MN CERT/CC

Mongolian Cyber Emergency Response Team / Coordination Center

KUBERNETES SECURITY

NASANTOGTOKH AMARSAIKHAN
MNCERT/CC

CONTENTS

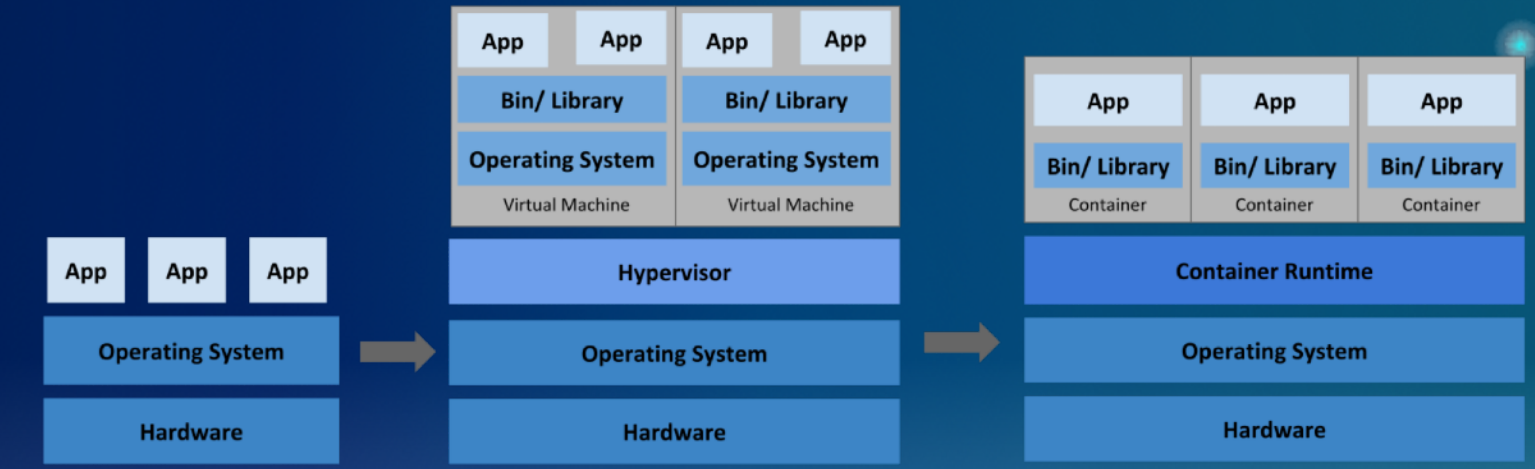
CONTAINER

WHAT IS IT

CONTAINER

All-in-one, standardised unit - Packaged software into standardised Units for development, shipment & deployment

- Less overhead
- Increased portability
- More consistent operation
- Greater Efficiency



How deployment evolved?

KUBERNETES

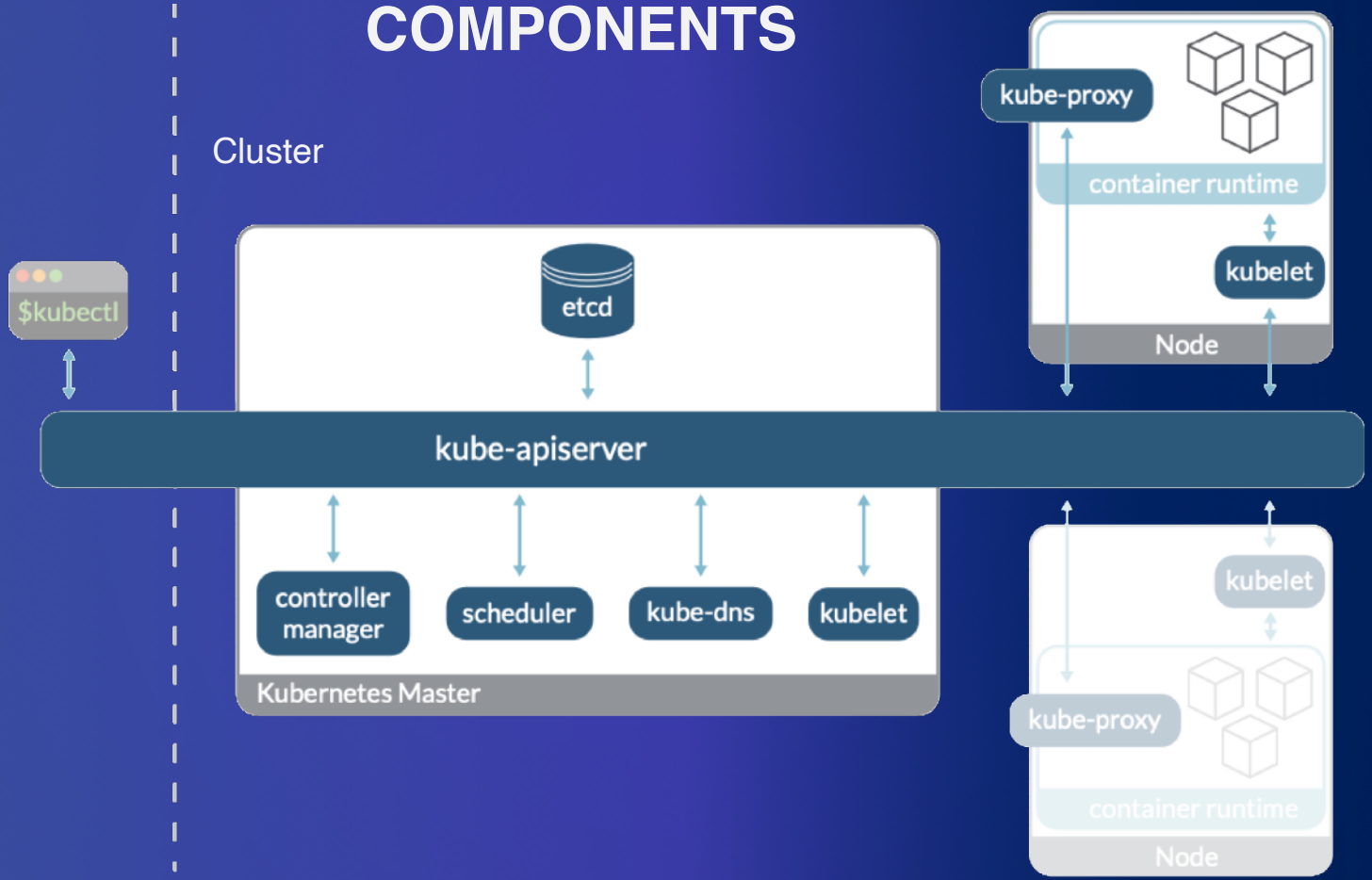
WHAT AND HOW?

KUBERNETES

Open source **Container Orchestration** engine for automating

- Deployment
- Scaling
- Management of containerized applications

COMPONENTS


Cluster
$kubectl
etcd
kube-apiserver
controller manager
scheduler
kube-dns
kubelet
Kubernetes Master
kube-proxy
container runtime
kubelet
Node
kubelet
kube-proxy
container runtime
Node

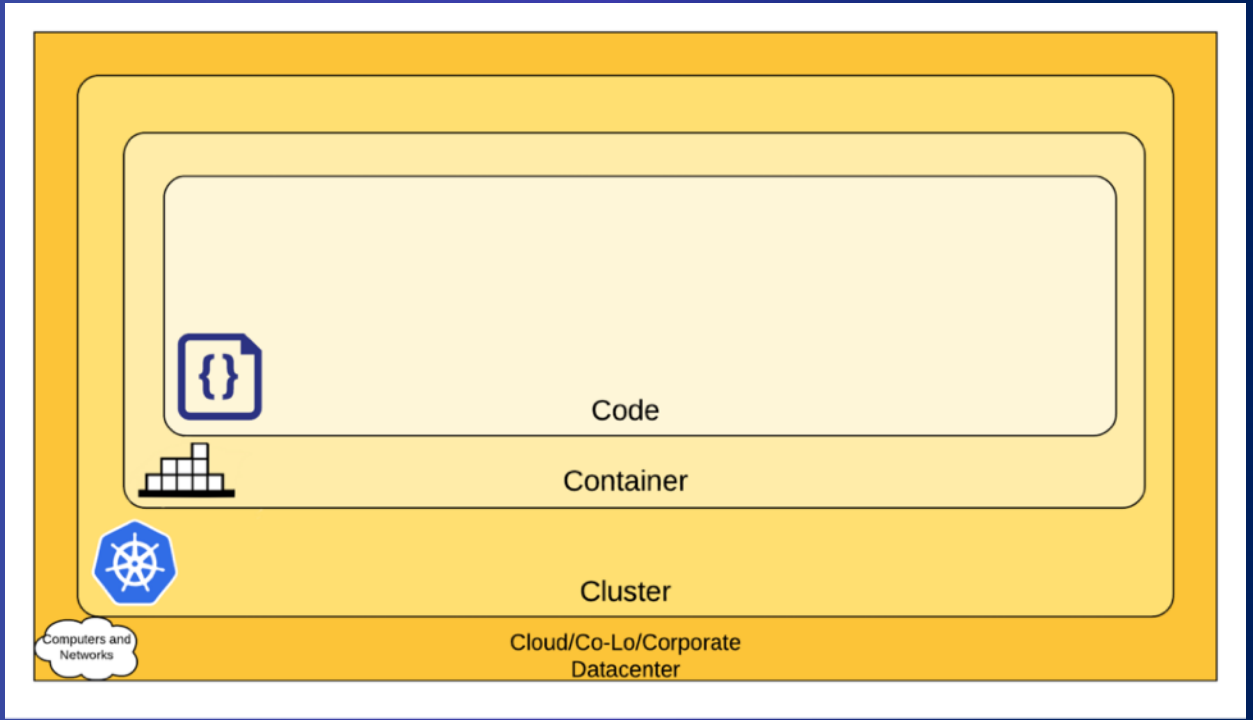
KUBERNETES CAN DO

- Run distributed system resiliently
- Scaling, failover
- Service discovery & load balancing
- Storage orchestration
- Automated rollouts and rollbacks
- Automatic bin packing - Set limit to CPU & RAM and best utilization of resource
- Self-Healing - Container restart
- Secret and configuration management
- Kubernetes comprises set of independent, composable **control processes** that continuously drive the current state → desired state.

KUBERNETES SECURITY

WHAT AND HOW?

KUBERNETES SECURITY | 4C MODEL

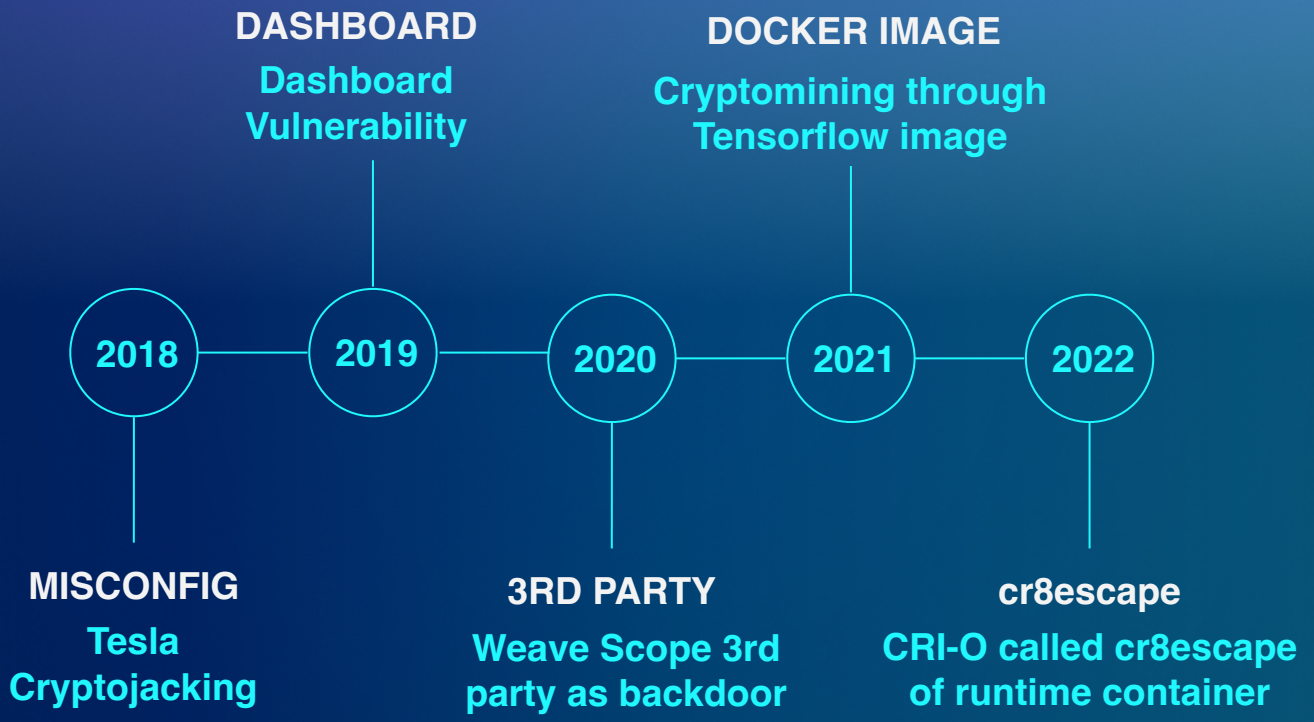


Source: Kubernetes Documentation, The 4C's of Cloud Native security

KUBERNETES SECURITY POSTURE

- **96%** of organizations using or evaluating k8s
- **53%** detected misconfiguration in Kubernetes in last 12 months
- **51%** require to use validated **images**
- **57%** worry the most about securing workloads at runtime
- Adversaries shifted their attention Docker →K8s and CI/CD (10% increase 2020-2021)

KUBERNETES HACKS

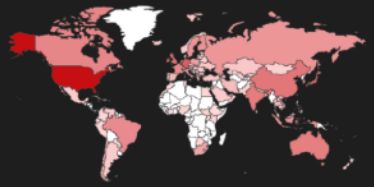


SHODAN | Explore | Pricing | kubernetes | Login

TOTAL RESULTS

1,040,075

TOP COUNTRIES



United States	606,128
Germany	62,265
Ireland	46,372
Belgium	45,006
Singapore	33,371

More...

TOP PORTS

443	973,775
6443	62,653
8443	1,206
10250	715
4443	233

View Report | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

15.188.108.149

2022-10-04T13:19:09.999057

ec2-15-188-108-149.eu-west-3.compute.amazonaws.com

Amazon Data Services France

France, Paris

cloud | devops

SSL Certificate

Issued By:
|- Common Name:
kubernetes

Issued To:
|- Common Name:
kube-apiserver

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 403 Forbidden
Audit-Id: 3fbffafc-85e3-4ee5-b67a-3851b6392eec
Cache-Control: no-cache, private
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Kubernetes-Pf-Flowschema-Uid: 1e3abc9e-b4b7-43ac-942e-af0df96e2c91
X-Kubernetes-Pf-Prioritylevel-Uid: d75b0c1d-59f3-465e-b9...
```

180.184.138.224

2022-10-04T13:18:48.875025

Beijing Volcano Engine Technology Co., Ltd.

China, Beijing

devops

SSL Certificate

Issued By:
|- Common Name:
kubernetes

Issued To:
|- Common Name:
kube-apiserver

Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 403 Forbidden
Cache-Control: no-cache, private
Content-Type: application/json
X-Content-Type-Options: nosniff
X-Kubernetes-Pf-Flowschema-Uid: 354940a1-f243-447f-8c64-2911fe63ab23
X-Kubernetes-Pf-Prioritylevel-Uid: b9aaeced-dccb-4d9a-8835-ecdc16fa9e3f
Date: Tue, 04 Oct 2022 13:18:48...
```

35.193.163.201

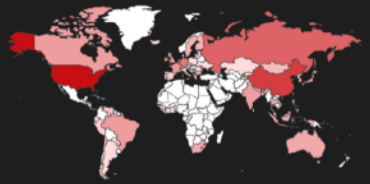
2022-10-04T13:18:46.343390

SHODAN | Explore | Pricing | kubernetes 200 | Login

TOTAL RESULTS

1,937

TOP COUNTRIES



United States	866
China	348
Russian Federation	140
Germany	67
Singapore	57

More...

TOP PORTS

6443	611
443	463
51235	228
5000	93
8001	73

View Report | View on Map

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

54.156.97.229

ec2-54-156-97-229.compute-1.amazonaws.com

Amazon Technologies Inc.

United States, Ashburn

cloud

SSL Certificate

Issued By:
|- Common Name:
kube-apiserver-service-network-signer

Issued To:
|- Common Name:
172.30.0.1

Supported SSL Versions:
TLSv1.2

2022-10-04T13:21:44.775768

```
HTTP/1.1 200 OK
Audit-Id: 9ec280d3-d5b5-426e-ba64-fb4e35969e06
Cache-Control: no-cache, private
Content-Type: application/json
X-Kubernetes-Pf-Flowschema-Uid: 630e4eb9-2566-407b-a55b-022b16ae92d6
X-Kubernetes-Pf-Prioritylevel-Uid: 4218b22c-72a2-4f0b-bdb1-945d3cdac956
Date: Tue, 04 Oct 2022 ...
```

178.154.207.252

test-y8068.skyengschool.link
test-y8068.skysmart.link
api.content.vimbox.test-y8068.skyeng.link
test-y8068.skypro.link
api.content.vimbox.test-y8068.skyengschool.link

YANDEX LLC

Russian Federation, Moscow

cloud

SSL Certificate

Issued By:
|- Common Name:
R3

|- Organization:
Let's Encrypt

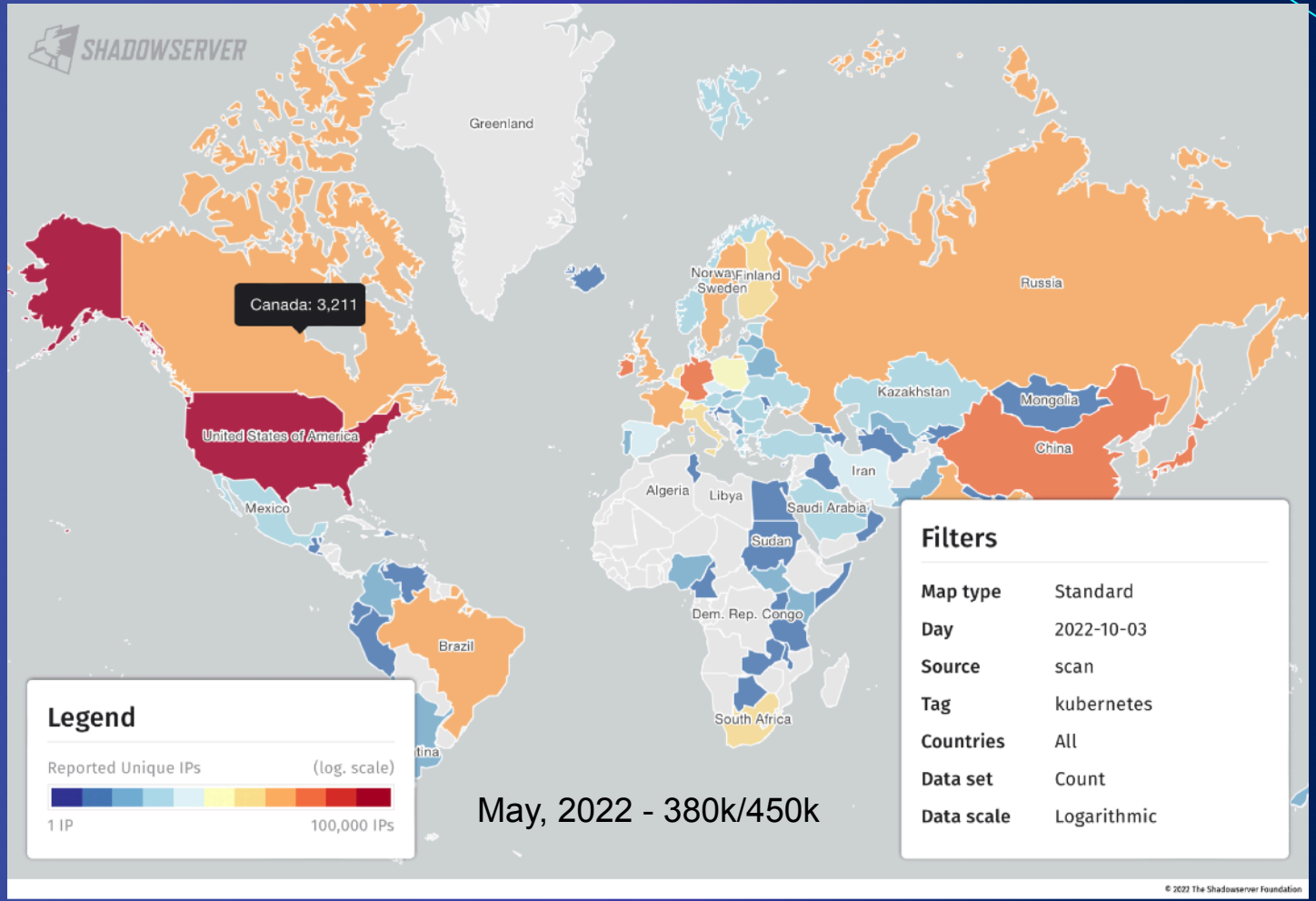
Issued To:
|- Common Name:
test-y8068.skyeng.link

Supported SSL Versions:
TLSv1, TLSv1.1,

2022-10-04T13:11:08.286507

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 04 Oct 2022 13:11:08 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Vary: Accept-Encoding
Cache-Control: no-cache, private
Request-Id: c78818783b33c27e34e803c4316e9f97
Reques...
```

```
{
  "paths": [
    "/.well-known/openid-configuration",
    "/api",
    "/api/v1",
    "/apis",
    "/apis/",
    "/apis/admissionregistration.k8s.io",
    "/apis/admissionregistration.k8s.io/v1",
    "/apis/apiextensions.k8s.io",
    "/apis/apiextensions.k8s.io/v1",
    "/apis/apiregistration.k8s.io",
    "/apis/apiregistration.k8s.io/v1",
    "/apis/apiserver.openshift.io",
    "/apis/apiserver.openshift.io/v1",
    "/apis/apps",
    "/apis/apps.openshift.io",
    "/apis/apps.openshift.io/v1",
    "/apis/apps/v1",
    "/apis/argoproj.io",
    "/apis/argoproj.io/v1alpha1",
    "/apis/authentication.k8s.io",
    "/apis/authentication.k8s.io/v1",
    "/apis/authorization.k8s.io",
    "/apis/authorization.k8s.io/v1",
    "/apis/authorization.openshift.io",
    "/apis/authorization.openshift.io/v1",
    "/apis/authorization.openshift.io/v1/rolebindingrestrictions",
    "/apis/autoscaling",
    "/apis/autoscaling.openshift.io",
    "/apis/autoscaling.openshift.io/v1",
    "/apis/autoscaling.openshift.io/v1beta1",
    "/apis/autoscaling/v1",
    "/apis/autoscaling/v2",
    "/apis/autoscaling/v2beta1",
    "/apis/autoscaling/v2beta2",
    "/apis/batch",
    "/apis/batch/v1",
    "/apis/batch/v1beta1",
    "/apis/build.openshift.io",
    "/apis/build.openshift.io/v1",
    "/apis/ceph.rook.io",
    "/apis/ceph.rook.io/v1",
    "/apis/certificates.k8s.io",
```


SHADOWSERVER
Greenland
Canada: 3,211
United States of America
Mexico
Brazil
Norway
Sweden
Finland
Russia
Kazakhstan
Mongolia
China
Iran
Algeria
Libya
Saudi Arabia
Sudan
Dem. Rep. Congo
South Africa
Legend
Reported Unique IPs
(log. scale)
1 IP
100,000 IPs
May, 2022 - 380k/450k
Filters
Map type Standard
Day 2022-10-03
Source scan
Tag kubernetes
Countries All
Data set Count
Data scale Logarithmic
© 2022 The Shadowserver Foundation

KUBERNETES COMMON THREAT

- **Misconfigured** docker, like running on root
- Malicious **docker image**
- Unintentional cluster **misconfiguration**
- **Insider Threat**
- For more info: NIST & CISA Kubernetes Hardening Guide, Threat model

ATTACK PATTERNS

- ABUSING PUBLIC FACING KUBERNETES COMPONENTS
- SCRAPING AND ABUSING CREDENTIALS
- SPINNING UP CRYPTOMINERS
- LATERAL MOVEMENT

ABUSING PUBLIC FACING KUBERNETES COMPONENTS

- Exploiting public, vulnerable Kubernetes components, like kubelet
- **PROTECTION**:
  - Scan for vulnerability in images and packages
  - Use managed Kubernetes →less susceptible

SCRAPING AND ABUSING CREDENTIALS

- Attack into Kubernetes through misconfigured Kubelet or other approach, then look for credentials
  - Cloud access key
  - Access token
  - SSH key etc
- **PROTECTION**:
  - Manage credentials securely
  - Don’t inject into image or repo
  - Inject only when necessary

SPIN UP CRYPTOMINERS

- Run cryptominer containers or inject it.
  - Can be injected via image file
- **PROTECTION**:
  - Monitor network traffic, IP, C&C?
  - Monitor workload of container and node

LATERAL MOVEMENT

- Using weak point and sits in Kubernetes until he needs it
- **PROTECTION**:
  - Microsegmentation, limit resource, privilege and service connection

- Container RAM/CPU spike
- Anomalous in/out traffic
- Attachment of Cluster-admin role
- Unexpected change in Filesystem/Dir
- Anomalous DNS req or spike
- Unusual HTTP response size
- 403/404 HTTP code spike
- Unknown binary

INDICATOR OF COMPROMISE

4C BEST PRACTICE - INFRASTRUCTURE

- Control plane should not be connected from public IP
- Nodes should be only accessible via control plane via whitelist (IP, port)
- etcd encryption at rest

- RBAC Authorization
- Authentication
- Application secret manager
- Pod security standard
- Network policy
- TLS for k8s ingress

4C BEST PRACTICE - CLUSTER

4C BEST PRACTICE - CONTAINER SECURITY

- Vulnerability scanning, OS dependency security
- Image signing, and validation enforcement
- Disallow privileged users
- Use container runtime with stronger isolation

- Access over TLS only
- Limit port ranges of communication
- 3rd party dependency security
- Static code analysis

4C BEST PRACTICE - CODE SECURITY

WHAT'S NEXT?

HOW CAN YOU SECURE YOUR KUBERNETES?

What next?

- Check if control plane/node is public accessible?
- Disable anonymous access (--anonymous-auth=false)
- etcd encryption at rest (etcdctl)
- Verify docker images
- Container runtime hardening, (non-root etc)
- Scan on deploy
- Pod security standard
- RBAC
- Logging, Monitoring, and incident response
- Kubernetes hardening [NIST, CISA guide]

QUESTION?

THANKS FOR YOUR ATTENTION