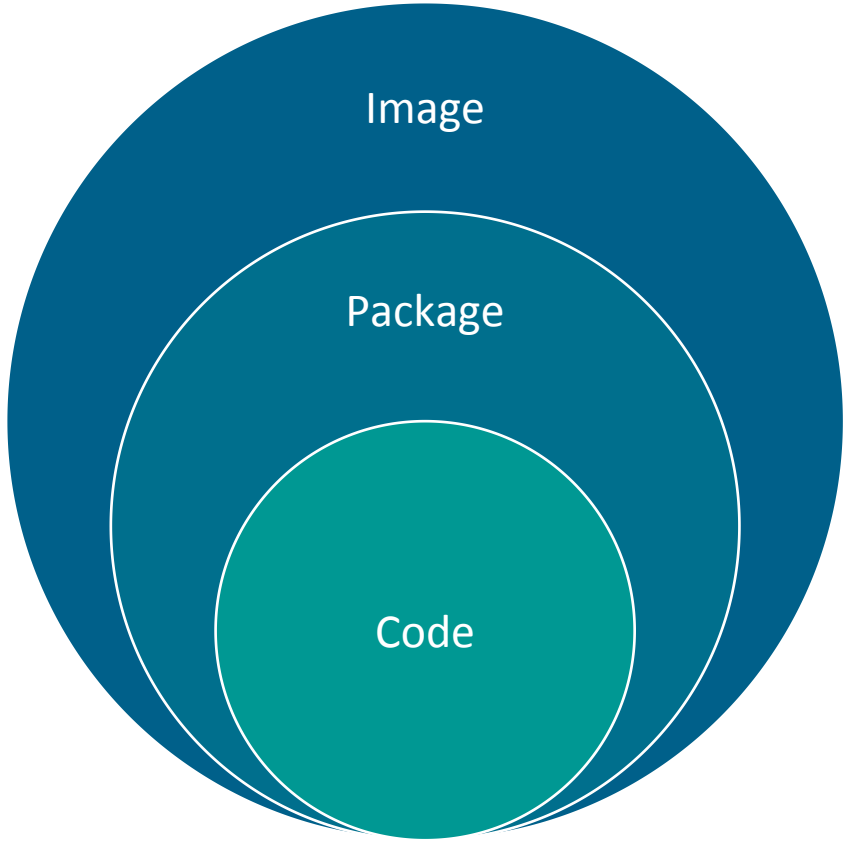
Experience Sharing of Trustworthiness Improvement In ONAP Development

Jing Lu
Huawei Technologies co.

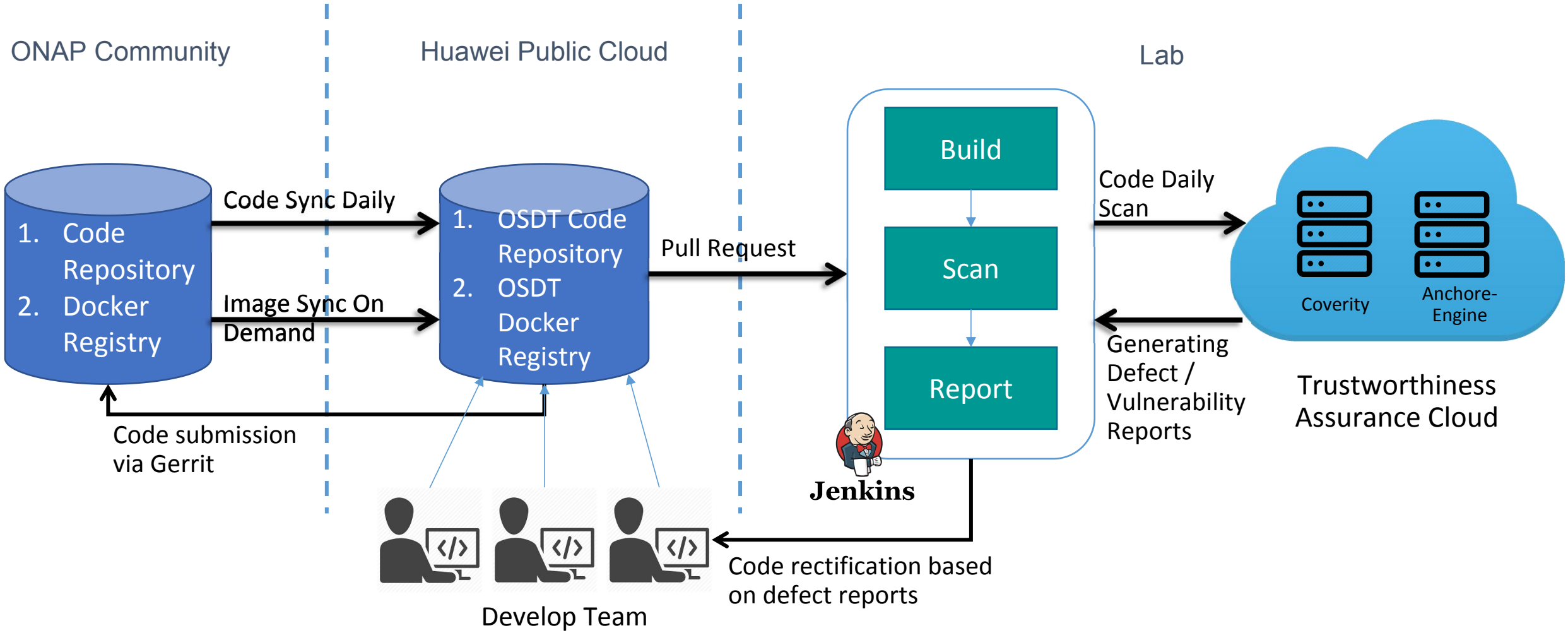
June , 2019

Focus Area

We focus on



Development Workflow Overview



Coverity

Free cloud-based service for the open source community

Coverity founders first published work reported over 500 defects in the Linux kernel

2000

Coverity Scan began

2006

Proven developer adoption

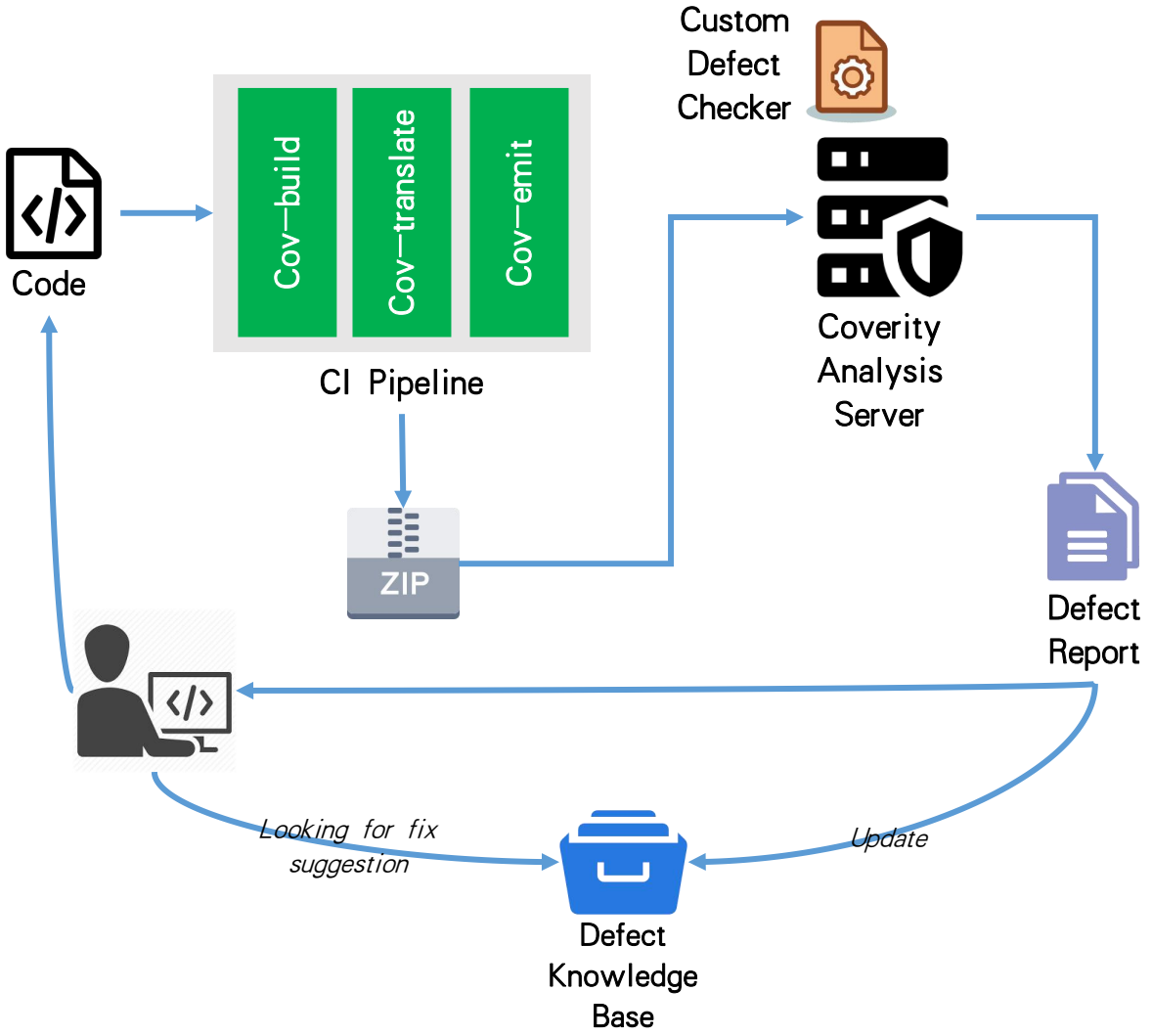
2013

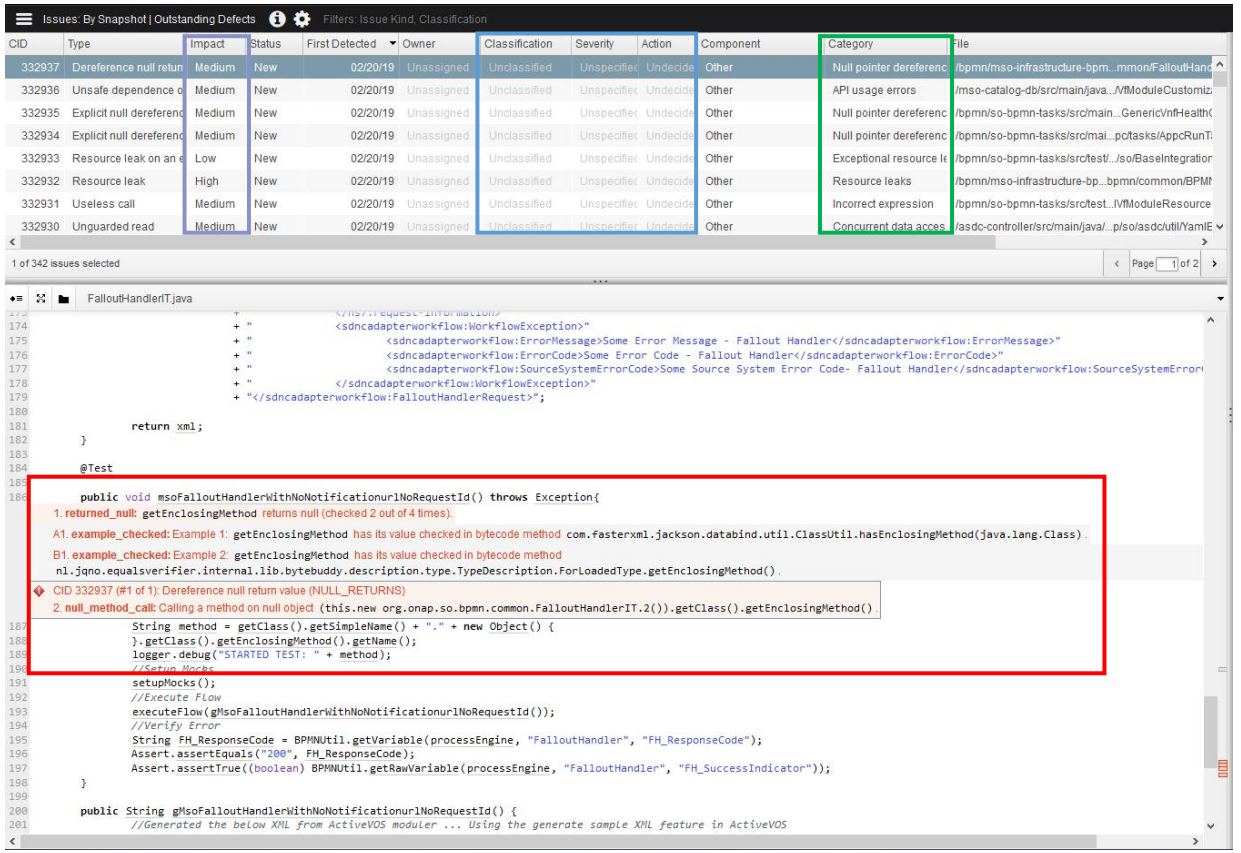
Over 600 projects and 300M lines of code

Over 45,000 defects fixed by the community

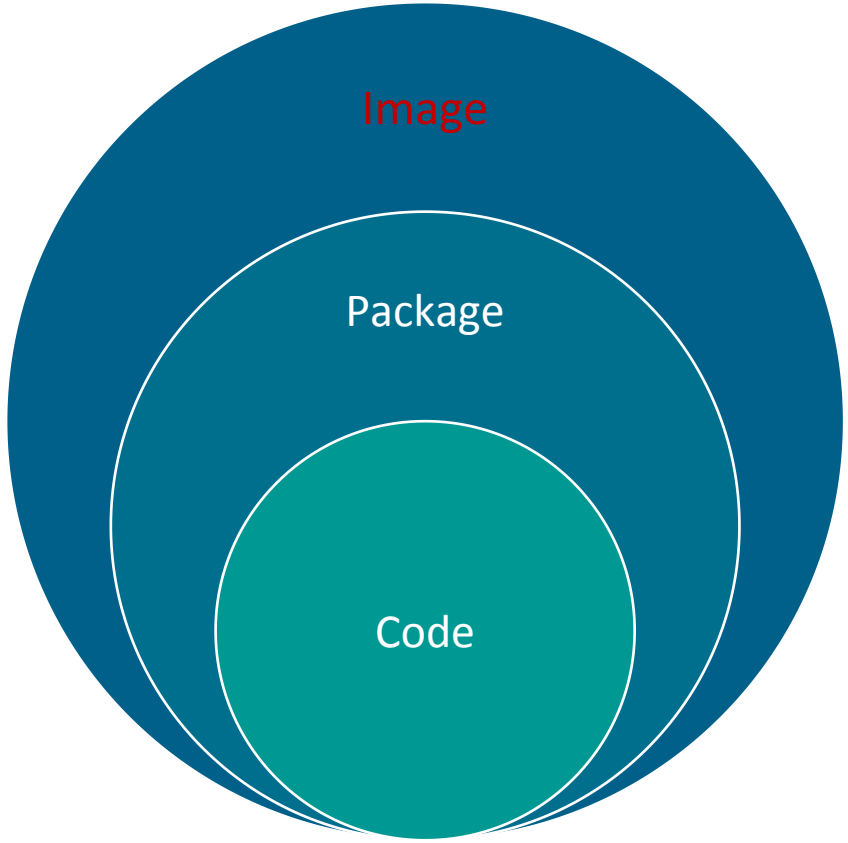
Source: [1]

Pipeline & Defect Report





Let’s Continue



Vulnerabilities In the Container Ecosystem

"Top container vulnerabilities in 2017 ~ 2019"

CVE	Description	Affected System
CVE-2017-1002101	subPath Volume Mount Vulnerability	Docker
CVE-2017-16995	eBPF Vulnerability	Linux
CVE-2018-1002105	Severe Privilege Escalation Vulnerability	Kubernetes
CVE-2018-8115	Windows Host Compute Service Shim (hcsshim)	Windows
CVE-2018-11757	Docker Skeleton Runtime Vulnerability	Docker
CVE-2018-1000056	Jenkins JUnit Plugin Vulnerability	Jenkins
CVE-2019-1002100	API Server Patch Permission DoS Vulnerability	Kubernetes
CVE-2019-5736	High Severity RunC Vulnerability	Docker
CVE-2019-1003065	Jenkins CloudShare Docker-Machine Plugin Vulnerability	Jenkins

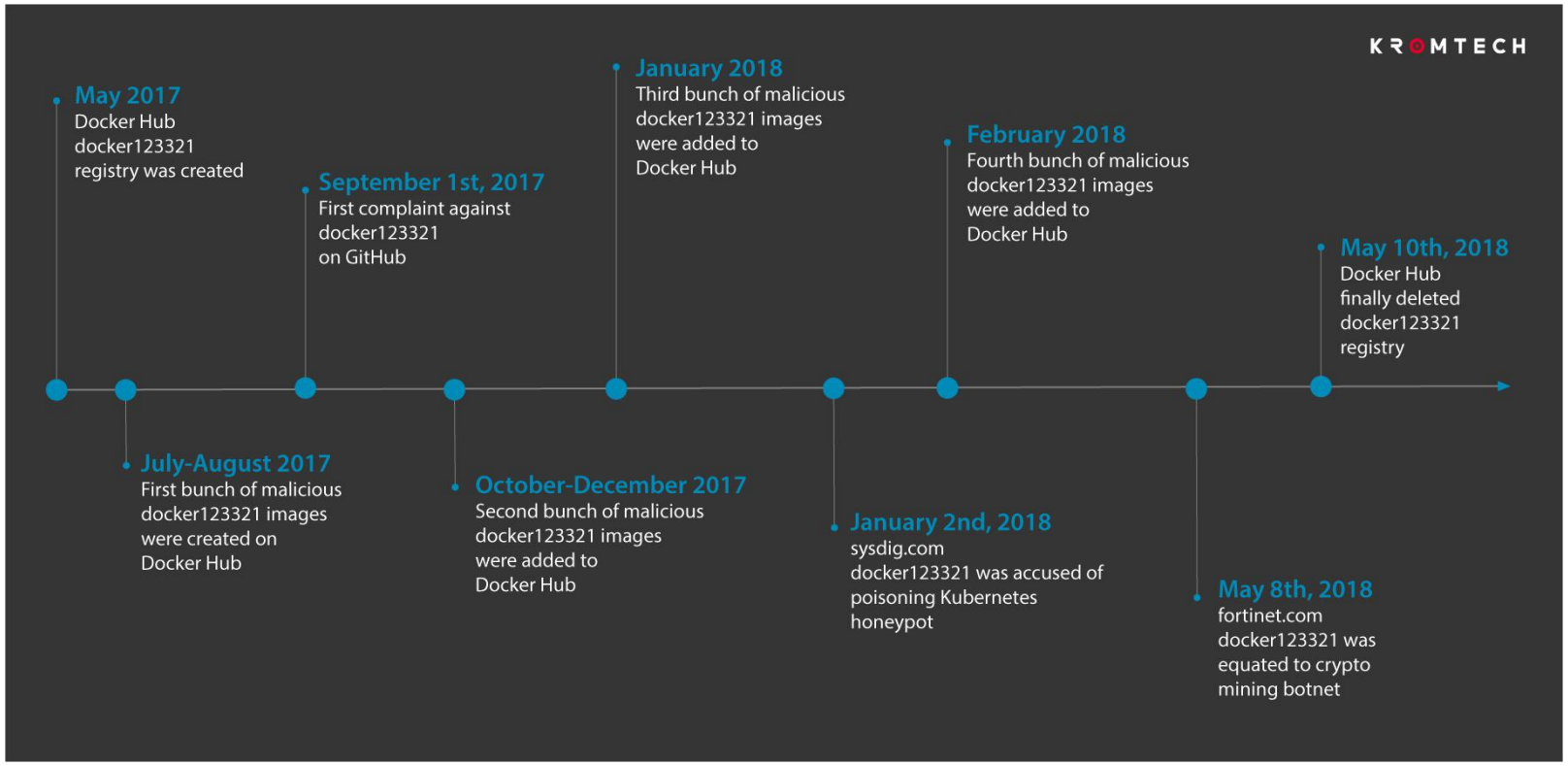
Software has always had flaws and will continue to have them.

For containerized applications, we should take proactive measures to reduce their proliferation.

In addition to the shift-left approach of dealing with security issues early in the design phase and mitigating vulnerabilities during the coding phase, **we suggest ONAP also adopt container vulnerability analysis.**

Source: [2]

Tainted Docker image be exploited for crypto-mining



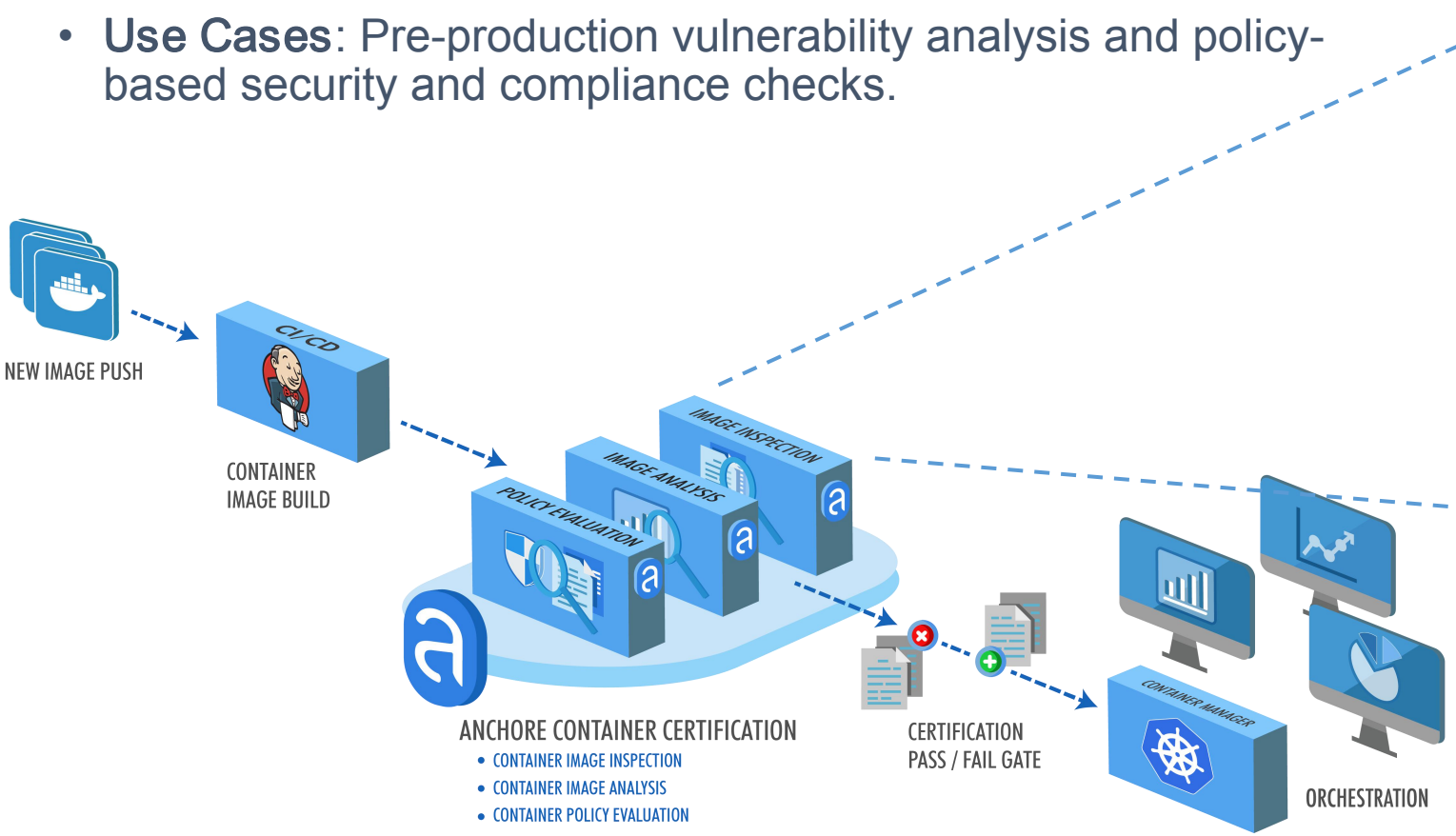
- 17 malicious Docker images that have been backdoored and used to install reverse shells and crypto-currency miners were downloaded collectively 5 million times in a year
- Malware included crypto mining software, netting ~$90,000 of Monero

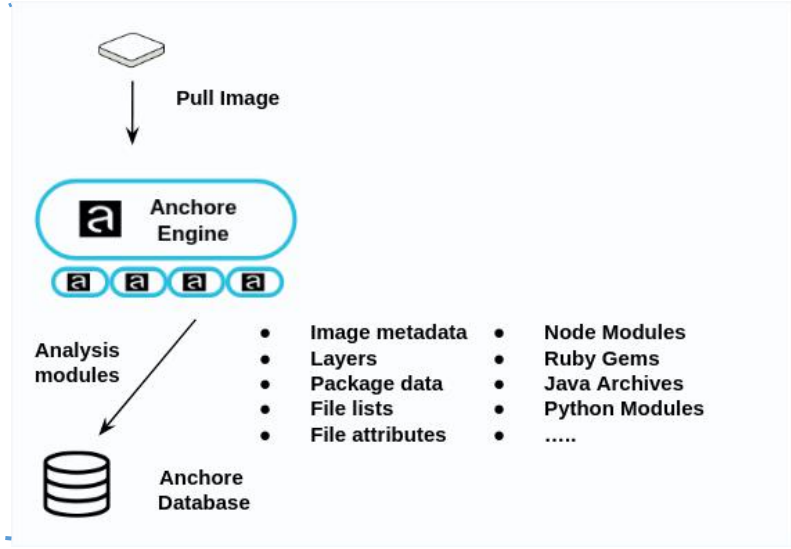
Source: [3]

Anchore

Anchore is an ***open source*** tool for conducting *vulnerability analysis* of application containers.

- **Use Cases**: Pre-production vulnerability analysis and policy-based security and compliance checks.



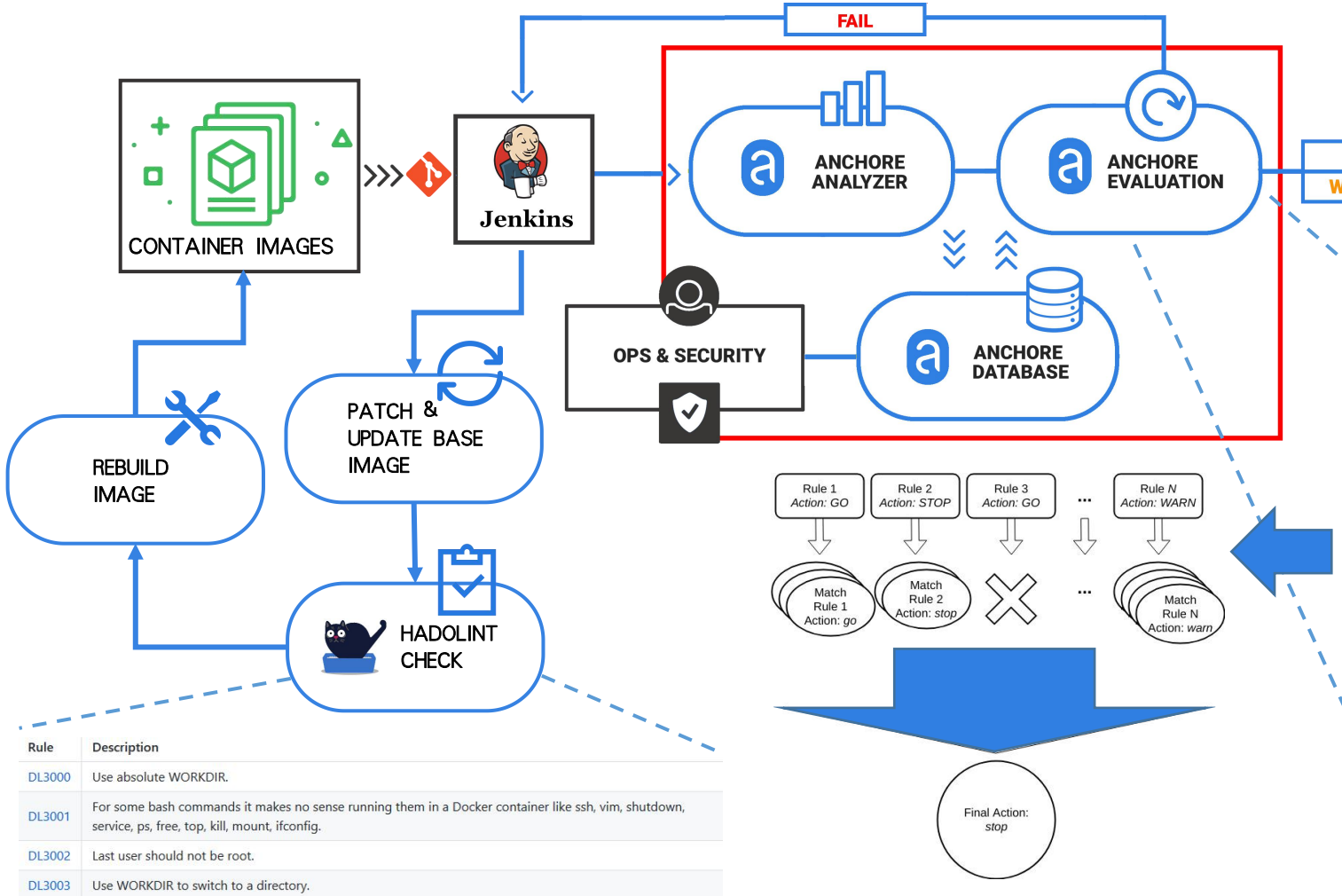


Features:

- Deep image inspection
- Easy Jenkins integration
- Continuously monitoring
- Policy-based evaluation

Image Analysis Workflow

"Scan images for vulnerabilities, misconfigurations and enforce through policy"



Rule	Description
DL3000	Use absolute WORKDIR.
DL3001	For some bash commands it makes no sense running them in a Docker container like ssh, vim, shutdown, service, ps, free, top, kill, mount, ifconfig.
DL3002	Last user should not be root.
DL3003	Use WORKDIR to switch to a directory.

```
{
  "name": "DefaultPolicy",
  "version": "1_0",
  "comment": "Policy for basic checks",
  "id": "policy1",
  "rules": [
      {
        "action": "STOP",
        "gate": "vulnerabilities",
        "id": "rule1",
        "params": [
          { "name": "package_type", "value": "all" },
          { "name": "severity_comparison", "value": ">=" },
          { "name": "severity", "value": "medium" }
        ],
        "trigger": "package"
      }
  ]
}
```

Vulnerability Report

Policy | Security

Common Vulnerabilities and Exposures (CVE) List

Show 100 entries Search:

Tag	CVE ID	Severity	Vulnerability Package	Fix Available	URL
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2018:2181	High	gnupg2-2.0.22-4.el7	0:2.0.22-5.el7_5	https://access.redhat.com/errata/RHSA-2018:2181
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2018:1649	High	java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4	1:1.8.0.171-8.b10.el7_5	https://access.redhat.com/errata/RHSA-2018:1649
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0775	High	java-1.8.0-openjdk-1.8.0.161-0.b14.el7_4	1:1.8.0.212.b04-0.el7_6	https://access.redhat.com/errata/RHSA-2019:0775
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2018:1649	High	java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4	1:1.8.0.171-8.b10.el7_5	https://access.redhat.com/errata/RHSA-2018:1649
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0775	High	java-1.8.0-openjdk-devel-1.8.0.161-0.b14.el7_4	1:1.8.0.212.b04-0.el7_6	https://access.redhat.com/errata/RHSA-2019:0775
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2018:1649	High	java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4	1:1.8.0.171-8.b10.el7_5	https://access.redhat.com/errata/RHSA-2018:1649
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0775	High	java-1.8.0-openjdk-headless-1.8.0.161-0.b14.el7_4	1:1.8.0.212.b04-0.el7_6	https://access.redhat.com/errata/RHSA-2019:0775
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0679	High	libssh2-1.4.3-10.el7_2.1	0:1.4.3-12.el7_6.2	https://access.redhat.com/errata/RHSA-2019:0679
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2018:1700	High	procps-ng-3.3.10-16.el7	0:3.3.10-17.el7_5.2	https://access.redhat.com/errata/RHSA-2018:1700
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0710	High	python-2.7.5-58.el7	0:2.7.5-77.el7_6	https://access.redhat.com/errata/RHSA-2019:0710
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0710	High	python-libs-2.7.5-58.el7	0:2.7.5-77.el7_6	https://access.redhat.com/errata/RHSA-2019:0710
159.138.11.6:10001/onap/clamp-dashboard-logstash:latest	RHSA-2019:0049	High	systemd-219-42.el7_4.6	0:219-62.el7_6.2	https://access.redhat.com/errata/RHSA-2019:0049

Image Vulnerabilities Countermeasures

Auditing Docker Images: Use vulnerability management tools that are specifically designed for containers to continuous scan your images for vulnerabilities, malware, and other security issues.

Policy-driven enforcement: Adopt policy-driven enforcement to create “quality gates” to ensure that only images that meet certain vulnerability and configuration policies are allowed to progress.

Establish a set of trusted images and only permit these images to be run in your environments.

Reference

[1] https://scan.coverity.com/

[2] https://blog.aquasec.com/container-security-vulnerabilities

[3] https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers


ONAP
OPEN NETWORK AUTOMATION PLATFORM