



KubeCon



CloudNativeCon

Europe 2019

Container Forensics :: When your cluster becomes a cluster

Maya Kaczorowski & Ann Wallace, Google Cloud



Maya Kaczorowski

Security PM, Google Cloud

 @MayaKaczorowski



Ann Wallace

Security Global Practice Lead,
Google Cloud

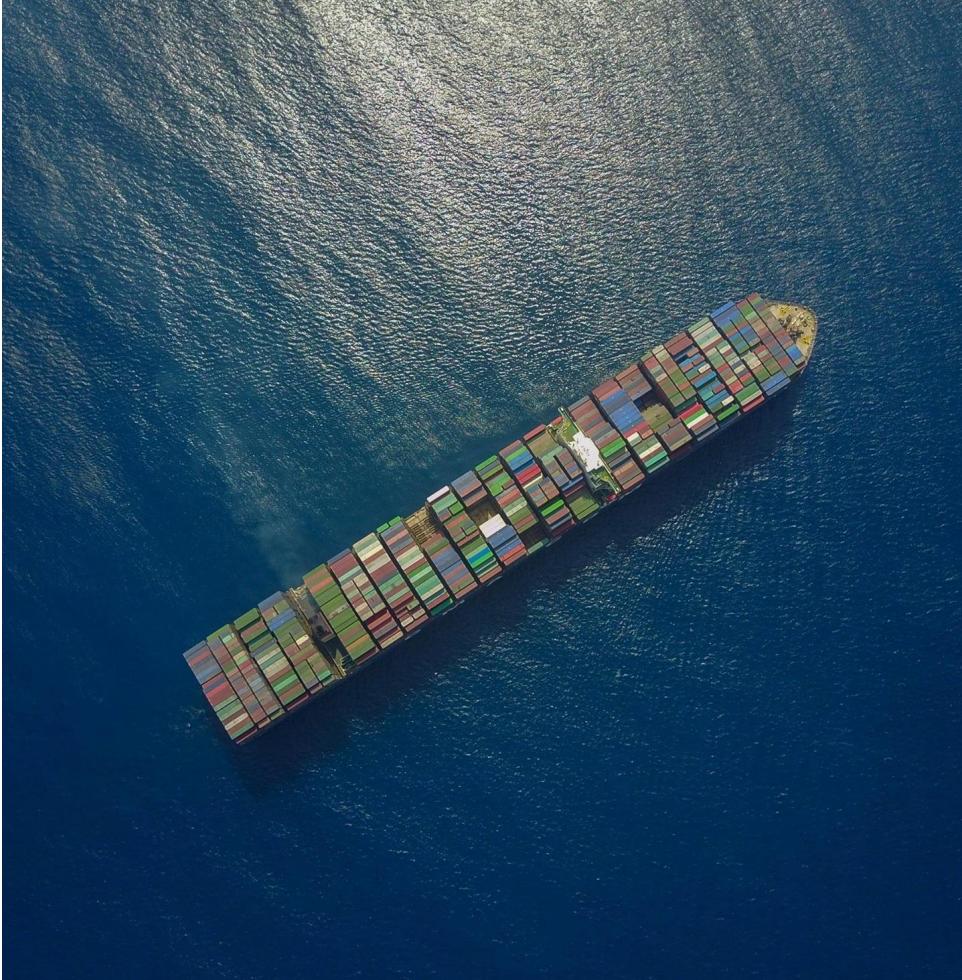
 @AnnNWallace





Container attacks happen

Google Cloud



Threats seen in the wild

	2018	February	May	June		2019	April
Tesla							
Unsecured Kubernetes dashboard with cloud account credentials							
Used to mine cryptocurrency							
Shopify							
Researcher could access and replay kubelet credentials							
Not exploited							
Weight Watchers							
Unsecured Kubernetes dashboard with sensitive data, including credentials							
Not exploited							
Docker Hub							
Public images with embedded cryptocurrency mining malware							
Used to mine cryptocurrency							
Docker Hub							
Database with 190k+ Docker Hub accounts exposed							
Unknown impact							



Security forensics 101

Google Cloud

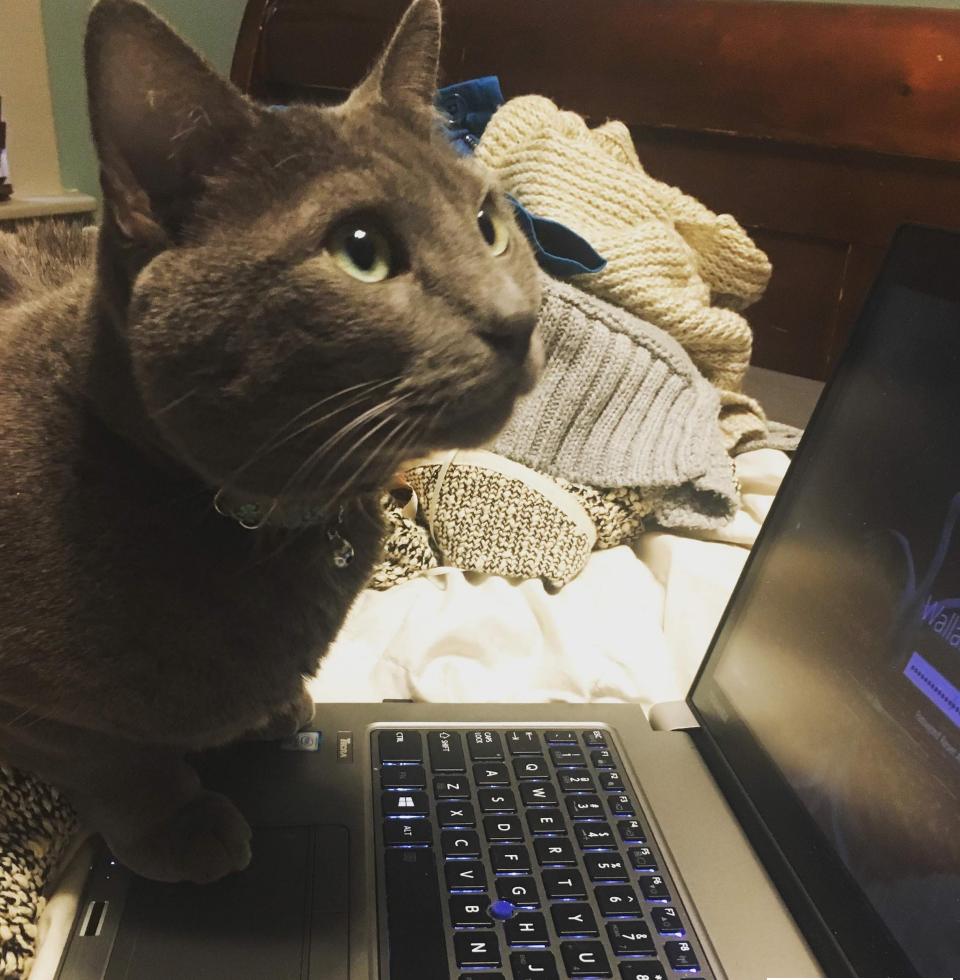
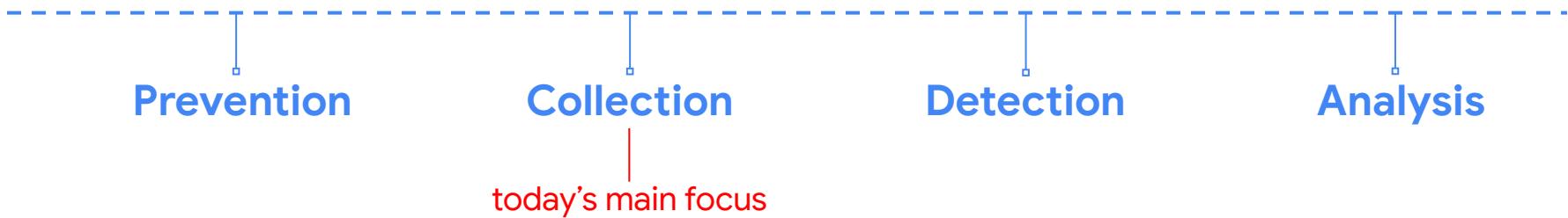
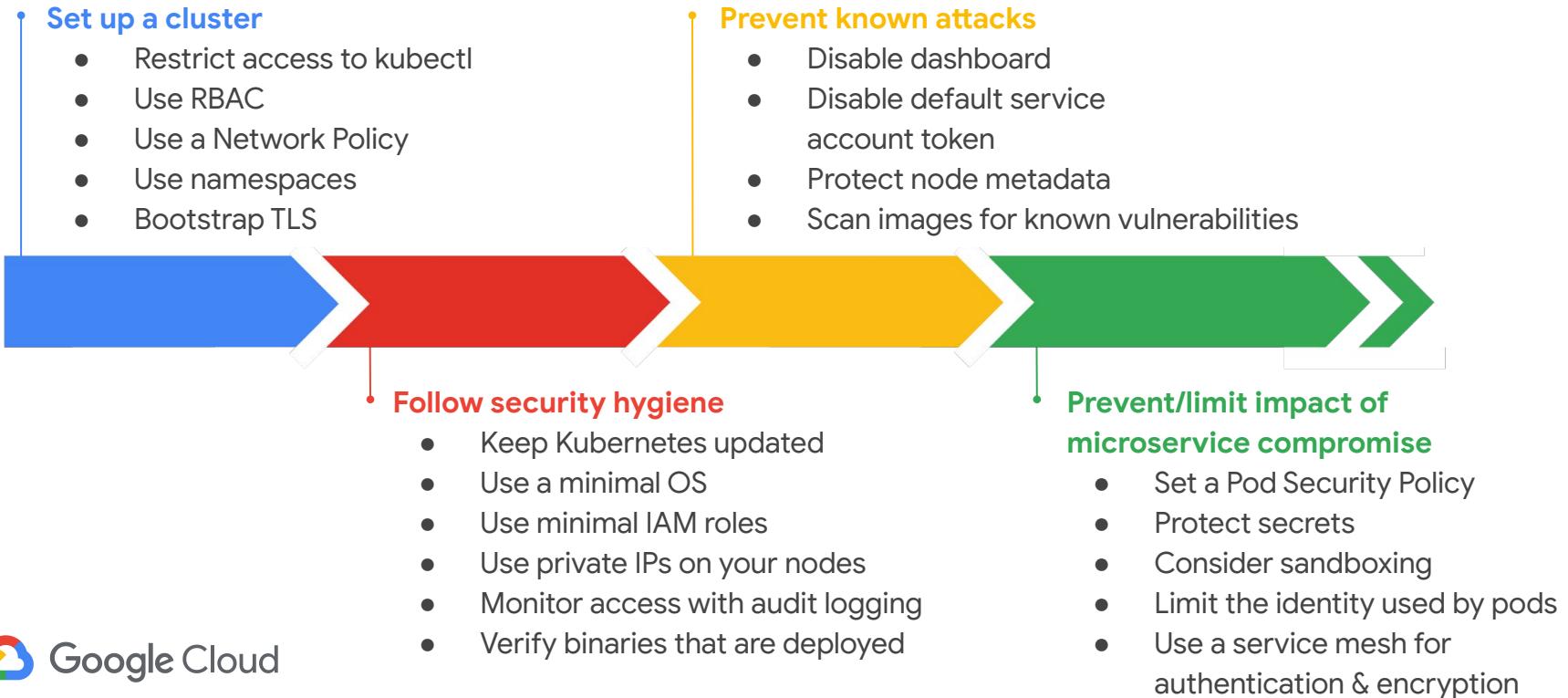


Image by Ann Wallace

Incident preparedness



Prevention



Don't Panic

DO NOT!

(immediately)
terminate and
delete all
nodes,
containers
& disks

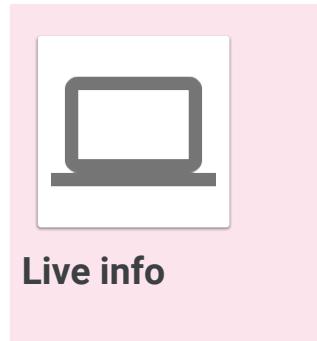
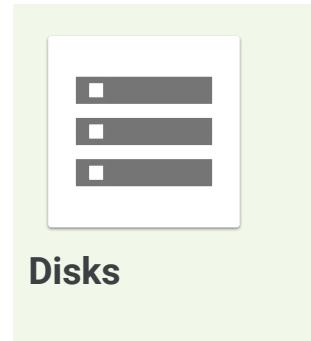
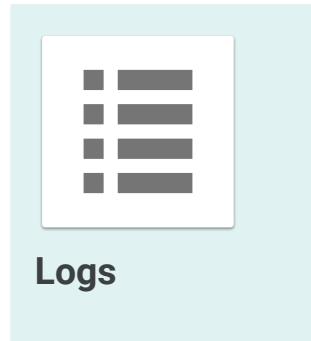
DO NOT!

login to the
server /
container to
see if you can
'track it down'

Collection

How do you
build a story?

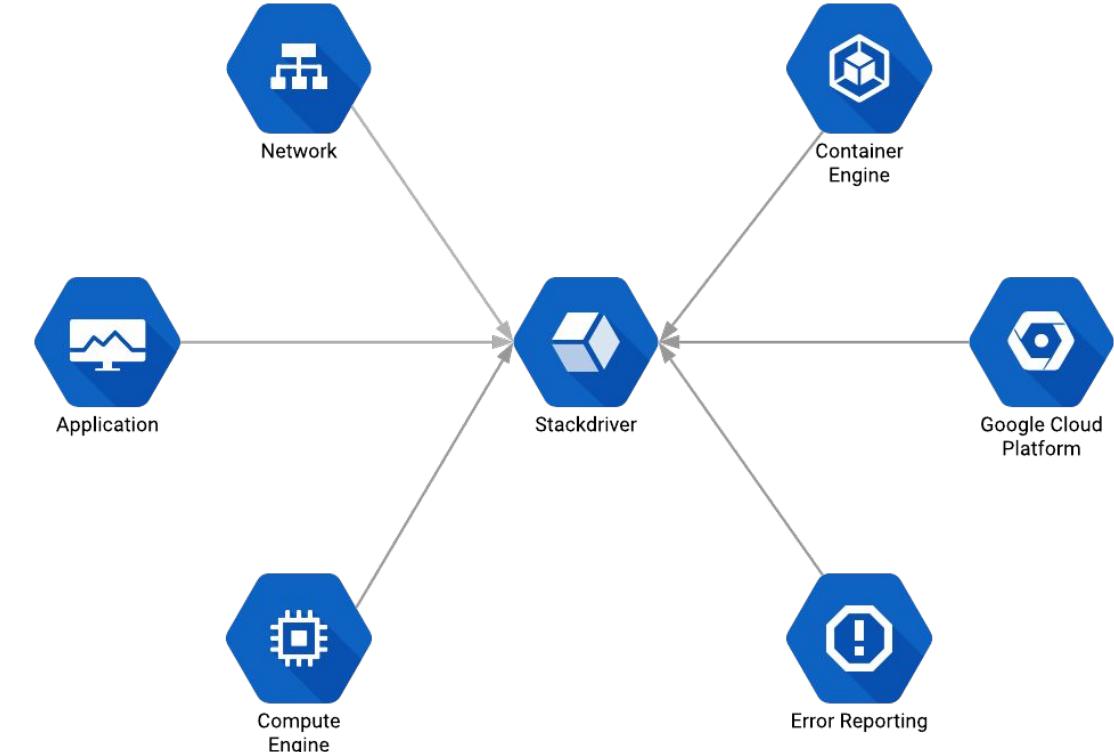
Start by
gathering
artifacts



Logs

Who did what, when
and where?

System
Application
Network
Deployment
Cloud
Container



Disks

Traditional

'Grab the disks' for offline analysis
Takes machine off the network

Cloud

Use cloud APIs to make a snapshot
Can be done transparently

Containers

There is no container snapshot mechanism

Live and Recorded Info

Client agents

What is happening on the system?

Container sidecar

How do you get real time info without logging in?

How do you gather information remotely from multiple systems?

Hope for the best but plan for the worst

Create an incident response plan

Who to contact

What actions to take

How to collect data

Critical systems to keep the business running

Communication plan





Applying forensics to containers

Google Cloud



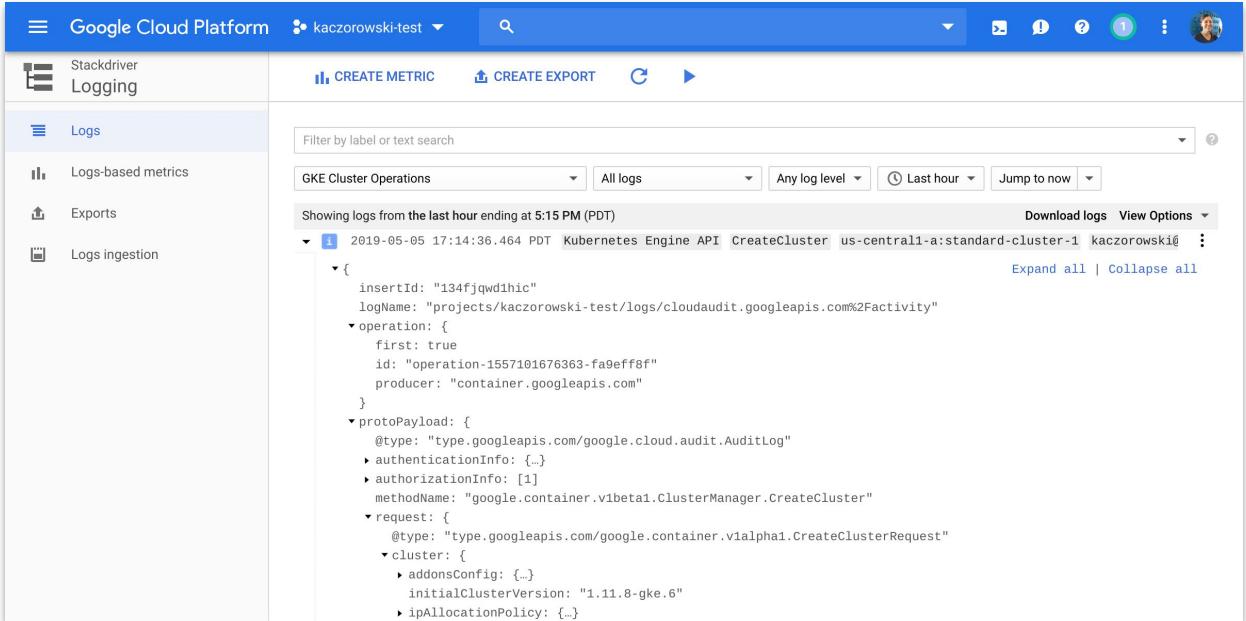
Image by Ann Wallace

Logs

1. **Infrastructure logs:** what the infrastructure does, and what a human does to the infrastructure
2. **Kubernetes logs:** what the control plane does, what a container does to the control plane, and what a human does to the control plane
3. **Operating system logs:** what a container does to the node
4. **Application logs:** what an application does (in a container)

1. Infrastructure logs

Sample
Cloud
Audit Log



The screenshot shows the Google Cloud Platform Stackdriver Logging interface. The left sidebar has 'Logs' selected. The main area displays a log entry from 'GKE Cluster Operations' on May 5, 2019, at 17:14:36 PDT. The log details a 'CreateCluster' operation for the 'us-central1-a:standard-cluster-1' project by user 'kaczorowski'. The log message is a JSON object representing the audit log payload, which includes fields like insertId, logName, operation, protoPayload, and request.

```
{
  "insertId": "134fjqwd1hic",
  "logName": "projects/kaczorowski-test/logs/cloudaudit.googleapis.com%2Factivity",
  "operation": {
    "first": true,
    "id": "operation-1557101676363-fa9eff8f",
    "producer": "container.googleapis.com"
  },
  "protoPayload": {
    "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
    "authenticationInfo": {...},
    "authorizationInfo": [1],
    "methodName": "google.container.v1beta1.ClusterManager.CreateCluster",
    "request": {
      "@type": "type.googleapis.com/google.container.v1alpha1.CreateClusterRequest",
      "cluster": {
        "addonsConfig": {...},
        "initialClusterVersion": "1.11.8-gke.6",
        "ipAllocationPolicy": {...}
      }
    }
  }
}
```



2. Kubernetes logs

Kubernetes audit policy

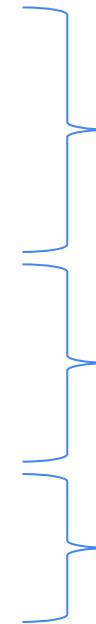
None <

Metadata <

Request <

RequestResponse

```
- level: Request
  verbs: ["get", "list", "watch"]
  resources: ${known_apis}
  omitStages:
    - "RequestReceived"
- level: RequestResponse
  resources: ${known_apis}
  omitStages:
    - "RequestReceived"
- level: Metadata
  omitStages:
    - "RequestReceived"
```



'get' responses can be large

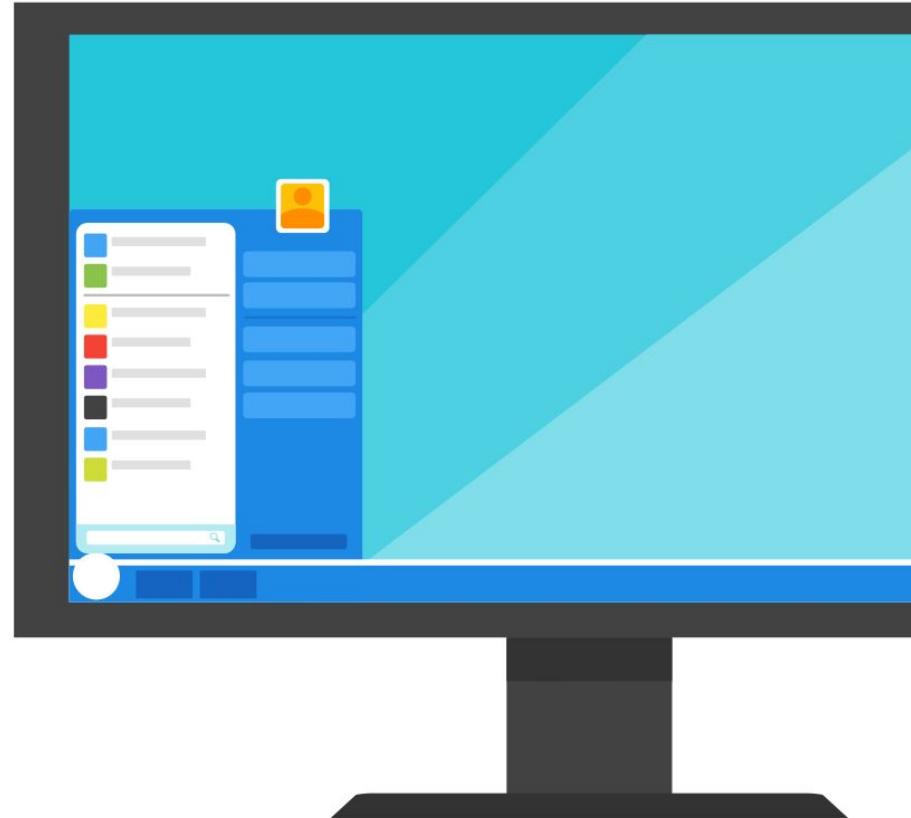
'RequestResponse'
default for known APIs

'Metadata' default for all other requests

3. Operating system logs

- Network connections
- User logins
- SSH sessions
- Executions like execve()

[See recommended auditd fluentd config for COS logs on GKE](#)



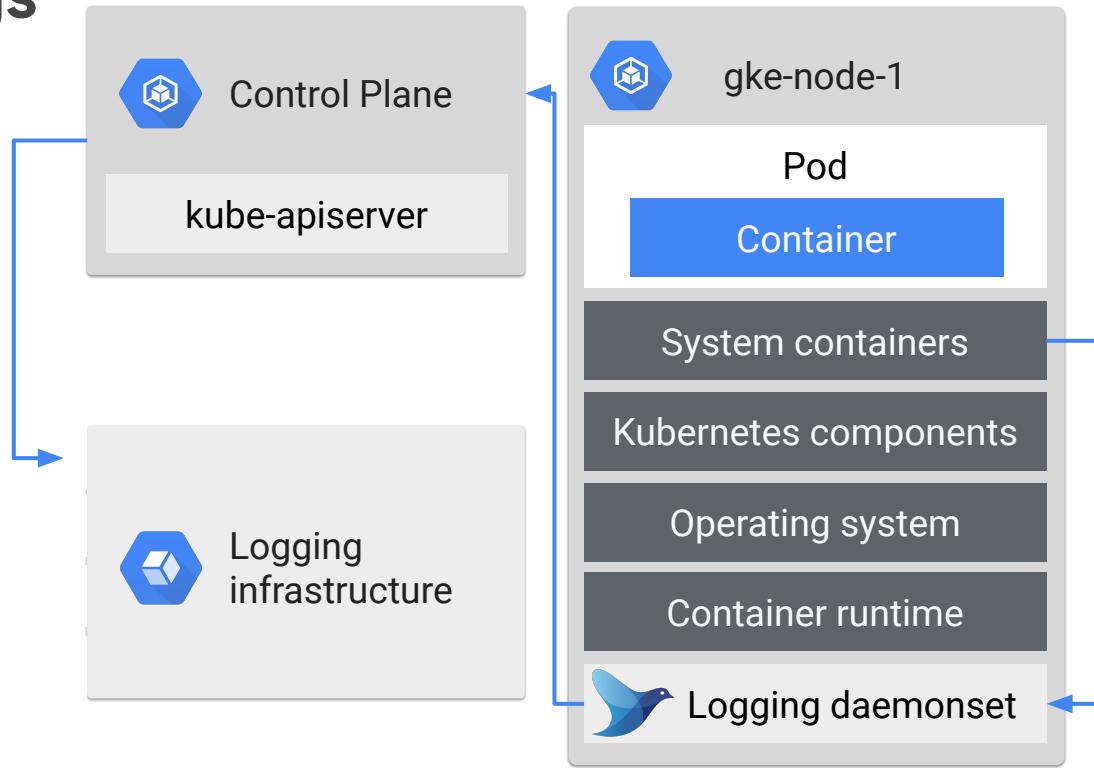
4. Application logs

- Errors
- Warnings
- Operations and other events



Collecting all the logs

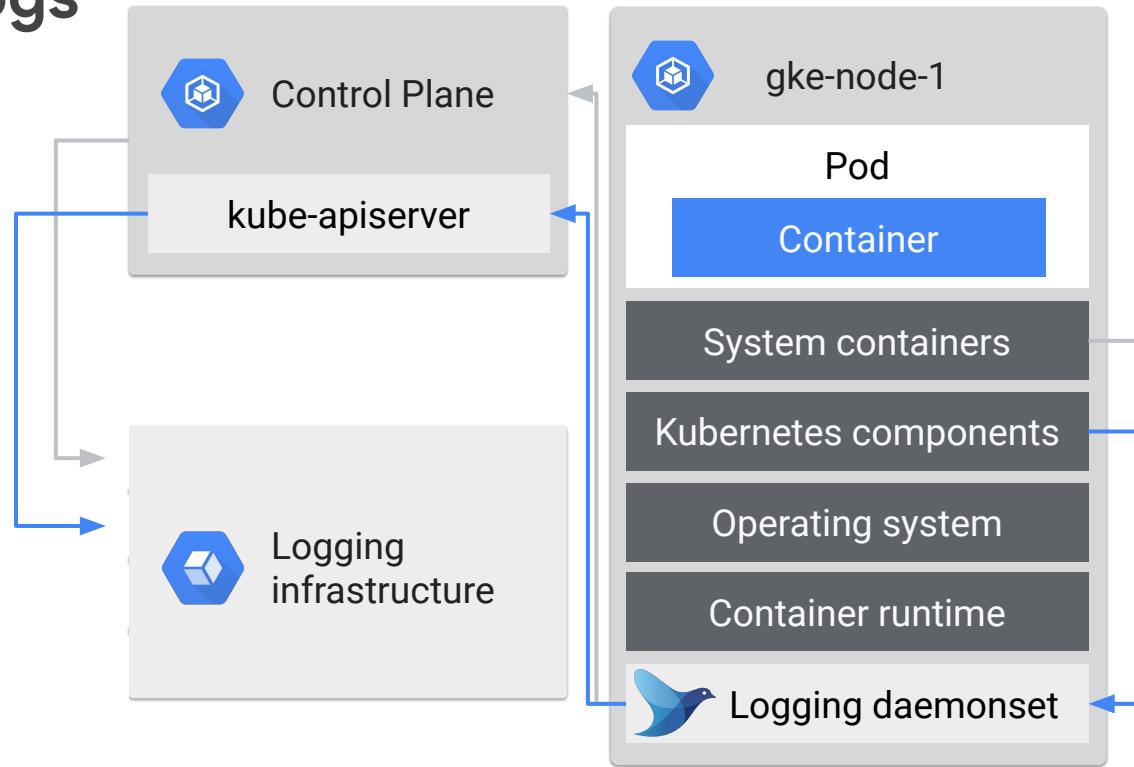
Infrastructure logs



Collecting all the logs

Infrastructure logs

Kubernetes logs

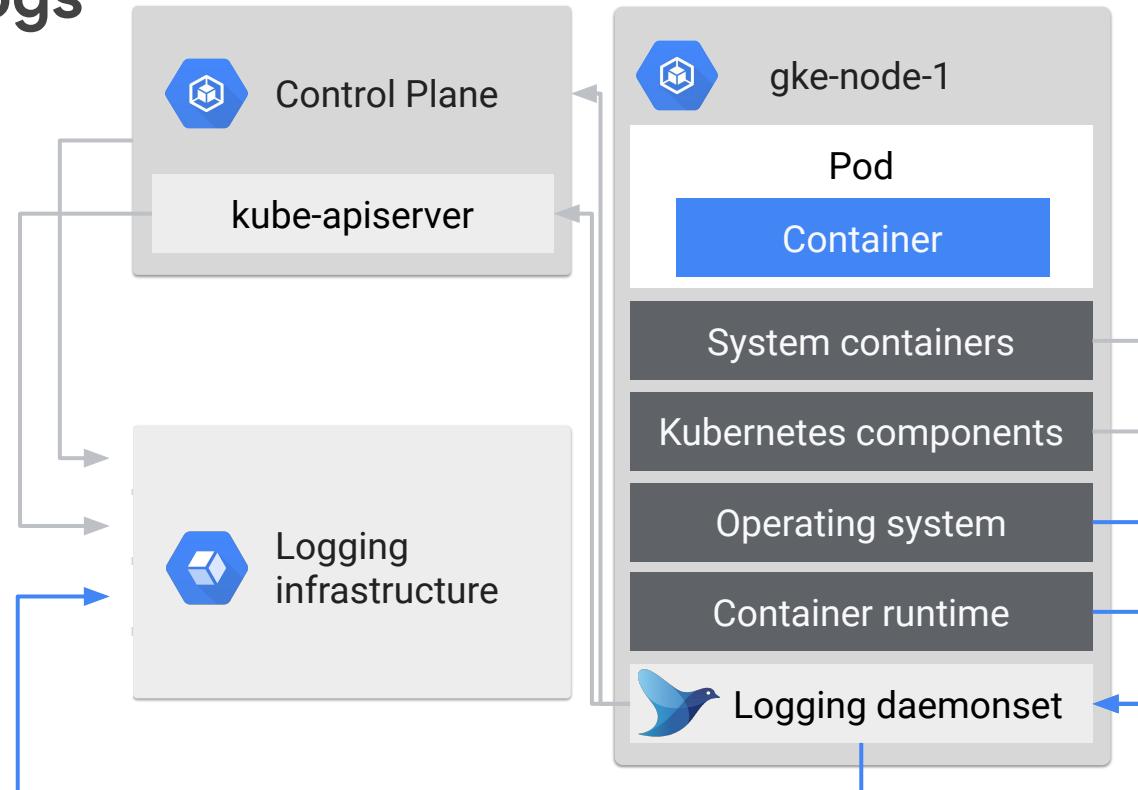


Collecting all the logs

Infrastructure logs

Kubernetes logs

OS logs



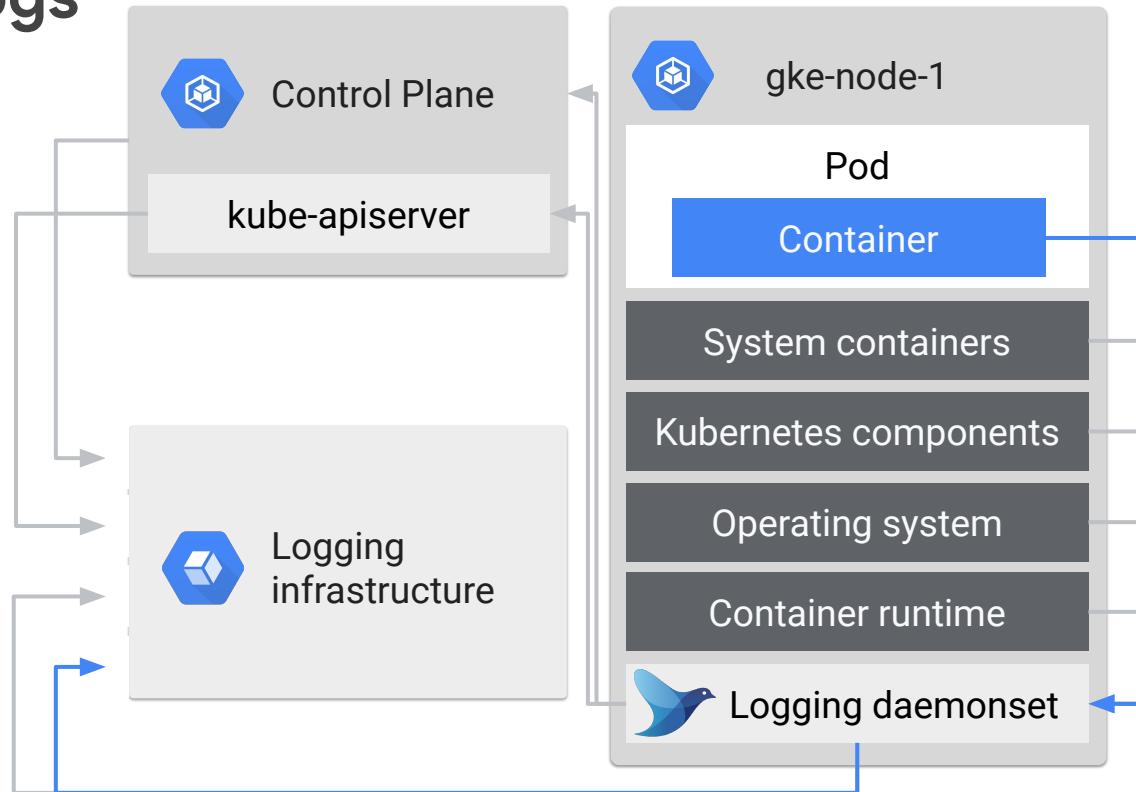
Collecting all the logs

Infrastructure logs

Kubernetes logs

OS logs

Application logs

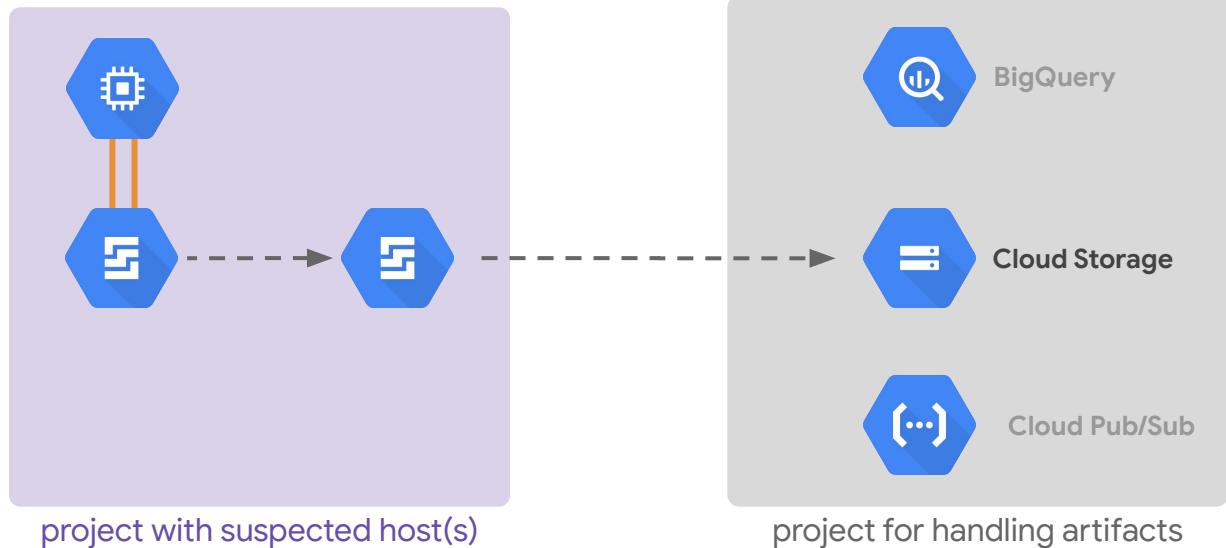


Snapshot the node

Identify affected node(s) and all attached disks

Create an duplicate of the disk(s) while online

Send the duplicated disk image for analysis



docker-explorer

attach and mount
the snapshot

find the container id

mount the container
filesystem

```
# mount /dev/sda1 /mnt/root
```

```
# de.py -r /mnt/root/var/lib/docker list running_containers
Container id: 7b02fb3e8a665a63e32b909af5babb7d6ba0b64e10003b2d9534c7d5f2af8966 / Labels :
  Start date: 2017-02-13T16:45:05.785658046Z
  Image ID: 7968321274dc6b6171697c33df7815310468e694ac5be0ec03ff053bb135e768
  Image Name: busybox
```

```
# de.py -r /tmp/ mount 7b02fb3e8a665a63e32b909af5babb7d6ba0b64e10003b2d9534c7d5f2af8966 /tmp/test
mount -t aufs -o ro,br=/tmp/docker/aufs/diff/b16a494082bba0091e572b58ff80af1b7b5d28737a3eedbe01e73
mount -t aufs -o ro,remount,append:/tmp/docker/aufs/diff/b16a494082bba0091e572b58ff80af1b7b5d28737
mount -t aufs -o ro,remount,append:/tmp/docker/aufs/diff/d1c54c46d331de21587a16397e8bd95bdbb1015e1
Do you want to mount this container Id: /tmp/docker/aufs/diff/b16a494082bba0091e572b58ff80af1b7b5d28737
(ie: run these commands) [Y/n]
```

```
root@test-VirtualBox:~# ls /tmp/test
bin  dev  etc  home  proc  root  sys  tmp  usr  var
```

Live and Recorded Info

GRR (GRR Rapid Response)

Sysdig Inspect & Capture

What is happening on the system?

How do you get real time info without logging in?

How do you gather information remotely from multiple systems?

GRR know-before-you-go

With great power
comes....

Secure access to
the GRR server

...extensive forensic capabilities that can aid in uncovering issues throughout your environment

- root privileges
- admin interface
- GRR raw datastore

<https://grr-doc.readthedocs.io/en/latest/installing-grr-server/securing-access.html>

GRR admin console

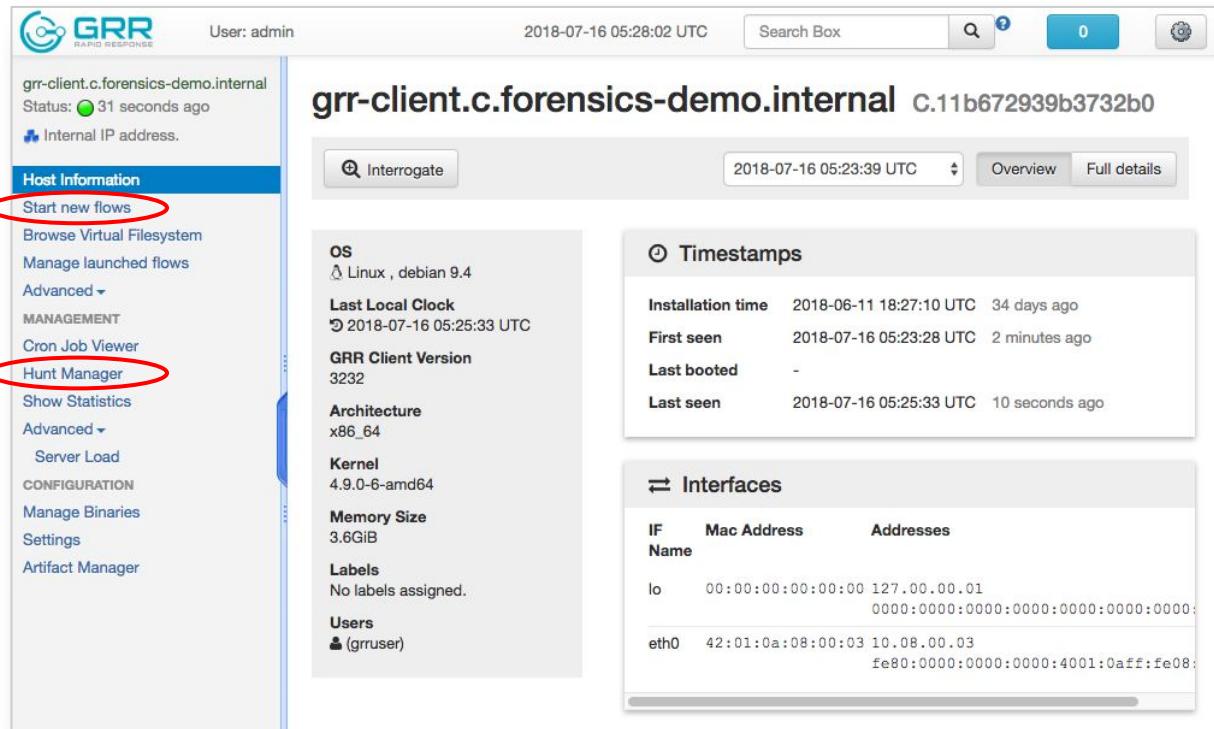
Flows

Activities related to something that you've asked GRR to find out on the target machine:

- download browser history
 - get details about a file
 - dump memory for a process

Hunt

Running flows on a (large) set of instances looking for something specific, i.e. searching for a bad JAR or malware signature. You can monitor the progress of a hunt.



Sysdig Inspect & Capture

observability

investigation

container history





Common mitigation options

Google Cloud



Mitigation options

Alert	Send an alert
Isolate	Restrict from other workloads
Pause	Stop running processes
Restart	Kill and restart running processes
Kill	Kill running processes but not restart

Mitigation options

Alert	<p><i>What it is:</i></p> <ul style="list-style-type: none">• Alert your security response team to investigate
Isolate	
Pause	<p><i>When you'd do it:</i></p> <ul style="list-style-type: none">• Initial triage<ul style="list-style-type: none">◦ Large SecOps team with container expertise◦ New environment not yet fine-tuned
Restart	
Kill	<p><i>How you would do it:</i></p> <ul style="list-style-type: none">• Trigger on specific metrics or specific actions• Metrics on centralized logs, to SMS/ email/ Slack/ etc.

Mitigation options

Alert

What it is:

- Quarantine the container to watch what it does

Isolate

When you'd do it:

- Get more info to know what's going on

Pause

How you would do it:

- Get on its own node
 - `kubectl cordon`
- Restrict connectivity, e.g., Network Policy
- Monitor with live forensics, agent, or filtering

Restart

Kill

Mitigation options

Alert

What it is:

- Suspend running processes

Isolate

When you'd do it:

- Get further data for forensics
 - Auditing
 - Confirm the issue

Restart

How you would do it:

- docker pause

Kill

Mitigation options

Alert

What it is:

- Kill and restart a running container

Isolate

When you'd do it:

- Roll out a fix

Pause

How you would do it:

- docker restart
- kubectl delete pod
- Roll out a new image!

Restart

Kill

Mitigation options

Alert	<p><i>What it is:</i></p> <ul style="list-style-type: none">• Stop running processes, without restart
Isolate	<p><i>When you'd do it:</i></p> <ul style="list-style-type: none">• As a last resort (sh*t's on fire, yo)
Pause	<p><i>How you would do it:</i></p> <ul style="list-style-type: none">• docker stop = SIGTERM, and SIGKILL after 10 sec or crictl stop• docker kill = SIGKILL• docker rm -f = SIGKILL or crictl rm -f
Restart	
Kill	



Tying it all together

Google Cloud



Image by Ann Wallace

Privilege escalation

TL;DR - an attacker is able to break out of the container and effectively becoming root on the node.



Gather some evidence

1. What do you already know?
2. What do you have in place to help you determine: Who, What, How, When, Where?



Tying it all together :: logs

Deployment or OS logs

How was the container launched?

Container logs

Are there unexpected commands being ran?
ln, mv, cp, cat, *.sh, tar, curl, wget
Are files in /dev or /proc being touched?

Network logs

Is there unexpected network traffic or increased egress traffic from a particular node?

Tying it all together :: disks

Container & Nodes:

Have any binaries changed?

Are there any unexpected files?



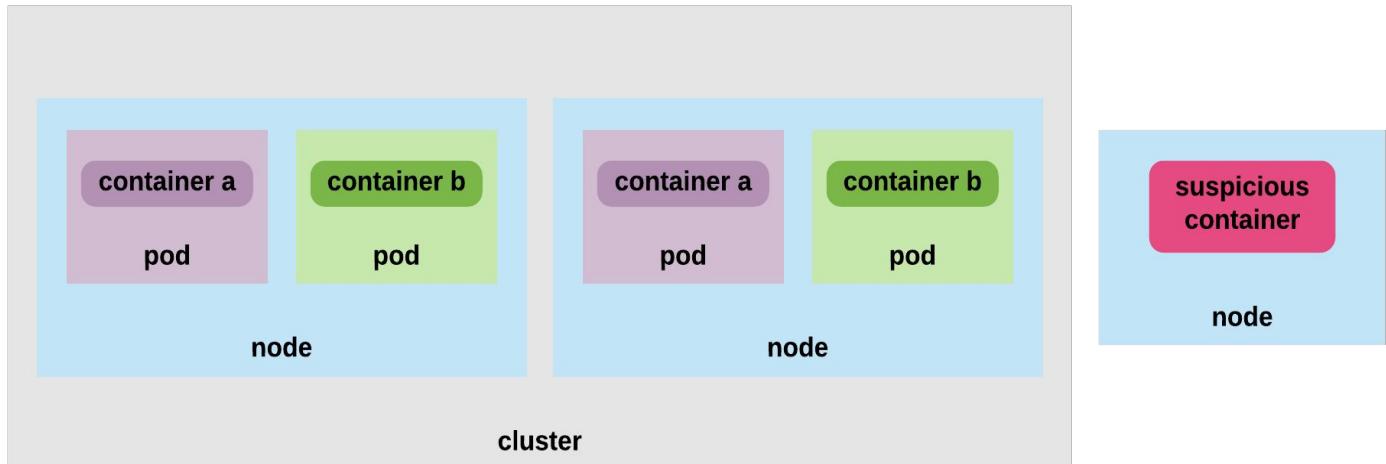
Tying it all together :: live & recorded info

What interesting
things happened on
the system?

- Processes
- System Calls
- Files
- Network
- I/O
- Users

Tying it all together :: mitigation options

Alert
Isolate
Deploy



Tying it all together :: prevention

Preventing privilege escalation

- Scan your images for vulnerabilities
- Only allowed signed images to be deployed
- Don't run containers with the root user
- Use user namespace isolation



Steps to take today

Google Cloud

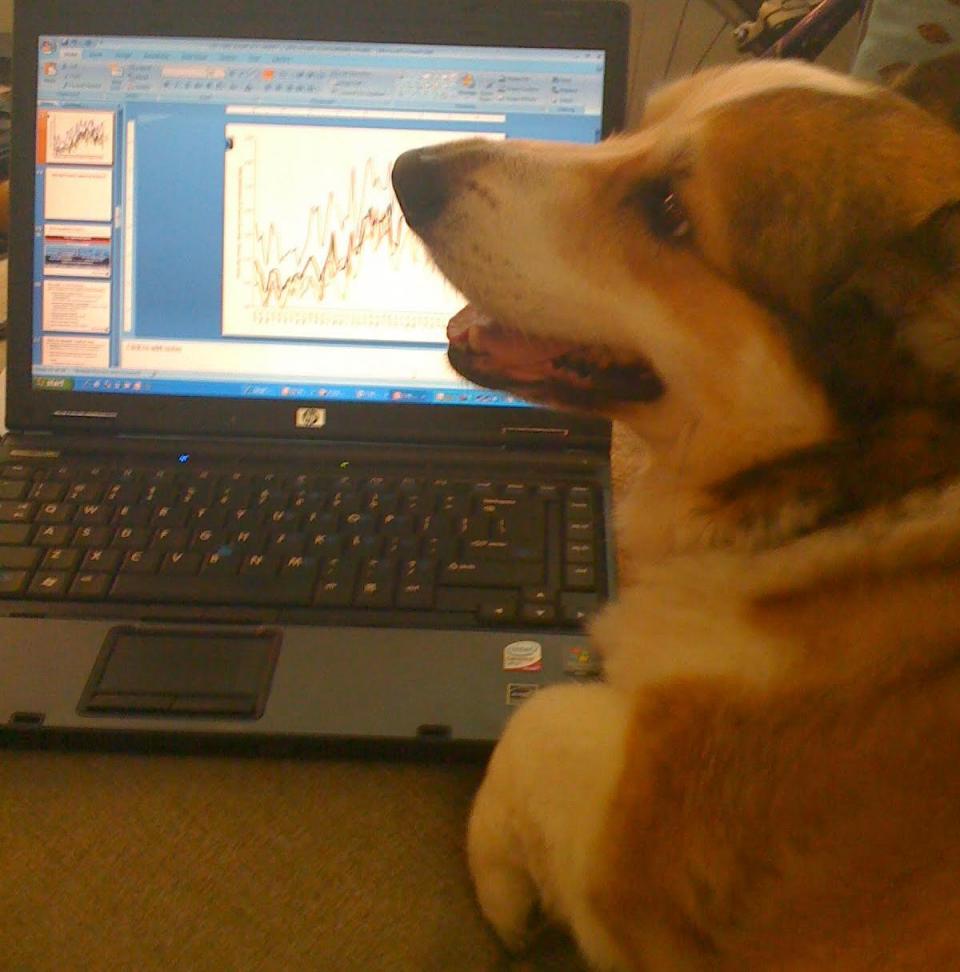


Image by Ann Wallace

You've got this!

- Create an incident response plan
- Follow container security best practices
- Sync all your logs to a central location
- Invest in container specific security tools (OSS or off the shelf)
- Rehearse the process with a fake event
- Don't panic - Sh*t happens



Read

cloud.google.com/containers/security

sysdig.com/blog/gke-security-using-falco/

Watch

[“Cloud Forensics 101” on YouTube](#)

Clone

github.com/google/grr

github.com/spotify/terraform-google-grr

github.com/google/docker-explorer

github.com/sysdiglabs/kubectl-capture

github.com/draios/sysdig-inspect

github.com/GoogleCloudPlatform/k8s-node-tools/tree/master/os-audit

Questions?

