



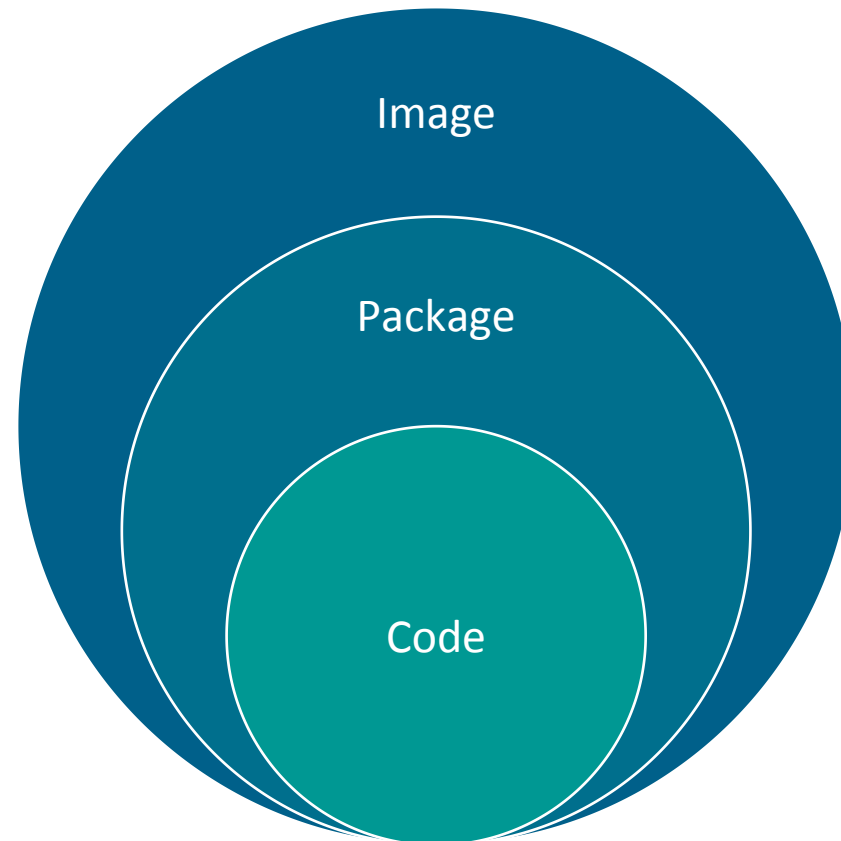
Experience Sharing of Trustworthiness Improvement In ONAP Development

Jing Lu
Huawei Technologies co.

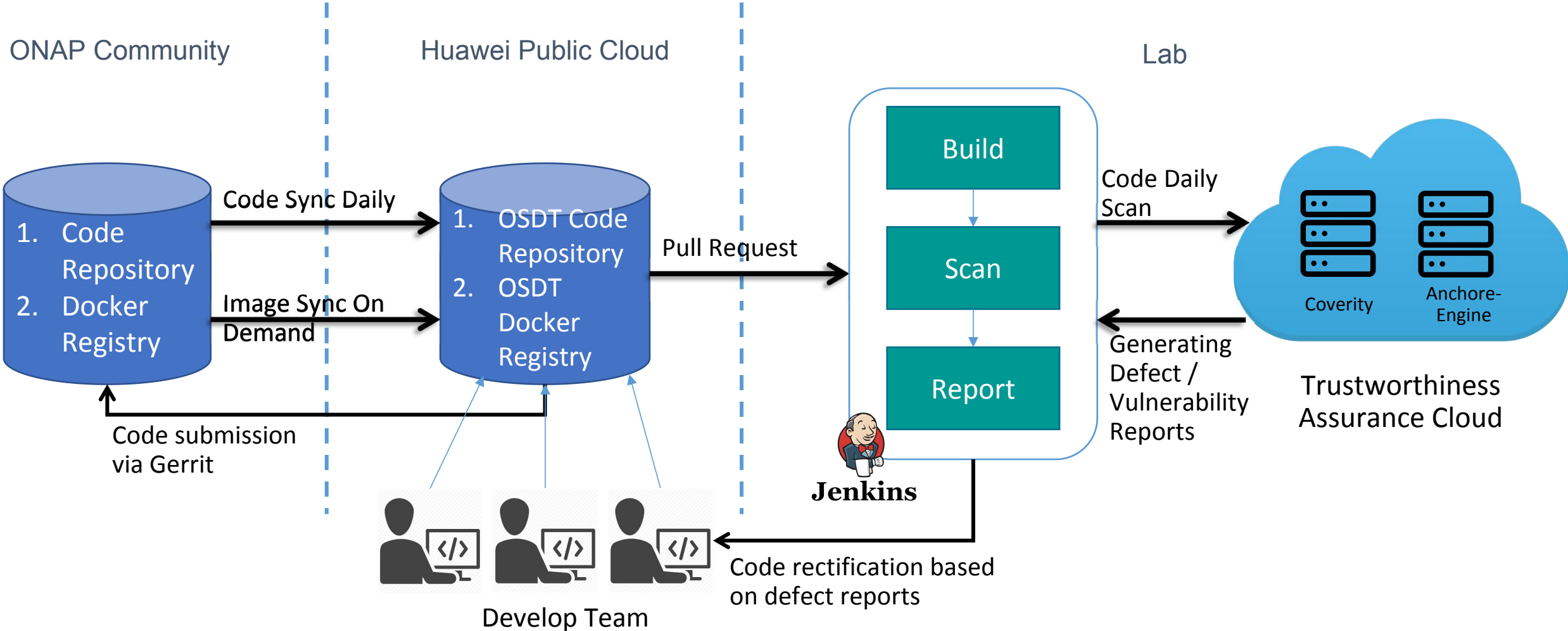
June , 2019

Focus Area

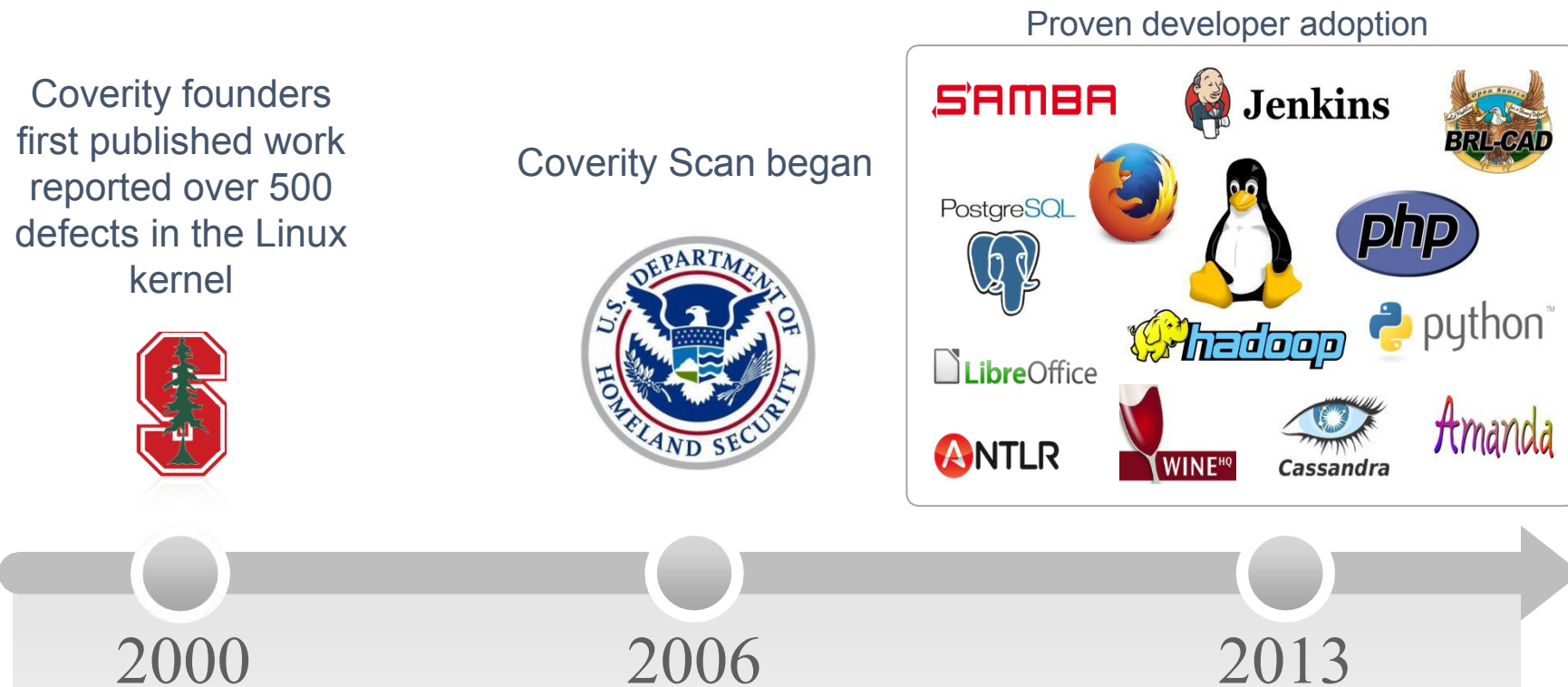
We focus on



Development Workflow Overview



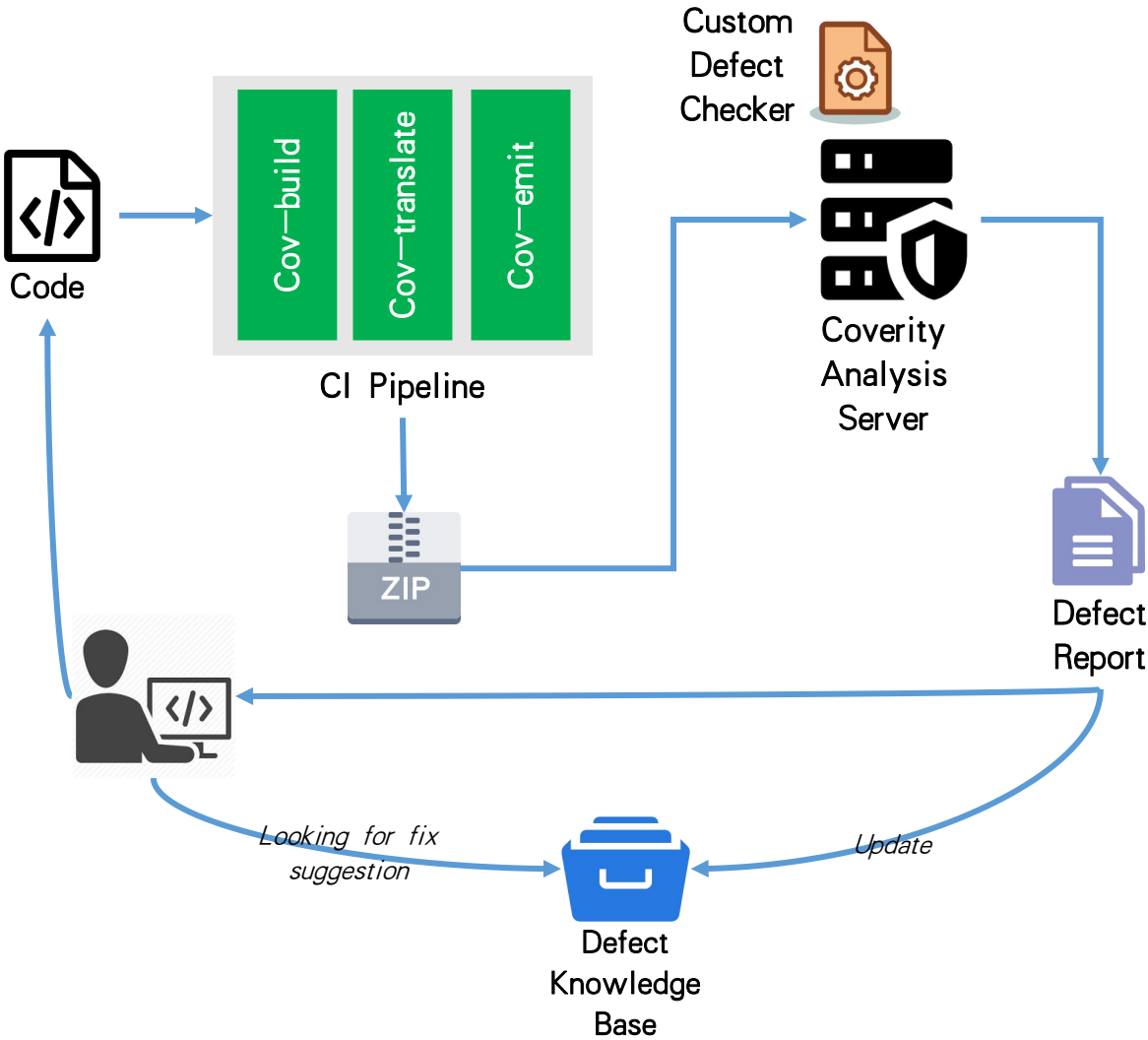
Free cloud-based service for the open source community



Over **600** projects and **300M** lines of code
Over **45,000** defects fixed by the community

Source: [1]

Pipeline & Defect Report



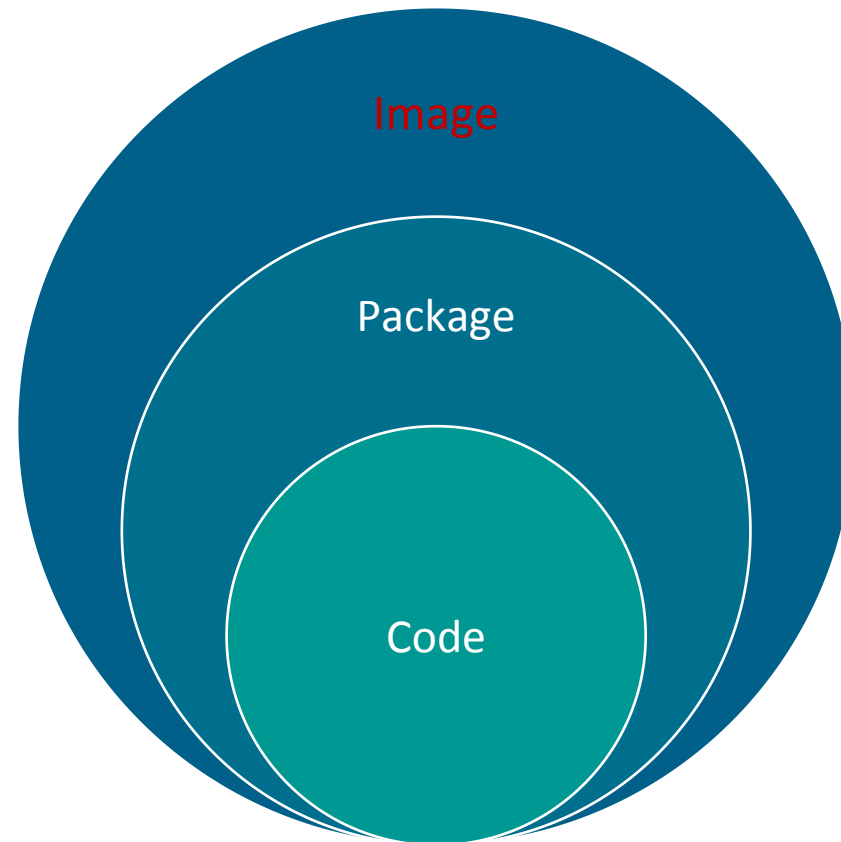
CID	Type	Impact	Status	First Detected	Owner	Classification	Severity	Action	Component	Category	File
332937	Dereference null return	Medium	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Null pointer dereferenc	/bpmn/mso-infrastructure-bpm_mmon/FalloutHand
332936	Unsafe dependence o	Medium	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	API usage errors	/mso-catalog-db/src/main/java.../ModuleCustomiz
332935	Explicit null dereferenc	Medium	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Null pointer dereferenc	/bpmn/mso-bpmn-tasks/src/main...GenericVnfHealthC
332934	Explicit null dereferenc	Medium	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Null pointer dereferenc	/bpmn/mso-bpmn-tasks/src/mai...pctasks/AppRunT
332933	Resource leak on an e	Low	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Exceptional resource le	/bpmn/mso-bpmn-tasks/src/test.../so/BaseIntegrator
332932	Resource leak	High	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Resource leaks	/bpmn/mso-infrastructure-bp...bpmn/common/BPM
332931	Useless call	Medium	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Incorrect expression	/bpmn/mso-bpmn-tasks/src/test.../ModuleResource
332930	Unguarded read	Medium	New	02/20/19	Unassigned	Unclassified	Unspecified	Undecided	Other	Concurrent data acces	/asdc-controller/src/main/javal.../ps/asdcUtil/YamlE


```

187     }
188     return xml;
189 }
190
191 @Test
192 public void msoFalloutHandlerWithNoNotificationurlNoRequestId() throws Exception {
193     1. returned_null: getEnclosingMethod returns null (checked 2 out of 4 times).
194     A1. example_checked: Example 1: getEnclosingMethod has its value checked in bytecode method com.fasterxml.jackson.databind.util.ClassUtil.hasEnclosingMethod(java.lang.Class).
195     B1. example_checked: Example 2: getEnclosingMethod has its value checked in bytecode method n1.jqno.equalsverifier.internal.lib.bytebuddy.description.type.TypeDescription.ForLoadedType.getEnclosingMethod().
196     CID 332937 (#1 of 1): Dereference null return value (NULL_RETURNS)
197     2. null_method_call: Calling a method on null object (this.new org.onap.so.bpmn.common.FalloutHandlerIT.2()).getClass().getEnclosingMethod().
198     String method = getClass().getSimpleName() + "." + new Object() {
199     }.getClass().getEnclosingMethod().getName();
200     logger.debug("STARTED TEST: " + method);
201     //Setup Mocks
202     setupMocks();
203     //Execute Flow
204     executeFlow(gMsoFalloutHandlerWithNoNotificationurlNoRequestId());
205     //Verify Error
206     String FH_ResponseCode = BPMNUtil.getVariable(processEngine, "FalloutHandler", "FH_ResponseCode");
207     Assert.assertEquals("200", FH_ResponseCode);
208     Assert.assertTrue((boolean) BPMNUtil.getRawVariable(processEngine, "FalloutHandler", "FH_SuccessIndicator"));
209 }
210
211 public String gMsoFalloutHandlerWithNoNotificationurlNoRequestId() {
212     //Generated the below XML from ActiveVOS moduler ... Using the generate sample XML feature in ActiveVOS

```

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.

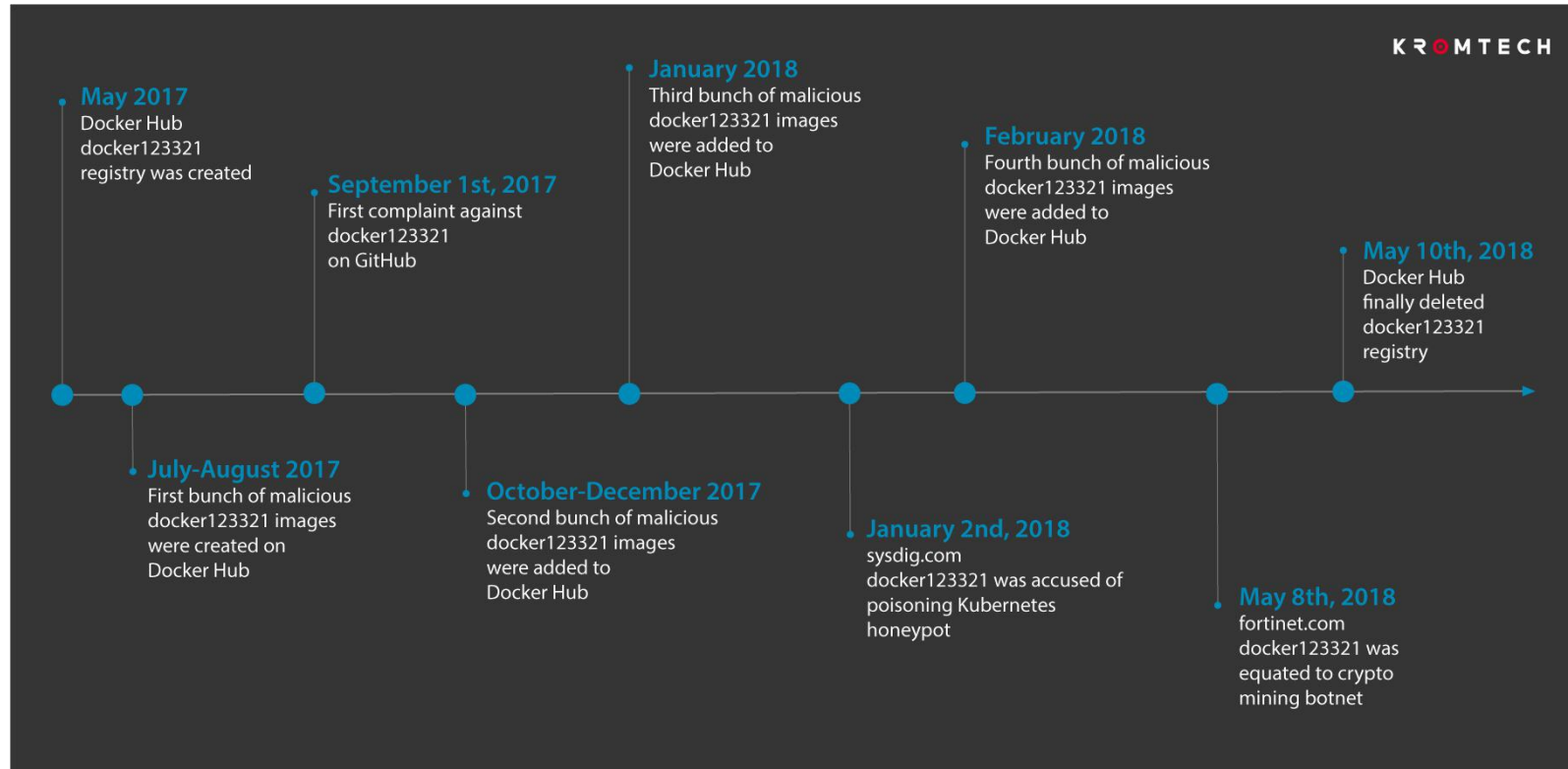
For containerized applications, we should take proactive measures to reduce their proliferation.



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



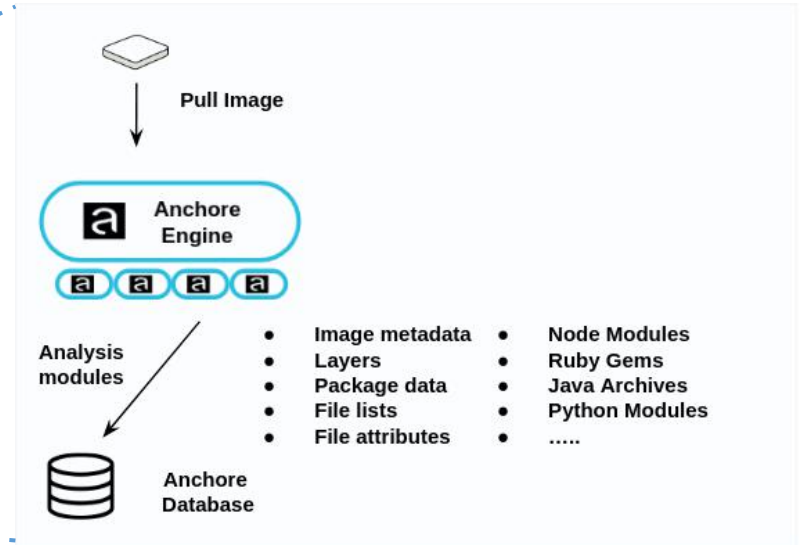
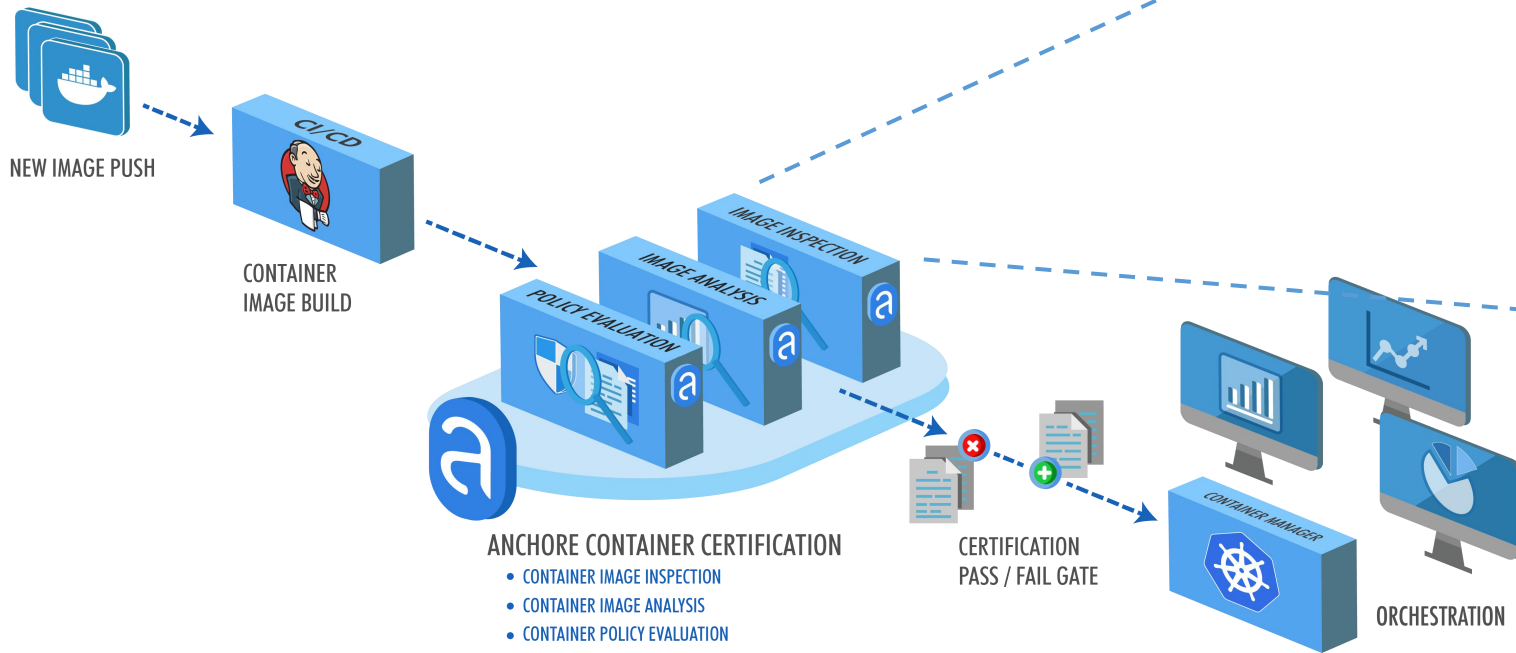
- 17 malicious Docker images that have been backdoored and used to install reverse shells and crypto-currency miners were downloaded collectively **5 million times** in a year
- Malware included crypto mining software, netting **~\$90,000** of Monero

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.

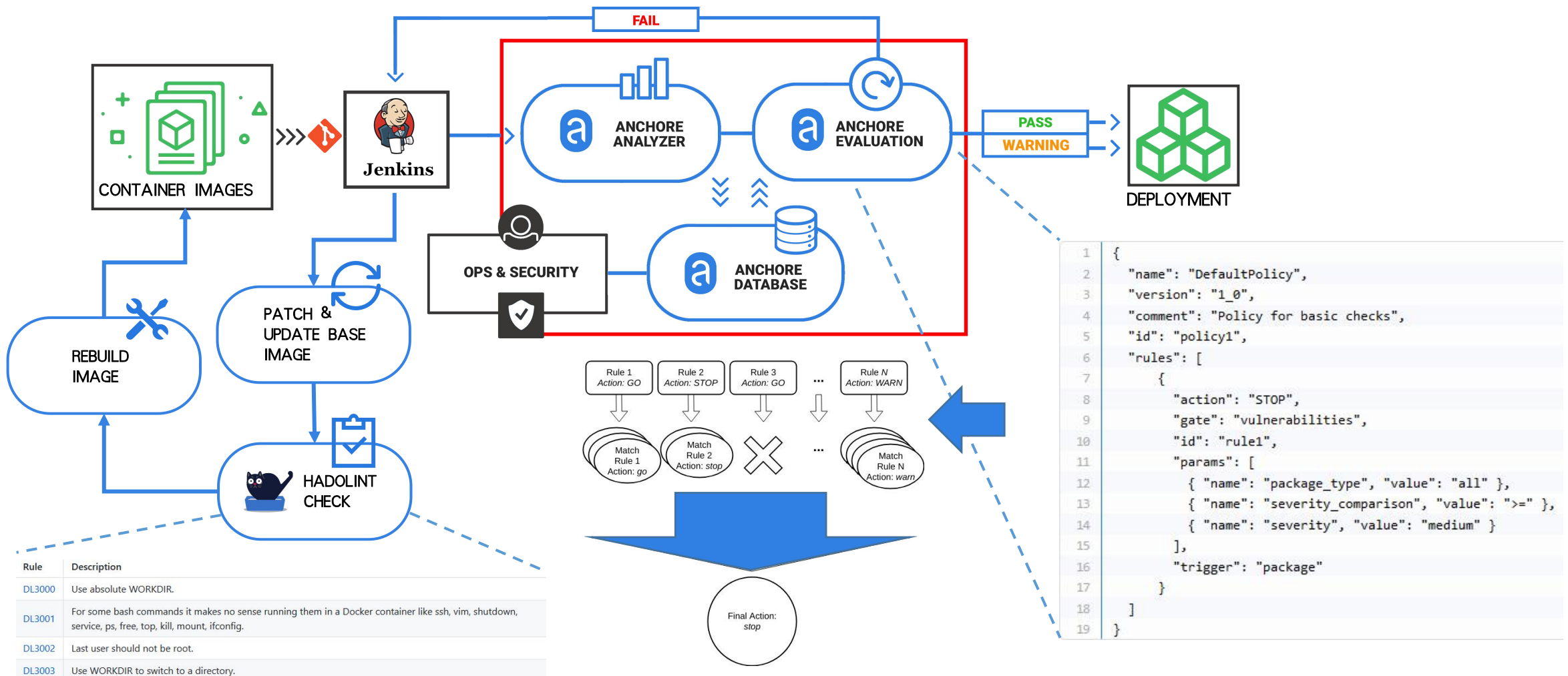


Features:

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

Image Analysis Workflow

“Scan images for vulnerabilities, misconfigurations and enforce through policy”



Vulnerability Report

Policy

Security

Common Vulnerabilities and Exposures (CVE) List

Show 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 continuously 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