Patch It Up: Real-Time Vulnerability Management with Kyverno and KubeArmor

Barun Acharya
@daemon1024

$ whoami

❑ Maintainer @ **KubeArmor** 🛡️

❑ Tech Lead (Open Source) @ **Accuknox**

❑ Google **Summer of Code**

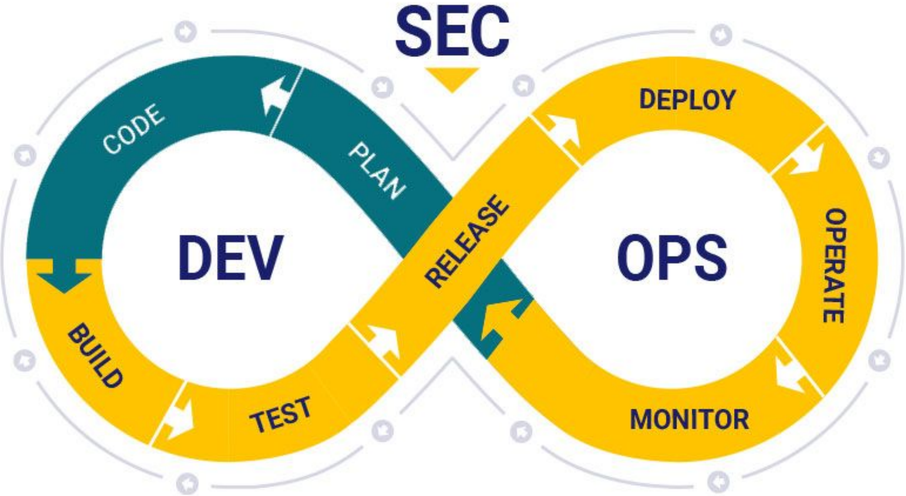
❑ **LFX** Mentorship

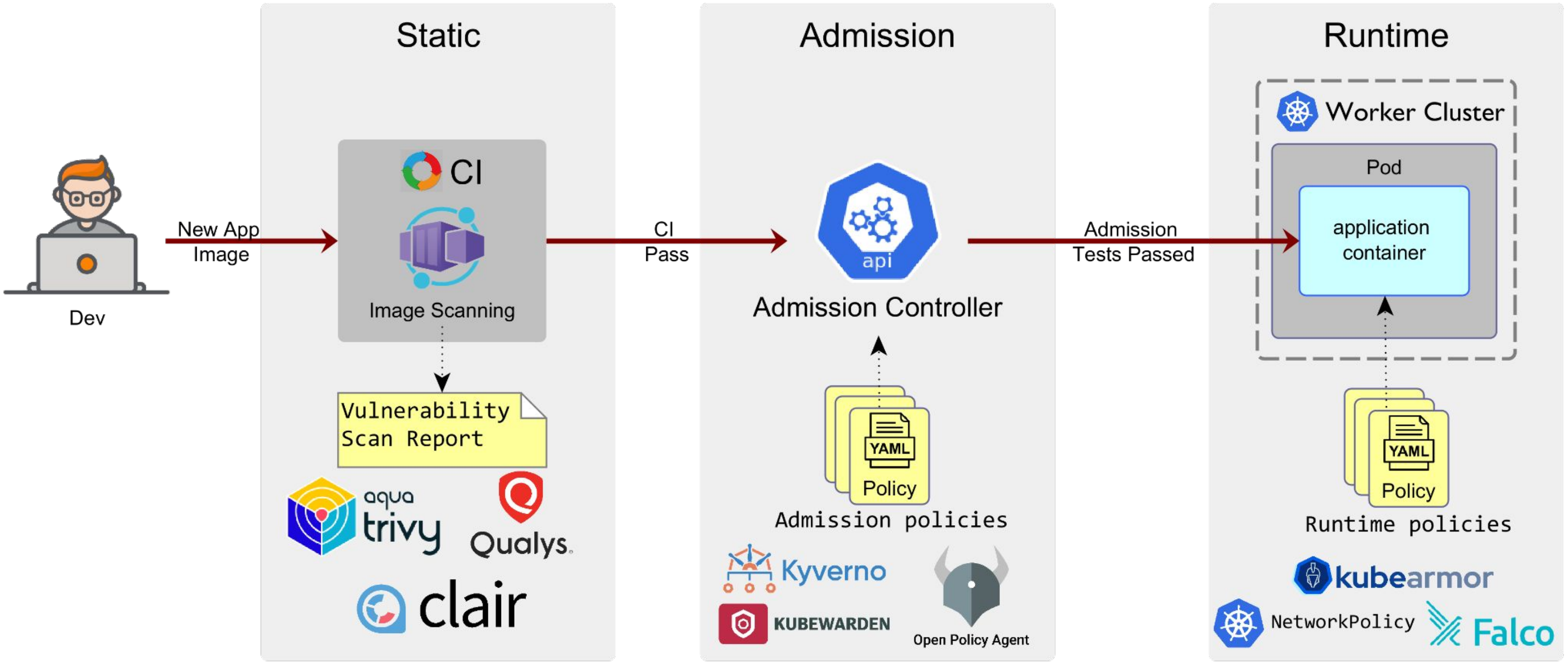
❑ **CNCF** Ambassador

❑ Volunteer @ **CNCG New Delhi**

❑ Organiser @ **CNCG KubeArmor**

Vulnerability Management


SEC
CODE
PLAN
DEV
BUILD
TEST
RELEASE
DEPLOY
OPS
OPERATE
MONITOR


Static
Admission
Runtime
Dev
New App Image
CI
Image Scanning
Vulnerability Scan Report
aqua trivy
Qualys.
clair
CI Pass
api
Admission Controller
YAML
Policy
Admission policies
Kyverno
KUBEWARDEN
Open Policy Agent
Admission Tests Passed
Worker Cluster
Pod
application container
YAML
Policy
Runtime policies
kubearmor
NetworkPolicy
Falco

Challenges with Vulnerability Management

Handling
Zero Day
Vulnerability

Log4J Timeline

- **November 24** - **CVE-2021-44228** announced
- **December 6** - Apache Log4j releases version **2.15.0**. Shortly after, **CVE-2021-45046** which was further exploited
- **December 13** - Version **2.16.0** released to remediate. Yet another vulnerability is discovered **CVE-2021-45105**
- **December 18** - The Log4j team releases version **2.17.0**
- **December 28** - Yet another patch is released, version **2.17.1**, this time to remediate **CVE-2021-44832**

Log4J Timeline

Nov 24 → Dec 28

> 1 month

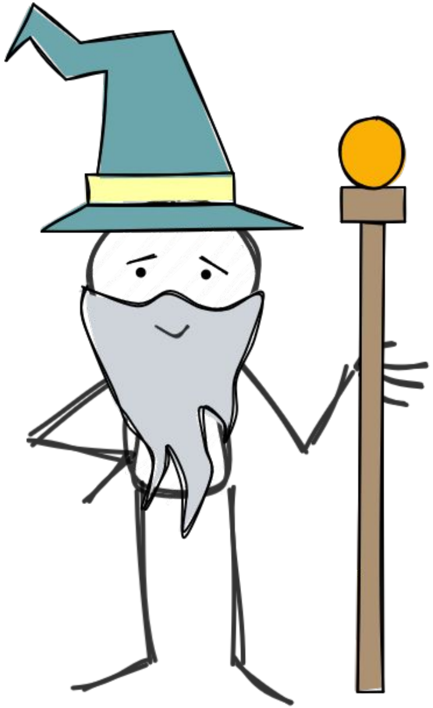
ShellShock

ShellShock

- **1989** - **Exists v1.0.3**
- **September 12, 2014 –** Shellshock vulnerability discovered **(CVE-2014-6271).**
- **September 24, 2014 –** Public disclosure and initial patch.
- **September 25, 2014 –** Second vulnerability **(CVE-2014-7169) identified**; second patch released.
- **September 26, 2014 –** Two additional vulnerabilities **(CVE-2014-7186, CVE-2014-7187)** identified; updated patches.
- **September 29, 2014 – CVE-2014-6277** and **CVE-2014-6278** identified; more updates released.
- **October 1, 2014 –** Stable patches released, systems secure after applying all updates.

Do you wait for the patch?

Have Application Downtime?



Virtual
Patch

Kyverno allows cluster administrators to manage environment specific configurations independently of workload configurations and **enforce configuration best practices** for their clusters.

aqua

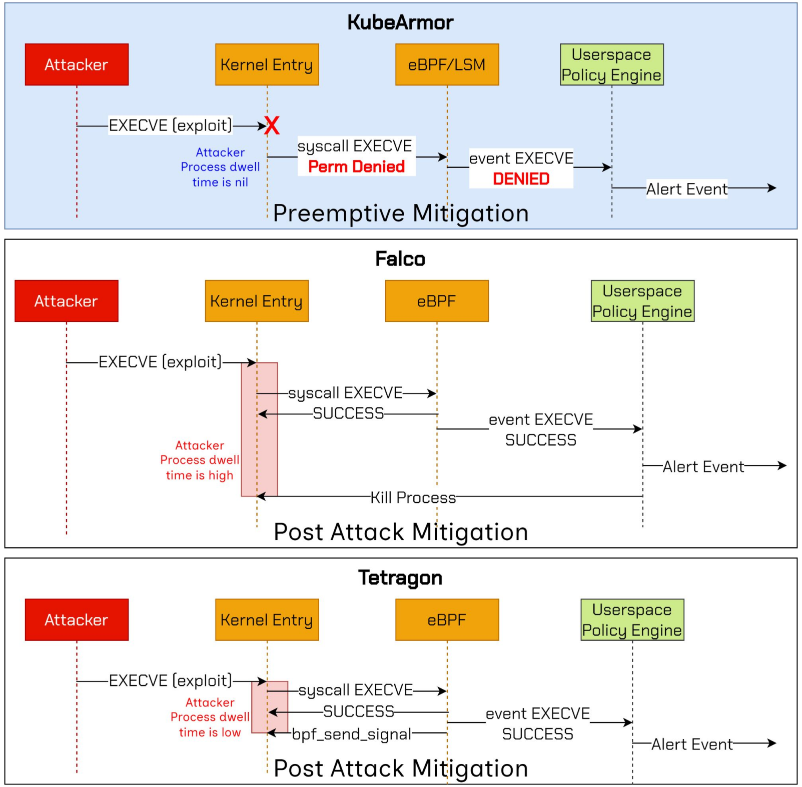
trivy-operator

Trivy is a comprehensive and versatile security **scanner**. Trivy has scanners that look for security issues, and targets where it can find those issues.

kubearmor

KubeArmor is a cloud-native runtime security **enforcement** system that restricts the behavior (such as **process execution, file access, and networking operations**)

KubeArmor fundamentally...



- Detect & Respond Model aka Post Attack Mitigation vs Preemptive Security
- Linux Security Modules
  - AppArmor
  - BPF-LSM

Demo

Thank You!!

(づ｡◕‿‿◕｡)づ

kubearmor.io

@daemon1024

Thank You!!

Questions? (づ｡◕‿‿◕｡)づ

barun.cc