Secure Kubernetes Strong Applications!

Who Am I ?

Rumeysa Kumru

Cloud Native Engineer @ BESTCLOUDFOR.ME

www.linkedin.com/in/rumeysa-kumru/
medium.com/@rumeysa_25373
kumrur0@gmail.com

Agenda

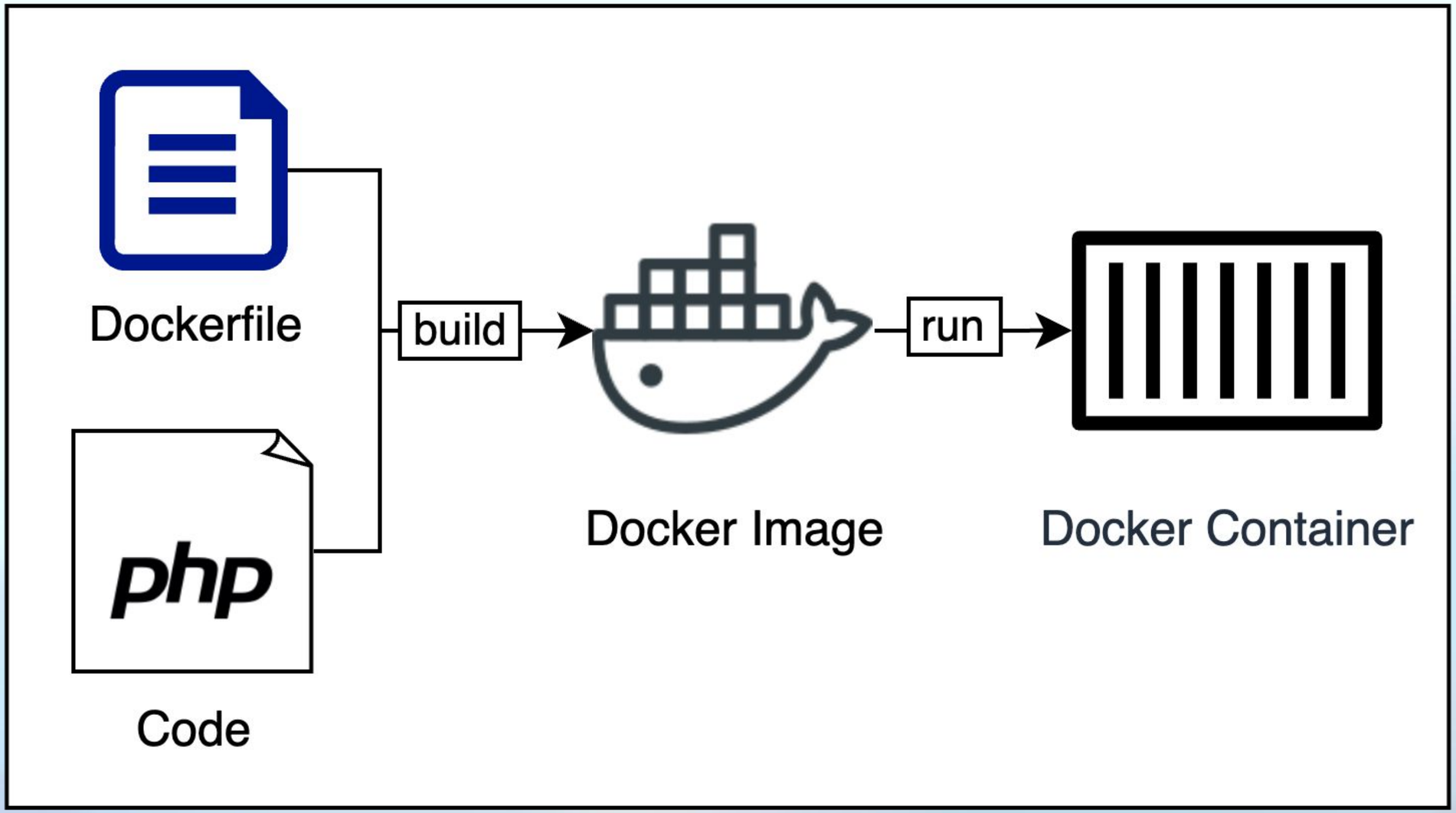
Containerization: What is a Container?

Orchestration Tools: Managing Containerized Applications

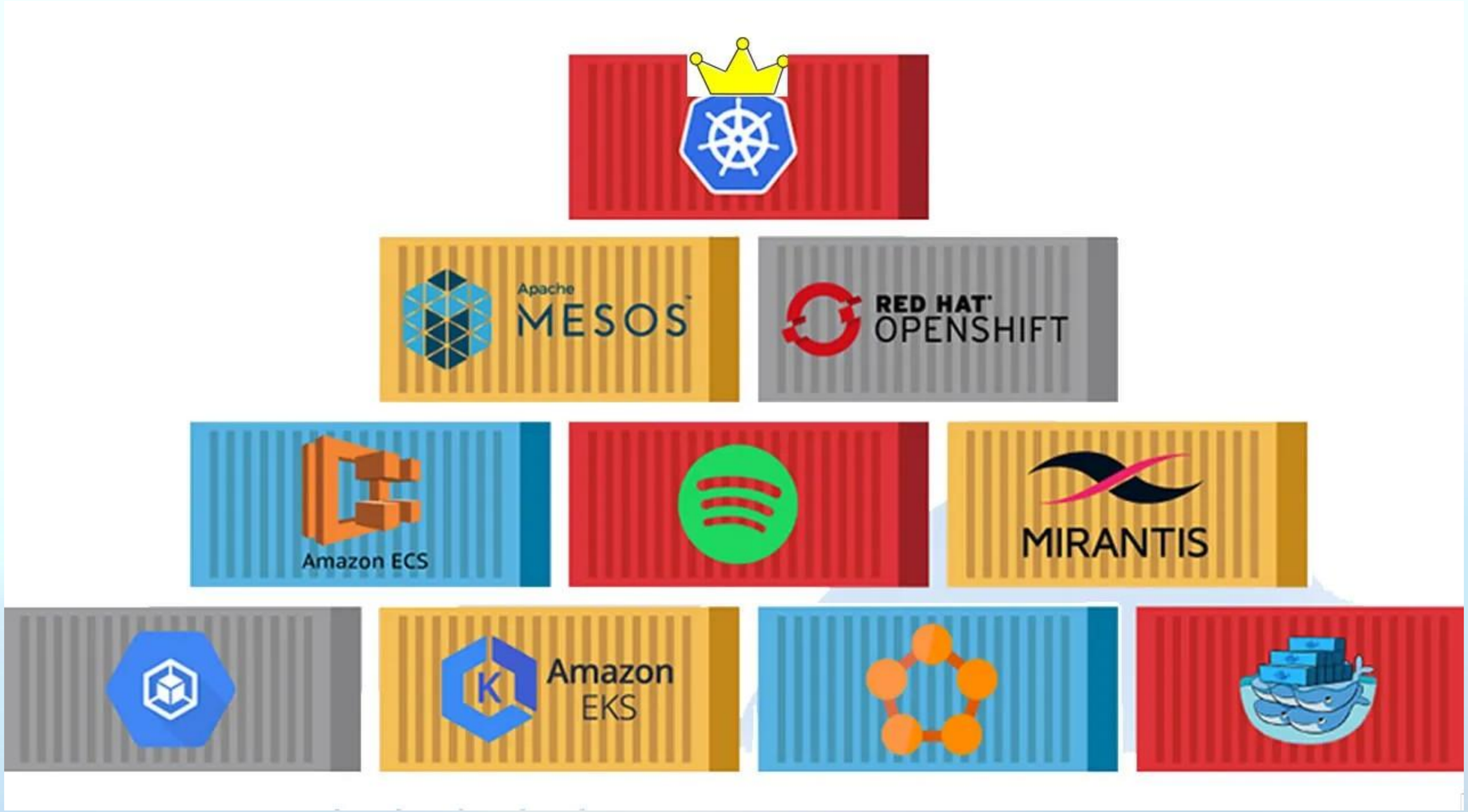
Kubernetes Overview

Kubernetes Security

What is Container?



Orchestration Tools



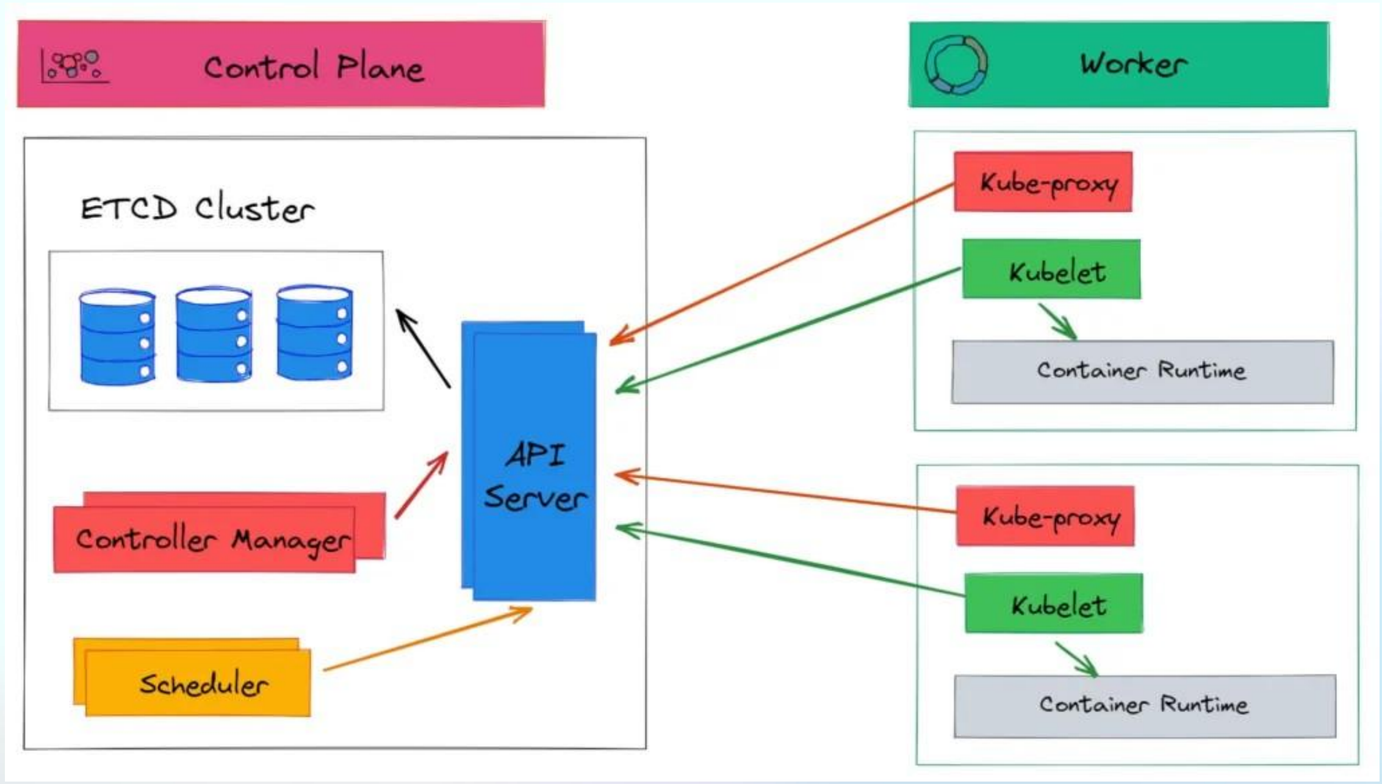
Kubernetes Components

Master Components

- API Server
- etcd
- Controller Managers
- Scheduler

Node Components

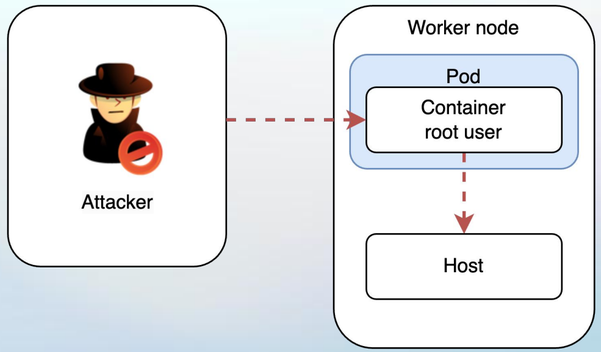
- Kubelet
- Kube-proxy
- Container Runtime



Kubernetes Security

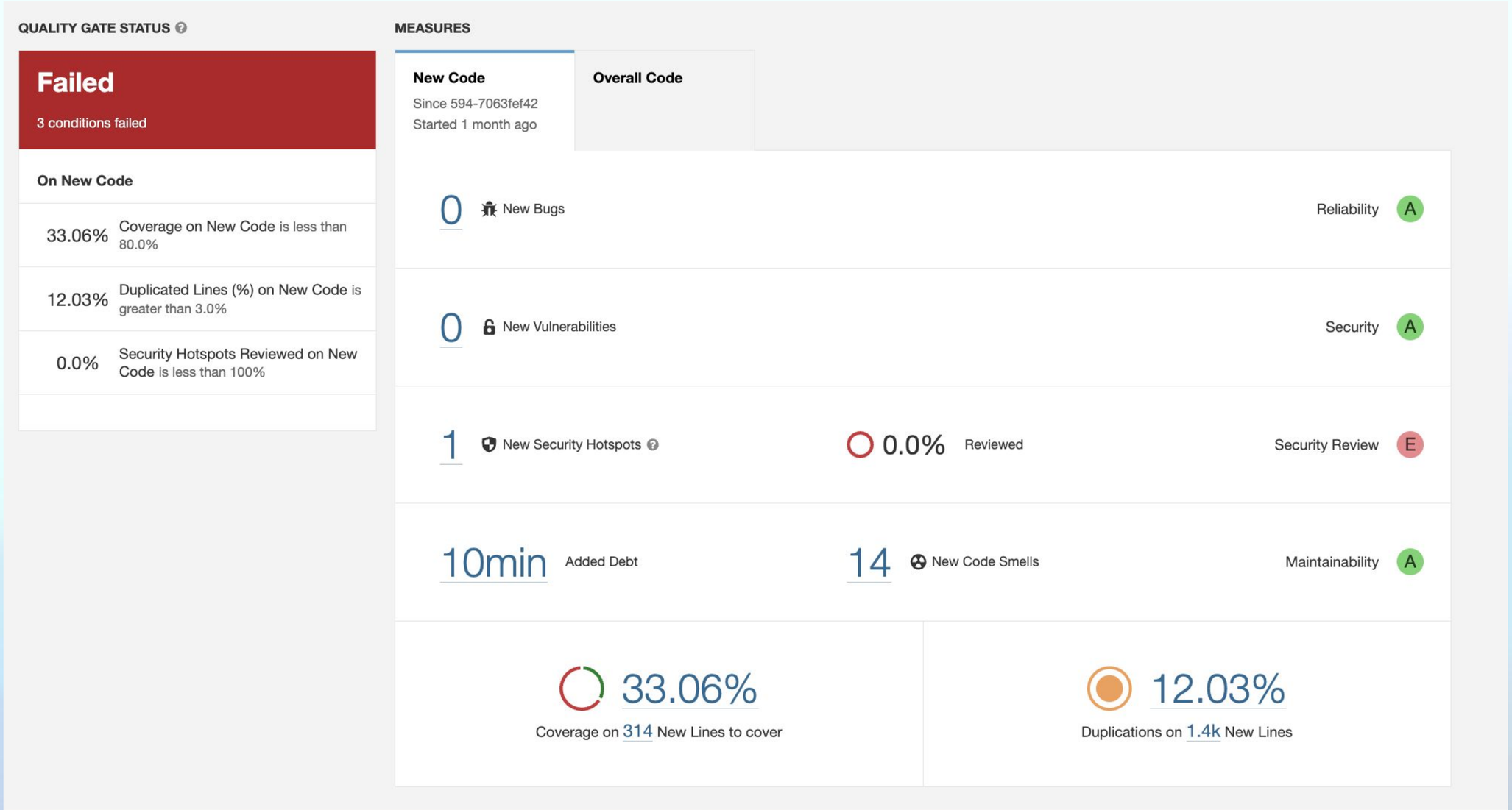
- Cluster Security
  - Segregation
  - Network Policies
  - Use Hardening Images

- Pod Security
  - Code Analysis (SonarQube)
  - Image Scan (Trivy)
  - Pod Isolation
  - Run as Non Root User
  - Patch Management




```yaml
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
```

Kubernetes Security



Kubernetes Security

```
~
└─ trivy image php:7.4
2024-05-08T19:38:34.757+0300    INFO    Vulnerability scanning is enabled
2024-05-08T19:38:34.758+0300    INFO    Secret scanning is enabled
2024-05-08T19:38:34.758+0300    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-05-08T19:38:34.758+0300    INFO    Please see also https://aquasecurity.github.io/trivy/v0.50/docs/scanner/secret/#recommendation for faster secret detection
```

perl-modules-5.32	CVE-2020-16156	HIGH				perl-CPAN: Bypass of verification of signatures in CHECKSUMS files https://avd.aquasec.com/nvd/cve-2020-16156
	CVE-2023-31484					perl: CPAN.pm does not verify TLS certificates when downloading distributions over HTTPS... https://avd.aquasec.com/nvd/cve-2023-31484
	CVE-2023-47038		fixed		5.32.1-4+deb11u3	perl: Write past buffer end via illegal user-defined Unicode property https://avd.aquasec.com/nvd/cve-2023-47038
	CVE-2011-4116	LOW	affected			perl: File::Temp insecure temporary file handling https://avd.aquasec.com/nvd/cve-2011-4116
	CVE-2023-31486					http-tiny: insecure TLS cert default https://avd.aquasec.com/nvd/cve-2023-31486
re2c	CVE-2018-21232			2.0.3-1		re2c: uncontrolled recursion that causes stack consumption in find_fixed_tags https://avd.aquasec.com/nvd/cve-2018-21232
	CVE-2022-23901					A stack overflow re2c 2.2 exists due to infinite recursion issues in... https://avd.aquasec.com/nvd/cve-2022-23901
sysvinit-utils	TEMP-0517018-A83CE6			2.96-7+deb11u1		[sysvinit: no-root option in expert installer exposes locally exploitable security flaw] https://security-tracker.debian.org/tracker/TEMP-0517018-A83CE6
tar	CVE-2005-2541			1.34+dfsg-1		tar: does not properly warn the user when extracting setuid or setgid... https://avd.aquasec.com/nvd/cve-2005-2541
	CVE-2022-48303		fixed		1.34+dfsg-1+deb11u1	tar: heap buffer overflow at from_header() in list.c via specially crafted checksum... https://avd.aquasec.com/nvd/cve-2022-48303
	CVE-2023-39804					tar: Incorrectly handled extension attributes in PAX archives can lead to a... https://avd.aquasec.com/nvd/cve-2023-39804
	TEMP-0290435-0B57B5		affected			[tar's rmt command may have undesired side effects] https://security-tracker.debian.org/tracker/TEMP-0290435-0B57B5
util-linux	CVE-2024-28085	HIGH	fixed	2.36.1-8+deb11u1	2.36.1-8+deb11u2	util-linux: CVE-2024-28085: wall: escape sequence injection https://avd.aquasec.com/nvd/cve-2024-28085
	CVE-2022-0563	LOW	affected			util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled... https://avd.aquasec.com/nvd/cve-2022-0563
zlib1g	CVE-2023-45853	CRITICAL	will_not_fix	1:1.2.11.dfsg-2+deb11u2		zlib: integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_6 https://avd.aquasec.com/nvd/cve-2023-45853

Kubernetes Security

- RBAC
  - User Permissions
- Secret Management
  - Encrypted Storage
  - Rotational Policies

```
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: default
  name: pod-reader
rules:
- apiGroups: [""] # "" indicates the core API group
  resources: ["pods"]
  verbs: ["get", "watch", "list"]
```

Kubernetes Security

- Continuous Monitoring
  - Event Logging
  - Audit Trail

- Regular Security
  - Penetration Tests
  - Compliance Checks (PCI DSS etc.)
  - Update Regularly

- Disaster Recovery

Now, with the measures and strategies we've discussed about Kubernetes security, *how can you improve the security status of our organization or project*?