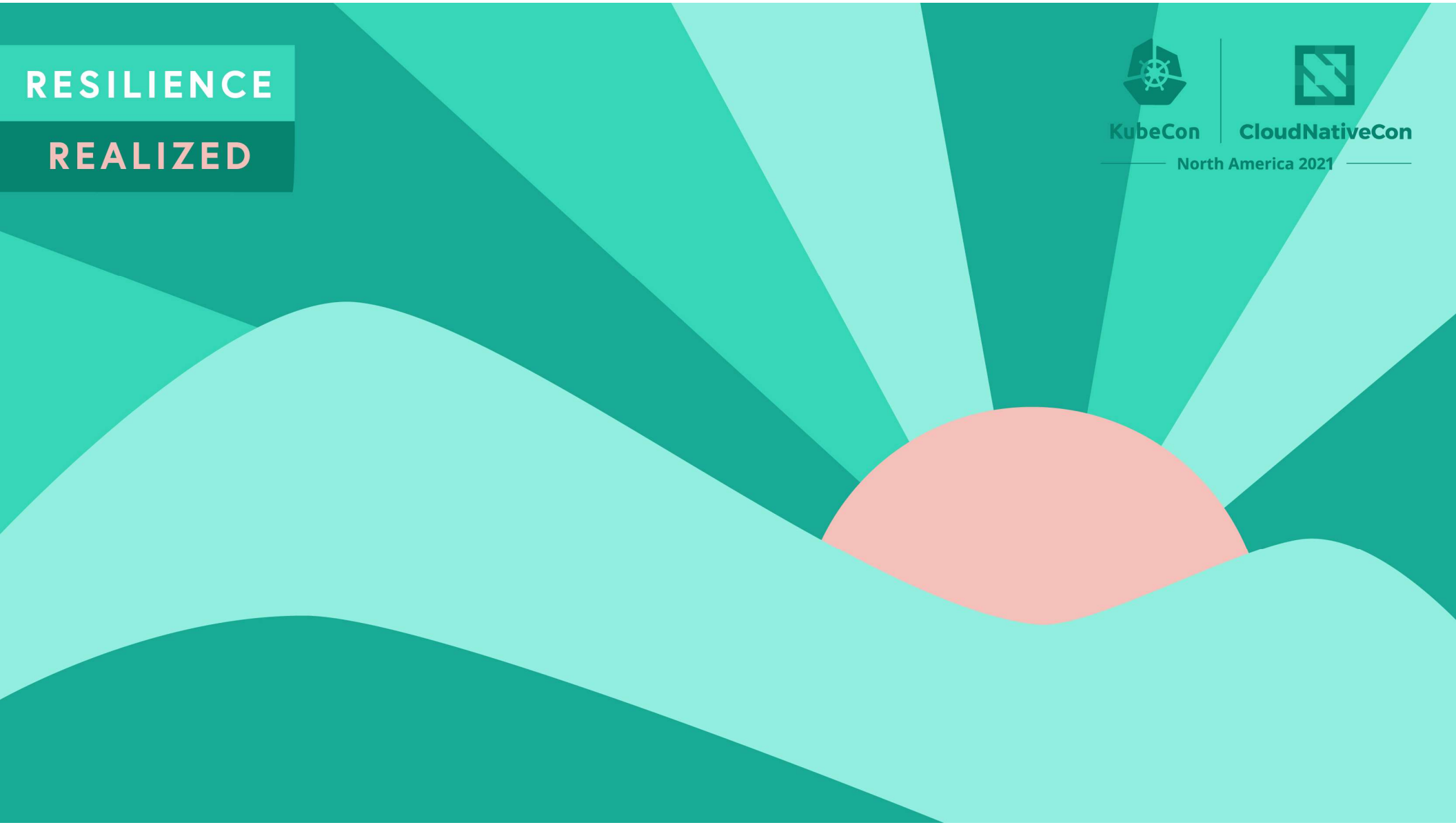

RESILIENCE
REALIZED
KubeCon
CloudNativeCon
North America 2021

RESILIENCE
REALIZED

Know Your Enemy: Mapping Security Risks Using Threat Matrix for Kubernetes

Yossi Weizman, Senior Security Researcher, Microsoft

Ram Pliskin, Principal Security Research Manager, Microsoft

Agenda

- Introducing the problem space

Agenda

- Introducing the problem space
- Threat Matrix for Kubernetes

Agenda

- Introducing the problem space
- Threat Matrix for Kubernetes
- Measuring security posture

Agenda

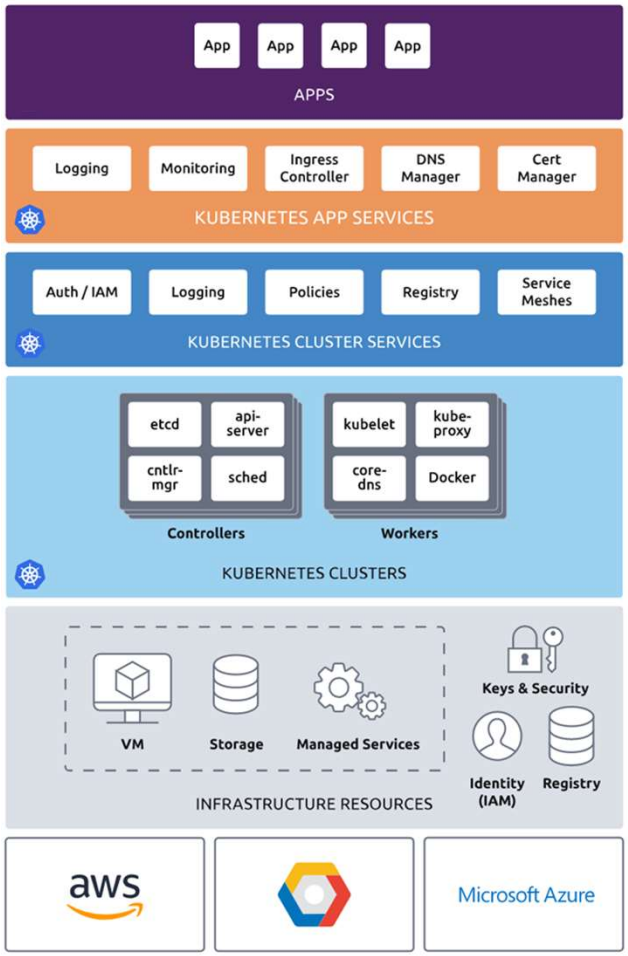
- Introducing the problem space
- Threat Matrix for Kubernetes
- Measuring security posture
- MITRE ATT&CK for Containers

Where did we start?

- The problem space

Where did we start?

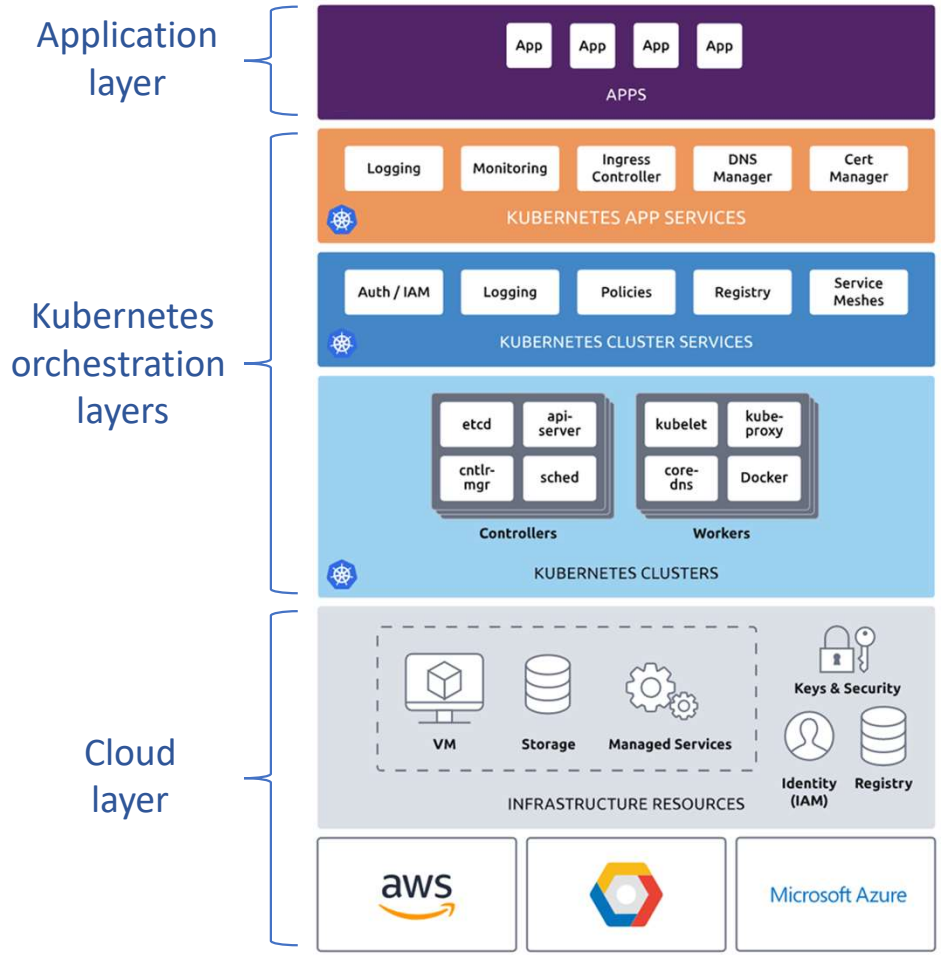
- The problem space
- Kubernetes as an abstraction layer



Source: https://www.pulumi.com/images/docs/quickstart/kubernetes/cake.svg

Where did we start?

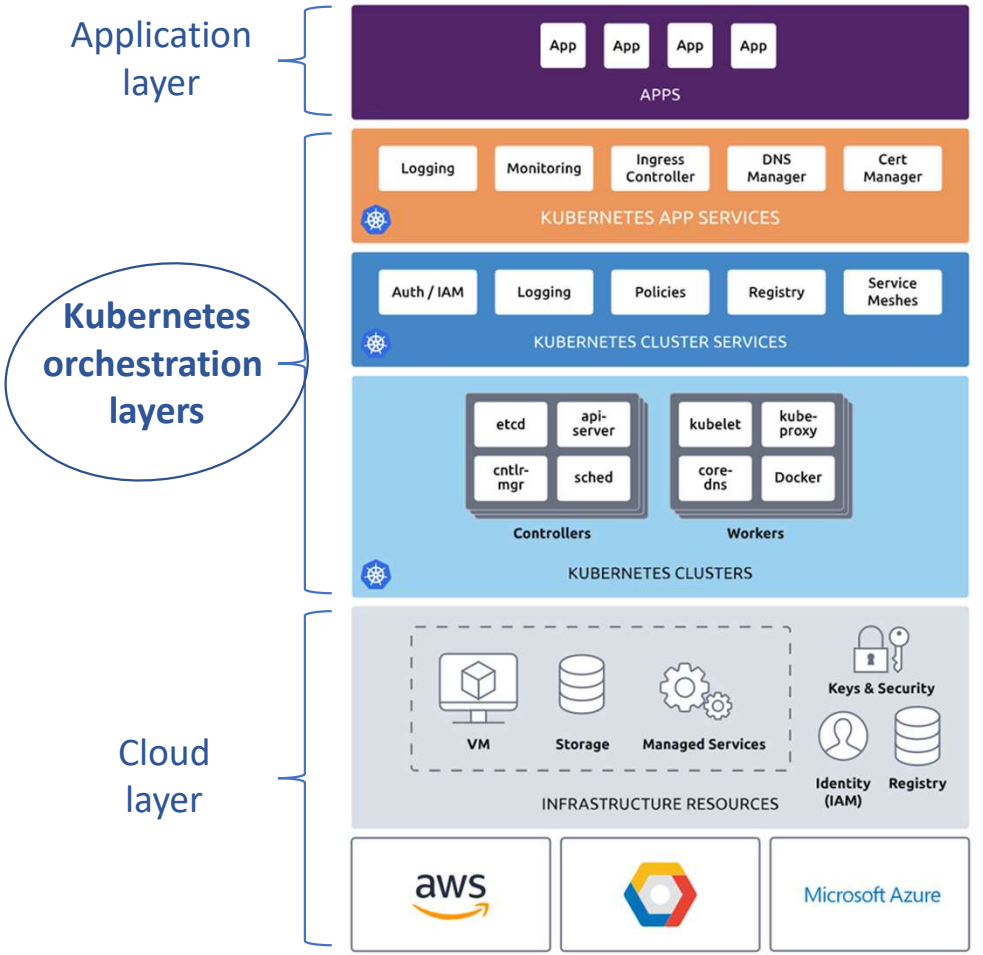
- The problem space
- Kubernetes as an abstraction layer
- Focusing on the Kubernetes layers



Source: https://www.pulumi.com/images/docs/quickstart/kubernetes/cake.svg

Where did we start?

- The problem space
- Kubernetes as an abstraction layer
- Focusing on the Kubernetes layers

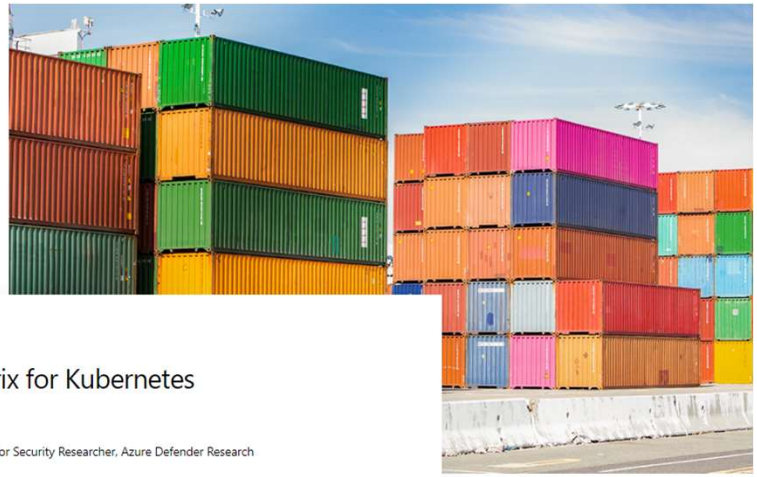


Source: https://www.pulumi.com/images/docs/quickstart/kubernetes/cake.svg

Kubernetes threat landscape

KubeCon | CloudNativeCon
North America 2021

The goal:
Mapping the main threats of Kubernetes



April 2, 2020

Threat matrix for Kubernetes

Yossi Weizman Senior Security Researcher, Azure Defender Research

Share

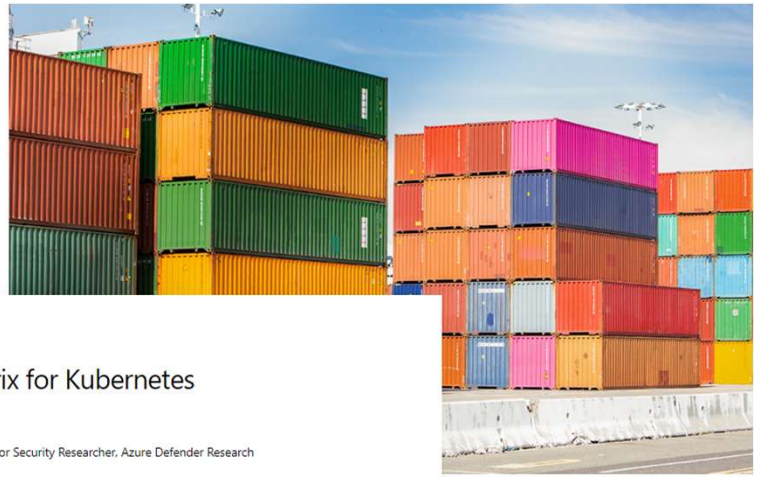
Updated on May 10, 2021: An updated version of the threat matrix for containers is available here.

Kubernetes, the most popular container orchestration system and one of the fastest-growing projects in the history of open source, becomes a significant part of many companies' compute stack. The flexibility and scalability of containers encourage many developers to move their workloads to Kubernetes. While Kubernetes has many advantages, it also brings new security challenges that should be considered. Therefore, it is crucial to understand the various security risks that exist in containerized environments, and specifically in Kubernetes.

Kubernetes threat landscape

KubeCon CloudNativeCon North America 2021

The goal:
Mapping the main threats of Kubernetes



April 2, 2020

Threat matrix for Kubernetes

Yossi Weizman Senior Security Researcher, Azure Defender Research

ATT&CK® https://attack.mitre.org/

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	17 techniques	12 techniques	32 techniques	14 techniques	22 techniques	9 techniques	15 techniques	16 techniques	8 techniques	13 techniques
Drive-by Compromise	Command and Scripting Interpreter (5)	Account Manipulation (1)	Abuse Elevation Control Mechanism (1)	Abuse Elevation Control Mechanism (1)	Brute Force (4)	Account Discovery (3)	Exploitation of Remote Services	Archive Collected Data (3)	Application Layer Protocol (4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Credentials from Password Stores (1)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (2)	Boot or Logon Autostart Execution (9)	Boot or Logon Autostart Execution (9)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (1)	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Phishing (3)	Scheduled Task/Job (5)	Browser Extensions	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	File and Directory Discovery	Remote Services (6)	Data from Information Repositories (1)	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Supply Chain Compromise (3)	Software Deployment Tools	Create Account (3)	Event Triggered Execution (15)	Execution Guardrails (1)	Man-in-the-Middle (2)	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Trusted Relationship	System Services (2)	Create or Modify System Process (4)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (4)	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (4)	User Execution (2)	Event Triggered Execution (15)	Hijack Execution Flow (11)	File and Directory Permissions Modification (2)	Network Sniffing	Password Policy Discovery		Data Staged (2)	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation			Hide Artifacts (10)	OS Credential Dumping (8)	Peripheral Device Discovery		Email Collection (3)	Non-Application Layer Protocol		Network Denial of Service (2)
				Hijack Execution Flow (11)		Permission Groups Discovery (3)					Resource Hijacking

Share

Updated on May 10, 2021: An updated version of the threat matrix for containers is available here.

Kubernetes, the most popular container orchestration system and one of the fastest-growing projects in the history of open source, becomes a significant part of many companies' compute stack. The flexibility and scalability of containers encourage many developers to move their workloads to Kubernetes. While Kubernetes has many advantages, it also brings new security challenges that should be considered. Therefore, it is crucial to understand the various security risks that exist in containerized environments, and specifically in Kubernetes.

Threat Matrix for Kubernetes

KubeCon CloudNativeCon North America 2021

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

aka.ms/K8sThreatMatrixV2

Threat Matrix for Kubernetes

KubeCon CloudNativeCon North America 2021

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

aka.ms/K8sThreatMatrixV2

Examples

Access managed identity credential

Managed identities are identities that are managed by the cloud provider and can be allocated to cloud resources, such as virtual machines. Those identities are used to authenticate with cloud services. The identity's secret is fully managed by the cloud provider, which eliminates the need to manage the credentials. Applications can obtain the identity's token by accessing the Instance Metadata Service (IMDS). Attackers who get access to a Kubernetes pod can leverage their access to the IMDS endpoint to get the managed identity's token. With a token, the attackers can access cloud resources.

Examples


KubeCon | CloudNativeCon
North America 2021

CoreDNS poisoning

CoreDNS is a modular Domain Name System (DNS) server written in Go, hosted by Cloud Native Computing Foundation (CNCF). CoreDNS is the main DNS service that is being used in Kubernetes. The configuration of CoreDNS can be modified by a file named corefile. In Kubernetes, this file is stored in a ConfigMap object, located at the kube-system namespace. If attackers have permissions to modify the ConfigMap, for example by using the container's service account, they can change the behavior of the cluster's DNS, poison it, and take the network identity of other services.

Examples

Images from private registry

The images that are running in the cluster can be stored in a private registry. For pulling those images, the container runtime engine (such as Docker or containerd) needs to have valid credentials to those registries. If the registry is hosted by the cloud provider, in services like Azure Container Registry (ACR) or Amazon Elastic Container Registry (ECR), cloud credentials are used to authenticate to the registry. If attackers get access to the cluster, in some cases they can obtain access to the private registry and pull its images. For example, attackers can use the managed identity token as described in the "Access managed identity credential" technique. Similarly, in EKS, attackers can use the AmazonEC2ContainerRegistryReadOnly policy that is bound by default to the node's IAM role.

Threat Matrix for Kubernetes

How to use the Threat Matrix to measure our coverage to threats?

Threat Matrix for Kubernetes

How to use the Threat Matrix to measure our coverage to threats?

Let’s see an example

Kubeflow Pipelines campaign

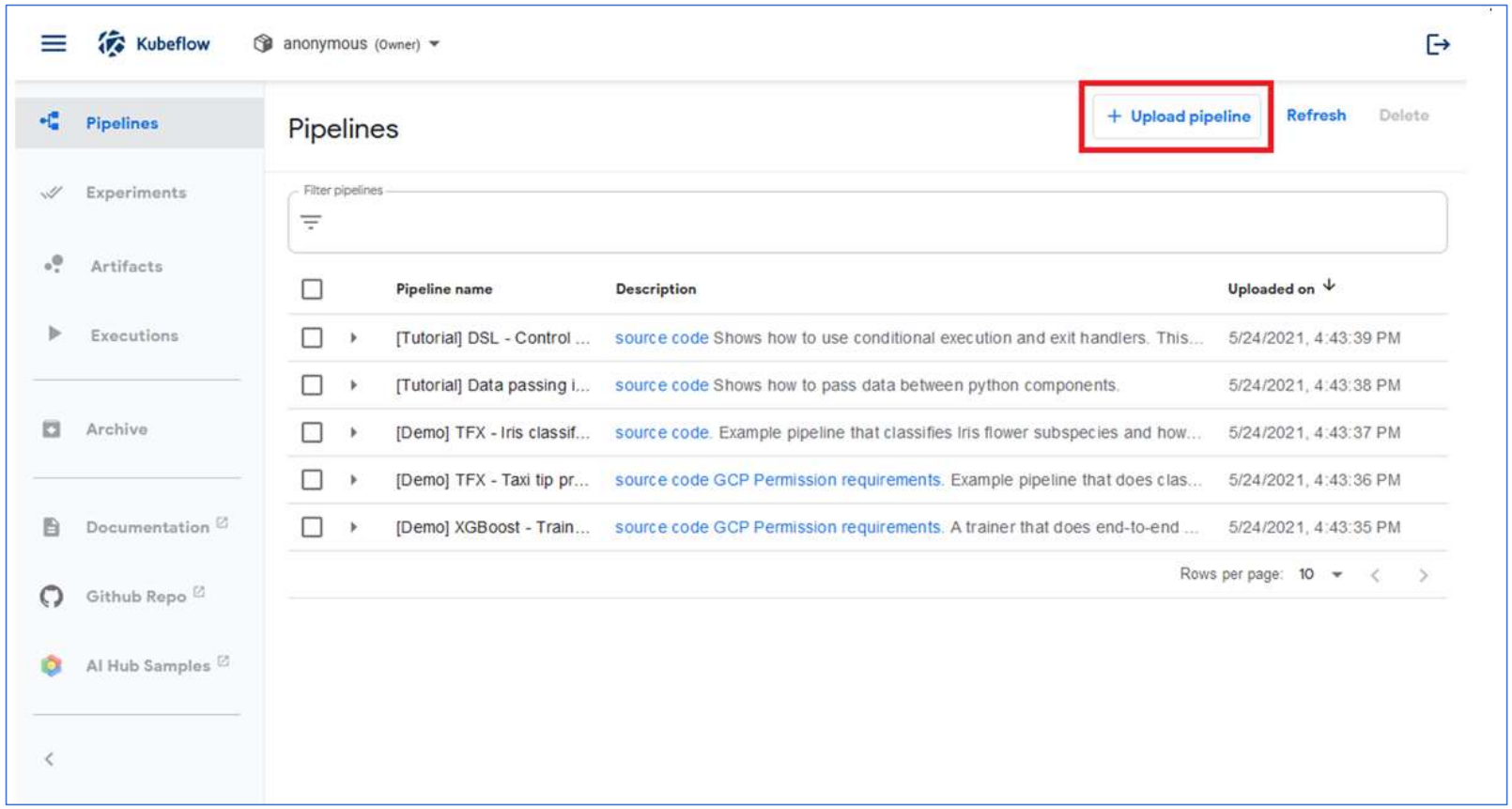
- Kubeflow is a framework for running ML tasks in Kubernetes.
- Some of its functionality is exposed via the Kubernetes API server (CRDs) and some via a centralized dashboard that is deployed with the framework.
- In some configurations, Kubeflow doesn’t require authentication.
- If the dashboard’s service is exposed externally, it allows free access to the Kubeflow management interface.

Kubeflow Pipelines campaign

- In May 2021, a large-scale campaign impacted Internet-accessible Kubeflow deployments.
- Attackers used open dashboards for deploying a malicious Kubeflow Pipeline.
- Kubeflow pipeline is a service for creating ML pipelines, based on Argo Workflow.

Kubeflow Pipelines campaign

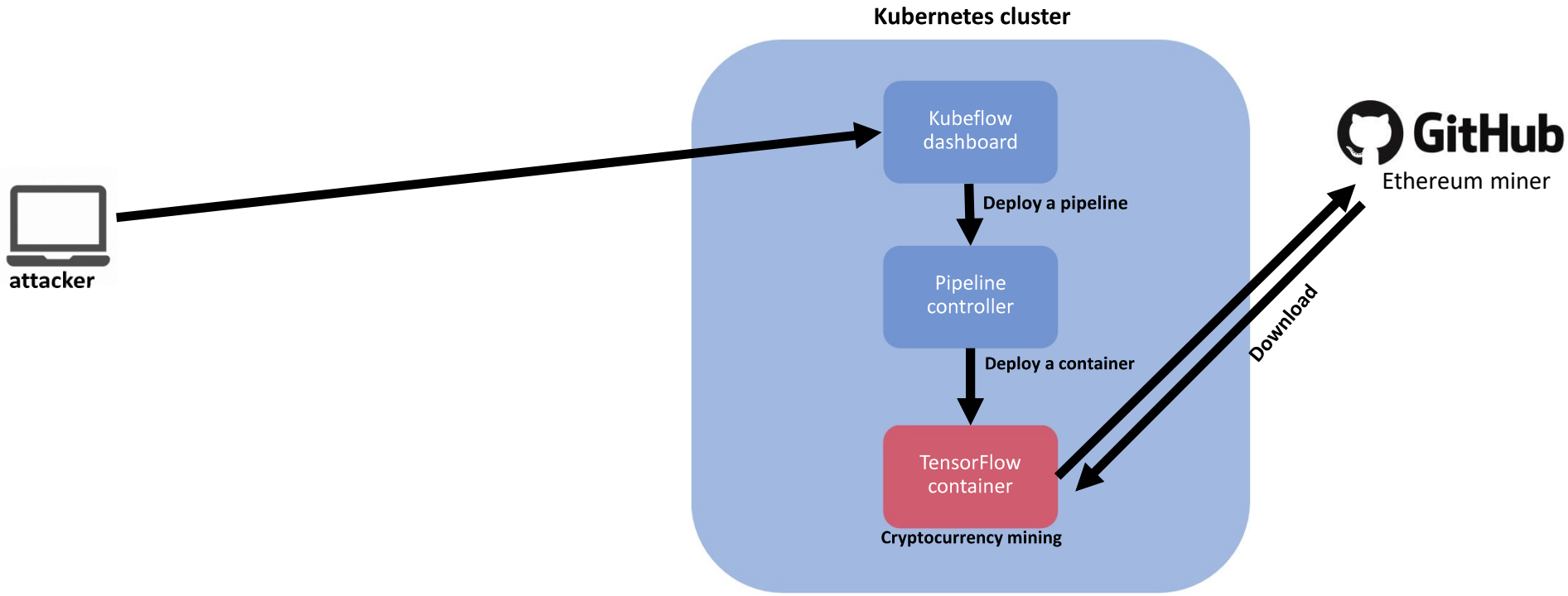
KubeCon CloudNativeCon North America 2021



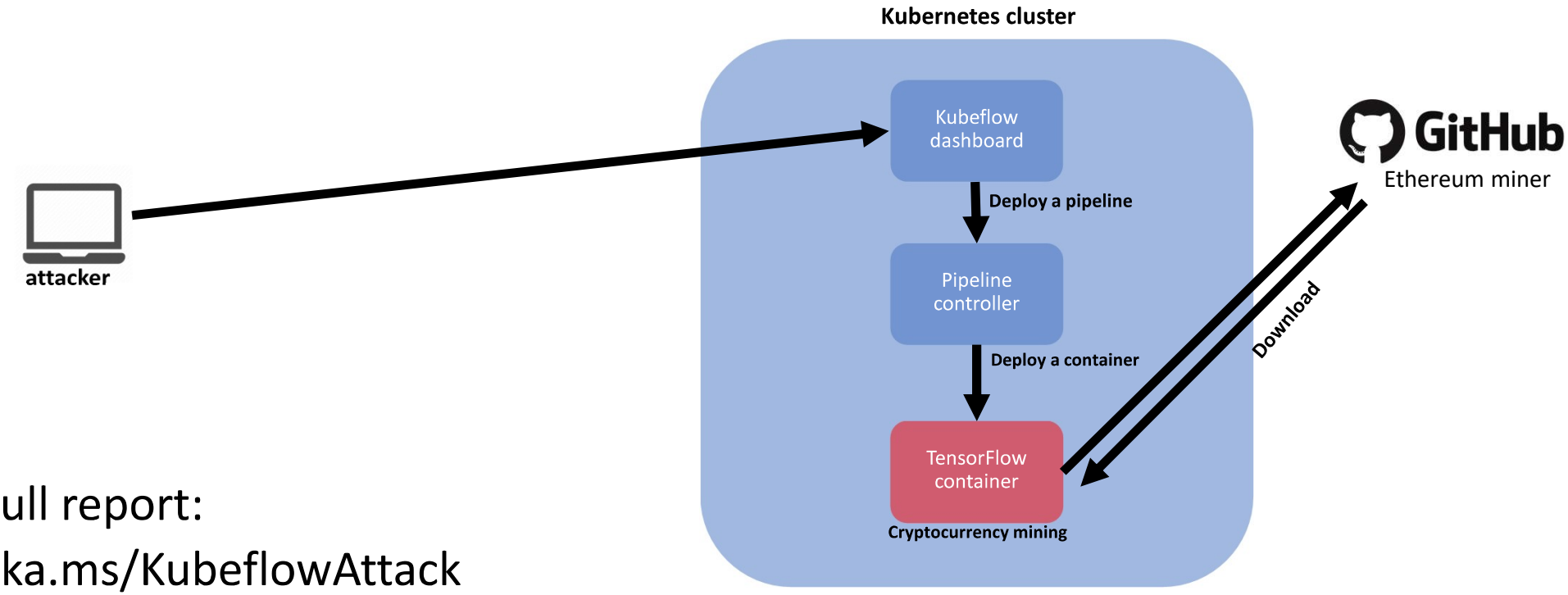
Kubeflow Pipelines campaign

- Using Kubeflow pipelines, the attackers deployed malicious containers in the cluster.
- Those containers were used for running crypto mining tasks on the cluster (using both CPU and GPU).
- The containers ran on top of a legitimate TensorFlow image.

Kubeflow Pipelines campaign



Kubeflow Pipelines campaign



Full report:
aka.ms/KubeflowAttack

Measuring the security coverage

How can we use the Threat Matrix to measure our coverage to this attack?

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Step 1: Mark the relevant techniques

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Step 1: Mark the relevant techniques

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Step 2: Evaluate our coverage

Measuring the security coverage

KubeCon CloudNativeCon North America 2021

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Monitor exposure of services to the Internet.
For example: Monitor LoadBalancer service creations

Measuring the security coverage

KubeCon CloudNativeCon North America 2021

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Monitor container deployments:

- **Image**
- **Entry points \ args**
- **Configurations**
- **etc**

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Monitor the images of the workload's containers

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

Monitor excessive permissions and suspicious operations of service accounts (Kubernetes audit log)

Measuring the security coverage

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

In orchestration level: Monitor the container's entry point, arguments, exec commands

In node level: Monitor running processes, memory consumption, CPU etc.

MITRE ATT&CK for Containers

KubeCon | CloudNativeCon
North America 2021

- **Dec 2020 –**
  Based on the community interest
  (and inspiration from the Threat Matrix)
  MITRE started to work on
  ATT&CK matrix for Containers.

Help Shape ATT&CK for Containers

Jen Burns Follow
Dec 17, 2020 · 2 min read

Written by Jen Burns

One of the questions that pops up often for the MITRE ATT&CK® team is whether or not we have considered expanding ATT&CK to cover container technologies such as Kubernetes and Docker. We've heard your need for coverage in this space, and we're thrilled to announce that in partnership with the Center for Threat-Informed Defense, **the ATT&CK team is now investigating adversarial behavior in containers for potential inclusion in ATT&CK.** If we find that there's enough adversary behavior in containers to warrant ATT&CK coverage, we'll consider that content for a future ATT&CK release.

MITRE ATT&CK for Containers

KubeCon | CloudNativeCon
North America 2021

- **Dec 2020 –**
  Based on the community interest
  (and inspiration from the Threat Matrix)
  MITRE started to work on
  ATT&CK matrix for Containers.

- **Apr 2021 –**

ATT&CK® for Containers now available!

Jen Burns Follow
Apr 29 · 5 min read

Written by Jen Burns, Chris Ante, and Matt Bajzek

We're excited to announce the official release of ATT&CK for Containers!

Help Shape ATT&CK for Containers

Jen Burns Follow
Dec 17, 2020 · 2 min read

Written by Jen Burns

One of the questions that pops up often for the MITRE ATT&CK® team is whether or not we have considered expanding ATT&CK to cover container technologies such as Kubernetes and Docker. We've heard your need for coverage in this space, and we're thrilled to announce that in partnership with the Center for Threat-Informed Defense, **the ATT&CK team is now investigating adversarial behavior in containers for potential inclusion in ATT&CK.** If we find that there's enough adversary behavior in containers to warrant ATT&CK coverage, we'll consider that content for a future ATT&CK release.

MITRE ATT&CK for Containers

KubeCon | CloudNativeCon
North America 2021

- **Dec 2020 –**
  Based on the community interest
  (and inspiration from the Threat Matrix)
  MITRE started to work on
  ATT&CK matrix for Containers.

Help Shape ATT&CK for Containers

Jen Burns Follow
Dec 17, 2020 · 2 min read

Written by Jen Burns

One of the questions that pops up often for the MITRE ATT&CK® team is whether or not we have considered expanding ATT&CK to cover container technologies such as Kubernetes and Docker. We've heard your need for coverage in this space, and we're thrilled to announce that in partnership

- **Apr 2021 –**

ATT&CK® for Containers available!

Jen Burns Follow
Apr 29 · 5 min read

Written by Jen Burns, Chris Ante, and Matt Bajzek

We're excited to announce the official release of ATT&CK

Containers Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering techniques against container technologies. The Matrix contains information for the Containers platform.

layout: flat | show sub-techniques | hide sub-techniques | help

Initial Access (3 techniques)	Execution (4 techniques)	Persistence (4 techniques)	Privilege Escalation (4 techniques)	Defense Evasion (6 techniques)	Credential Acces (2 techniques)
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials (2)
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)	
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host	
				Masquerading (1)	
				Valid Accounts (2)	

Last modified: 29 April 2021

Which matrix should I use?

KubeCon | CloudNativeCon
North America 2021

Threat Matrix for Kubernetes

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

MITRE | ATT&CK® for Containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
3 techniques	4 techniques	4 techniques	4 techniques	6 techniques	2 techniques	2 techniques	3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials (2)	Network Service Scanning	Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)			Resource Hijacking
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host			
				Masquerading (1)			
				Valid Accounts (2)			

Which matrix should I use?

KubeCon CloudNativeCon North America 2021

Threat Matrix for Kubernetes

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

MITRE ATT&CK® for Containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
3 techniques	4 techniques	4 techniques	4 techniques	6 techniques	2 techniques	2 techniques	3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials (2)	Network Service Scanning	Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)			Resource Hijacking
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host			
				Masquerading (1)			
				Valid Accounts (2)			

Key differences:

1. ATT&CK is focused on in-the-wild adversary behaviors.

Which matrix should I use?

KubeCon | CloudNativeCon North America 2021

Threat Matrix for Kubernetes

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

MITRE | ATT&CK® for Containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
3 techniques	4 techniques	4 techniques	4 techniques	6 techniques	2 techniques	2 techniques	3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials (2)	Network Service Scanning	Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)			Resource Hijacking
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host			
				Masquerading (1)			
				Valid Accounts (2)			

Key differences:

1. ATT&CK is focused on in-the-wild adversary behaviors.
2. ATT&CK matrix is built on existing techniques.

Which matrix should I use?

KubeCon | CloudNativeCon North America 2021

Threat Matrix for Kubernetes

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

MITRE | ATT&CK® for Containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
3 techniques	4 techniques	4 techniques	4 techniques	6 techniques	2 techniques	2 techniques	3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials (2)	Network Service Scanning	Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)			Resource Hijacking
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host			
				Masquerading (1)			
				Valid Accounts (2)			

Key differences:

1. ATT&CK is focused on in-the-wild adversary behaviors.
2. Build upon existing Enterprise ATT&CK matrix.

Which matrix should I use?

KubeCon | CloudNativeCon North America 2021

Threat Matrix for Kubernetes

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

MITRE ATT&CK® for Containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
3 techniques	4 techniques	4 techniques	4 techniques	6 techniques	2 techniques	2 techniques	3 techniques
Exploit Public-Facing Application	Container Administration Command	External Remote Services	Escape to Host	Build Image on Host	Brute Force (3)	Container and Resource Discovery	Endpoint Denial of Service
External Remote Services	Deploy Container	Implant Internal Image	Exploitation for Privilege Escalation	Deploy Container	Unsecured Credentials (2)	Network Service Scanning	Network Denial of Service
Valid Accounts (2)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Scheduled Task/Job (1)	Impair Defenses (1)			Resource Hijacking
	User Execution (1)	Valid Accounts (2)	Valid Accounts (2)	Indicator Removal on Host			
				Masquerading (1)			
				Valid Accounts (2)			

Core similarities:

1. Both matrices combine techniques for orchestration-level and container-level adversary behaviors.
2. Both matrices should be considered as an abstraction level.

Which matrix should I use?

KubeCon CloudNativeCon North America 2021

Threat Matrix for Kubernetes

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	Instance Metadata API	Applications credentials in configuration files		
Exposed sensitive interfaces	SSH server running inside container				Access managed identity credential		Writable volume mounts on the host		
	Sidecar injection				Malicious admission controller		CoreDNS poisoning		
							ARP poisoning and IP spoofing		

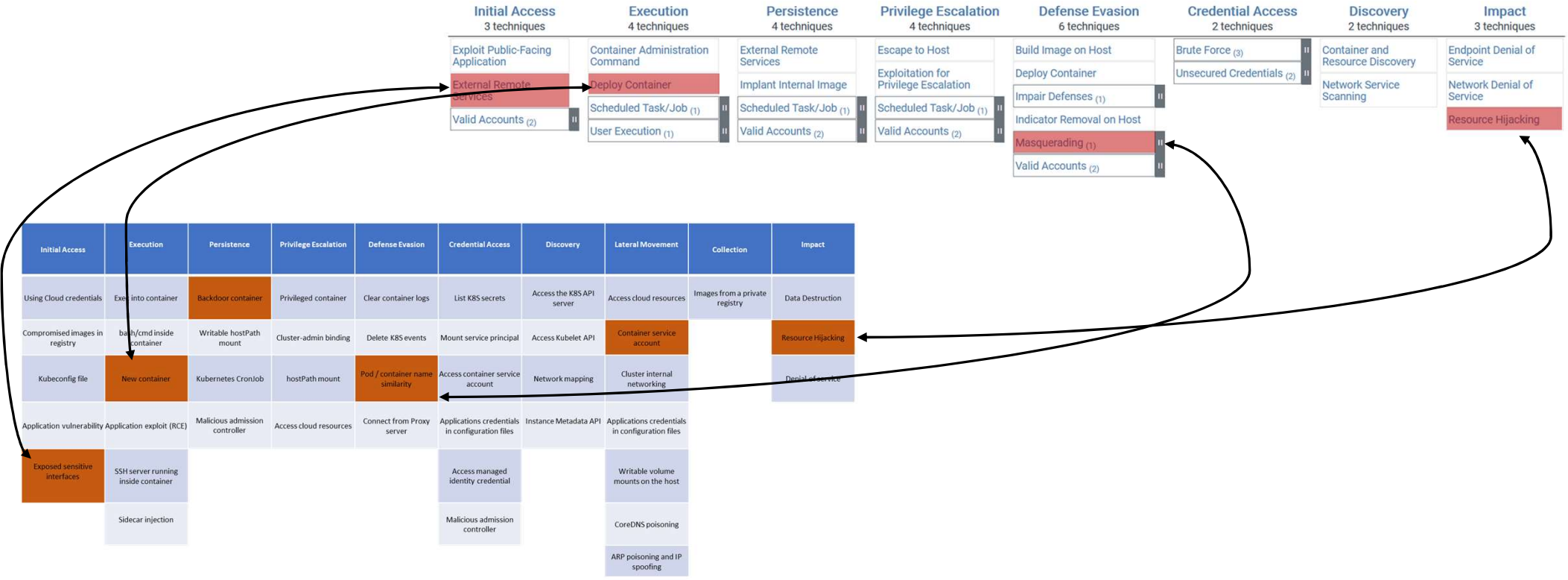
MITRE ATT&CK® for Containers

MITRE and Microsoft's joint publication: aka.ms/mitreContainers

Which matrix should I use?

KubeCon CloudNativeCon North America 2021

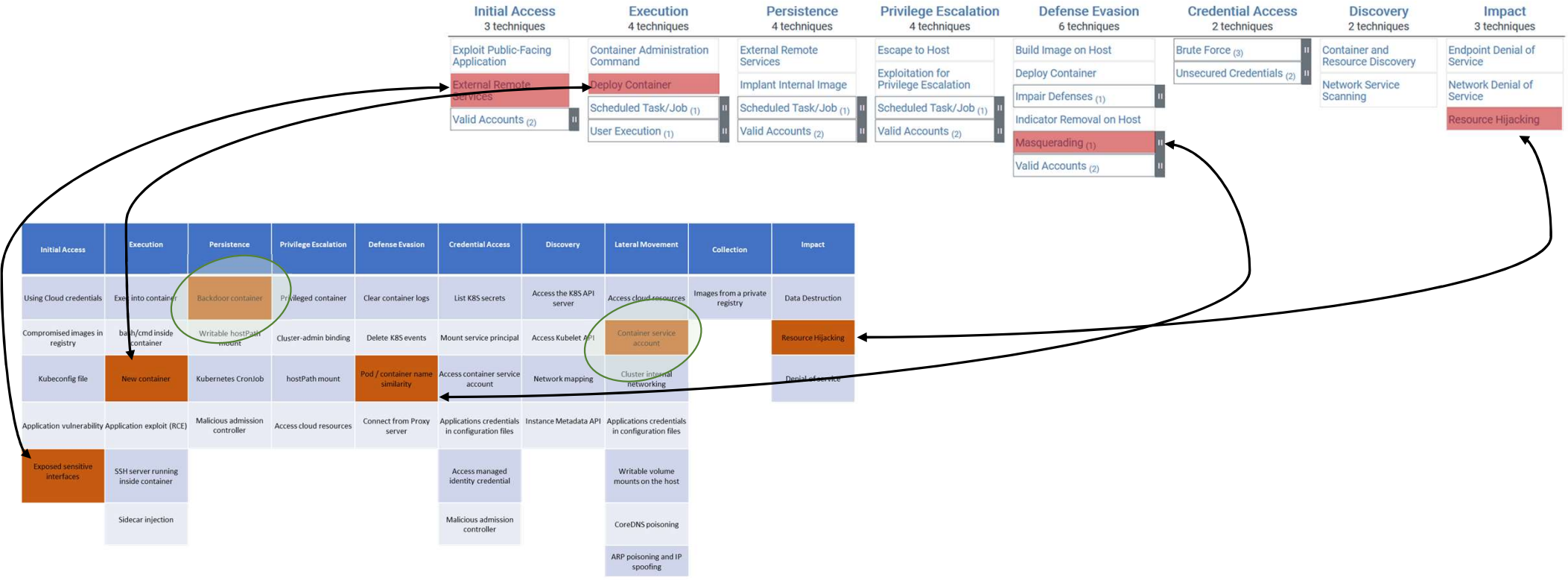
Kubeflow Pipelines campaign reflection on both matrices



Which matrix should I use?

KubeCon CloudNativeCon North America 2021

Kubeflow Pipelines campaign reflection on both matrices



Key takeaways

- Building a knowledge base, and always keep challenging it.
- Defenders closing ranks – Microsoft and MITRE collaboration.

Final words

- Kubernetes is evolving.
- The threats are also evolving.
- Therefore, the Threat Matrix is updated over time (a second version was released earlier this year).

Useful links

- aka.ms/K8sThreatMatrixV2
- aka.ms/KubeflowAttack
- aka.ms/MitreContainers
- https://attack.mitre.org/


KubeCon | CloudNativeCon

North America 2021

RESILIENCE

REALIZED

Thank You!

Yossi Weizman in *yossi-weizman*

Ram Pliskin