeaveNet

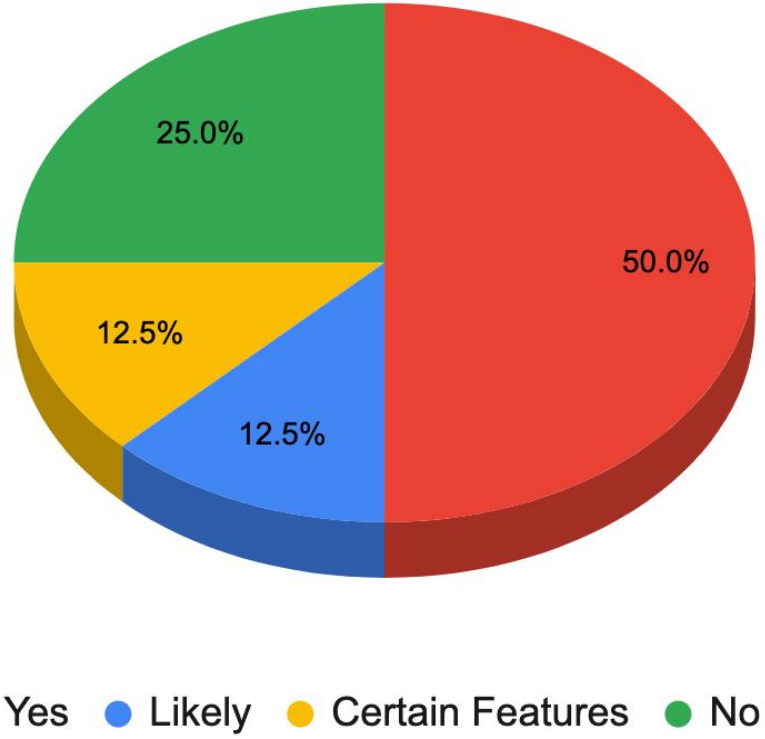
Trampoline DaemonSets (Feb 22)

- Most (62.5%) installed Trampoline DS by default!



Container Escape == Cluster Admin? (Feb)

- In half the platforms escape == admin by default
  - (no panic pls)



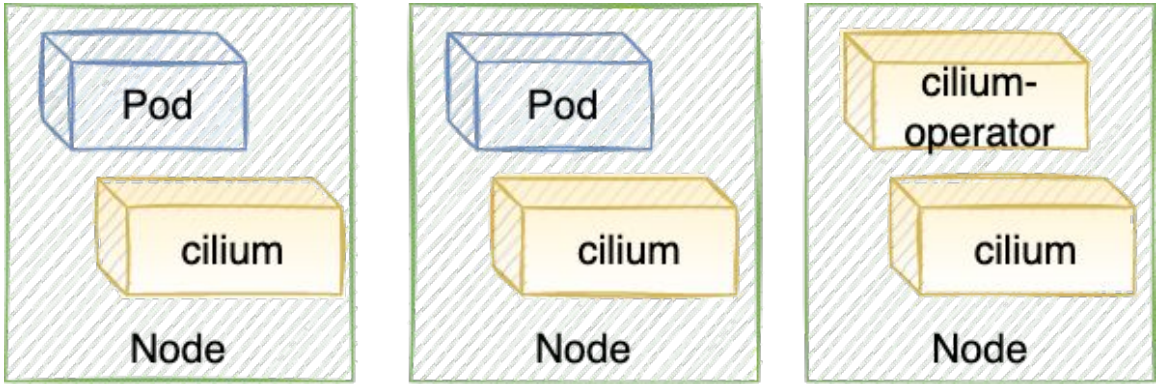
Attack on a Popular K8s Platform

Cilium

- Cilium - popular Container Network Interface (CNI)
  - GKE Dataplane v2
- Showcases a number of attack classes
- Released fixes!

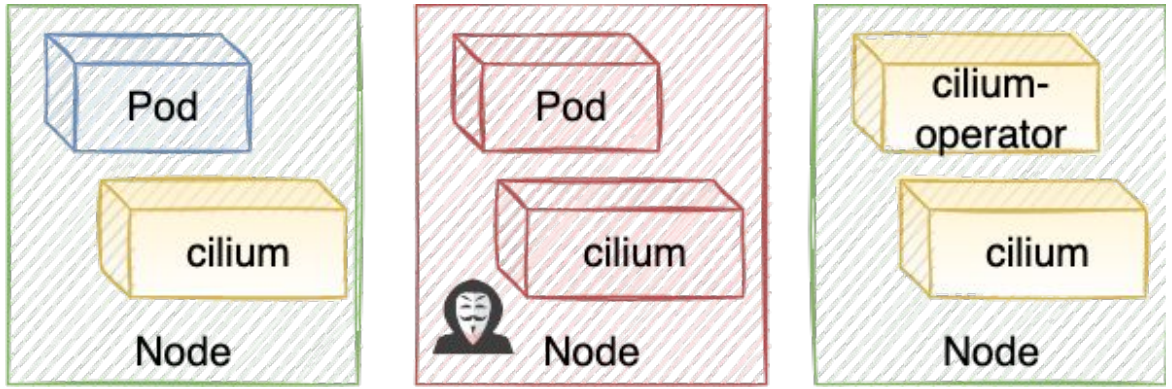
Cilium: Trampolines

- cilium DaemonSet
  - Can **delete pods** & **update nodes/status** (Steal Pods)
- cilium-operator Deployment
  - Can **list secrets** (Acquire Tokens)



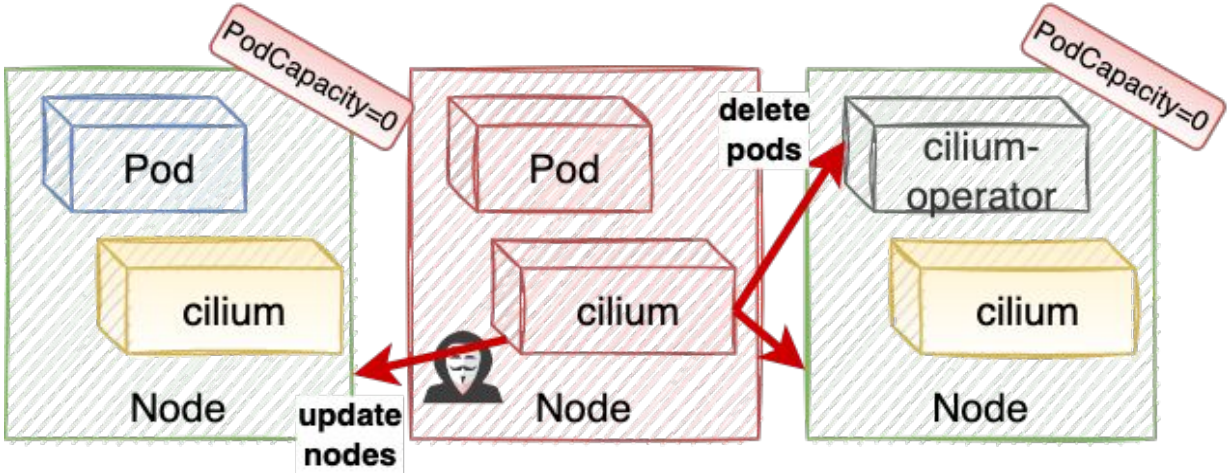
Cilium: Trampolines

- Compromised pod and escaped to node
- Goal: cluster admin



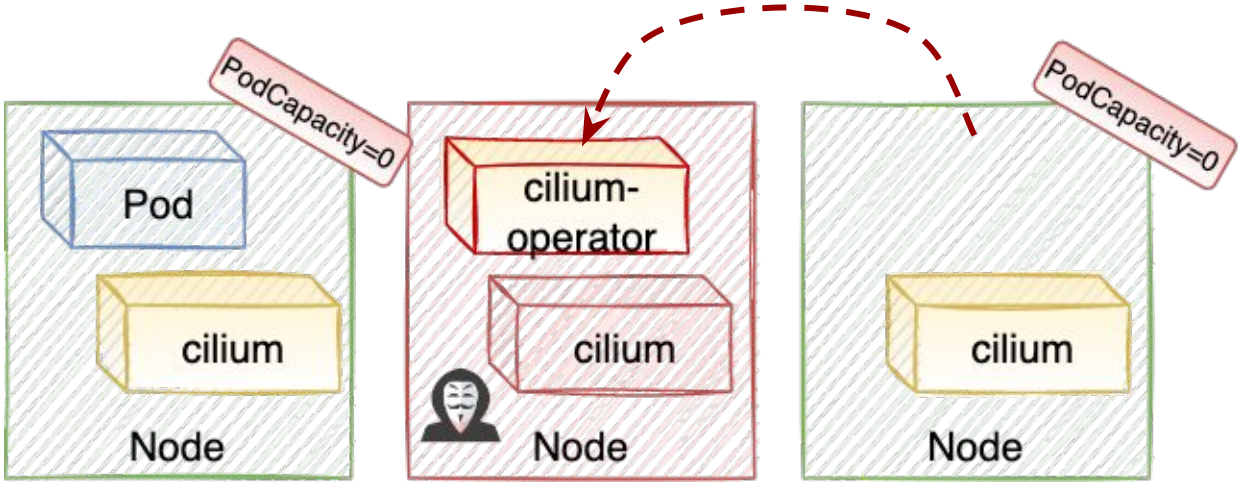
Cilium: Trampolines

1. Zero other nodes' capacity & delete cilium-operator



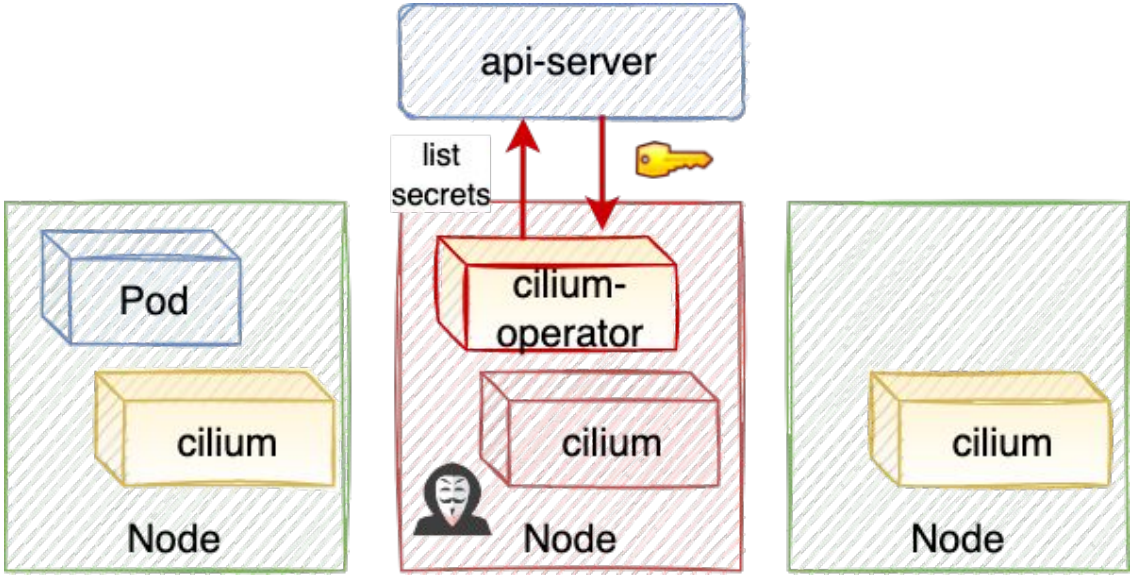
Cilium: Trampolines

1. Zero other nodes' capacity & delete cilium-operator



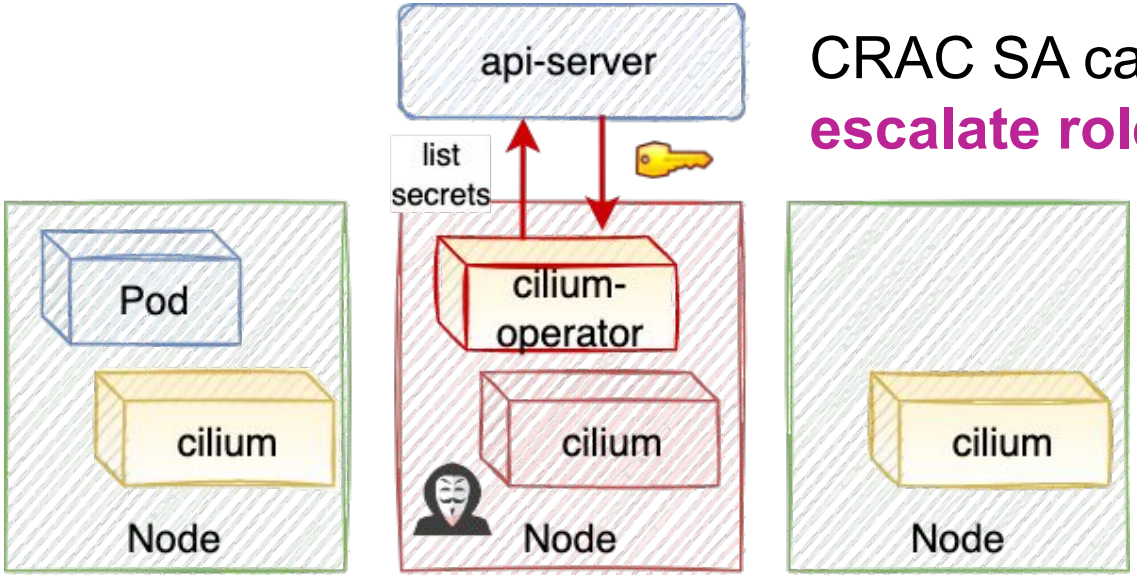
Cilium: Trampolines

1. Zero other nodes' capacity & delete cilium-operator
2. Abuse operator to retrieve powerful built-in token



Cilium: Trampolines

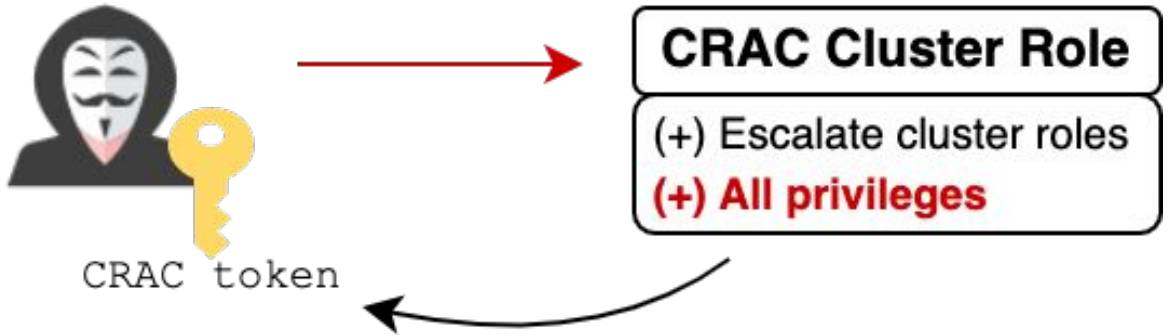
1. Zero other nodes' capacity & delete cilium-operator
2. Abuse operator to retrieve powerful built-in token



CRAC SA can
escalate roles

Cilium: Trampolines

1. Zero other nodes' capacity & delete cilium-operator
2. Abuse operator to retrieve powerful built-in token
3. Add admin perms to CRAC's ClusterRole



Demo!

Cilium: Trampolines

1. Zero other nodes' pod capacity & delete cilium-operator

Steal Pods

2. Abuse cilium-operator to retrieve powerful built-in token

Acquire Tokens

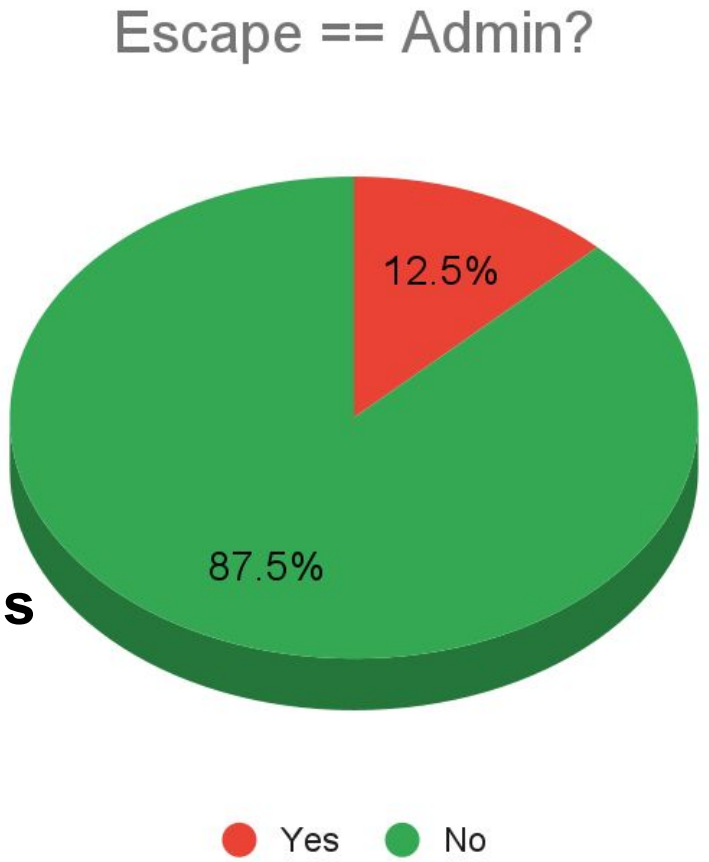
3. Add admin perms to the ClusterRole binded to our token

Manipulate AuthN/Authz

Fixes by Affected Platforms

Fixes

- Disclosed all findings
  - Great experience all around (:
- Most fixed!
  - Remove
  - Relocate
  - Restrain
- **But countless other K8s add-ons & distribution out there**



Platform	Had Trampoline DaemonSets	Fixed
AKS	Yes	No
EKS	Yes	Yes, >=v1.18
GKE	With Dataplane v2	Yes, >=1.23.4-gke.900, 13022$ Bounty
OCP	Yes	Yes, >=v4.11
Antrea	Yes	Yes, v1.6.1 + an admission policy
Calico	No	-
Cilium	Yes	Yes, >=v1.12.0-rc2
Weave Net	No	-

Identifying Risky Perms

rbac-police

- New open-source tool
- Evaluate the RBAC perms of pods, SA & nodes
- ~20 policies out-of-the-box
  - Each targets risky perm / privEsc technique
  - Identify powerful pods & the attacks they enable
- Customizable! policies written in Rego (OPA)
  - CRDs? Platform specific attacks? PrivEsvs we missed?

github.com/PaloAltoNetworks/rbac-police

```
yavrahami@M-C02YT7FTLVDQ:~/rbac-police$ ./rbac-police eval lib
{
    "policyResults": [
        {
            "policy": "lib/modify_pods.rego",
            "severity": "High",
            "description": "SAs and nodes that can update and patch p
(kube-system) can gain code execution on pods that are likey to be pr
            "violations": {
                "serviceAccounts": [
                    {
                        "name": "cilium",
                        "namespace": "kube-system",
                        "nodes": [
                            {
                                "ip-172-31-20-29.ec2.internal": [
                                    "cilium-66ssg",
```

Policy & Severity

Violating SAs and their Pods

Checkov

- Open source Infra-as-Code (IaC) security scanner
- Alerts on risky perms before they're installed to cluster
  - Inspect add-ons prior to deployment

github.com/bridgecrewio/checkov

checkov by bridgecrew

Takeaways

Takeaways

- Trampolines introduce new privEsc avenues to K8s
  - Up to escape == admin
- K8s attack classes & powerful perms
- Tricky to safely configure RBAC
  - Seemingly restricted perms may allow privEsc
  - Not in checklists / benchmarks
- Good RBAC hygiene is key:
  - Regularly monitor RBAC (rbac-police / Checkov)
  - Minimize distribution of powerful tokens
  - Admission / audit policies to detect attacks! (see report)

Report

Questions?

rbac-police