2021
Arab Security Conference
المؤتمر العربي لأمن المعلومات
5th-7th of September 2021
Hybrid Edition

Mohammad Khreesha

Cybersecurity Manager @ Baaz Inc.

Attacking and Securing Kubernetes Clusters

STRATEGIC SPONSORS

TREND MICRO

HUAWEI

STRATEGIC SUPPORT

itida

PLATINUM SPONSORS

CYSHIELD

iSEC

ORGANIZED BY

ASC Arab Security Consultants

www.arabsecurityconference.com

Whoami?

13+ Years of IT & Infosec Experience

Cybersecurity Manager at Baaz Inc.

OWASP Amman Chapter Leader

Youtuber, Blogger, & CTF Maker

OFFENSIVE security OSCP

eCPPT V2

eWPTXv2

eWPT V1

eWPTXv2

C EH Certified Ethical Hacking

PECB ISO/IEC 27001 Lead Implementer

E CSA EC-Council Certified Security Analyst

C HFI Computer Hacking Forensic INVESTIGATOR

LPT LICENSED PENETRATION TESTER MASTER

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Workshop Target Audience

Pentesters/Red Teamers
Blut Teamers
Devop/Devsecops
Developers

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Agenda

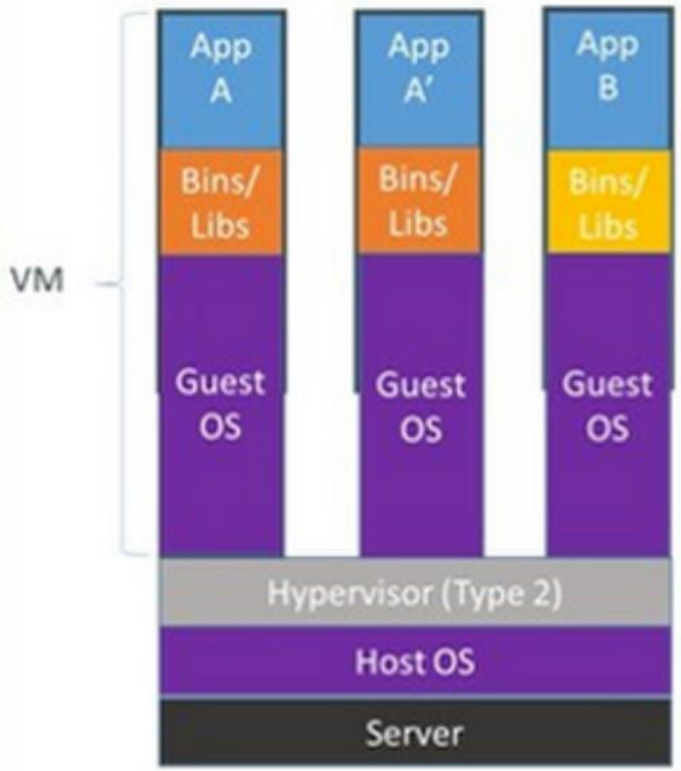
Introduction
Kubernetes Basics
MITRE ATT&CK Framework
Kubernetes Attack Surface
Kubernetes Pentesting
Kubernetes Hardening
Q&A

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

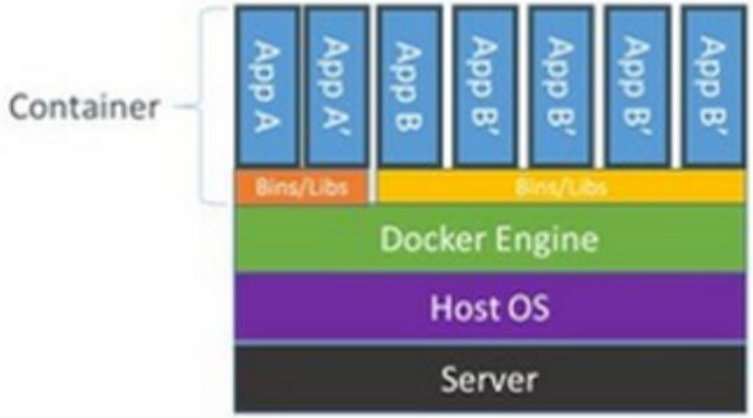
Introduction

The Age Containerization

Containers vs. VMs

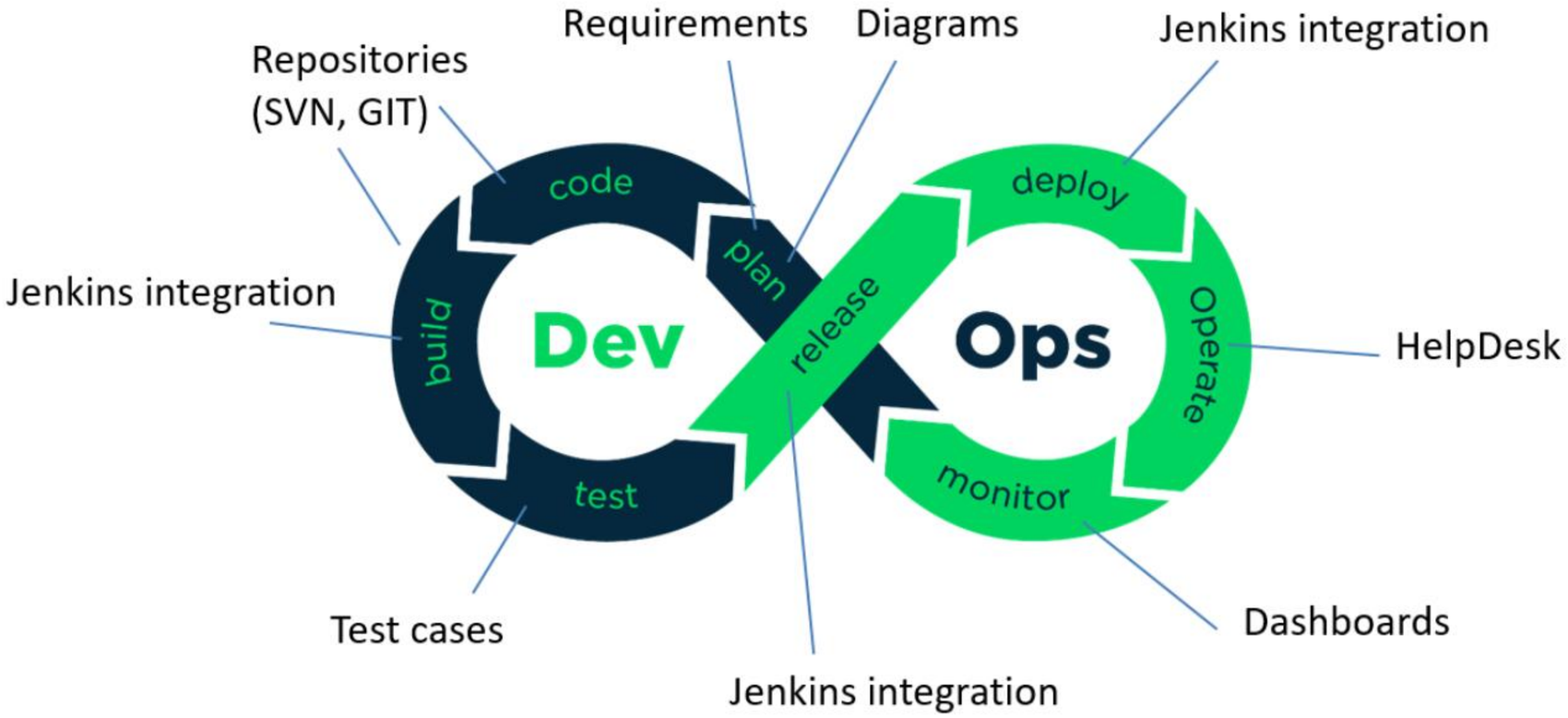


Containers are isolated, but share OS and, where appropriate, bins/libraries



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

What is Devops?



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Basics

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSEC
ORGANIZED BY
ASC Arab Security Consultants

What is Kubernetes?

It is a powerful container management open-source tool that automates the deployment and management of containers.

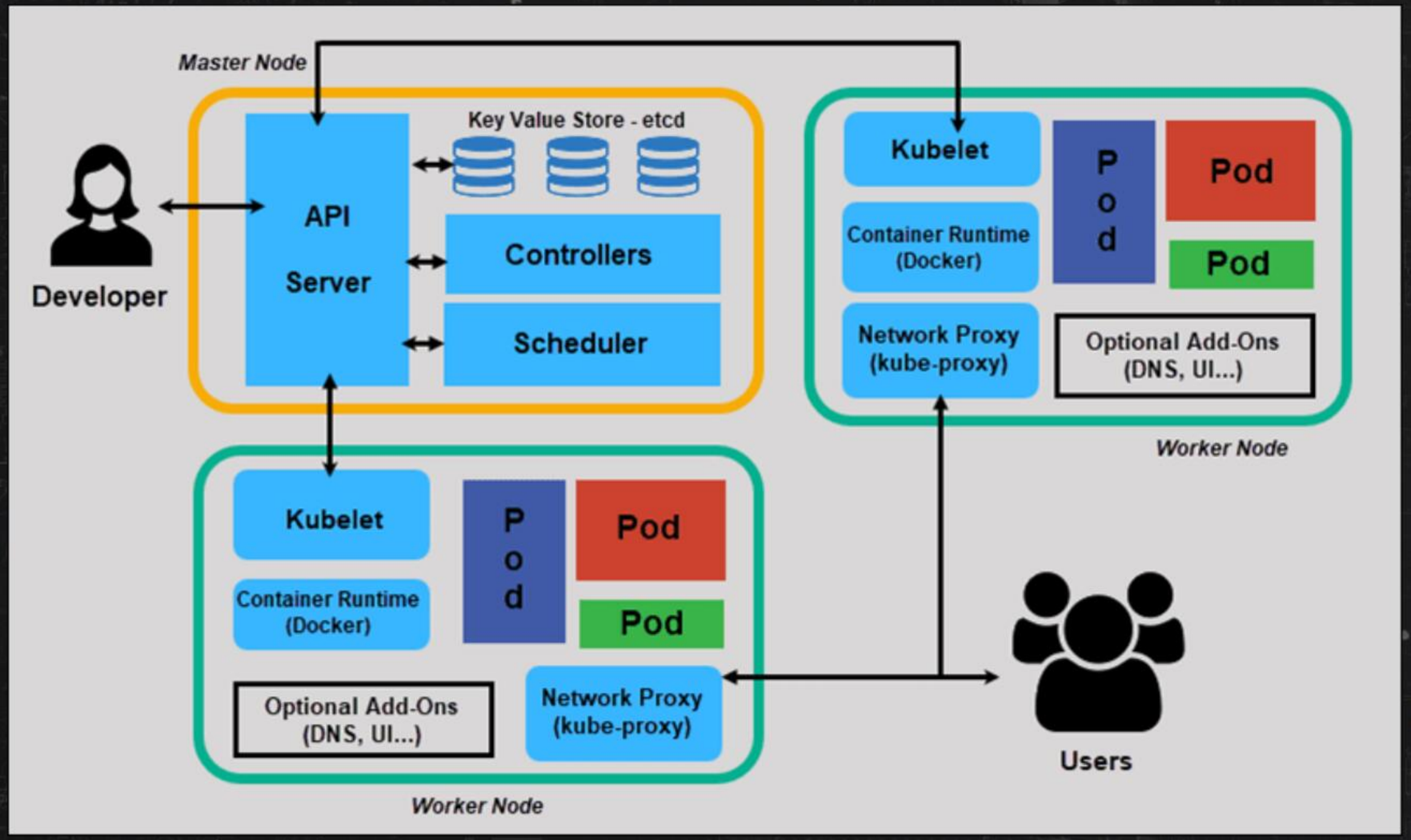
Kubernetes is the next big wave in cloud computing and it's easy to see why as businesses migrate their infrastructure and architecture to reflect a cloud-native, data-driven era.

It used when :

1. Your application uses a microservices architecture.
2. If you're suffering from slow development and deployment.
3. If you need to optimize your infrastructure costs.

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Architecture



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSEC
ORGANIZED BY
ASC Arab Security Consultants

Master Node

- API Server : it receives requests and serves as first point of contact.
- etcd Server : Stores the state of the cluster, alerts subscribed components.
- Controller Manager : Runs control loops to bring state to parity with etcd.
- Scheduler : Bin-packs containers onto nodes.
- Kube-DNS : Gives every requested network endpoint a name.

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

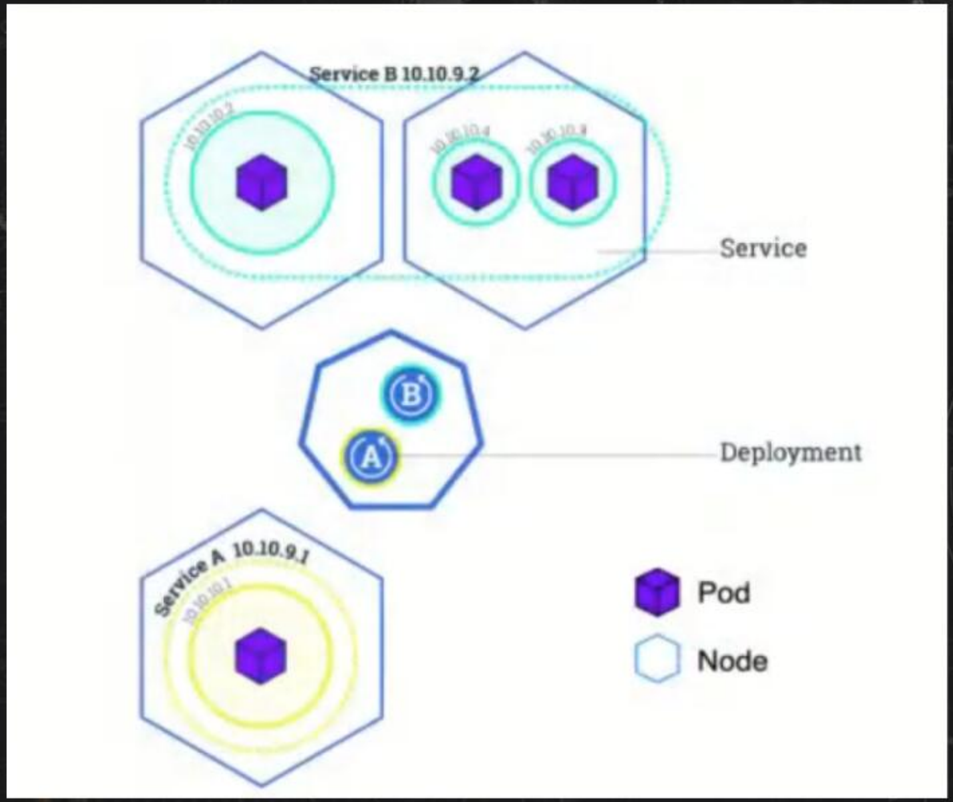
Worker Node

- **Kubelet : Ties the node back to the master components.**
- **Container Runtime : Instruct the Linux kernel to create containers (e.g. Docker).**
- **Host Operating System**
  - **Filesyetem**
  - **Network**
  - **Kernel**
- **Workloads : Containers on the system.**
- **Kube-Proxy : forwards traffic to each pod in a load-balanced network service.**

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Key Components

- Pods
- Services
- Deployments
- Secrets
- Configmap
- Volumes

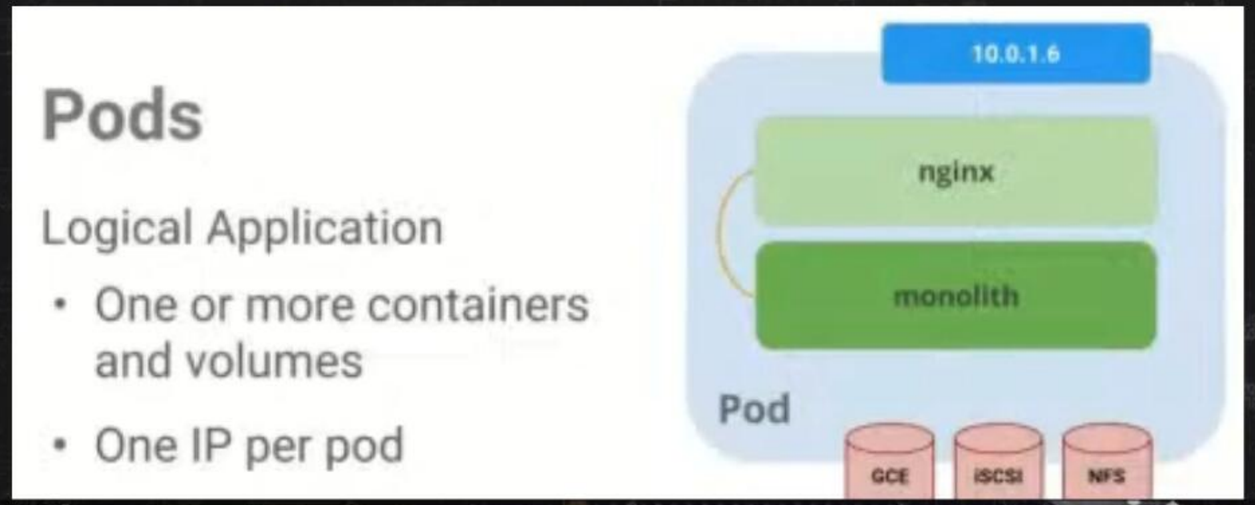


- Note: All Units represented by: YAML format (.yaml files).

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Pods

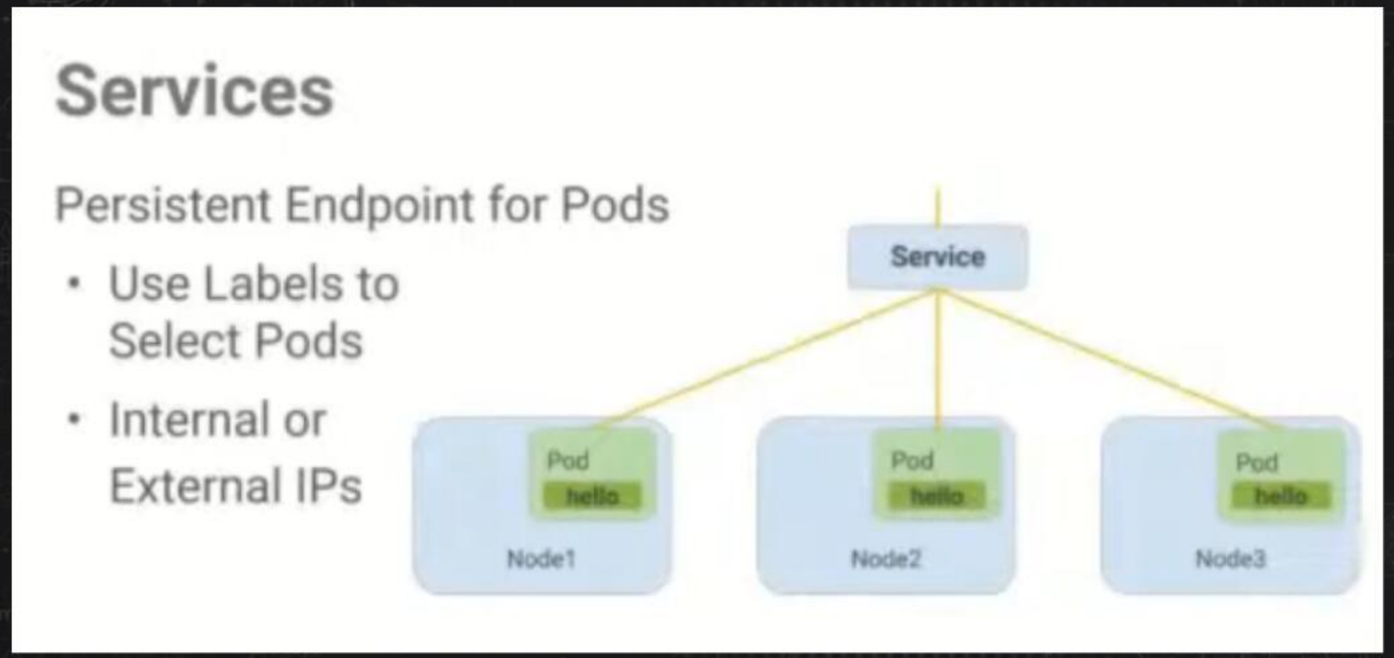
- The smallest, simplest and basic unit in the Kubernetes object model that you create or deploy.
- A Pod represents processes running on you Kubernetes cluster.
- Pods represent and hold a collection of one or more containers.



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Services

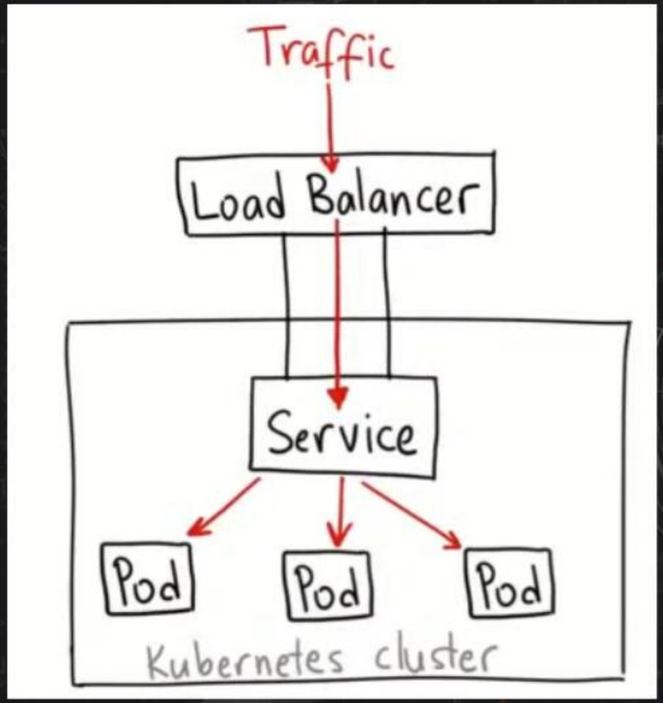
- Service provide stable endpoints for Pods.
- Pods are automatically picked up and exposed by our services.
- Services use labels to determine what Pods they operate on.



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Services Types

- **ClusterIP (internal): the default type means that this service is only visible inside of the cluster.**
- **NodePort: gives each node in the cluster and externally accessible IP.**
- **Load Balancer: adds a load balancer from the cloud provider which forward traffic from the service to Nodes within it.**

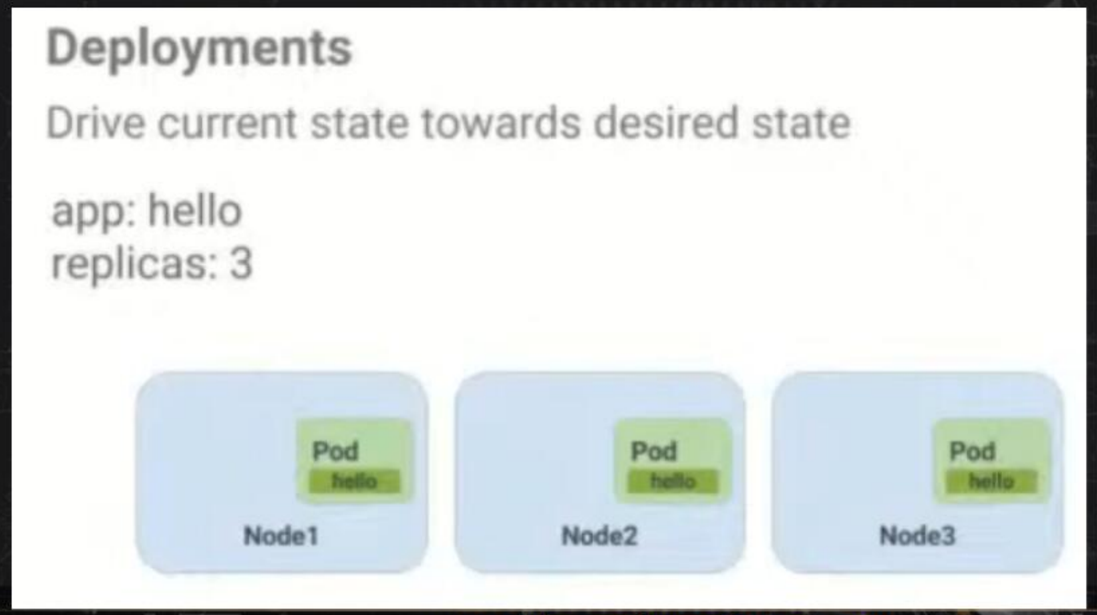


STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Deployments

- **Deployments : You describe a desired state in a Deployment. It gives you the ability to do roll-outs (undo).**

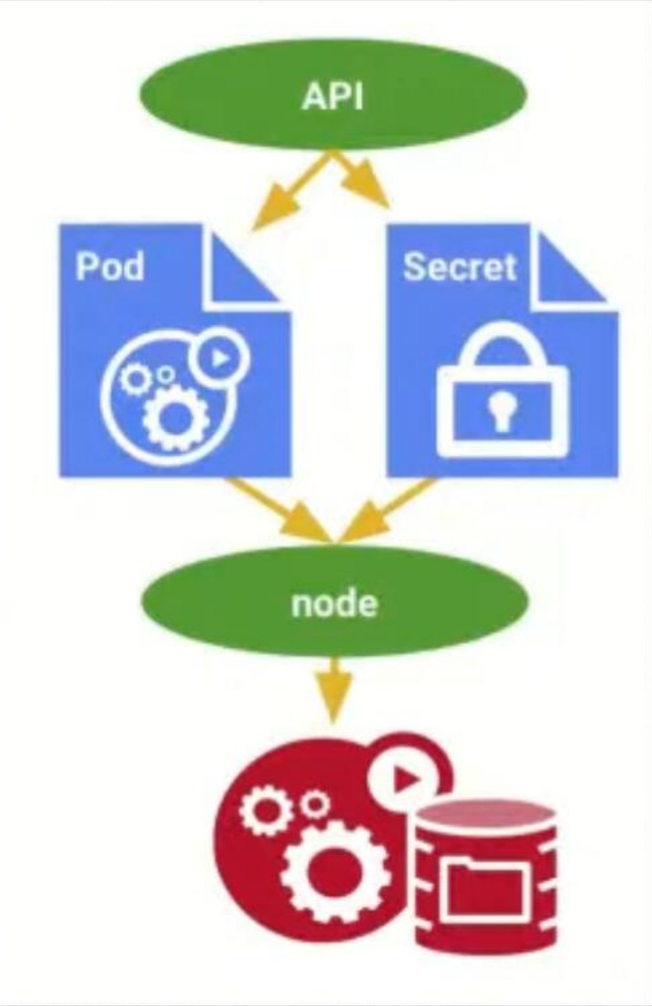
- **Replicas :**
- **Number of running Pods needs to be maintained.**



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Secrets

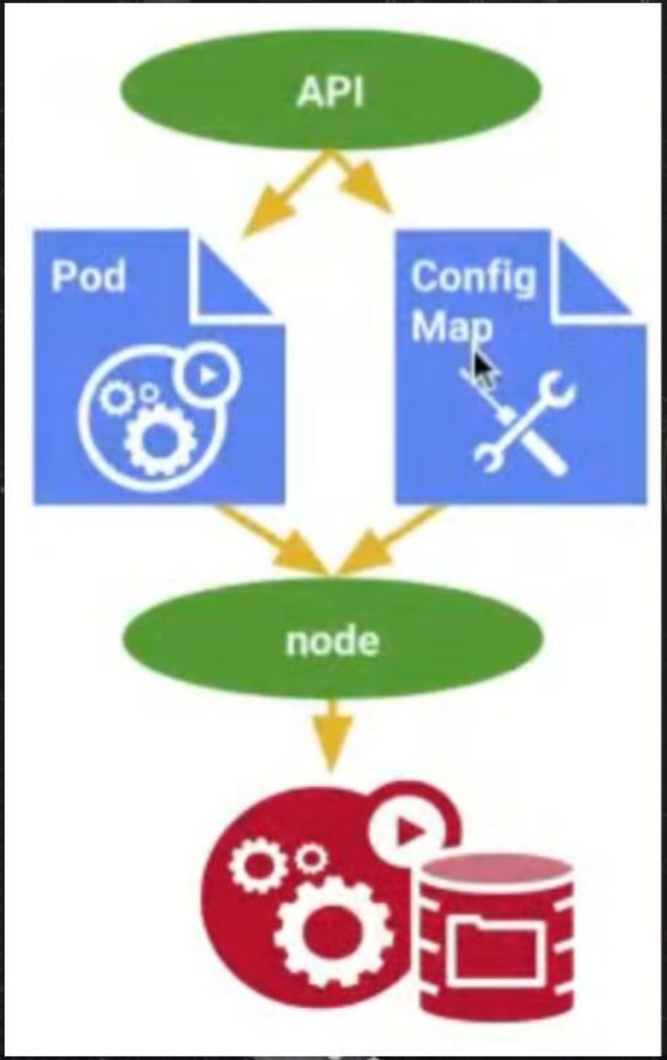
- A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key.



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes ConfigMaps

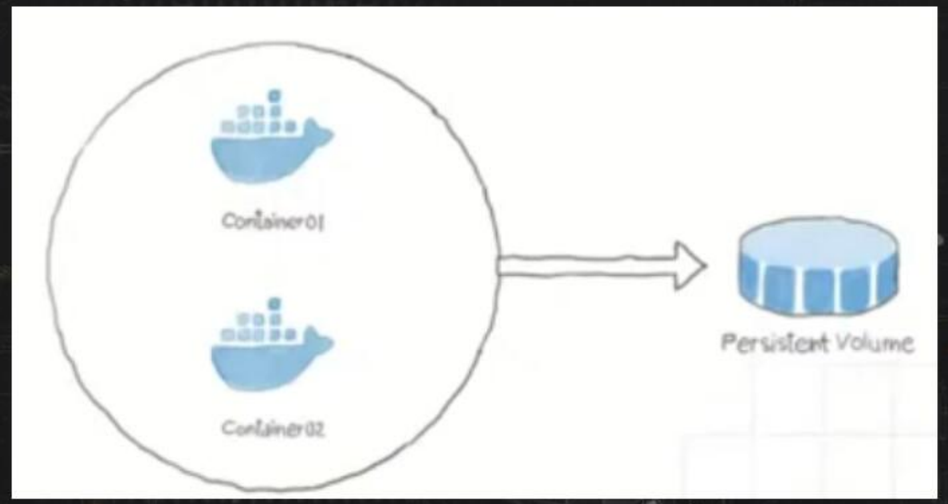
- ConfigMaps are Kubernetes objects that allow you to separate configuration data/files from image content to keep containerized applications portable.
- ConfigMaps bind configuration files, command-line arguments, surroundings variables, port numbers, and alternative configuration artifacts to your Pods containers and system parts at run-time.
- ConfigMaps are helpful for storing and sharing non-sensitive, unencrypted configuration data. Like Secrets, you'll be able to produce config maps from files and with yaml declaration.



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Volumes

- On-disk files in a container are ephemeral.
- First, when a container crashes, kubelet will restart it, but the files will be lost - the container starts with a clean state.
- Second, when running containers together in a Pod it is often necessary to share files between those containers.
- Types of volumes :
  - Logic Disks
  - gcePersistentDisk
  - awdElasticBlockStore
  - ...etc



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

So, What is Kubernetes?

- **Kubernetes is the Maestro of the Orchestra.**

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

2021
Arab Security Conference
المؤتمر العربي لأمن المعلومات
5th-7th of September 2021
Hybrid Edition

MITRE ATT&CK Framework

STRATEGIC SPONSORS

TREND MICRO

HUAWEI

STRATEGIC SUPPORT

itida

PLATINUM SPONSORS

CYSHIELD

iSEC

ORGANIZED BY

ASC Arab Security Consultants

www.arabsecurityconference.com

ATT&CK Matrix

Reconnaissance (10 techniques)	Resource Development (6 techniques)	Initial Access (9 techniques)	Execution (10 techniques)	Persistence (18 techniques)	Privilege Escalation (12 techniques)	Defense Evasion (37 techniques)	Credential Access (14 techniques)	Discovery (25 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (16 techniques)	Exfiltration (9 techniques)	Impact (13 techniques)
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/4)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/2)	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/12)	Boot or Logon Autostart Execution (0/12)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Scheduled Task/Job (0/6)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	Cloud Service Dashboard	Remote Services (0/6)	Data from Cloud Storage Object	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/2)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (0/2)	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)		Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/3)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/4)	Domain Trust Discovery	Software Deployment Tools	Data from Information Repositories (0/2)	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/2)		Valid Accounts (0/4)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Network Service Scanning	Use Alternate Authentication Material (0/4)	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection (0/11)	Hide Artifacts (0/7)	Steal Application Access Token	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service (0/2)
				Hijack Execution Flow (0/11)	Scheduled Task/Job (0/6)	Hijack Execution Flow (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Sniffing		Data Staged (0/2)	Non-Standard Port		Resource Hijacking
				Implant Container Image	Valid Accounts (0/4)	Impair Defenses (0/7)	Steal Web Session Cookie	Password Policy Discovery		Email Collection (0/3)	Protocol Tunneling		Service Stop
				Office Application Startup (0/6)		Indicator Removal on Host (0/6)	Two-Factor Authentication Interception	Peripheral Device Discovery		Input Capture (0/4)	Proxy (0/4)		System Shutdown/Reboot
				Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (0/6)	Permission Groups Discovery (0/3)		Man in the Browser	Remote Access Software		
				Scheduled Task/Job (0/6)		Masquerading (0/6)		Process Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				Server Software Component (0/3)		Modify Authentication Process (0/4)		Query Registry		Screen Capture	Web Service (0/3)		
						Modify Cloud Compute Infrastructure (0/4)		Remote System Discovery		Video Capture			
								Software Discovery (0/1)					

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

2021
Arab Security Conference
المؤتمر العربي لأمن المعلومات
5th-7th of September 2021
Hybrid Edition

Kubernetes Attack Surface

STRATEGIC SPONSORS

TREND MICRO

HUAWEI

STRATEGIC SUPPORT

itida

PLATINUM SPONSORS

CYSHIELD

iSEC

ORGANIZED BY

ASC Arab Security Consultants

www.arabsecurityconference.com

Real-world Kubernetes Cluster Attack

Cryptojacking Attacks in Kubernetes: How to Stop Them

Wei Lien Dang | Jul 02, 2020

SUBSCRIBE TO OUR BLOG

Email Address:

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Threat Modeling

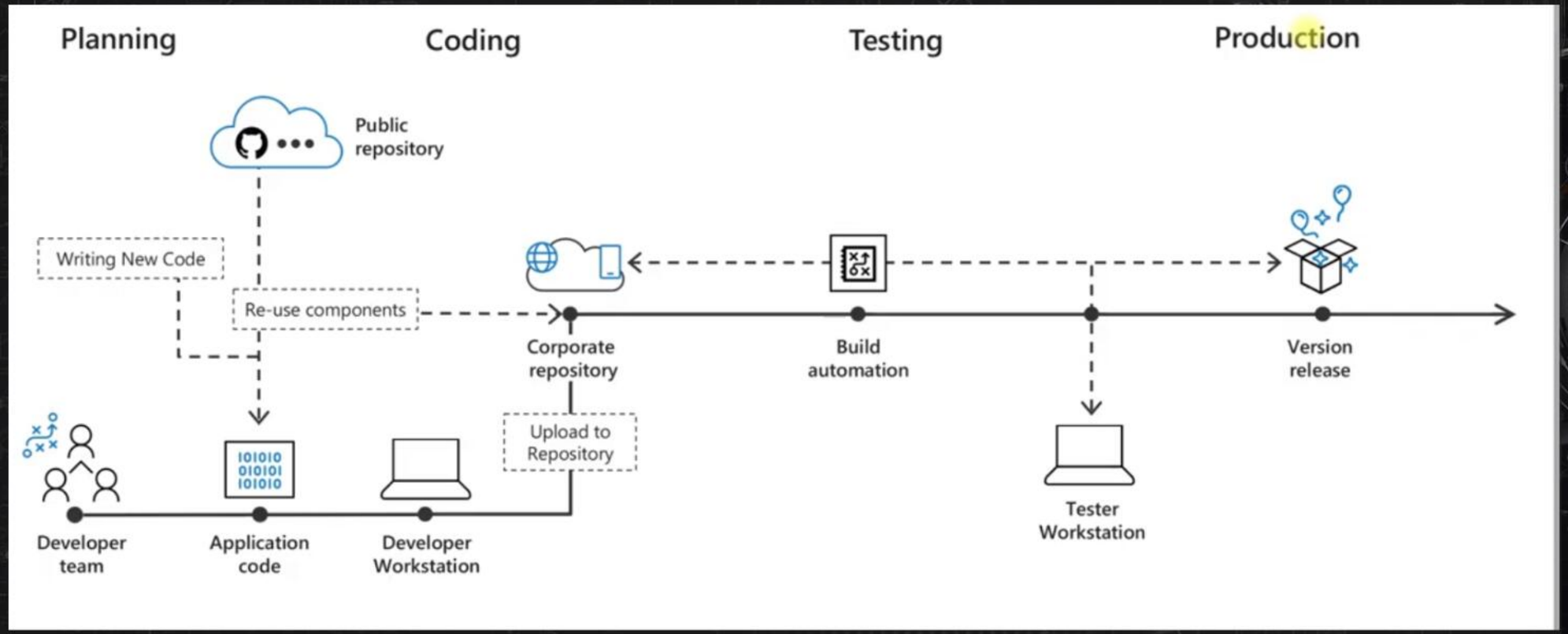
- Kubernetes can be a valuable target for data and/or compute power theft.

- Cyber actors may target kubernetes clusters for:
  - Data theft
  - Seeking computational power
  - Denial of Service
  - … etc

- The following threats represent some of the most likely sources of compromise for a Kubernetes cluster:
  - Supply Chain Risk
  - Malicious Threat Actor
  - Insider Threat

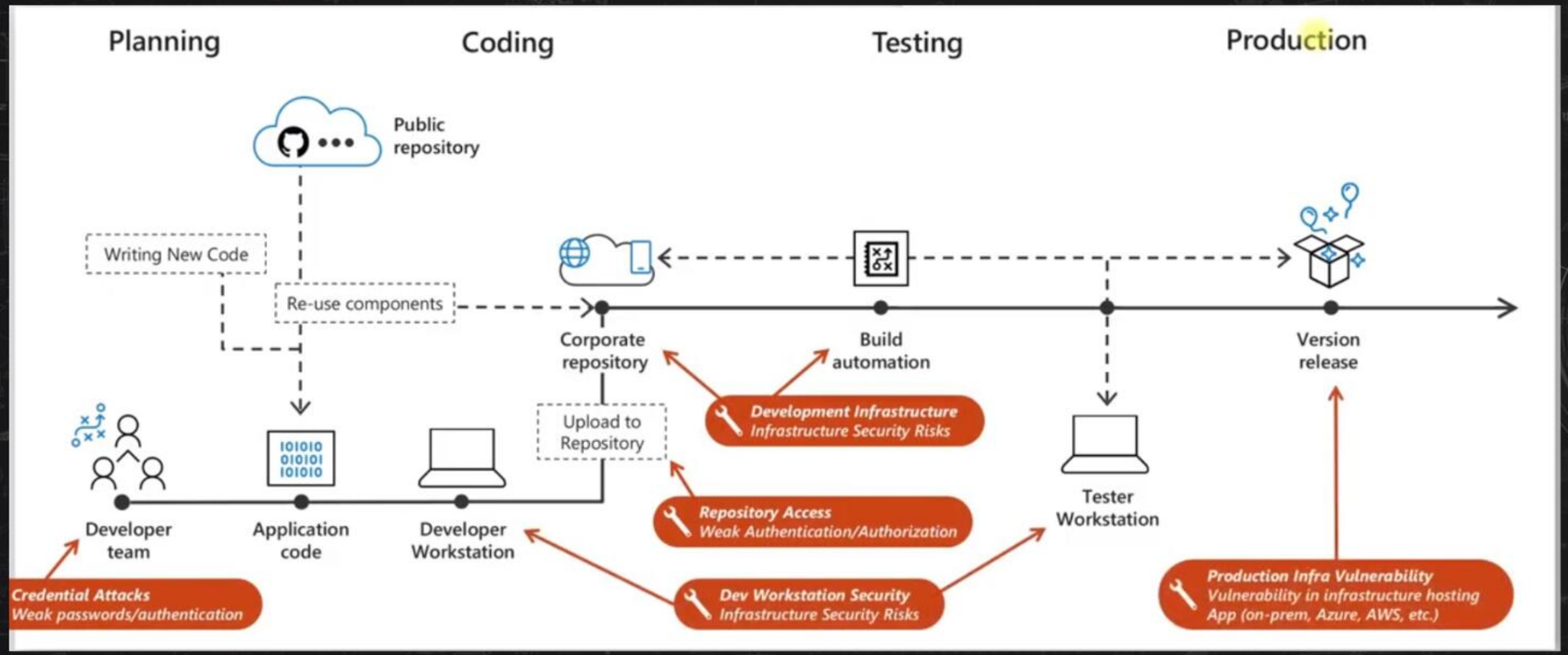
STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

CI/CD Pipeline



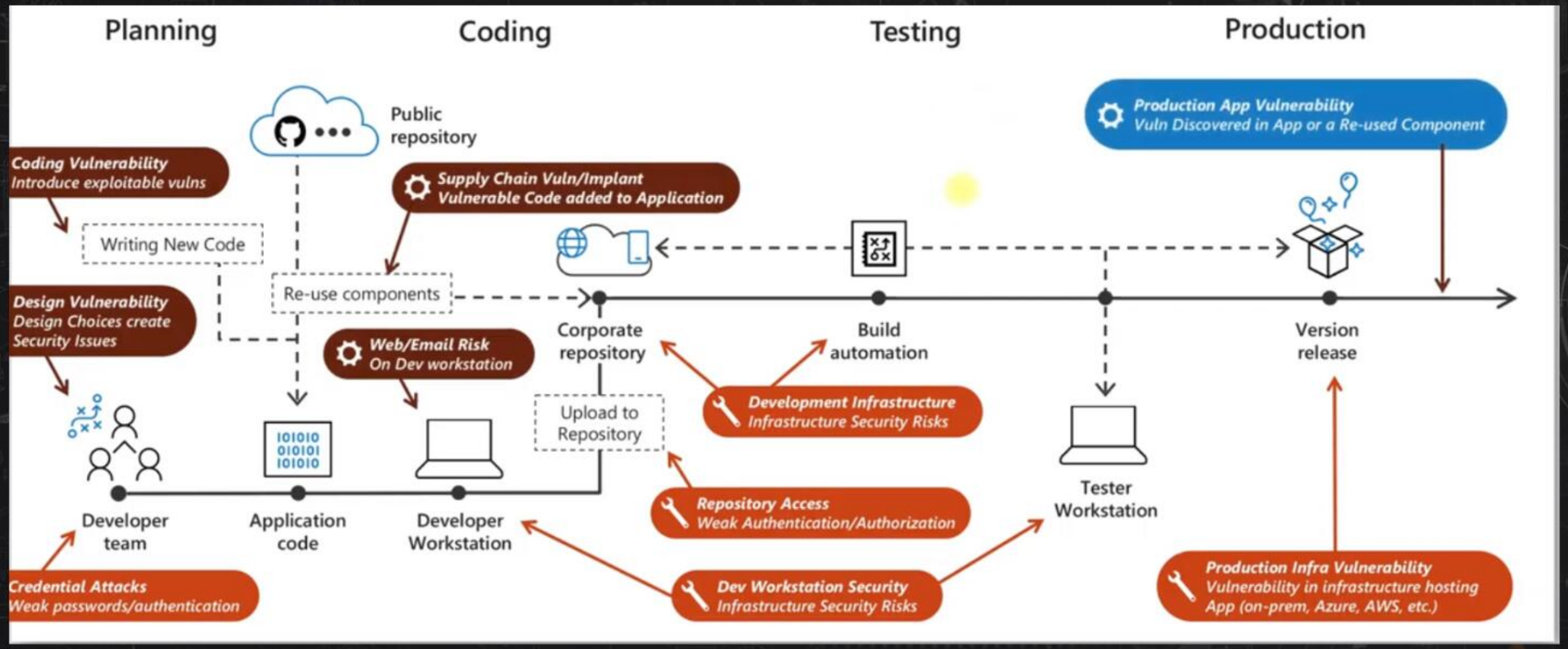
STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Attack Surface - Developer Attacks



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Attack Surface - IT & Operations Attacks



STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSEC
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes ATT&CK Matrix

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

STRATEGIC SPONSORS

TREND MICRO

HUAWEI

STRATEGIC SUPPORT

itida

PLATINUM SPONSORS

CYSHIELD

iSec

ORGANIZED BY

ASC Arab Security Consultants

2021
Arab Security Conference
المؤتمر العربي لأمن المعلومات
5th-7th of September 2021
Hybrid Edition

Kubernetes Pentesting

STRATEGIC SPONSORS

TREND MICRO

HUAWEI

STRATEGIC SUPPORT

itida

PLATINUM SPONSORS

CYSHIELD

iSEC

ORGANIZED BY

ASC Arab Security Consultants

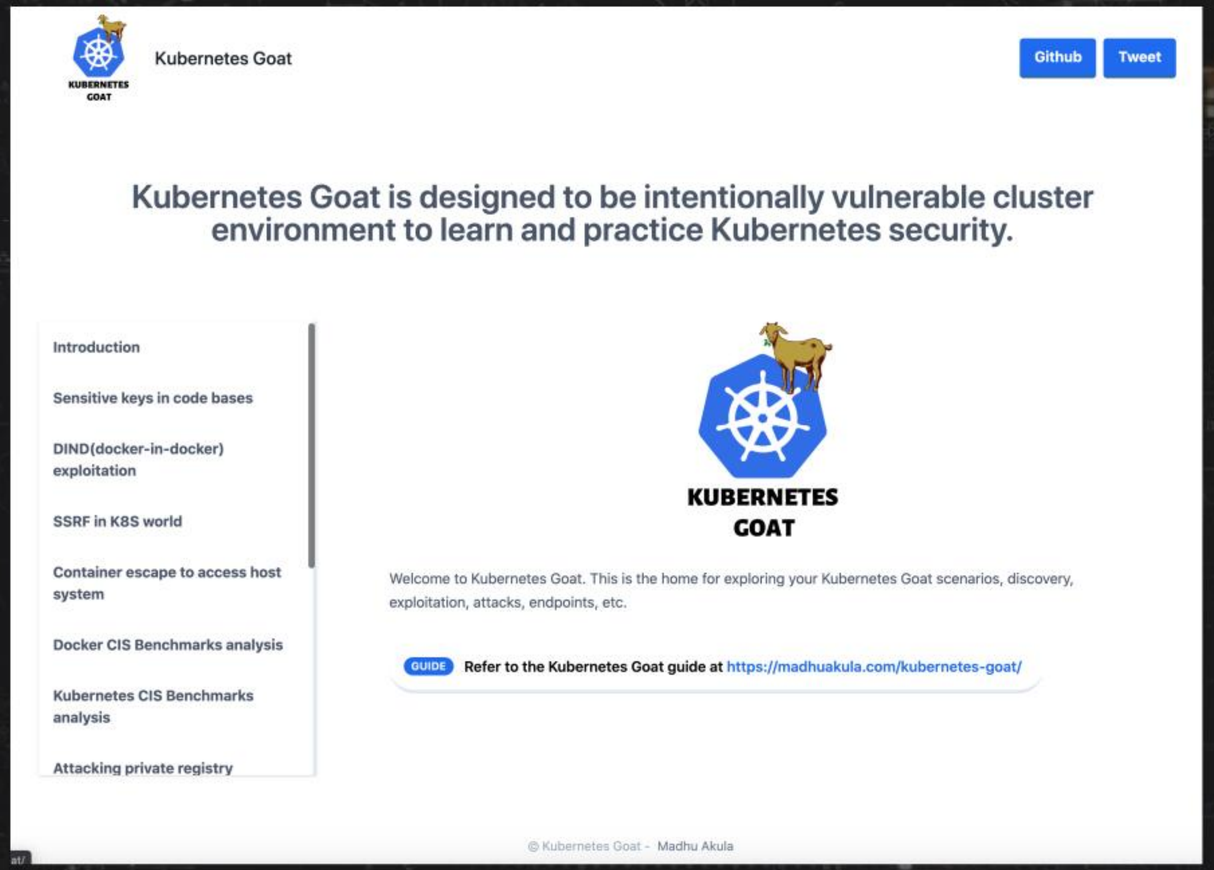
Kubernetes Pentesting Tools

https://github.com/inguardians/peirates

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes-goat

The Kubernetes Goat is designed to be an intentionally vulnerable cluster environment to learn and practice Kubernetes security.



https://github.com/madhuakula/kubernetes-goat

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Pentesting kubernetes - Demo

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Hardening

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSEC
ORGANIZED BY
ASC Arab Security Consultants
www.arabsecurityconference.com

Relevant Kubernetes Tools – Awesome Devsecops

https://github.com/devsecops/awesome-devsecops

README.md

Awesome DevSecOps awesome

Inspired by the awesome-* trend on GitHub. This is a collection of documents, presentations, videos, training materials, tools, services and general leadership that support the DevSecOps mission. These are the essential building blocks and tidbits that can help you to arrange for a DevSecOps experiment or to help you build out your own DevSecOps program.

This list will not be fully comprehensive and will change as DevSecOps matures. We intend for it to be an awesome list that grows and changes as the community learns and improves how DevSecOps is implemented and adopted. To be included in this list, the information, tools, vendors or initiative must provide for Free or Open Source capabilities that help with the DevSecOps mission. Links that lead to a commercial aspect are noted with a (P).

Table of Contents *generated with DocToc*

- Information
  - Guidelines
  - Presentations
  - Initiatives
  - Keeping Informed
  - Wardley Maps for Security
- Training
  - Labs
  - Vulnerable Test Targets
  - Conferences
  - Podcasts
  - Books
- Tools
  - Dashboards

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Relevant Kubernetes Tools – Container Scanning

Gives you CVEs for OS dependencies, and sometimes application dependencies (depending on scanning tool).

Value os dubious, but still worth doing.

Little to no coverage of application security, but people go wild for charts and empirical data.

https://docs.gitlab.com/ee/user/application_security/container_scanning/

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Relevant Kubernetes Tools – CIS Benchmarks

Security configuration baselines for Kubernetes, Docker, Nginx, and lots of other software.

https://www.cisecurity.org/cis-benchmarks/

Cloud Providers	**IBM Cloud Foundations** Expand to see related content	Download CIS Benchmark
Server Software Database Server	**IBM Db2** Expand to see related content	Download CIS Benchmark
Operating Systems IBM	**IBM I** Expand to see related content	Download CIS Benchmark
Network Devices	**Juniper** Expand to see related content	Download CIS Benchmark
Server Software Virtualization	**Kubernetes** Expand to see related content	Download CIS Benchmark
Operating Systems Linux	**LXD** Expand to see related content	Download CIS Benchmark
Server Software Authentication Ser...	**MIT Kerberos** Expand to see related content	Download CIS Benchmark

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Relevant Kubernetes Tools - KubeTap

Deploy mitmproxy in from of Kubernetes service.

Unlike Burpsuite, this captures all incoming kubernetes service traffics, not just traffic originated from the tester device.

https://github.com/soluble-ai/kubetap

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC
Arab Security Consultants

Relevant Kubernetes Tools - Helm

Helm is a package manager for Kubernetes.

Helm is the Kubernetes equivalent of yum or apt.

Helm deploys charts, which you can think of as a packaged application. It is a collection of all your versioned, pre-configured application resources which can be deployed as one unit.

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Relevant Kubernetes Tools – kube-bench

kube-bench is tool that checks whether Kubernetes is deployed securely by running the checks documented in the CIS Kubernetes Benchmark.

aqua
kube-bench

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Auditing - Demo

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

Kubernetes Hardening Tips

- Build a debugging container.
- Debug the network traffic before debugging the application.
- Test the application with all configuration options (including infrastructure).
- Implement NetworkPolicies.
- Follow Pod Security Standards (https://kubernetes.io/docs/concepts/security/pod-security-standards/)
- Look DoS issues.
- Use rbac-view tool.
- Remove Helm2.

STRATEGIC SPONSORS
TREND MICRO
HUAWEI
STRATEGIC SUPPORT
itida
PLATINUM SPONSORS
CYSHIELD
iSec
ORGANIZED BY
ASC Arab Security Consultants

2021
Arab Security Conference
المؤتمر العربي لأمن المعلومات
5th-7th of September 2021
Hybrid Edition

Thanks

STRATEGIC SPONSORS

TREND MICRO

HUAWEI

STRATEGIC SUPPORT

itida

PLATINUM SPONSORS

CYSHIELD

iSEC

ORGANIZED BY

ASC Arab Security Consultants

www.arabsecurityconference.com