




Falco gestionado con Sysdig



Soporte empresarial de Falco con Sysdig

Crear una cuenta de prueba

- <https://sysdig.com/company/free-trial/>
- Gratuita 30 días
- No es necesario proporcionar tarjeta de crédito
- Activa de inmediato tras validar email

Runtime Policies

+ Add Policy

High
Medium
Low
Info

		Create/Modify Configmap With Private Credentials Entire Infrastructure	Updated 7 days ago 1 rules Notify Only
		Ingress Object Without TLS Cert Created Entire Infrastructure	Updated 7 days ago 1 rules Notify Only
		Launch Suspicious Network Tool in Container Entire Infrastructure	Updated 7 days ago 1 rules Notify Only
		Unexpected outbound connection destination Entire Infrastructure	Updated 7 days ago 1 rules Notify Only
		Sensitive Info Exfiltration kubernetes.namespace.name = "store-frontend"	Updated 6 hours ago 1 rules Notify Only Capture 25 secs
		Terminal shell in container kubernetes.pod.label.terminal_shell_in_container = "allowed"	Updated 7 hours ago 1 rules Notify Only Capture 30 secs
		Disallowed K8s Activity Entire Infrastructure	Updated 7 days ago 3 rules Notify Only
		Inadvised K8s Activity Entire Infrastructure	Updated 7 days ago 5 rules Notify Only
		Create Privileged Pod Entire Infrastructure	Updated 7 days ago 1 rules Notify Only
		Suspicious K8s User Activity Entire Infrastructure	Updated 7 days ago 1 rules Notify Only
		Inadvised K8s User Activity	Updated 7 days ago

Terminal shell in container

High Severity


Description
A shell was spawned by a program in a container with an attached terminal.

Scope
kubernetes.pod.label.terminal_shell_in_container = "allowed"


Rules
- rule: Terminal shell in container

Action
Capture 10 secs before, 20 secs after

POLICIES Rules Library + Add Rule				
<input type="text" value="Select Tags"/>				
Rules	Published By	Last Updated	Tags	
All K8s Audit Events	Sysdig 0.6.1	2 months ago	k8s	
Anonymous Request Allowed	Sysdig 0.6.1	2 months ago	k8s	
Apache writing to non allowed directory	Secure UI	7 days ago	filesystem	
Attach to cluster-admin Role	Sysdig 0.6.1	2 months ago	k8s	
Attach/Exec Pod	Sysdig 0.6.1	2 months ago	k8s	
Blacklist commands	Secure UI	7 days ago	filesystem	
Change thread namespace	Sysdig 0.6.1	2 months ago	process	
Change thread namespace (WP)	Secure UI	7 days ago	process	
Clear Log Activities	Sysdig 0.6.1	2 months ago	mitre_defense_evasion file	
ClusterRole With Pod Exec Created	Sysdig 0.6.1	2 months ago	k8s	
ClusterRole With Wildcard Created	Sysdig 0.6.1	2 months ago	k8s	
ClusterRole With Write Privileges Created	Sysdig 0.6.1	2 months ago	k8s	
Contact cloud metadata service from container	Sysdig 0.6.1	2 months ago	container mitre_discovery network	
Contact EC2 Instance Metadata Service From Container	Sysdig 0.6.1	2 months ago	container aws mitre_discovery n	
Contact K8S API Server From Container	Sysdig 0.6.1	2 months ago	container k8s mitre_discovery n	
Create Disallowed Namespace	Sysdig 0.6.1	2 months ago	k8s	
Create Disallowed Pod	Sysdig 0.6.1	2 months ago	k8s	
Create files below dev	Sysdig 0.6.1	2 months ago	mitre_persistence filesystem	



VH



Actions

Containers

☒ Nothing(notify only) ☐ Stop ☐ Pause

Capture

☒

File Name

Terminal shell in container

Storage

Sysdig Secure Storage


10 secs before, 20 secs after the event

Filter

Optional: (e.g. proc.name=cat or proc.name=vi)

Notification Channels

Select notification channel...

 Slack Channel ×

The screenshot displays the Quantika14 security dashboard. On the left is a dark sidebar with navigation icons for Policy Events, Policies, Activity Audit, Captures, Benchmarks, Image Scanning, and a search icon. The main content area is titled 'Policy Events' and 'Entire infrastructure'. It features a 'Browse By Sysdig Monitor ...' dropdown menu. Below this is a list of infrastructure events with columns for event name, count, and status. A detailed view of a 'Terminal shell in container' event is shown on the right, including its timestamp, related resources, severity (High), triggered policy, rule type, and scope details.

Policy Events

Browse By Sysdig Monitor ...

Entire infrastructure

Event Name	Count	Status
> gke-de... e1d0-5sm1	0	
> gke-dem...e1d0-vsb0	0	
> gke-dem...e1d0-zvsn	0	
> ip-10-0-0-116	0	
> ip-172-20-52-124	0	
> ip-172-20-53-31	2	
> ip-172-20-54-83	2	
> ip-172-20-57-15	3	
> ip-192-168..._internal	0	
> ip-192-168..._internal	0	
> kube-bn... -000001c8	0	
> kube-bn... -0000025f	0	

Entire infrastructure

About 5 hours

- Terminal shell in container**
ip-172-20-54-83 > 3b0aaaf01256

About an hour

- Ingress Object Without TLS Cert Created**
ip-172-20-53-31

About 2 hours

- Create/Modify Configmap With Private Cred...**
ip-172-20-53-31

About an hour

- 1 policies triggered: Access Cryptomining N...**
ip-172-20-57-15 > d5b48b83e7f7

About 11 hours

- Terminal shell in container**
ip-172-20-54-83 > 3b0aaaf01256

About 4 hours

Policy Event Details

When
3/30/2020 1:18:03.583 pm (5 hours ago)

Related Resources
Capture and commands will cover 10 minutes around the time of the event.

VIEW CAPTURES **ACTIVITY AUDIT**

Severity
High

Triggered Policy
Terminal shell in container

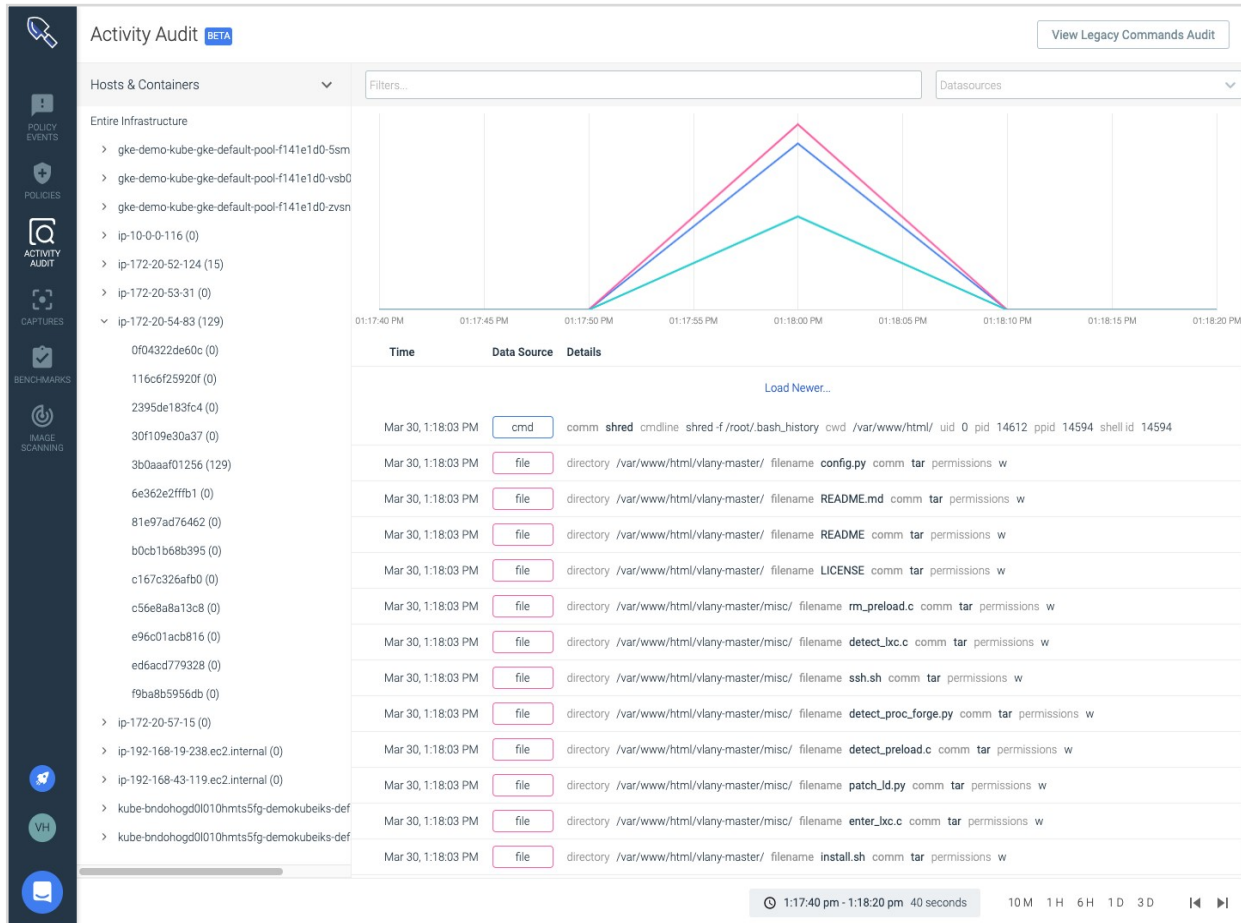
Triggered Rule Type
Ico

Scope
1. host.hostName: ip-172-20-54-83
2. container.id: 3b0aaaf01256

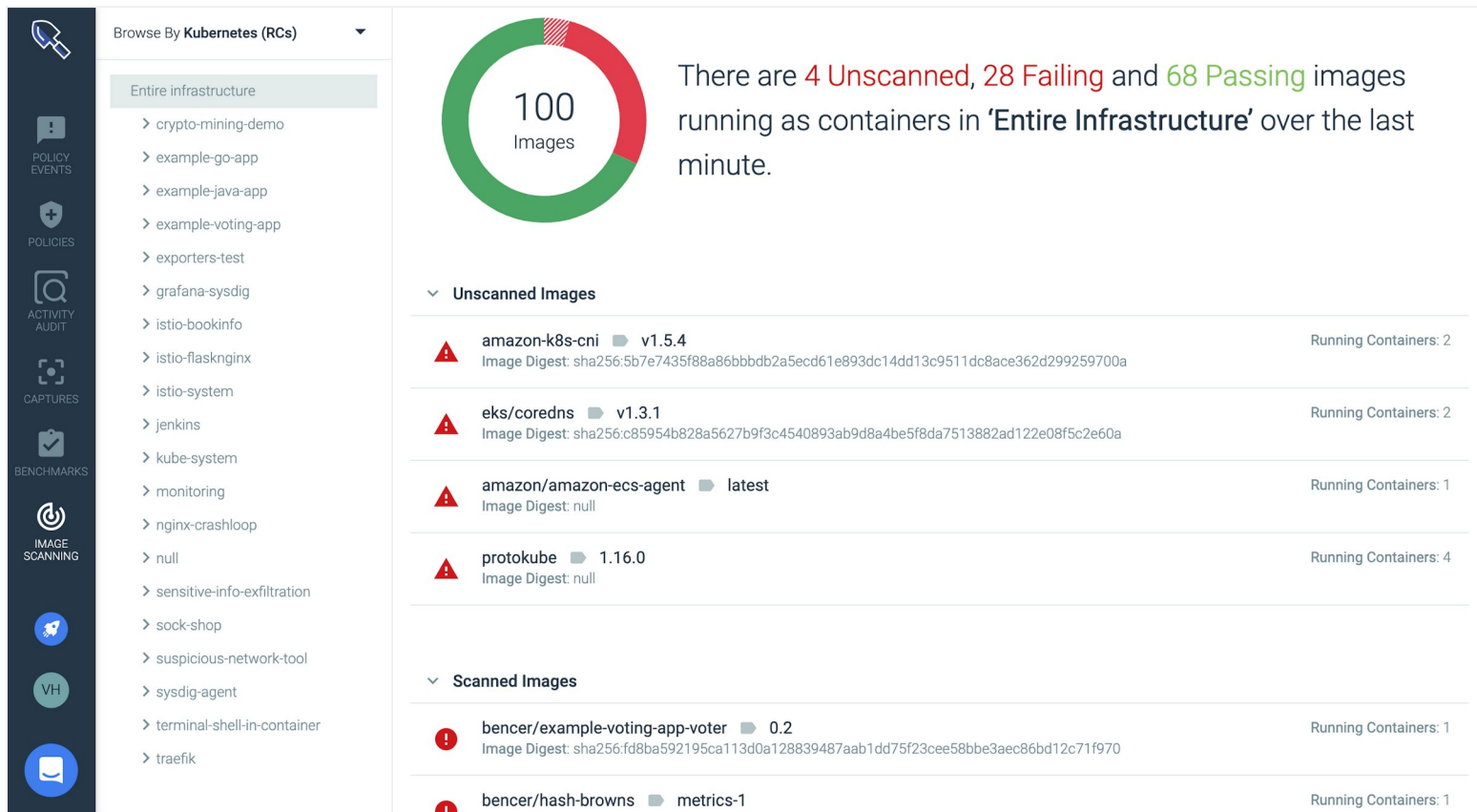
Host
Hostname: ip-172-20-54-83
MAC: 02:f2:bf:a5:75:c1

Container
ID: 3b0aaaf01256
Name: k8s_store-frontend-ping-php_store-frontend-ping-php-54664d4f44-g2t6c_terminal-shell-in-container_241e0cb0-05e4-47f7-97c1-c8a1bf9f7963_0
Image: sysdiglabs/workshop-forensics-1-phpping@sha256:74941e12721385c8f3d5b9438294eae9050087badfc8c4c9e67

LIVE: 3/29 5:49:50 PM - 3/30 5:49:50 PM (1 D) 10 M 30 M 1 H 6 H 1 D 3 D







BENCHMARKS
Results > Kubernetes Compliance Check

Download CSV

HIGH RISK

33
Fail

10
Warn

22
Pass

Completed on
Apr 14, 2020 - 8:00 am

Host Name
00-00-00-00-00-00

00-00-00-00-00-00:4f:18:1f

Kubernetes Master

Remediation
Run the below command (based on the file location on your system) on the master node. For example, `chmod 644 /etc/kubernetes/manifests/kube-apiserver.yaml`

1.1. Master Node Configuration Files

1.2. API Server

1.3. Controller Manager

1.4. Scheduler

1.1.1 Ensure that the API server pod specification file permissions are set to 644 or more restrictive (Scored)

1.1.2 Ensure that the API server pod specification file ownership is set to root:root (Scored)

1.1.3 Ensure that the controller manager pod specification file permissions are set to 644 or more restrictive (Scored)

1.1.4 Ensure that the controller manager pod specification file ownership is set to root:root (Scored)

1.1.5 Ensure that the scheduler pod specification file permissions are set to 644 or more restrictive (Scored)

1.1.6 Ensure that the scheduler pod specification file ownership is set to root:root (Scored)

1.1.7 Ensure that the etcd pod specification file permissions are set to 644 or more restrictive (Scored)

1.1.8 Ensure that the etcd pod specification file ownership is set to root:root (Scored)

1.1.9 Ensure that the Container Network Interface file permissions are set to 644 or more restrictive (Not Scored)

1.1.10 Ensure that the Container Network Interface file ownership is set to root:root (Not Scored)

1.1.11 Ensure that the etcd data directory permissions are set to 700 or more restrictive (Scored)

POLICY EVENTS

POLICIES

ACTIVITY AUDIT

CAPTURES

BENCHMARKS

IMAGE SCANNING

VH