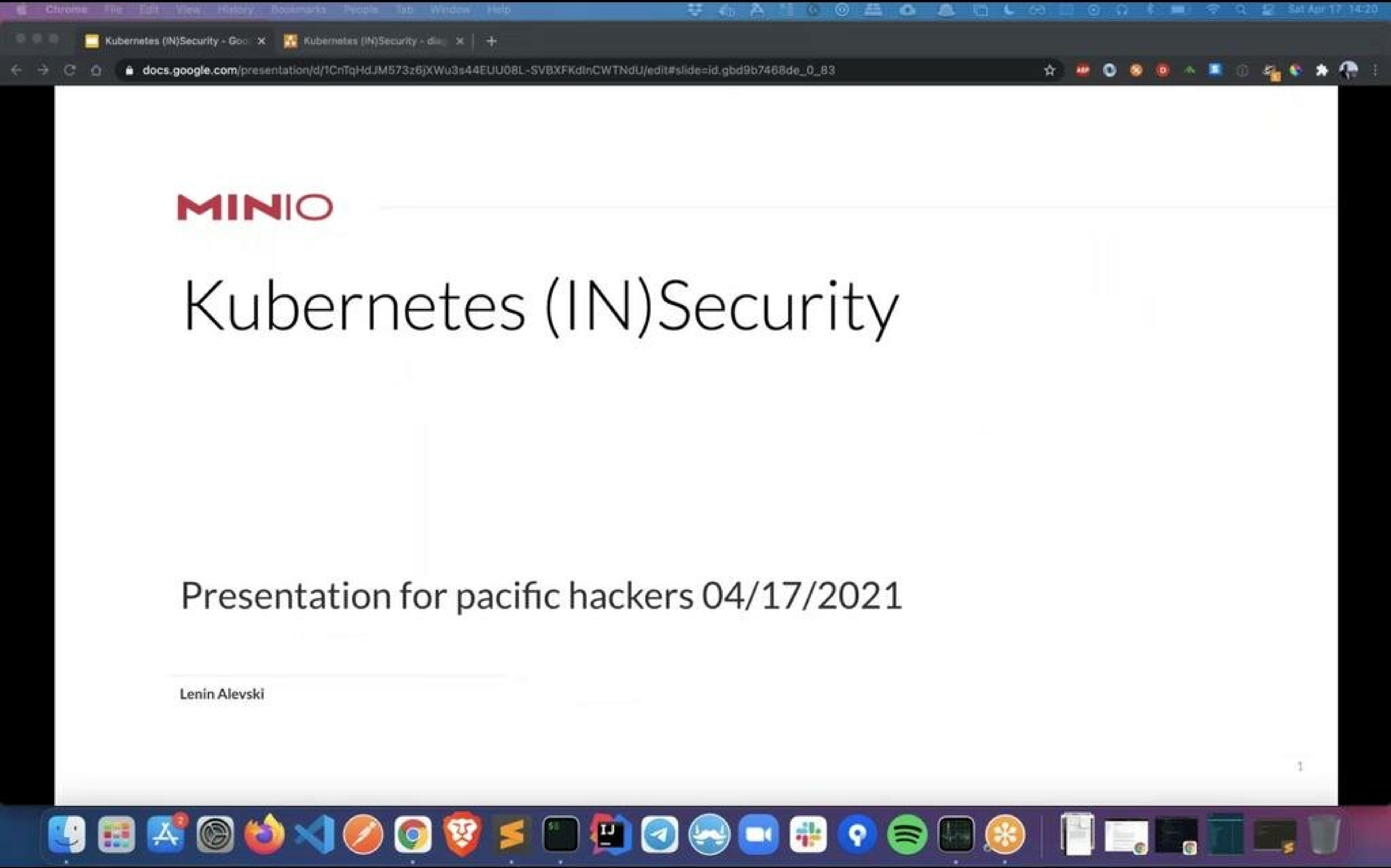
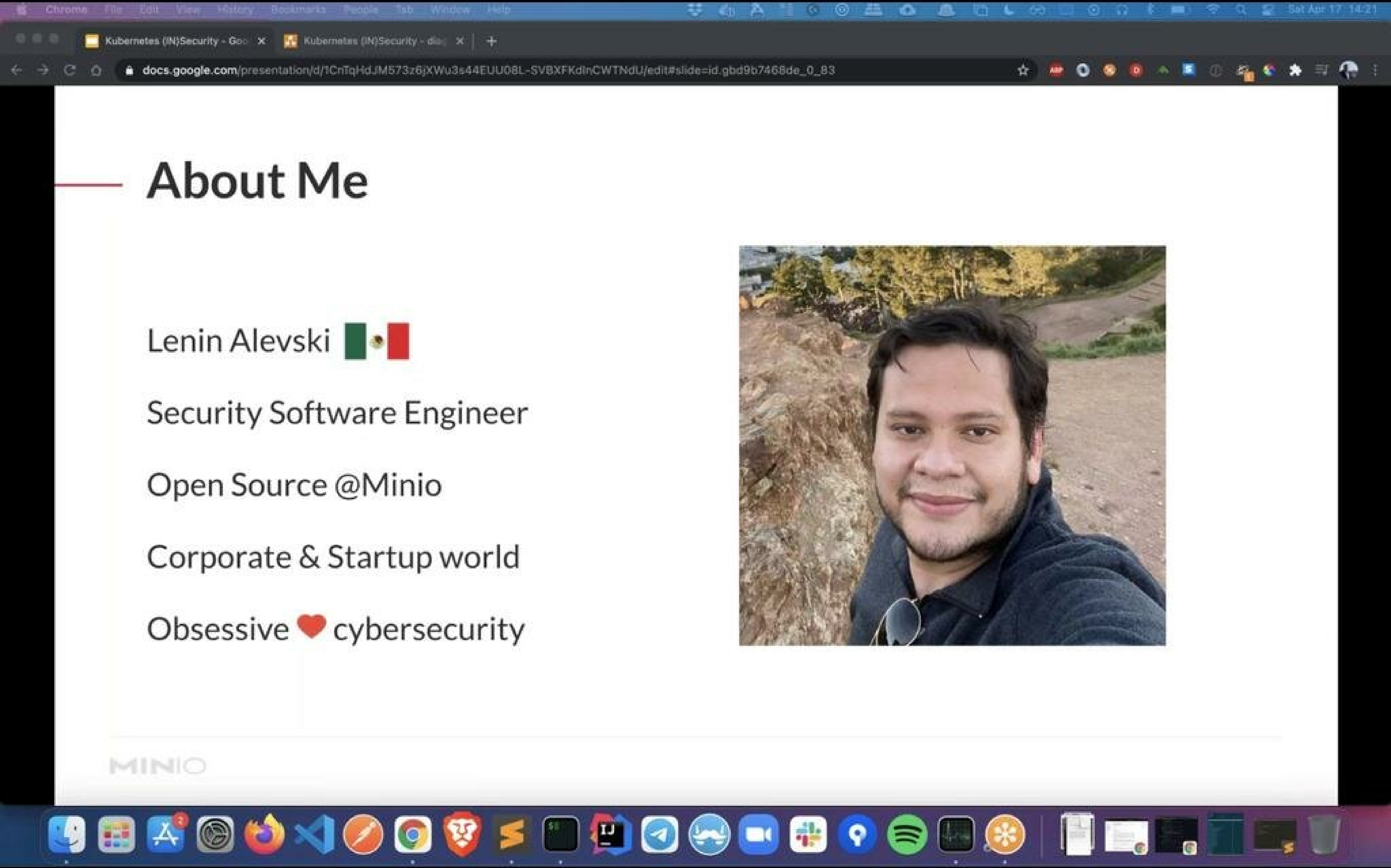

Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:20
Kubernetes (IN)Security - Goo
Kubernetes (IN)Security - dia
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gbd9b7468de_0_83

MINIO

Kubernetes (IN)Security

Presentation for pacific hackers 04/17/2021

Lenin Alevski


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:21
Kubernetes (IN)Security - Goo
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gbd9b7468de_0_83

About Me

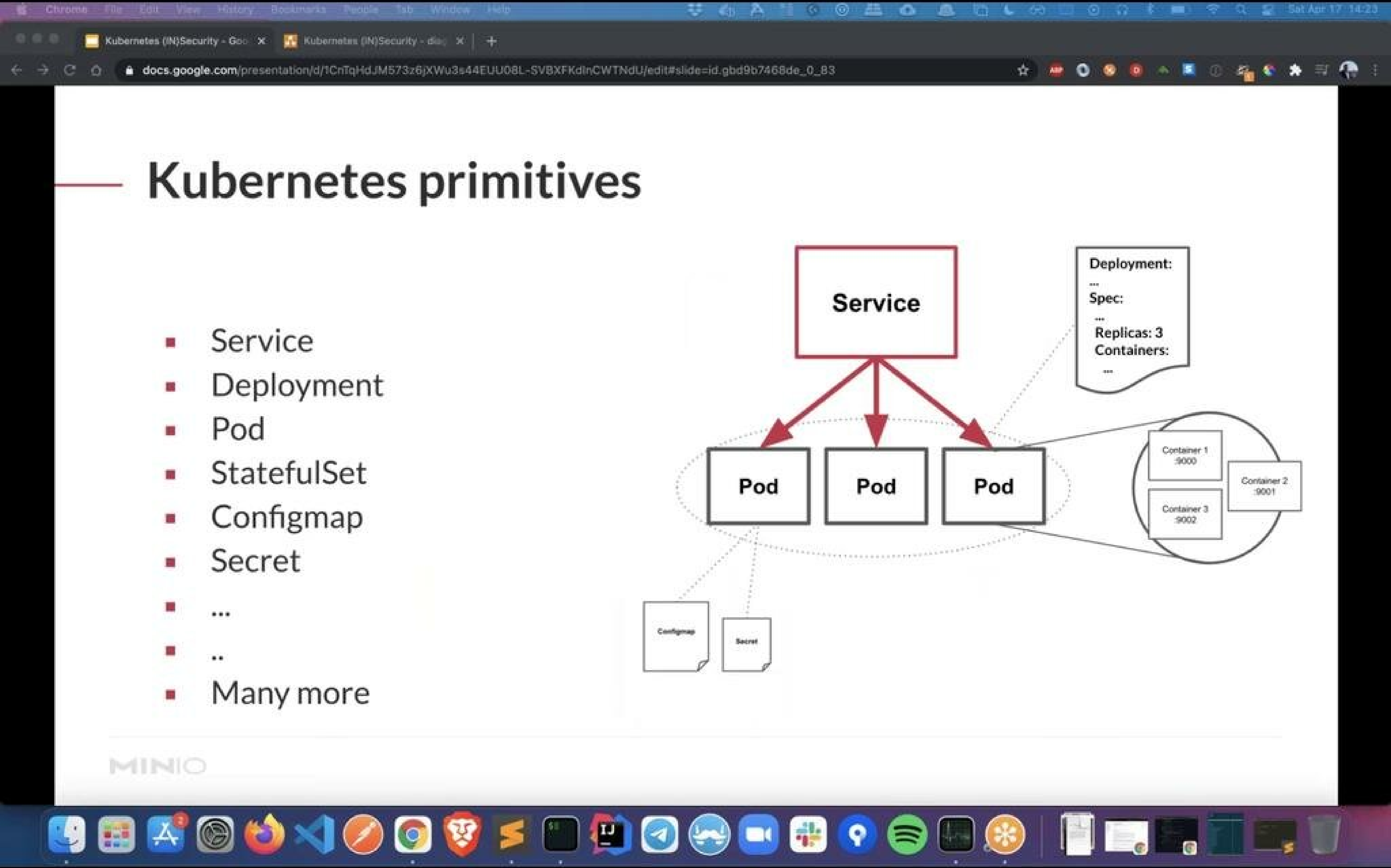
Lenin Alevski 🇲🇽

Security Software Engineer

Open Source @Minio

Corporate & Startup world

Obsessive ❤ cybersecurity


Kubernetes (IN)Security - Goo
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gbd9b7468de_0_83

Kubernetes primitives

- Service
- Deployment
- Pod
- StatefulSet
- Configmap
- Secret
- ...
- ..
- Many more

Deployment:
...
Spec:
...
Replicas: 3
Containers:
...

Service
Pod
Pod
Pod
Container 1
:9000
Container 2
:9001
Container 3
:9002
Configmap
Secret

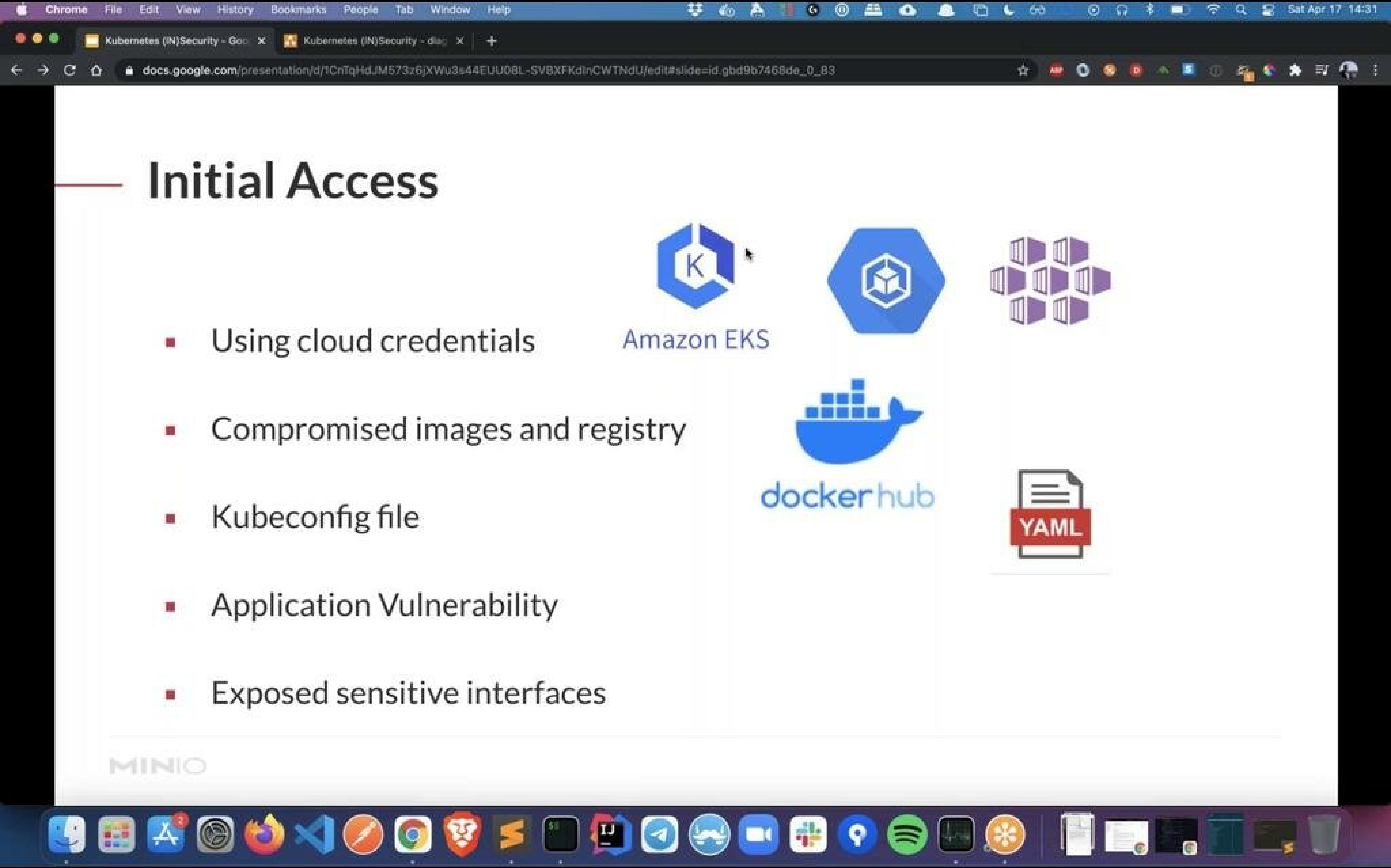
MINIO

Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:26
Kubernetes (IN)Security - Goo
Kubernetes (IN)Security - dia
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdInCWTNdU/edit#slide=id.gbd9b7468de_0_83

Kubernetes Components

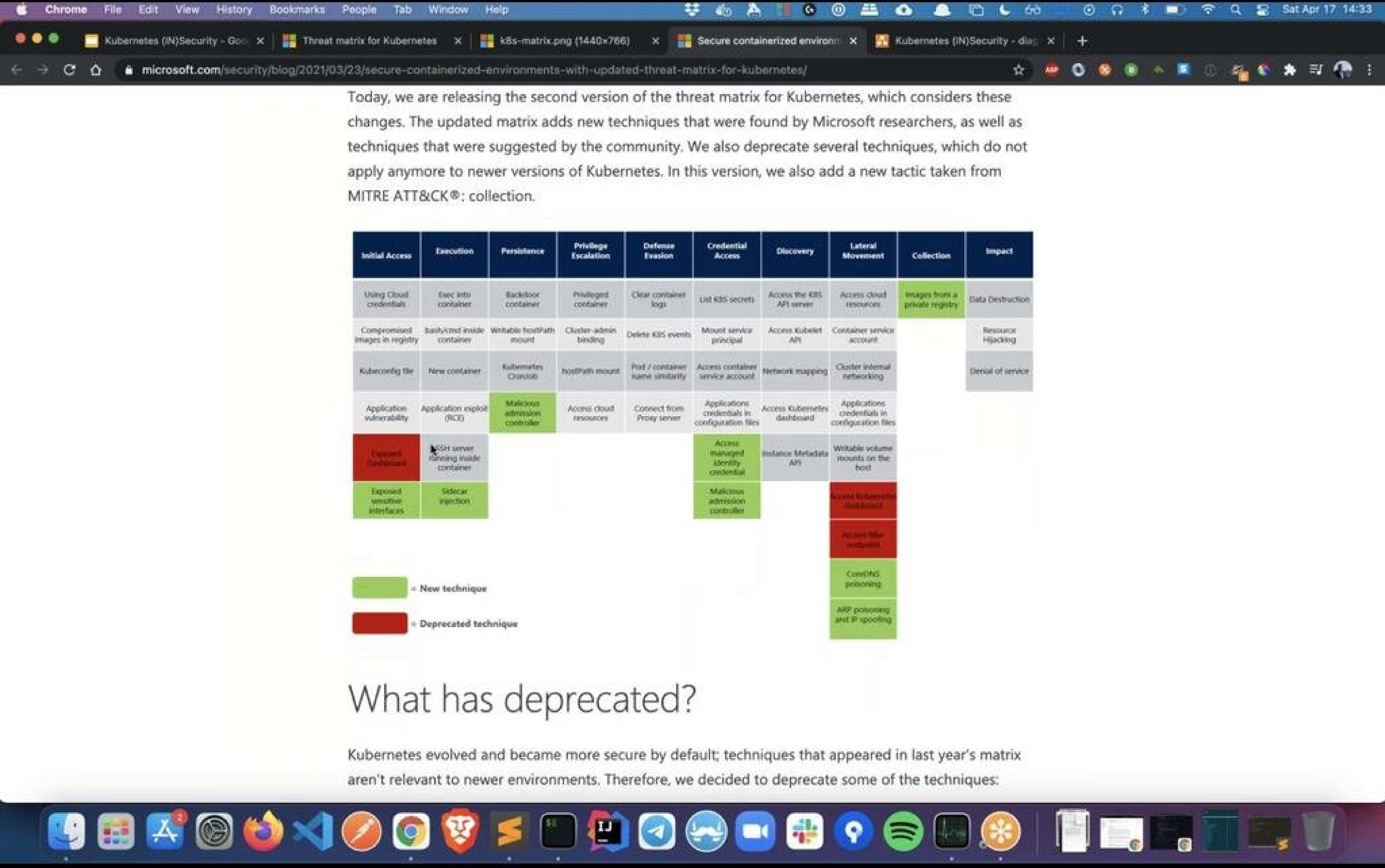
Chrome
File
Edit
View
History
Bookmarks
People
Tab
Window
Help
Sat Apr 17 14:31
Kubernetes (IN)Security - Goo
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gbd9b7468de_0_83

Kubernetes most common attack techniques


Chrome
File
Edit
View
History
Bookmarks
People
Tab
Window
Help
Sat Apr 17 14:31
Kubernetes (IN)Security - Goo
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gbd9b7468de_0_83
Amazon EKS
docker hub
YAML
MINIO

Initial Access

- Using cloud credentials
- Compromised images and registry
- Kubeconfig file
- Application Vulnerability
- Exposed sensitive interfaces


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:33
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - dia
microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/

Today, we are releasing the second version of the threat matrix for Kubernetes, which considers these changes. The updated matrix adds new techniques that were found by Microsoft researchers, as well as techniques that were suggested by the community. We also deprecate several techniques, which do not apply anymore to newer versions of Kubernetes. In this version, we also add a new tactic taken from MITRE ATT&CK®: collection.

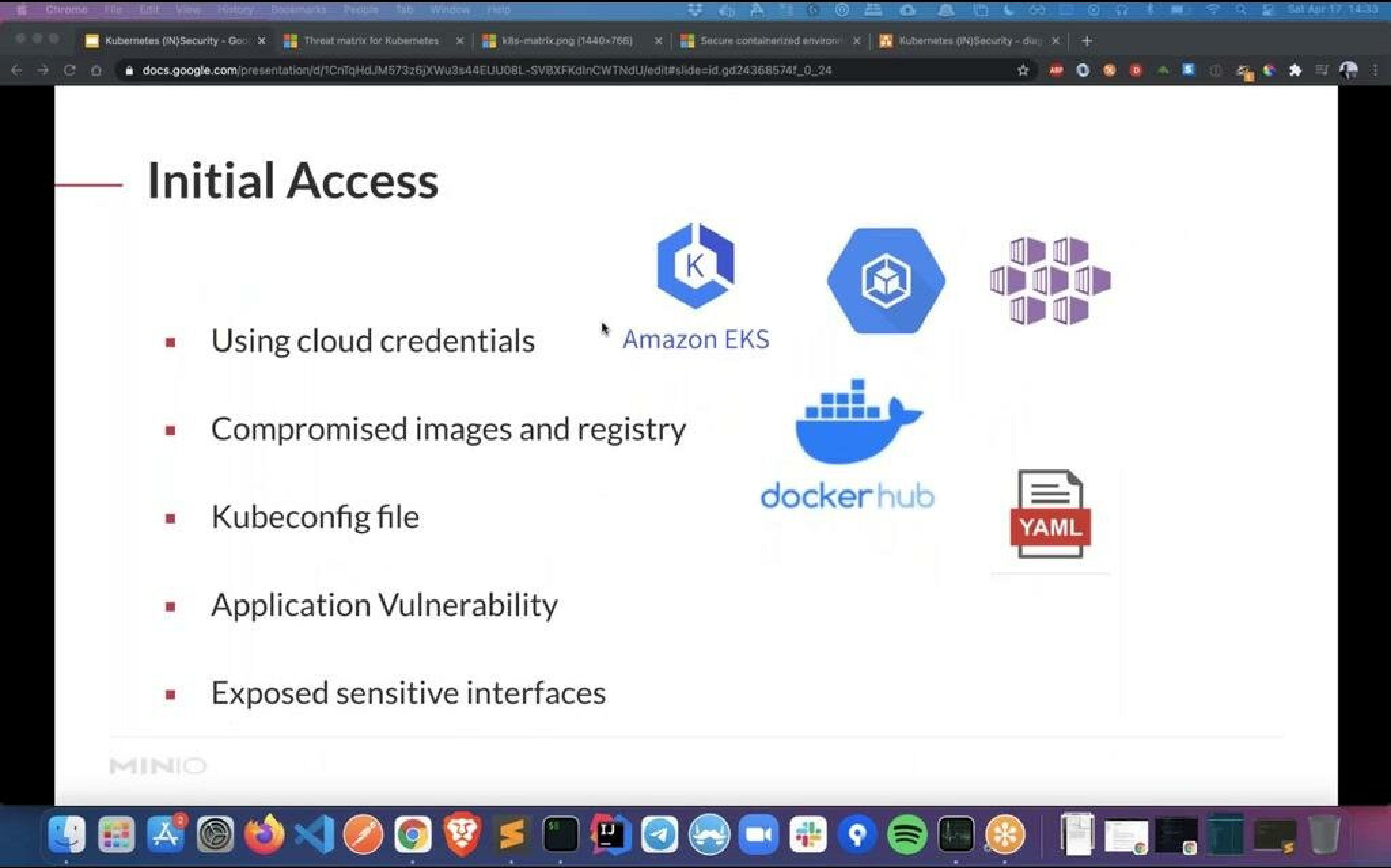
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
Using Cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List K8S secrets	Access the K8S API server	Access cloud resources	Images from a private registry	Data Destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account		Resource Hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod / container name similarity	Access container service account	Network mapping	Cluster internal networking		Denial of service
Application vulnerability	Application exploit (RCE)	Malicious admission controller	Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access Kubernetes dashboard	Applications credentials in configuration files		
Exposed Dashboard	SSH server running inside container				Access managed identity credential	Instance Metadata API	Writable volume mounts on the host		
Exposed sensitive interfaces	Sidecar injection				Malicious admission controller		Access Kubernetes dashboard		
							Access tiller endpoint		
							CoreDNS poisoning		
							ARP poisoning and IP spoofing		

🟩 = New technique

🟥 = Deprecated technique

What has deprecated?

Kubernetes evolved and became more secure by default; techniques that appeared in last year's matrix aren't relevant to newer environments. Therefore, we decided to deprecate some of the techniques:


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:33
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

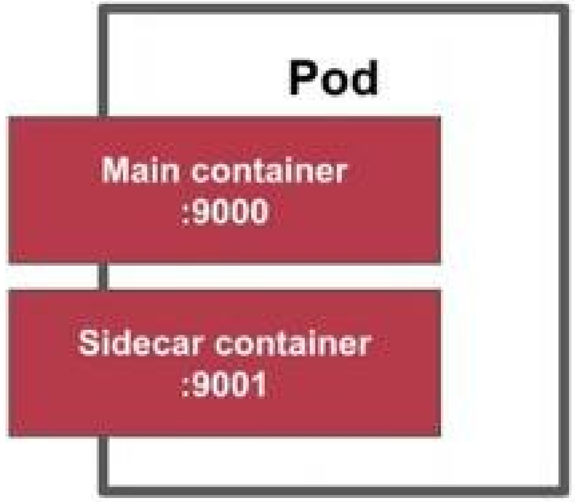
Initial Access

- Using cloud credentials
- Compromised images and registry
- Kubeconfig file
- Application Vulnerability
- Exposed sensitive interfaces

Amazon EKS
docker hub
YAML
MINIO

Execution

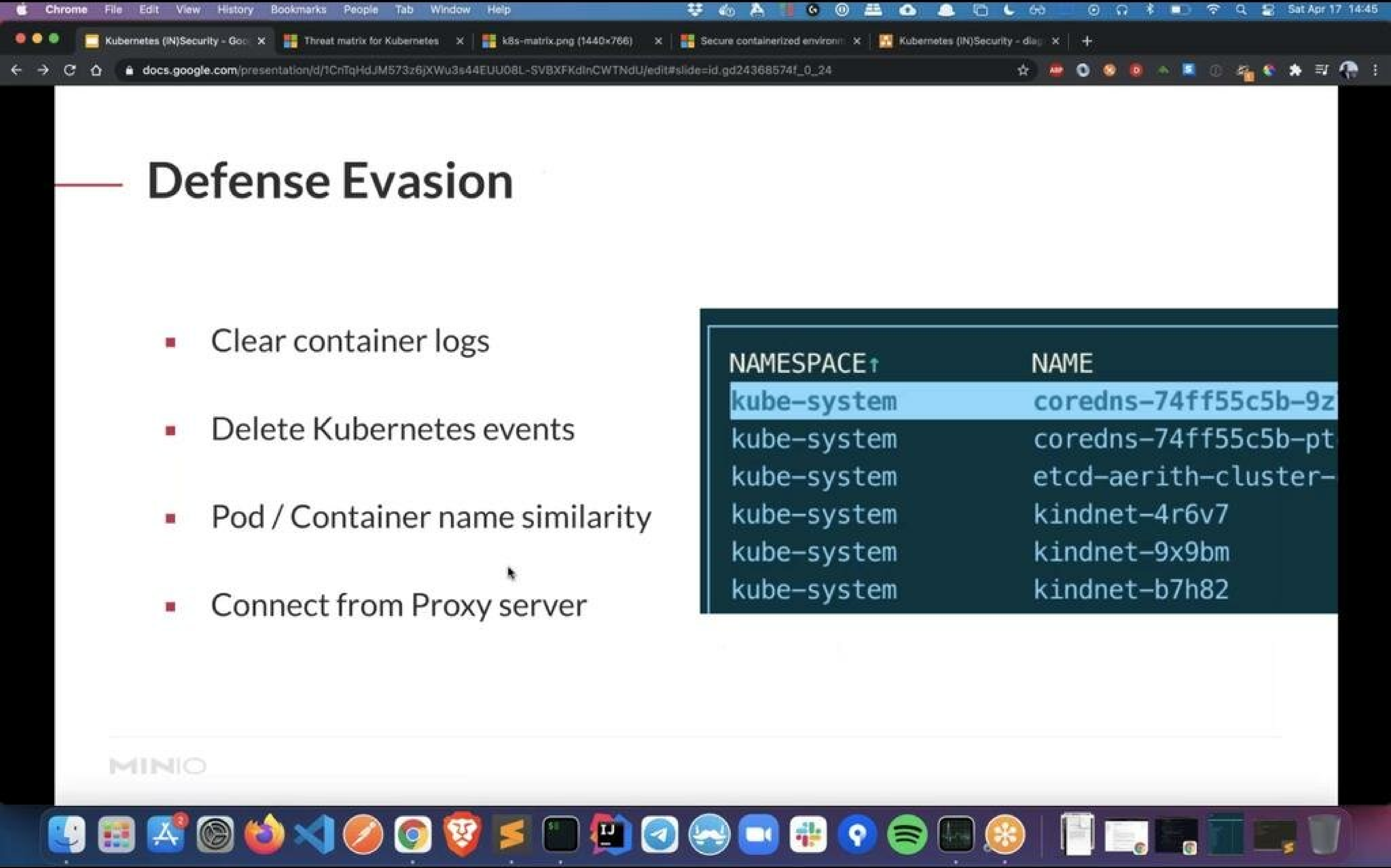
- Exec into container
- New container
- Application exploit (RCE)
- SSH server running inside container
- Sidecar Injection



Pod

Main container
:9000

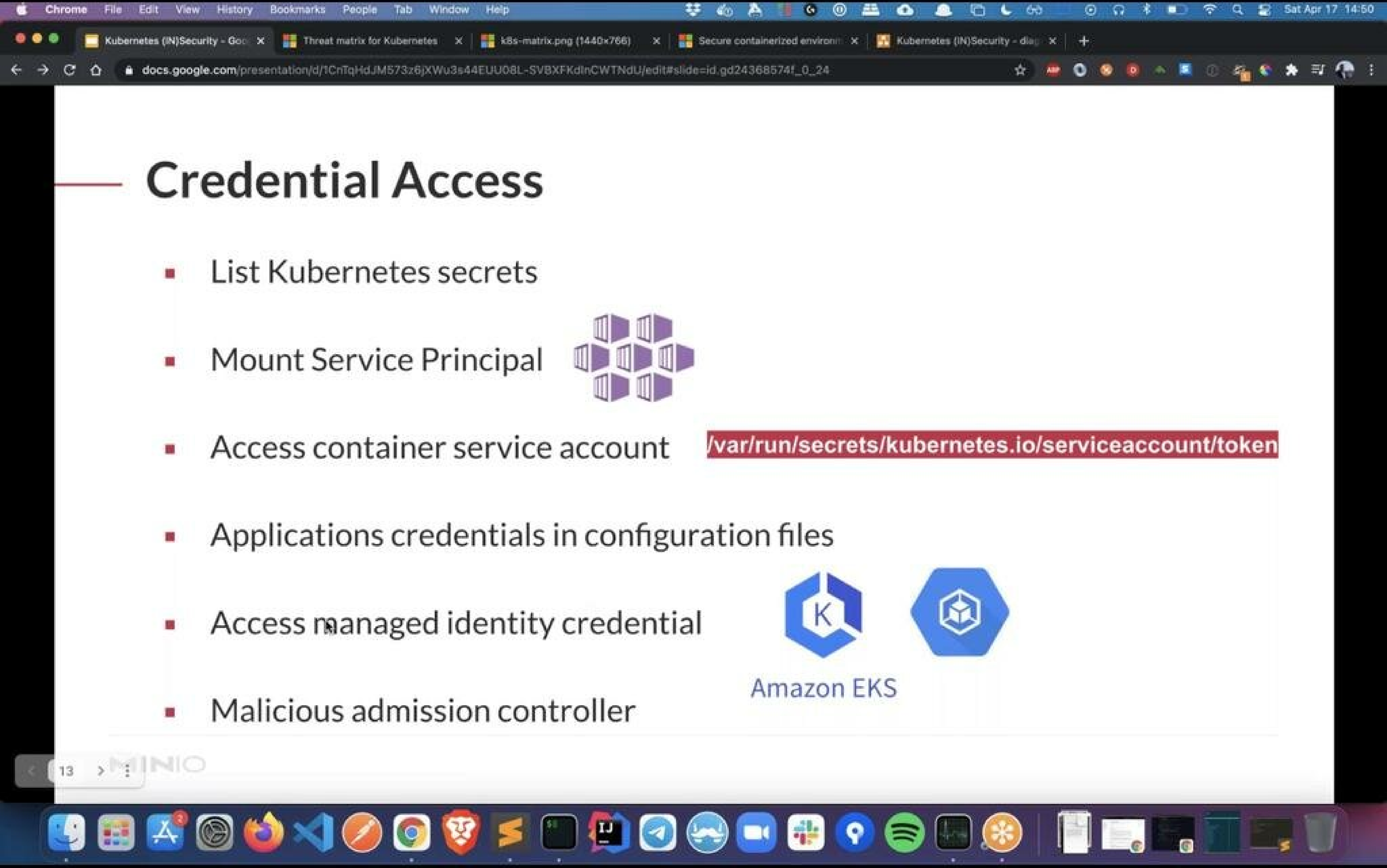
Sidecar container
:9001


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:45
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdInCWTNdU/edit#slide=id.gd24368574f_0_24

Defense Evasion

- Clear container logs
- Delete Kubernetes events
- Pod / Container name similarity
- Connect from Proxy server

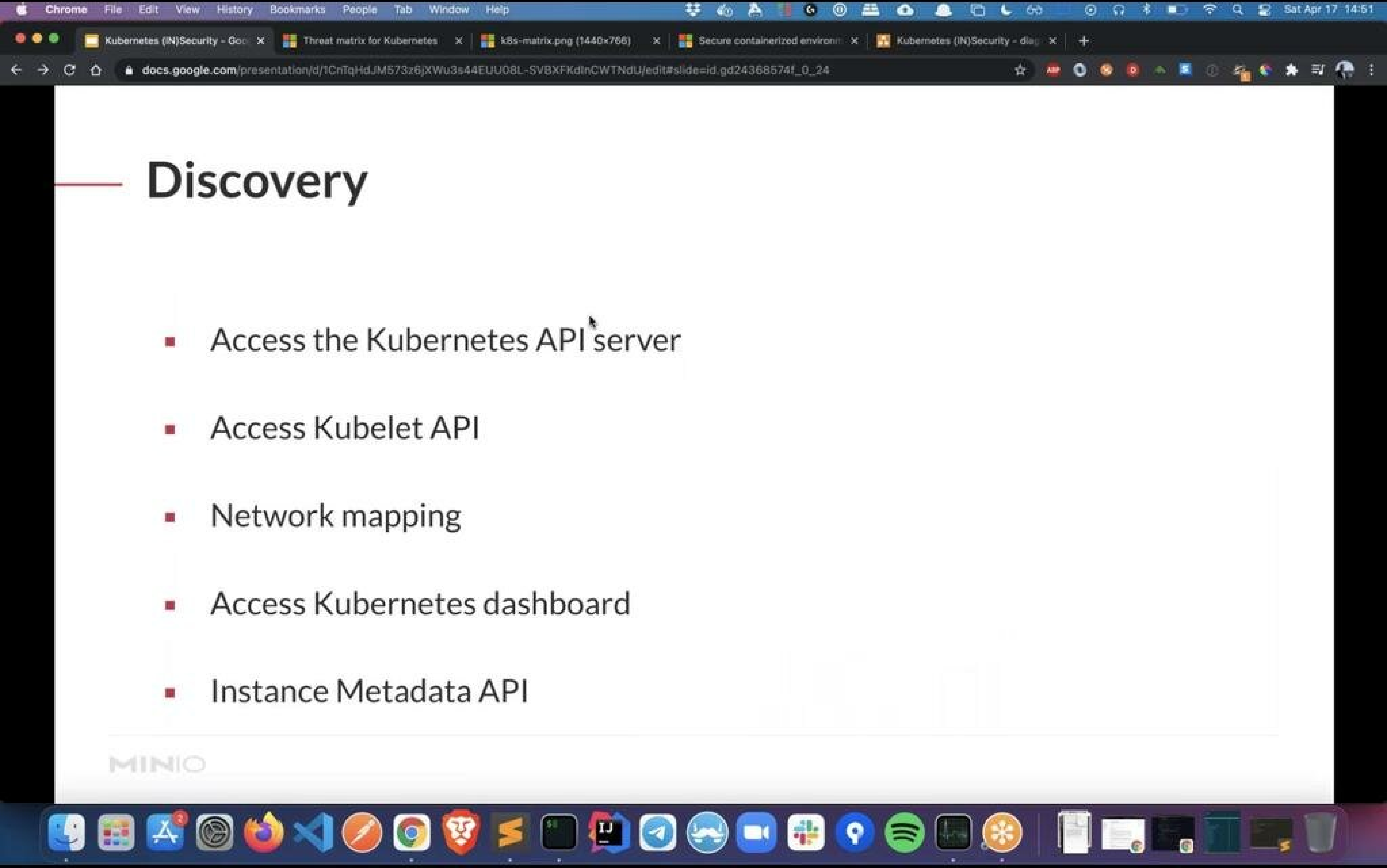
```
NAMESPACE↑          NAME
kube-system         coredns-74ff55c5b-9z
kube-system         coredns-74ff55c5b-pt
kube-system         etcd-aerith-cluster-
kube-system         kindnet-4r6v7
kube-system         kindnet-9x9bm
kube-system         kindnet-b7h82
```



Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:50
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24
Amazon EKS
MINIO
13

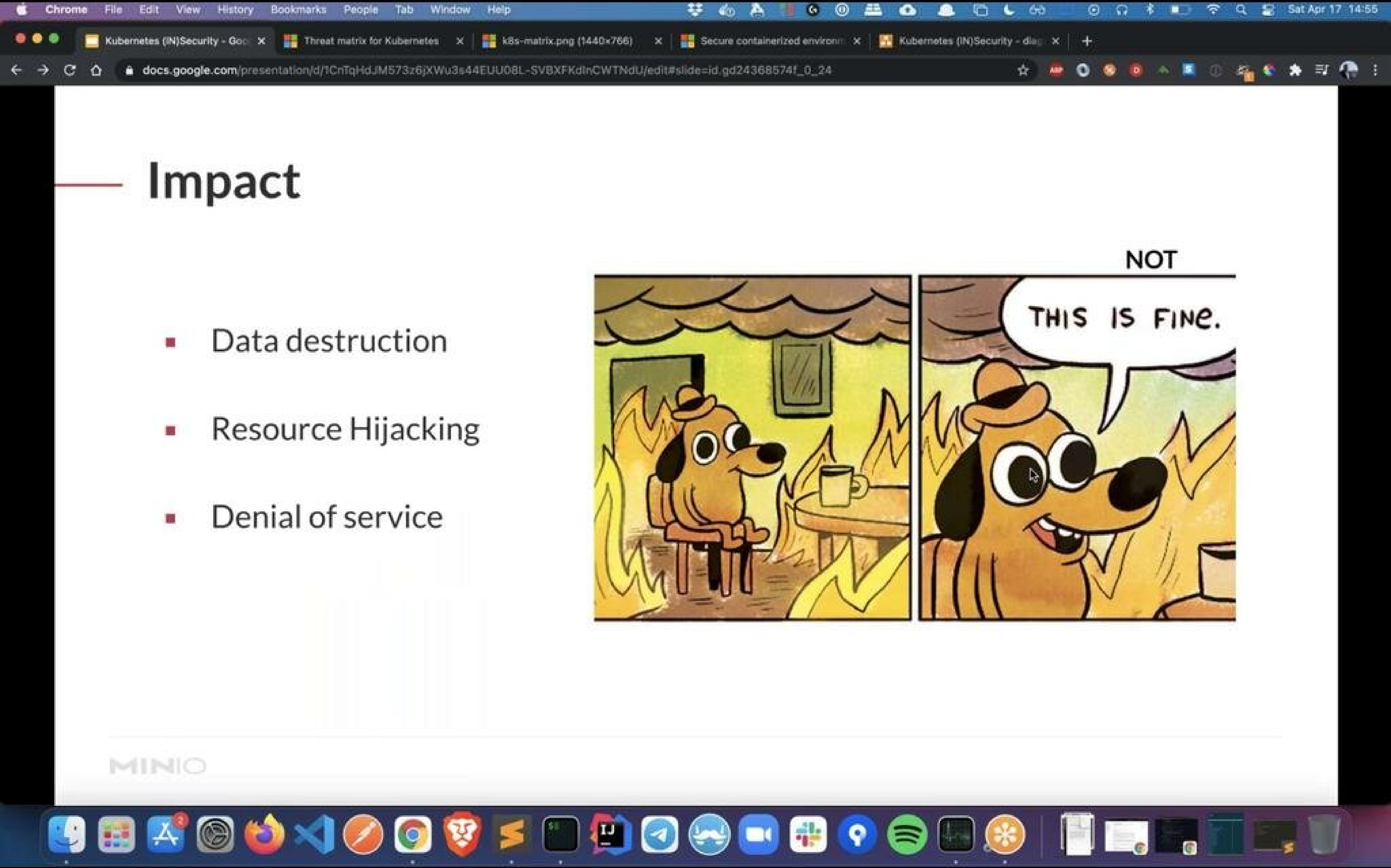
Credential Access

- List Kubernetes secrets
- Mount Service Principal
- Access container service account /var/run/secrets/kubernetes.io/serviceaccount/token
- Applications credentials in configuration files
- Access managed identity credential
- Malicious admission controller


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:51
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

Discovery

- Access the Kubernetes API server
- Access Kubelet API
- Network mapping
- Access Kubernetes dashboard
- Instance Metadata API



Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:55
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

Impact

- Data destruction
- Resource Hijacking
- Denial of service

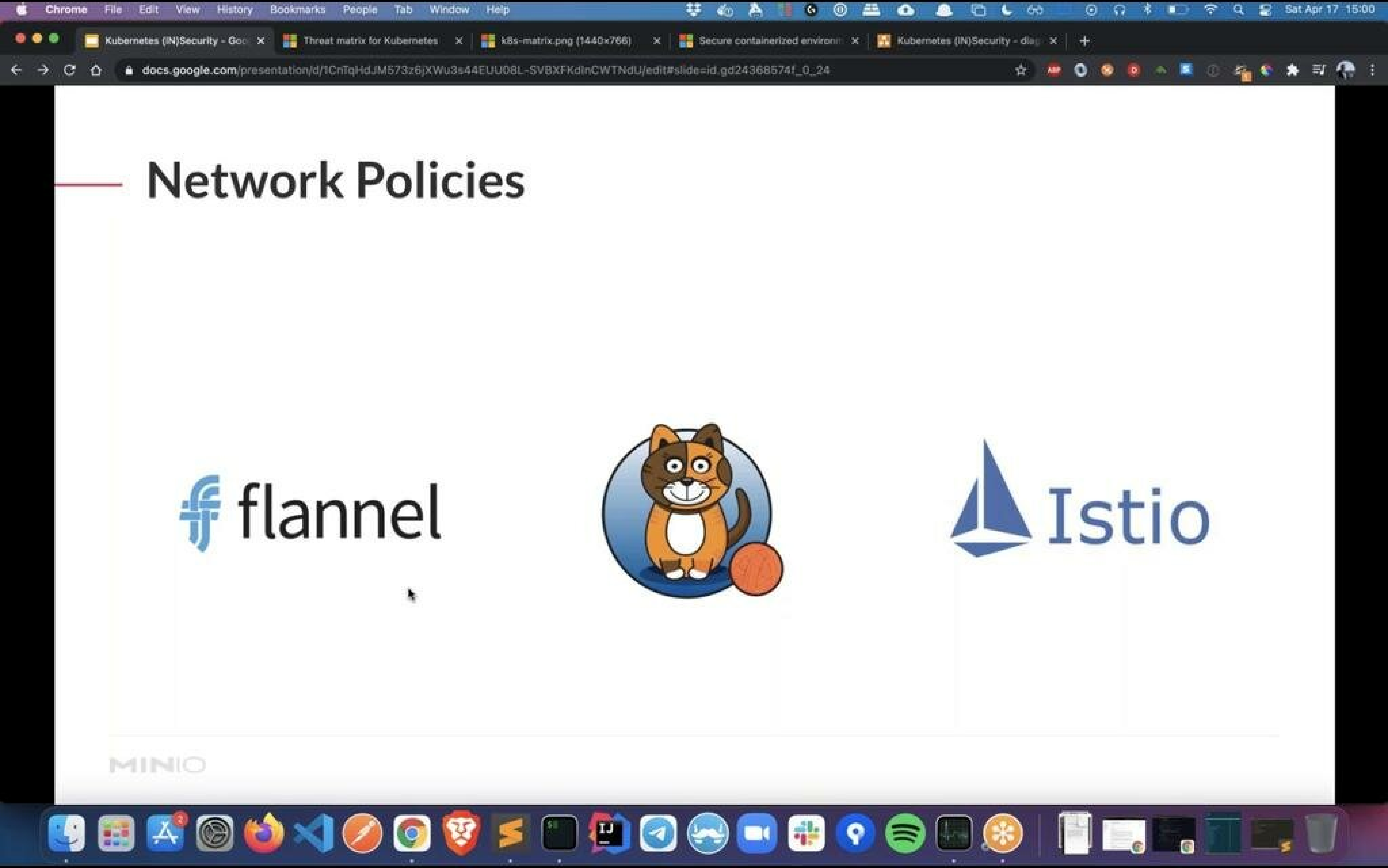
MINIO

Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:57
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24
MINIO

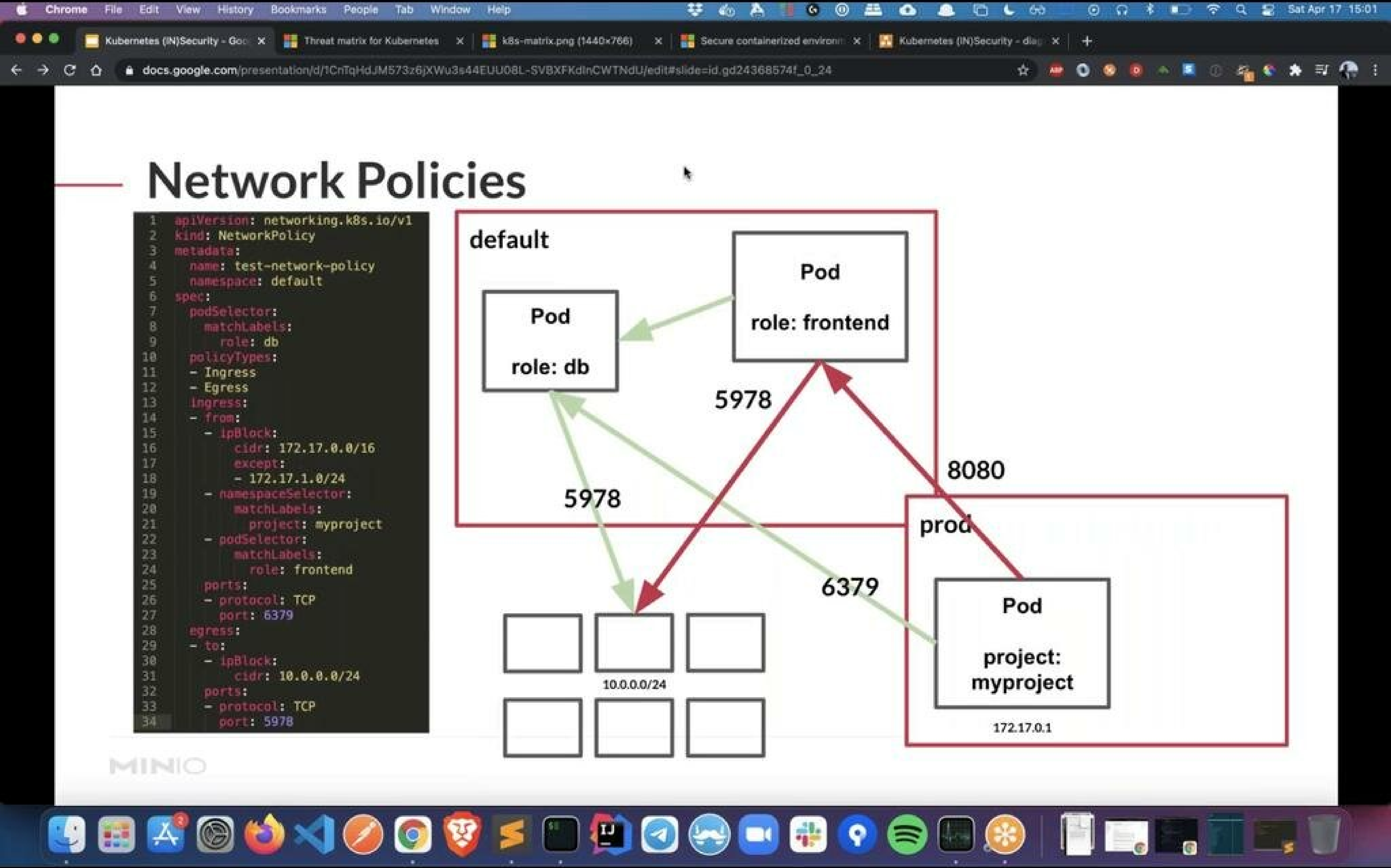
Kubernetes build-in defences

Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 14:57
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24
MINIO

Security Context for Pods


Chrome
File
Edit
View
History
Bookmarks
People
Tab
Window
Help
Sat Apr 17 15:00
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24
flannel
Istio
MINIO

Network Policies

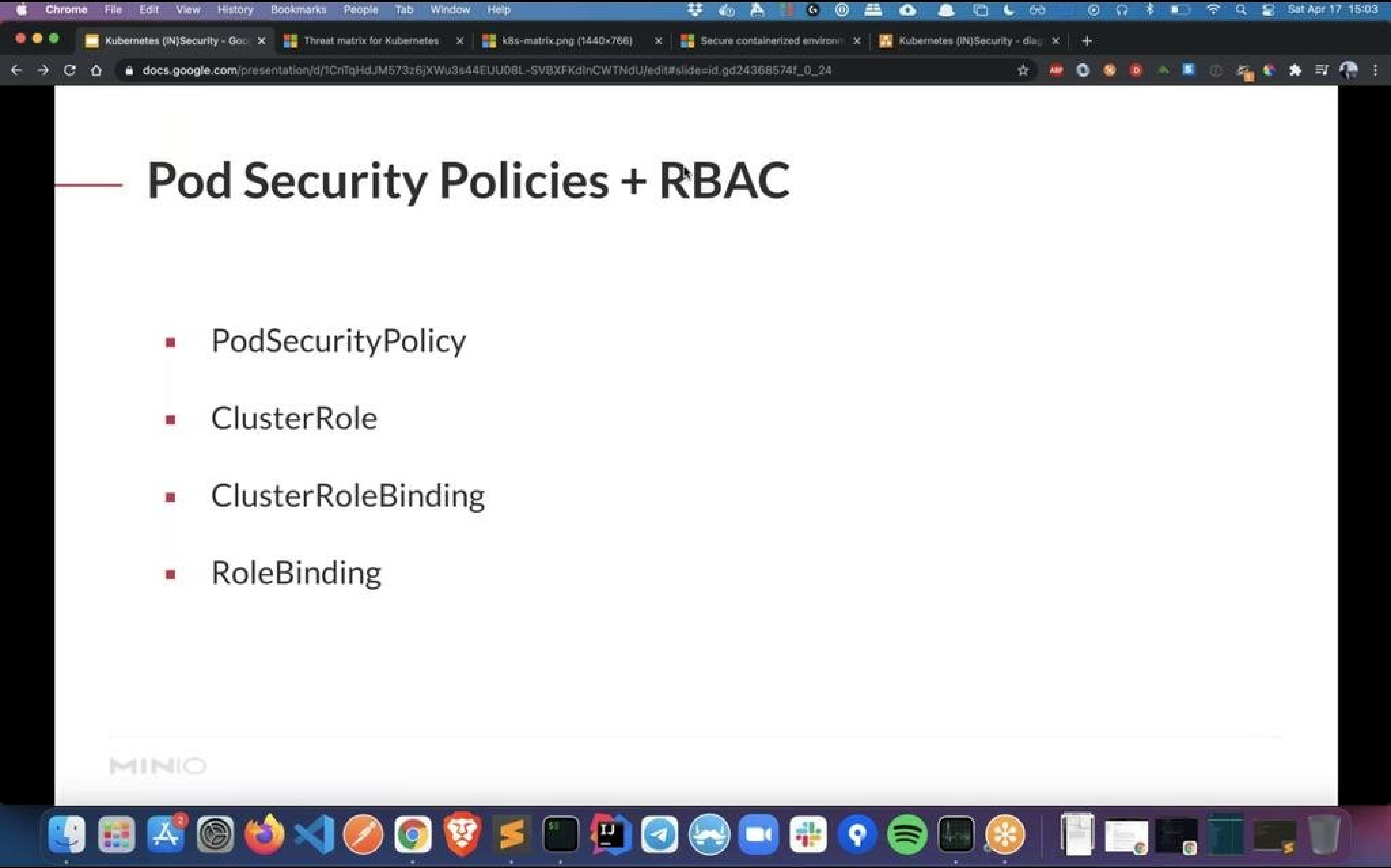

Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 15:01
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

Network Policies

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: test-network-policy
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: db
  policyTypes:
  - Ingress
  - Egress
  ingress:
  - from:
    - ipBlock:
        cidr: 172.17.0.0/16
        except:
        - 172.17.1.0/24
    - namespaceSelector:
        matchLabels:
          project: myproject
    - podSelector:
        matchLabels:
          role: frontend
    ports:
    - protocol: TCP
      port: 6379
  egress:
  - to:
    - ipBlock:
        cidr: 10.0.0.0/24
    ports:
    - protocol: TCP
      port: 5978
```

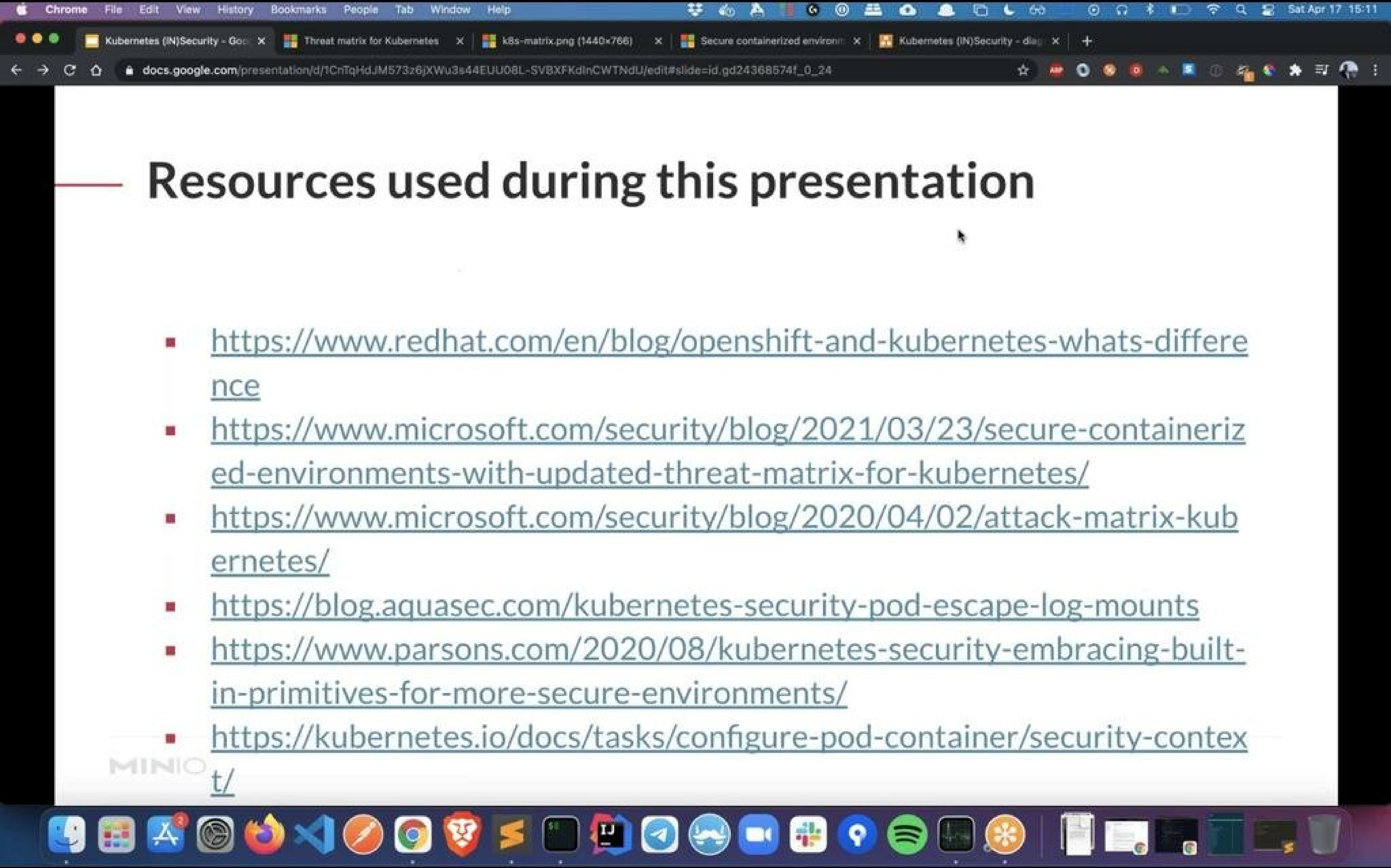
Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 15:02
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

Pod Security Policies


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 15:03
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

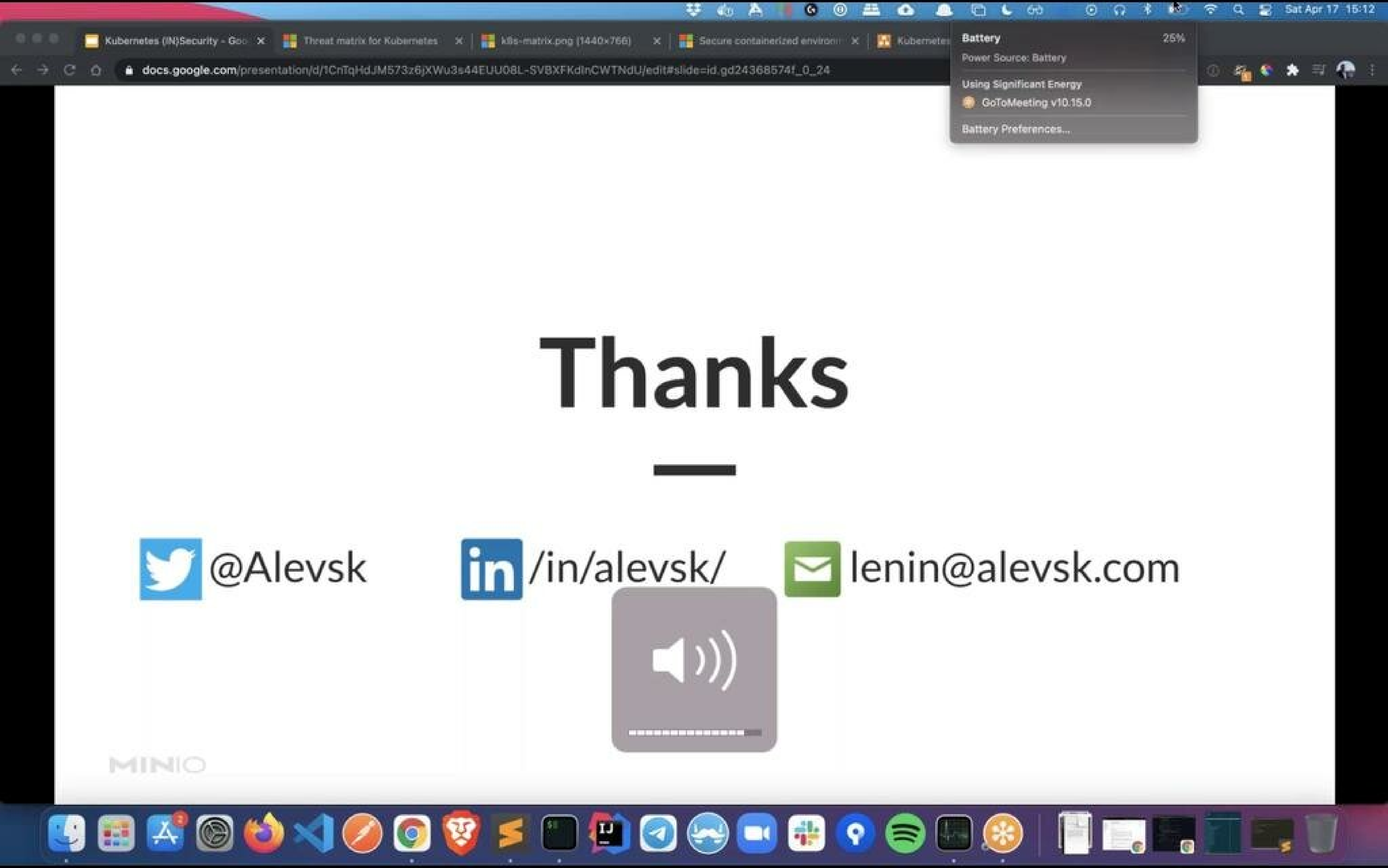
Pod Security Policies + RBAC

- PodSecurityPolicy
- ClusterRole
- ClusterRoleBinding
- RoleBinding


Chrome File Edit View History Bookmarks People Tab Window Help
Sat Apr 17 15:11
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes (IN)Security - diag
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24

Resources used during this presentation

- https://www.redhat.com/en/blog/openshift-and-kubernetes-whats-difference
- https://www.microsoft.com/security/blog/2021/03/23/secure-containerized-environments-with-updated-threat-matrix-for-kubernetes/
- https://www.microsoft.com/security/blog/2020/04/02/attack-matrix-kubernetes/
- https://blog.aquasec.com/kubernetes-security-pod-escape-log-mounts
- https://www.parsons.com/2020/08/kubernetes-security-embracing-built-in-primitives-for-more-secure-environments/
- https://kubernetes.io/docs/tasks/configure-pod-container/security-context/


Sat Apr 17 15:12
Kubernetes (IN)Security - Goo
Threat matrix for Kubernetes
k8s-matrix.png (1440×766)
Secure containerized environm
Kubernetes
docs.google.com/presentation/d/1CnTqHdJM573z6jXWu3s44EUU08L-SVBXFKdlnCWTNdU/edit#slide=id.gd24368574f_0_24
Battery 25%
Power Source: Battery
Using Significant Energy
GoToMeeting v10.15.0
Battery Preferences...
MINIO

Thanks

@Alevsk

/in/alevsk/

lenin@alevsk.com