

Intrusion Detection for Containers

Shane Lawrence Shopify

Intro to "Intro to <u>Intro to Falco</u>"

shanelawrence.info

Present

- Falco end user
- Infrastructure Security @Shopify

Past

- Intrusion Detection Systems (IDS)
- Security Information and Event Management (SIEM)

I. Intro

Intro to Intro to Falco

- Intro
- Deployment
- Technical Challenges
- Use Cases
- Next Steps

see also: "Open Source Intrusion Detection for Containers"

Not Intro to Falco:

new wave

1.14	Taico		× 🌢 d	
	Q All 🔓 Images 🗈 Videos	⊙ Maps III News I Mor	e Settings Tools	
	About 43,100,000 results (0.59 seconds)			
	en wikipedia.om) wiki) Falco (m	usician) *		
	Falco (musician) - Wikipedia			
	Johann Hölzel (German: []o:han	hoefts(); 19 February 1957 - 6 Feb	ruary 1998), better known	
	by his stage name Falco, was an	Austrian singer and songwriter.		
	Years active: 1977–1998 Genres: New wave; Neue Deutsc	he Welle; ro Labels: Sony; EP	cass; piano; bass guitar; gu Al; Warner; A&M	
	Rock Me Amadeus - Falco 3 - Fal	co discography · Der Kommissar		
	Videos			Falco <
				Austrian singer
				Available on
	1245 VERS			YouTube
	Falco - Rock Me	Falco - Der Kommissar	Falco - Jeanny (Official	> Spotfy
	Amadeus (Official Video) ((Onicial Video)	Video)	9 YouTube Music
				 More music services
	FalcoVEVO	FalcoVEVO	FalcoVEVO	Johann Hölzel, better known by his stage name Falco, was an
	YouTube - Oct 25, 2009	YouTube - Mar 24, 2017	YouTube - Oct 25, 2009	Austrian singer and songwriter. Falco had several international hits,
				"Rock Me Amadeus", "Der Kommissar", "Vienna Galing", "Jeanny", "The Sound of Musik", "Coming Home", and posthumously "Out of
	People also ask			the Dark". Wikipedia
	Million and have been added for	What ever happened to Falco?		Born: February 19, 1967, Vienna, Austria
	what ever happened to hai			Died: February 6, 1998, Dominican Republic
	Is Falco dead?		~	Full name: Johann Hötzel
				Music groups: Drahdiwaberl, Hallucination Company (1977 –



Not Intro to Falco:

- new wave
- all of the other things you should be doing to protect your clusters

Security Approach: Prevention

Kubernetes

- disable old APIs, unused features
- metadata proxy
- kubelet bootstrap
- Role Based Access Control
- seccomp & apparmor profiles
- network policies

In-house

- github.com/Shopify/kubeaudit
- security-auditors











50+

clusters





thousand

services

170+ thousand requests per second (peak)

The case for monitoring

Misconfiguration

- insecure API endpoints
- overprivileged roles
- weak security context
- assumptions about safety/identity

Software supply chain

- deliberate backdoors
- bugs in dependencies
- typo, tag hijacking

Unmitigated Vulnerabilities

- Heartbleed CVE-2014-0160
- Spectre v1 CVE-2017-5753
- Spectre v2
 CVE-2017-5715
- Meltdown CVE-2017-5754

• CVE-2019-5736 runc Container Escape

- CVE-2018-15664 Symlink directory traversal
- CVE-2018-1002105 Unauthenticated Remote Privilege Escalation
- CVE-2020-8558 Localhost Boundary Bypass

The case for Falco

- low-level
- container-aware
- Kubernetes-aware
- ebpf
- open source
- CNCF project

II. Deployment

Deploying Falco

The easiest way:

- 1. Get Falco's chart configuration.
- 2. Configure Falco to use the correct driver.
- 3. Add the repo.
- 4. Install falco.

Deploying Falco

A better way:

- validate rules before deploying
- pre-build the driver
- build your own image
- fine-tune the rules

III. Technical Challenges

Modifying rules

Challenge:

• update rules quickly without disruption

Potential solution:

• use Helm (and rules2helm)

Concerns:

- slow
- missed or duplicate events

Modifying rules

Challenge:

• update rules quickly without disruption

Scalable solution:

- ConfigMap -> volume -> /etc/falco
- inotifywait
- kill -HUP

Challenge:

• Falco alerts on normal behavior.

Solution:

- Add events to an allowlist.
- Be as specific as possible.

Challenge:

• Falco alerts on normal behavior.

Example problem:

• Falco flags itself as suspicious.

k8s nod name	proc cmdline		
Kos.pou.name	proc.cmunne		
falco-cq4m6	container:e854bc6a844b		
container.id e854bc6a844b	container.image.repository		
20040000440	Talcoseculity/Talco		
container.image.tag	k8s.ns.name		
0.24.0	falco		
rule	priority		
Launch Privileged Container	Notice		
time			
2020-07-27 05:20:29.610488 +0000 UTC			

Challenge:

• Falco alerts on normal behavior.

Example solution:

• Add the missing repository to the allowlist.

```
# falco_rules.local.yaml
- list: user_privileged_images
items: [
    gke.gcr.io/netd-amd64, gke.gcr.io/gke-metadata-server,
    gke.gcr.io/kube-proxy, falcosecurity/falco
]
- macro: user_privileged_containers
condition: (container.image.repository endswith sysdig/agent or
    container.image.repository in (user_privileged_images))
```

Challenge:

• Falco generates critical alerts when it drops syscall events.

(a small number of drops is expected)

Example Problem:

7:04	Falco internal: syscall event drop. 1 system n_drops_bug 0	n calls dropped in last second. n_drops_pf 1			
	n_evts 8207	ebpf_enabled 1			
	n_drops 1	n_drops_buffer O			
	rule Falco internal: syscall event drop	priority Critical			
	time 2020-07-23 23:04:19.478095127 +0000 UTC				
	https://github.com/falcosecurity/falcosidekick				

Challenge:

• Falco generates critical alerts when it drops syscall events.

(a small number of drops is expected)

Example Solution:

- Change the alert action to log only.
- Report the events less frequently.

```
# falco.yaml
syscall_event_drops:
    actions:
        - log
    # 1/60/60=once per hour
    rate: 0.00027777777778
max_burst: 1
```

IV. Use Cases

Suspicious shell access in container

Demo

Demo: Attacker running commands in container

keti <falco_pod>/bin/bash

apt-get install <package_name>

3:01:32.550604838: Error Package management process launched in container user=root command=apt container_id=e37bcea88845 ontainer_name=k8s_falco_falco-4w7d9_falco_0aae63a0-9ef9-41d9-8bfe- 7ee38298ec9_0 image=falcosecurity/falco:0.24.0) k8s.ns=falco k8s.pod=falco-4w7d9 ontainer=e37bcea88845 k8s.ns=falco k8s.pod=falco-4w7d9 ontainer=e37bcea88845					
ontainer.image.repository	container.image.tag				
alcosecurity/falco	0.24.0				
ontainer.name 8s_falco_falco-4w7d9_falco_0aae63a0-9ef9-41d9-8bfe-c7ee38298ec9_0					
8s.ns.name	k8s.pod.name				
alco	falco-4w7d9				
roc.cmdline	container.id				
pt	e37bcea88845				
iser.name	rule				
oot	Launch Package Management Process in				
	Container				
riority					
irror					
ime					
020-07-23 23:01:32.550604838 +0000 UTC					

Falco APP 7:00 PM

23:00:36.625246794: Notice A shell was spawned in a container with an attached terminal (user=root k8s.ns=falco k8s.pod=falco-4w7d9 container=e37bcea88845 shell=bash parent=runc cmdline=bash terminal=34816 container_id=e37bcea88845 image=falcosecurity/falco) k8s.ns=falco k8s.pod=falco-4w7d9 container=e37bcea88845 container.image.repository proc.name falcosecurity/falco bash container.id k8s.ns.name e37bcea88845 falco k8s.pod.name proc.cmdline falco-4w7d9 bash proc.pname user.name runc root rule priority Terminal shell in container Notice time 2020-07-23 23:00:36.625246794 +0000 UTC

https://github.com/falcosecurity/falcosidekick

https://github.com/falcosecurity/falcosidel

Instance metadata service

Demo

Instance metadata service

/ \$ wget -q0- --header 'Metadata-Flavor: Google' 169.254.169.254/computeMetadata/v1/instance/attributes/
cluster-location

cluster-name

cluster-uid

can only get things you should be allowed to access

/ \$ wget -q0- --header 'Metadata-Flavor: Google' 169.254.169.254/computeMetadata/v1/instance/service-accounts/default/
aliases
email
identity
scopes
token

/ \$ wget -q0- --header 'Metadata-Flavor: Google' 169.254.169.254/computeMetadata/v1/instance/service-accounts/default/email
falco-demo-test-app@shopify-codelab-and-demos.iam.gserviceaccount.com/
can only get a token for this app's service account:

Instance metadata service (hostNetwork)

Demo

Use case: instance metadata service (hostNetwork)

Falco APP 12:02 AM 04:02:18.323169867: Notice Outbound c service (command=wget -qOheader Me 169.254.169.254/computeMetadata/v1/i connection=10.104.204.46:56316->169.2 k8s.pod=test-hostnetwork container=d9b app k8s.pod=test-hostnetwork container=d9b k8s.pod=test-hostnetwork container=d9b k8s.pod=test-hostnetwork container=d9b k8s.pod.name test-hostnetwork proc.cmdline wget -qOheader Metadata-Flavor: Goo 169.254.169.254/computeMetadata/v1/i container.id d9b4c3cddd6d	onnection to cloud instance metadata etadata-Flavor: Google nstance/service-accounts/default/email 254.169.254:80 k8s.ns=test-app 4c3cddd6d image=alpine:latest) k8s.ns= d9b4c3cddd6d k8s.ns=test-app 4c3cddd6d gle nstance/service-accounts/default/email container.image.repository alpine			
container.image.tag latest fd.name 10.104.204.46:56316->169.254.169.254:80				
k8s.ns.name test-app	rule Contact cloud metadata service from container			
priority Notice time 2020-07-24 04:02:18.323169867 +0000 https://github.com/falcosecurity/falcosidekick	UTC			

test-

Use case: instance metadata service (privileged)

• provider needs to redirect to proxy

• generally this is done with the network fabric

(e.g. iptables rule points metadata.google.internal to the proxy)

• privileged container can just change the rules

Use case: CVE-2020-8557

Demo

V. Next Steps

Managing alerts

Output

- visible
- searchable
- aggregated
- annotated

Normalization

- prompt
- simple

Volume

• manageable



Reaching out

- #falco on Kubernetes Slack
- weekly community call
- GitHub Issue
- Pull Request 🏆

Thank you!

shanelawrence.info

shopify.com/careers

engineering.shopify.com

github.com/falcosecurity

falco.org

slack.k8s.io #falco