Sysdig

PromQL for security

Carlos Arilla

carlos@sysdig.com

carillan@gmail.com

@carillan_

November 2019

Hello World

Carlos Arilla

Tech Marketing Engineer @ Sysdig

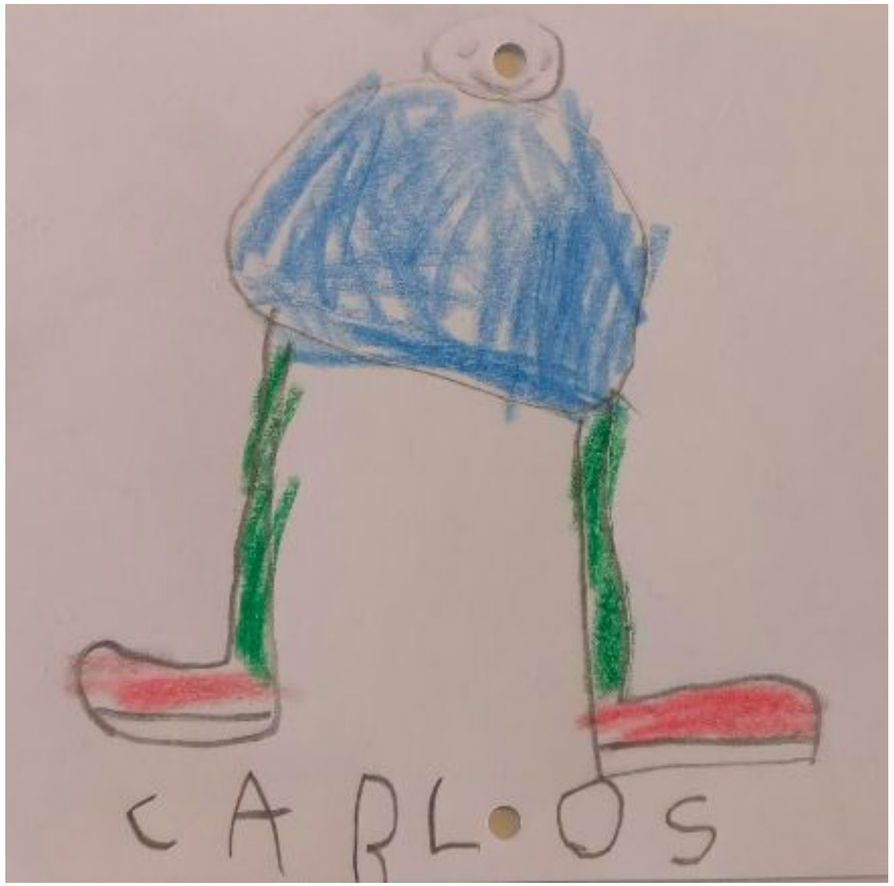
Father of 3!

Professional interests:

- Cloud Native
- Microservices
- Monitoring
- DevOps

Personal interests:

- SciFi
- Video-games
- Sports
- IoT and robots



My beloved children

Let’s talk about monitoring

Let’s talk about ~~monitoring~~ security

Monitoring and security

Are monitoring and security completely separated topics?

- Many times one of the first indicators of a security issue is a change in resource usage. Cryptojacking?
- Security usually is related to knowledge. Monitoring can provide insight and knowledge in real time.
- DevOps teams have been the paladins of monitoring. Now they are assuming security functions too. The ability of combining tools for both can be differential.

PromQL example 1: load increase

```
100 - (avg by (instance)
(irate(node_cpu_seconds_total{job="node",mode="idle"}[5m])) * 100)
```

Goals

- Many intrusions are a way to use your compute resources for different interests: cryptomining, spam, DDoS…
- A sudden increase of resources can be an indicator of a security breach being exploited.

Next level:

Pods running in Kubernetes without limits:

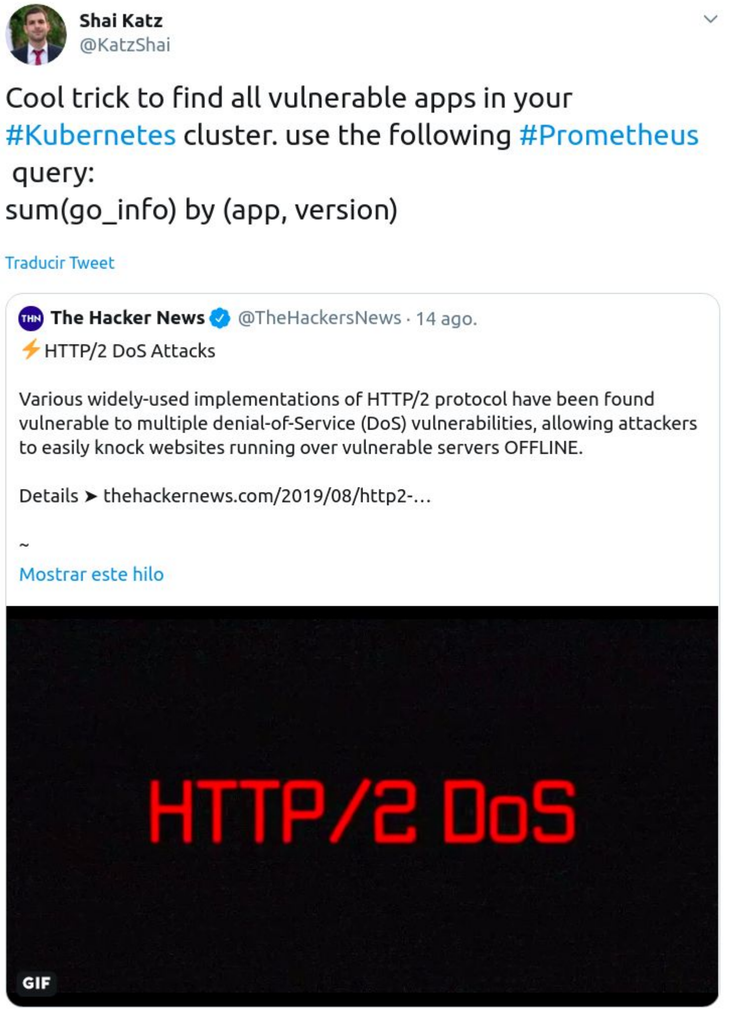
```
(sum(kube_pod_status_ready{condition="true"}) by (pod) == 1)
unless  sum(kube_pod_container_resource_limits_cpu_cores) by (pod)
```

PromQL example 2: Vulnerable versions

```
sum(go_info) by (app,version)
```

Goals:

- This allows to detect vulnerable versions of different libraries or implementations
- Instrumenting library versions can be an easy way to detect vulnerabilities in your system.



PromQL example 3: Certificate expiration change

```
change(rate(sum(ssl_certificate_expiry_seconds{}) by
(instance, path)))
```

Goals:

- Certificate expiration information is widely instrumented.
- Unexpected changes in expiration could indicate supplantation attacks.

Next level:

Check TLS/SSL version with blackbox exporter:

```
probe_tls_version_info{}
```

PromQL example 4: Cost increase control

AWS Cost Exporter can provide information of daily costs:

https://github.com/nachomillangarcia/prometheus_aws_cost_exporter

Kubernetes HPA can spawn new nodes, watch your clusters!

```
sum(up{job="node-exporter"})
```

Goals:

- A typical target for attacker is to spawn new machines to run crypto mining, spam or DDoS.
- ASG, HPA or other automated scaling methods should be watched.

PromQL example 5: 401 errors

```
sum(rate(apiserver_request_total{code=”401|403"}[5m]))
```

Goal:

- A good number of 401 (Unauthorized) can be a good indicator of illegitimate access tries.
- This can be extended to 403 (Forbidden).

Some more ideas...

- Network connections:

  https://github.com/hiveco/conntrack_exporter

-

What I learnt

Secure Devops is a necessity!

- Security has to be moved “left” in the development cycle.
- Instrumentation should have security information built-in by design.
- DevOps teams have real responsibility in security.

Thank you very much!!

Questions?

Carlos Arilla

carlos@sysdig.com

carillan@gmail.com

@carillan_