Checkmarx

KICS REPORT v2.1.1

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
0	105	140	149	17	411

PLATFORMS Kubernetes, Dockerfile, Common
START TIME 13:44:08, Jul 24 2024
END TIME 13:44:10, Jul 24 2024
SCANNED PATHS:
- /path

Container Is Privileged

Results 3

Severity HIGH
Platform Kubernetes
Cwe
Category Insecure Configurations

Description

Privileged containers lack essential security restrictions and should be avoided by removing the 'privileged' flag or by changing its value to false

../../path/scenarios/docker-bench-security/deployment.yaml:45

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.securityContext.privileged is unset or false

../../path/scenarios/system-monitor/deployment.yaml:41

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.privileged is unset or false

../../path/scenarios/health-check/deployment.yaml:25

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.privileged is unset or false

Missing User Instruction

Results 14

Severity HIGH
Platform Dockerfile
Cwe 250
Category Build Process

Description

A user should be specified in the dockerfile, otherwise the image will run as root

../../path/infrastructure/poor-registry/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/build-code/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/hidden-in-layers/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/internal-api/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/health-check/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/goat-home/Dockerfile:23

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/metadata-db/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/info-app/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/hunger-check/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/batch-check/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/system-monitor/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/cache-store/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/users-repo/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

../../path/infrastructure/helm-tiller/Dockerfile:1

Expected: The 'Dockerfile' should contain the 'USER' instruction

Non Kube System Pod With Host Mount

Results **33**

Severity	HIGH
Platform	Kubernetes
Cwe	
Category	Access Control

Description

A non kube-system workload should not have hostPath mounted

../../path/scenarios/kube-bench-security/master-job.yaml:77

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/etcd' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:95

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/srv/kubernetes' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:86

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/kube-controller-manager' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:83

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/kube-scheduler' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:88

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/usr/bin/runc' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:72

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/srv/kubernetes' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:57

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/kubelet' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:85

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/usr/bin/containerd' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:80

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/kubelet' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:66

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/systemd' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:92

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/lib/systemd' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:69

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/lib/systemd' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:110

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/passwd' mounted

Checkmarx

KICS REPORT v2.1.1

../../path/scenarios/kube-bench-security/node-job.yaml:84

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/opt/cni/bin/' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:75

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/kubernetes' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:89

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/systemd' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:101

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/usr/bin' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:78

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/usr/bin' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:91

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/var/run/docker.sock' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:81

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/cni/net.d/' mounted

../../path/scenarios/system-monitor/deployment.yaml:31

Expected: Resource name 'system-monitor-deployment' of kind 'Deployment' in non kube-system namespace 'default' should not have hostPath '/' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:98

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/kubernetes' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:82

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/lib/systemd/system' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:54

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/etcd' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:113

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/group' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:60

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/kube-scheduler' mounted

../../path/scenarios/kube-bench-security/node-job.yaml:63

Expected: Resource name 'kube-bench-node' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/var/lib/kube-controller-manager' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:73

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/var/lib' mounted

../../path/scenarios/health-check/deployment.yaml:32

Expected: Resource name 'health-check-deployment' of kind 'Deployment' in a non kube-system namespace 'default' should not have hostPath '/run/containerd/containerd.sock' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:76

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/usr/lib/systemd' mounted

../../path/scenarios/docker-bench-security/deployment.yaml:79

Expected: Resource name 'docker-bench-security' of kind 'DaemonSet' in a non kube-system namespace 'default' should not have hostPath '/etc' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:107

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/opt/cni/bin/' mounted

../../path/scenarios/kube-bench-security/master-job.yaml:104

Expected: Resource name 'kube-bench-master' of kind 'Job' in a non kube-system namespace 'default' should not have hostPath '/etc/cni/net.d/' mounted

Passwords And Secrets - Generic API Key

Results 2

Severity	HIGH
Platform	Common
Cwe	

https://kics.io

Checkmarx

KICS REPORT v2.1.1

Category Secret Management

Description

Query to find passwords and secrets in infrastructure code.

../../path/scenarios/hunger-check/deployment.yaml:53

Expected: Hardcoded secret key should not appear in source

../../path/scenarios/hunger-check/deployment.yaml:44

Expected: Hardcoded secret key should not appear in source

Privilege Escalation Allowed

Results **14**

Severity HIGH

Platform Kubernetes

Cwe

Category Insecure Configurations

Description

Containers should not run with allowPrivilegeEscalation in order to prevent them from gaining more privileges than their parent process

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/docker-bench-security/deployment.yaml:44

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/system-monitor/deployment.yaml:40

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.allowPrivilegeEscalation should be set to false

../../path/scenarios/health-check/deployment.yaml:24

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.securityContext.allowPrivilegeEscalation should be set and should be set to false

---

Checkmarx

KICS REPORT v2.1.1

RBAC Wildcard In Rule

Results 4

Severity	HIGH
Platform	Kubernetes
Cwe	
Category	Access Control

Description

Roles and ClusterRoles with wildcard RBAC permissions provide excessive rights to the Kubernetes API and should be avoided. The principle of least privilege recommends to specify only the set of needed objects and actions

../../path/infrastructure/helm-tiller/pwnchart/templates/clusterrole.yaml:5

Expected: metadata.name={{all-your-base}}.rules[0].verbs should list the minimal set of needed objects or actions

../../path/infrastructure/helm-tiller/pwnchart/templates/clusterrole.yaml:5

Expected: metadata.name={{all-your-base}}.rules[0].resources should list the minimal set of needed objects or actions

../../path/scenarios/hunger-check/deployment.yaml:14

Expected: metadata.name={{secret-reader}}.rules[0].resources should list the minimal set of needed objects or actions

../../path/infrastructure/helm-tiller/pwnchart/templates/clusterrole.yaml:5

Expected: metadata.name={{all-your-base}}.rules[0].apiGroups should list the minimal set of needed objects or actions

Shared Host PID Namespace

Results 4

Severity	HIGH
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Container should not share the host process ID namespace

../../path/scenarios/kube-bench-security/master-job.yaml:9

Expected: 'spec.template.spec.hostPID' should be set to false or undefined

../../path/scenarios/docker-bench-security/deployment.yaml:27

Expected: 'spec.template.spec.hostPID' should be set to false or undefined

../../path/scenarios/kube-bench-security/node-job.yaml:9

Expected: 'spec.template.spec.hostPID' should be set to false or undefined

../../path/scenarios/system-monitor/deployment.yaml:25

Expected: 'spec.template.spec.hostPID' should be set to false or undefined

Workload Mounting With Sensitive OS Directory

Results 31

Severity	HIGH
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Workload is mounting a volume with sensitive OS Directory

../../path/scenarios/kube-bench-security/master-job.yaml:86

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/kube-controller-manager' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:91

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/var/run/docker.sock' with hostPath

../../path/scenarios/health-check/deployment.yaml:32

Checkmarx

KICS REPORT v2.1.1

Expected: Workload name 'health-check-deployment' of kind 'Deployment' should not mount a host sensitive OS directory '/run/containerd/containerd.sock' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:95

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/srv/kubernetes' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:66

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/etc/systemd' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:72

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/srv/kubernetes' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:77

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/etcd' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:73

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/var/lib' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:79

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/etc' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:83

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/kube-scheduler' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:75

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/etc/kubernetes' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:85

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/usr/bin/containerd' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:110

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/etc/passwd' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:80

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/kubelet' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:78

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/usr/bin' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:76

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/usr/lib/systemd' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:104

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/etc/cni/net.d/' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:89

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/etc/systemd' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:82

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/lib/systemd/system' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:54

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/etcd' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:92

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/lib/systemd' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:113

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/etc/group' with hostPath

../../path/scenarios/docker-bench-security/deployment.yaml:88

Expected: Workload name 'docker-bench-security' of kind 'DaemonSet' should not mount a host sensitive OS directory '/usr/bin/runc' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:57

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/kubelet' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:63

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/kube-controller-manager' with hostPath

Checkmarx

KICS REPORT v2.1.1

../../path/scenarios/kube-bench-security/node-job.yaml:81

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/etc/cni/net.d/' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:101

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/usr/bin' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:69

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/lib/systemd' with hostPath

../../path/scenarios/kube-bench-security/node-job.yaml:60

Expected: Workload name 'kube-bench-node' of kind 'Job' should not mount a host sensitive OS directory '/var/lib/kube-scheduler' with hostPath

../../path/scenarios/system-monitor/deployment.yaml:31

Expected: Workload name 'system-monitor-deployment' of kind 'Deployment' should not mount a host sensitive OS directory '/' with hostPath

../../path/scenarios/kube-bench-security/master-job.yaml:98

Expected: Workload name 'kube-bench-master' of kind 'Job' should not mount a host sensitive OS directory '/etc/kubernetes' with hostPath

Add Instead of Copy

Results 1

Severity	MEDIUM
Platform	Dockerfile
Cwe	610
Category	Supply-Chain

Description

Using ADD to load external installation scripts could lead to an evil web server leveraging this and loading a malicious script.

../../path/infrastructure/hidden-in-layers/Dockerfile:5

Expected: 'COPY' secret.txt

Apt Get Install Pin Version Not Defined

Results 5

Severity	MEDIUM
Platform	Dockerfile
Cwe	1357
Category	Supply-Chain

Description

When installing a package, its pin version should be defined

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: Package 'libcap2-bin' has version defined

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: Package 'curl' has version defined

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: Package 'htop' has version defined

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: Package 'wget' has version defined

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: Package 'cd' has version defined

Container Running As Root

Results 14

Severity	MEDIUM
Platform	Kubernetes
Cwe	

Checkmarx

KICS REPORT v2.1.1

Category Best Practices

Description

Containers should only run as non-root user. This limits the exploitability of security misconfigurations and restricts an attacker's possibilities in case of compromise

../../path/scenarios/health-check/deployment.yaml:24

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/system-monitor/deployment.yaml:39

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/docker-bench-security/deployment.yaml:31

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.securityContext.runAsUser is higher than 0 and/or 'runAsNonRoot' is true

Container Running With Low UID

Results **14**

Severity MEDIUM

Platform Kubernetes

Cwe

Category Best Practices

Description

Check if containers are running with low UID, which might cause conflicts with the host's user table.

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.securityContext.runAsUser should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.securityContext.runAsUser should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Checkmarx

KICS REPORT v2.1.1

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.securityContext.runAsUser should be defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.runAsUser should be defined

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.securityContext.runAsUser should be defined

../../path/scenarios/docker-bench-security/deployment.yaml:31

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.securityContext.runAsUser should be set to a UID >= 10000

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.securityContext.runAsUser should be defined

../../path/scenarios/system-monitor/deployment.yaml:39

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.runAsUser should be defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.securityContext.runAsUser should be defined

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.runAsUser should be defined

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.securityContext.runAsUser should be defined

../../path/scenarios/health-check/deployment.yaml:24

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.runAsUser should be defined

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.securityContext.runAsUser should be defined

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.securityContext.runAsUser should be defined

Containers With Added Capabilities

Results 1

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Containers should not have extra capabilities allowed

../../path/scenarios/docker-bench-security/deployment.yaml:47

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}} has no capability added other than NET_BIND_SERVICE

Docker Daemon Socket is Exposed to Containers

Results 1

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Access Control

Description

Sees if Docker Daemon Socket is not exposed to Containers

../../path/scenarios/docker-bench-security/deployment.yaml:91

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.volumes.name={{docker-sock-volume}}.hostPath.path should not be '/var/run/docker.sock'

Image Version Not Explicit

Results 1

Checkmarx

KICS REPORT v2.1.1

Severity	MEDIUM
Platform	Dockerfile
Cwe	1357
Category	Supply-Chain

Description

Always tag the version of an image explicitly

../../path/infrastructure/goat-home/Dockerfile:1

Expected: FROM alpine:'version'

Image Version Using 'latest'

Results 3

Severity	MEDIUM
Platform	Dockerfile
Cwe	1357
Category	Best Practices

Description

When building images, always tag them with useful tags which codify version information, intended destination (prod or test, for instance), stability, or other information that is useful when deploying the application in different environments. Do not rely on the automatically-created latest tag

../../path/infrastructure/build-code/Dockerfile:1

Expected: FROM alpine:latest:'version' where version should not be 'latest'

../../path/infrastructure/batch-check/Dockerfile:1

Expected: FROM alpine:latest:'version' where version should not be 'latest'

../../path/infrastructure/hidden-in-layers/Dockerfile:1

Expected: FROM alpine:latest:'version' where version should not be 'latest'

Memory Limits Not Defined

Results 6

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Resource Management

Description

Memory limits should be defined for each container. This prevents potential resource exhaustion by ensuring that containers consume not more than the designated amount of memory

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.resources.limits.memory should be defined

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.resources.limits.memory should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.resources.limits.memory should be defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.resources.limits.memory should be defined

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.resources.limits.memory should be defined

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.resources.limits.memory should be defined

Memory Requests Not Defined

Results 11

Checkmarx

KICS REPORT v2.1.1

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Resource Management

Description

Memory requests should be defined for each container. This allows the kubelet to reserve the requested amount of system resources and prevents over-provisioning on individual nodes

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.resources.requests.memory should be defined

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.resources.requests.memory should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.resources.requests.memory should be defined

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.resources.requests.memory should be defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.resources.requests.memory should be defined

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.resources.requests.memory should be defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.resources.requests.memory should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.resources.requests.memory should be defined

../../path/scenarios/health-check/deployment.yaml:15

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.resources.requests.memory should be defined

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.resources.requests.memory should be defined

../../path/scenarios/system-monitor/deployment.yaml:33

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.resources.requests.memory should be defined

NET_RAW Capabilities Not Being Dropped

Results **14**

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Containers should drop 'ALL' or at least 'NET_RAW' capabilities

../../path/scenarios/docker-bench-security/deployment.yaml:46

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.securityContext.capabilities.drop should be defined

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.capabilities.drop should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.securityContext.capabilities.drop should be defined

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.securityContext.capabilities.drop should be defined

Checkmarx

KICS REPORT v2.1.1

../../path/scenarios/system-monitor/deployment.yaml:33

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.capabilities.drop should be defined

../../path/scenarios/health-check/deployment.yaml:15

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.capabilities.drop should be defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.securityContext.capabilities.drop should be defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.capabilities.drop should be defined

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.securityContext.capabilities.drop should be defined

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.securityContext.capabilities.drop should be defined

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.securityContext.capabilities.drop should be defined

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.securityContext.capabilities.drop should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.securityContext.capabilities.drop should be defined

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.securityContext.capabilities.drop should be defined

Permissive Access to Create Pods

Results **1**

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Access Control

Description

The permission to create pods in a cluster should be restricted because it allows privilege escalation.

../../path/infrastructure/helm-tiller/pwnchart/templates/clusterrole.yaml:8

Expected: metadata.name=all-your-base.rules.verbs should not contain a wildcard value when metadata.name=all-your-base.rules.resources contains a wildcard value

Readiness Probe Is Not Configured

Results **10**

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Availability

Description

Check if Readiness Probe is not configured.

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.readinessProbe should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.readinessProbe should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.readinessProbe should be defined

../../path/scenarios/system-monitor/deployment.yaml:33

Checkmarx

KICS REPORT v2.1.1

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.readinessProbe should be defined

../../path/scenarios/health-check/deployment.yaml:15

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.readinessProbe should be defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.readinessProbe should be defined

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.readinessProbe should be defined

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.readinessProbe should be defined

../../path/scenarios/docker-bench-security/deployment.yaml:33

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.readinessProbe should be defined

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.readinessProbe should be defined

Seccomp Profile Is Not Configured

Results **14**

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Containers should be configured with a secure Seccomp profile to restrict potentially dangerous syscalls

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/system-monitor/deployment.yaml:39

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/health-check/deployment.yaml:24

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/docker-bench-security/deployment.yaml:44

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.securityContext.seccompProfile.type should be defined

Checkmarx

KICS REPORT v2.1.1

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.securityContext.seccompProfile.type should be defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.seccompProfile.type should be defined

Service Account Token Automount Not Disabled

Results 13

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Insecure Defaults

Description

Service Account Tokens are automatically mounted even if not necessary

../../path/scenarios/hidden-in-layers/deployment.yaml:9

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/cache-store/deployment.yaml:34

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/batch-check/job.yaml:9

Expected: metadata.name={{batch-check-job}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/health-check/deployment.yaml:13

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/docker-bench-security/deployment.yaml:26

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/kube-bench-security/node-job.yaml:8

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/build-code/deployment.yaml:14

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/hunger-check/deployment.yaml:68

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/kubernetes-goat-home/deployment.yaml:14

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/kube-bench-security/master-job.yaml:8

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/internal-proxy/deployment.yaml:16

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/poor-registry/deployment.yaml:14

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

../../path/scenarios/system-monitor/deployment.yaml:24

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.automountServiceAccountToken should be defined and set to false

Shared Host IPC Namespace

Results 2

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Resource Management

Description

Container should not share the host IPC namespace

https://kics.io

Checkmarx

KICS REPORT v2.1.1

../../path/scenarios/docker-bench-security/deployment.yaml:28

Expected: 'spec.template.spec.hostIPC' should be set to false or undefined

../../path/scenarios/system-monitor/deployment.yaml:26

Expected: 'spec.template.spec.hostIPC' should be set to false or undefined

Shared Host Network Namespace

Results 1

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Resource Management

Description

Container should not share the host network namespace

../../path/scenarios/docker-bench-security/deployment.yaml:29

Expected: 'spec.template.spec.hostNetwork' should be set to false or undefined

Unpinned Package Version in Apk Add

Results 5

Severity	MEDIUM
Platform	Dockerfile
Cwe	1357
Category	Supply-Chain

Description

Package version pinning reduces the range of versions that can be installed, reducing the chances of failure due to unanticipated changes

../../path/infrastructure/batch-check/Dockerfile:1

Expected: RUN instruction with 'apk add <package>' should use package pinning form 'apk add <package>=<version>'

../../path/infrastructure/internal-api/Dockerfile:8

Expected: RUN instruction with 'apk add <package>' should use package pinning form 'apk add <package>=<version>'

../../path/infrastructure/build-code/Dockerfile:7

Expected: RUN instruction with 'apk add <package>' should use package pinning form 'apk add <package>=<version>'

../../path/infrastructure/goat-home/Dockerfile:7

Expected: RUN instruction with 'apk add <package>' should use package pinning form 'apk add <package>=<version>'

../../path/infrastructure/metadata-db/Dockerfile:11

Expected: RUN instruction with 'apk add <package>' should use package pinning form 'apk add <package>=<version>'

Unpinned Package Version in Pip Install

Results 2

Severity	MEDIUM
Platform	Dockerfile
Cwe	1357
Category	Supply-Chain

Description

Package version pinning reduces the range of versions that can be installed, reducing the chances of failure due to unanticipated changes

../../path/infrastructure/build-code/Dockerfile:7

Expected: RUN instruction with 'pip/pip3 install <package>' should use package pinning form 'pip/pip3 install <package>=<version>'

../../path/infrastructure/info-app/Dockerfile:6

Expected: RUN instruction with 'pip/pip3 install <package>' should use package pinning form 'pip/pip3 install <package>=<version>'

Checkmarx

KICS REPORT v2.1.1

Using Unrecommended Namespace

Results 21

Severity	MEDIUM
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Namespaces like 'default', 'kube-system' or 'kube-public' should not be used

../../path/scenarios/build-code/deployment.yaml:29

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/docker-bench-security/deployment.yaml:15

Expected: metadata.namespace should be defined and not null

../../path/scenarios/poor-registry/deployment.yaml:29

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/internal-proxy/deployment.yaml:5

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/system-monitor/deployment.yaml:58

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/system-monitor/deployment.yaml:5

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/batch-check/job.yaml:4

Expected: metadata.namespace should be defined and not null

../../path/scenarios/system-monitor/deployment.yaml:15

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/kube-bench-security/node-job.yaml:5

Expected: metadata.namespace should be defined and not null

../../path/scenarios/kubernetes-goat-home/deployment.yaml:5

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/kubernetes-goat-home/deployment.yaml:29

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/build-code/deployment.yaml:5

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/internal-proxy/deployment.yaml:58

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/hidden-in-layers/deployment.yaml:4

Expected: metadata.namespace should be defined and not null

../../path/scenarios/health-check/deployment.yaml:4

Expected: metadata.namespace should be defined and not null

../../path/scenarios/health-check/deployment.yaml:38

Expected: metadata.namespace should be defined and not null

../../path/scenarios/poor-registry/deployment.yaml:5

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/insecure-rbac/setup.yaml:5

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/internal-proxy/deployment.yaml:45

Expected: 'metadata.namespace' should not be set to default, kube-system or kube-public

../../path/scenarios/metadata-db/templates/service.yaml:4

Expected: metadata.namespace should be defined and not null

../../path/scenarios/kube-bench-security/master-job.yaml:5

Expected: metadata.namespace should be defined and not null

CPU Limits Not Set

Results 6

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Resource Management

Description

CPU limits should be set because if the system has CPU time free, a container is guaranteed to be allocated as much CPU as it requests

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: spec.template.spec.containers.name=hunger-check has resources defined

../../path/scenarios/batch-check/job.yaml:11

Expected: spec.template.spec.containers.name=batch-check has resources defined

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: spec.template.spec.containers.name=kube-bench has resources defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: spec.template.spec.containers.name=cache-store has resources defined

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: spec.template.spec.containers.name=hidden-in-layers has resources defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: spec.template.spec.containers.name=kube-bench has resources defined

CPU Requests Not Set

Results 11

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Resource Management

Description

CPU requests should be set to ensure the sum of the resource requests of the scheduled Containers is less than the capacity of the node

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: spec.template.spec.containers.name=hunger-check should have resources defined

../../path/scenarios/build-code/deployment.yaml:18

Expected: spec.template.spec.containers.name=build-code.resources should have requests defined

../../path/scenarios/poor-registry/deployment.yaml:18

Expected: spec.template.spec.containers.name=poor-registry.resources should have requests defined

../../path/scenarios/health-check/deployment.yaml:17

Expected: spec.template.spec.containers.name=health-check.resources should have requests defined

../../path/scenarios/system-monitor/deployment.yaml:35

Expected: spec.template.spec.containers.name=system-monitor.resources should have requests defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:18

Checkmarx

KICS REPORT v2.1.1

Expected: spec.template.spec.containers.name=kubernetes-goat-home.resources should have requests defined

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: spec.template.spec.containers.name=hidden-in-layers should have resources defined

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: spec.template.spec.containers.name=kube-bench should have resources defined

../../path/scenarios/batch-check/job.yaml:11

Expected: spec.template.spec.containers.name=batch-check should have resources defined

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: spec.template.spec.containers.name=kube-bench should have resources defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: spec.template.spec.containers.name=cache-store should have resources defined

Cluster Admin Rolebinding With Superuser Permissions

Results **1**

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Access Control

Description

Ensure that the cluster-admin role is only used where required (RBAC)

../../path/scenarios/insecure-rbac/setup.yaml:14

Expected: Resource name 'superadmin' of kind 'ClusterRoleBinding' isn't binding 'cluster-admin' role with superuser permissions

Healthcheck Instruction Missing

Results **14**

Severity	LOW
Platform	Dockerfile
Cwe	710
Category	Insecure Configurations

Description

Ensure that HEALTHCHECK is being used. The HEALTHCHECK instruction tells Docker how to test a container to check that it is still working

../../path/infrastructure/helm-tiller/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/internal-api/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/system-monitor/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/hidden-in-layers/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/batch-check/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/poor-registry/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/health-check/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/build-code/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

Checkmarx

KICS REPORT v2.1.1

../../path/infrastructure/info-app/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/metadata-db/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/hunger-check/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/users-repo/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/cache-store/Dockerfile:1

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

../../path/infrastructure/goat-home/Dockerfile:23

Expected: Dockerfile should contain instruction 'HEALTHCHECK'

Image Without Digest

Results **14**

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Images should be specified together with their digests to ensure integrity

../../path/scenarios/system-monitor/deployment.yaml:34

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.image should specify the image with a digest

../../path/scenarios/internal-proxy/deployment.yaml:30

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.image should specify the image with a digest

../../path/scenarios/docker-bench-security/deployment.yaml:34

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.image should specify the image with a digest

../../path/scenarios/kube-bench-security/master-job.yaml:29

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.image should specify the image with a digest

../../path/scenarios/kubernetes-goat-home/deployment.yaml:17

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.image should specify the image with a digest

../../path/scenarios/health-check/deployment.yaml:16

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.image should specify the image with a digest

../../path/scenarios/poor-registry/deployment.yaml:17

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.image should specify the image with a digest

../../path/scenarios/hunger-check/deployment.yaml:72

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.image should specify the image with a digest

../../path/scenarios/cache-store/deployment.yaml:37

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.image should specify the image with a digest

../../path/scenarios/kube-bench-security/node-job.yaml:12

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.image should specify the image with a digest

../../path/scenarios/internal-proxy/deployment.yaml:19

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.image should specify the image with a digest

../../path/scenarios/batch-check/job.yaml:12

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.image should specify the image with a digest

../../path/scenarios/build-code/deployment.yaml:17

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.image should specify the image with a digest

../../path/scenarios/hidden-in-layers/deployment.yaml:12

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.image should specify the image with a digest

Invalid Image Tag

Results 14

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Supply-Chain

Description

Image tag must be defined and not be empty or equal to latest.

../../path/scenarios/kubernetes-goat-home/deployment.yaml:17

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.image tag is provided and not latest

../../path/scenarios/kube-bench-security/node-job.yaml:12

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.image tag is provided and not latest

../../path/scenarios/internal-proxy/deployment.yaml:30

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.image tag is provided and not latest

../../path/scenarios/docker-bench-security/deployment.yaml:34

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.image tag is provided and not latest

../../path/scenarios/build-code/deployment.yaml:17

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.image tag is provided and not latest

../../path/scenarios/batch-check/job.yaml:12

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.image tag is provided and not latest

../../path/scenarios/kube-bench-security/master-job.yaml:29

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.image tag is provided and not latest

../../path/scenarios/hunger-check/deployment.yaml:72

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.image tag is provided and not latest

../../path/scenarios/internal-proxy/deployment.yaml:19

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.image tag is provided and not latest

../../path/scenarios/health-check/deployment.yaml:16

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.image tag is provided and not latest

../../path/scenarios/hidden-in-layers/deployment.yaml:12

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.image tag is provided and not latest

../../path/scenarios/poor-registry/deployment.yaml:17

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.image tag is provided and not latest

../../path/scenarios/cache-store/deployment.yaml:37

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.image tag is provided and not latest

../../path/scenarios/system-monitor/deployment.yaml:34

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.image tag is provided and not latest

Missing AppArmor Profile

Results 14

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Access Control

Checkmarx

KICS REPORT v2.1.1

Description

Containers should be configured with an AppArmor profile to enforce fine-grained access control over low-level system resources

../../path/scenarios/hidden-in-layers/deployment.yaml:7

Expected: metadata.name={{hidden-in-layers}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{hidden-in-layers}}

../../path/scenarios/docker-bench-security/deployment.yaml:23

Expected: metadata.name={{docker-bench-security}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{docker-bench}}

../../path/scenarios/system-monitor/deployment.yaml:21

Expected: metadata.name={{system-monitor-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{system-monitor}}

../../path/scenarios/poor-registry/deployment.yaml:11

Expected: metadata.name={{poor-registry-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{poor-registry}}

../../path/scenarios/internal-proxy/deployment.yaml:13

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{internal-api}}

../../path/scenarios/internal-proxy/deployment.yaml:13

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{info-app}}

../../path/scenarios/kube-bench-security/node-job.yaml:5

Expected: metadata.name={{kube-bench-node}}.annotations should specify an AppArmor profile for container {{kube-bench}}

../../path/scenarios/build-code/deployment.yaml:11

Expected: metadata.name={{build-code-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{build-code}}

../../path/scenarios/health-check/deployment.yaml:10

Expected: metadata.name={{health-check-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{health-check}}

../../path/scenarios/cache-store/deployment.yaml:31

Expected: metadata.name={{cache-store-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{cache-store}}

../../path/scenarios/kubernetes-goat-home/deployment.yaml:11

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{kubernetes-goat-home}}

../../path/scenarios/hunger-check/deployment.yaml:65

Expected: metadata.name={{hunger-check-deployment}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{hunger-check}}

../../path/scenarios/kube-bench-security/master-job.yaml:5

Expected: metadata.name={{kube-bench-master}}.annotations should specify an AppArmor profile for container {{kube-bench}}

../../path/scenarios/batch-check/job.yaml:7

Expected: metadata.name={{batch-check-job}}.spec.template.metadata.annotations should specify an AppArmor profile for container {{batch-check}}

Multiple RUN, ADD, COPY, Instructions Listed

Results **2**

Severity	LOW
Platform	Dockerfile
Cwe	710
Category	Best Practices

Description

Multiple commands (RUN, COPY, ADD) should be grouped in order to reduce the number of layers.

../../path/infrastructure/health-check/Dockerfile:12

Expected: There isn´t any RUN instruction that could be grouped

../../path/infrastructure/metadata-db/Dockerfile:11

Expected: There isn´t any RUN instruction that could be grouped

No Drop Capabilities for Containers

Results **14**

Checkmarx

KICS REPORT v2.1.1

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Best Practices

Description

Sees if Kubernetes Drop Capabilities exists to ensure containers security context

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.containers.name=kubernetes-goat-home.securityContext should be set

../../path/scenarios/system-monitor/deployment.yaml:39

Expected: metadata.name={{system-monitor-deployment}}.spec.containers.name={{system-monitor}}.securityContext.capabilities should be set

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.containers.name=internal-api.securityContext should be set

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.containers.name=build-code.securityContext should be set

../../path/scenarios/batch-check/job.yaml:11

Expected: metadata.name={{batch-check-job}}.spec.containers.name=batch-check.securityContext should be set

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.containers.name=kube-bench.securityContext should be set

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.containers.name=info-app.securityContext should be set

../../path/scenarios/docker-bench-security/deployment.yaml:46

Expected: spec.containers[docker-bench].securityContext.capabilities.drop should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.containers.name=poor-registry.securityContext should be set

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.containers.name=hidden-in-layers.securityContext should be set

../../path/scenarios/health-check/deployment.yaml:24

Expected: metadata.name={{health-check-deployment}}.spec.containers.name={{health-check}}.securityContext.capabilities should be set

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.containers.name=kube-bench.securityContext should be set

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.containers.name=hunger-check.securityContext should be set

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.containers.name=cache-store.securityContext should be set

Pip install Keeping Cached Packages

Results **2**

Severity	LOW
Platform	Dockerfile
Cwe	459
Category	Best Practices

Description

When installing packages with pip, the '--no-cache-dir' flag should be set to make Docker images smaller

../../path/infrastructure/build-code/Dockerfile:7

Expected: The '--no-cache-dir' flag should be set when running 'pip/pip3 install'

../../path/infrastructure/info-app/Dockerfile:6

Expected: The '--no-cache-dir' flag should be set when running 'pip/pip3 install'

Pod or Container Without LimitRange

Results 13

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Each namespace should have a LimitRange policy associated to ensure that resource allocations of Pods, Containers and PersistentVolumeClaims do not exceed the defined boundaries

../../path/scenarios/internal-proxy/deployment.yaml:5

Expected: metadata.name={{internal-proxy-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/batch-check/job.yaml:4

Expected: metadata.name={{batch-check-job}} has a 'LimitRange' policy associated

../../path/scenarios/system-monitor/deployment.yaml:15

Expected: metadata.name={{system-monitor-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/kubernetes-goat-home/deployment.yaml:5

Expected: metadata.name={{kubernetes-goat-home-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/hunger-check/deployment.yaml:59

Expected: metadata.name={{hunger-check-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/kube-bench-security/master-job.yaml:5

Expected: metadata.name={{kube-bench-master}} has a 'LimitRange' policy associated

../../path/scenarios/docker-bench-security/deployment.yaml:15

Expected: metadata.name={{docker-bench-security}} has a 'LimitRange' policy associated

../../path/scenarios/build-code/deployment.yaml:5

Expected: metadata.name={{build-code-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/cache-store/deployment.yaml:22

Expected: metadata.name={{cache-store-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/health-check/deployment.yaml:4

Expected: metadata.name={{health-check-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/poor-registry/deployment.yaml:5

Expected: metadata.name={{poor-registry-deployment}} has a 'LimitRange' policy associated

../../path/scenarios/kube-bench-security/node-job.yaml:5

Expected: metadata.name={{kube-bench-node}} has a 'LimitRange' policy associated

../../path/scenarios/hidden-in-layers/deployment.yaml:4

Expected: metadata.name={{hidden-in-layers}} has a 'LimitRange' policy associated

Pod or Container Without ResourceQuota

Results 13

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Each namespace should have a ResourceQuota policy associated to limit the total amount of resources Pods, Containers and PersistentVolumeClaims can consume

../../path/scenarios/cache-store/deployment.yaml:22

Expected: metadata.name={{cache-store-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/kubernetes-goat-home/deployment.yaml:5

Expected: metadata.name={{kubernetes-goat-home-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/kube-bench-security/master-job.yaml:5

Expected: metadata.name={{kube-bench-master}} has a 'ResourceQuota' policy associated

../../path/scenarios/internal-proxy/deployment.yaml:5

Expected: metadata.name={{internal-proxy-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/batch-check/job.yaml:4

Expected: metadata.name={{batch-check-job}} has a 'ResourceQuota' policy associated

../../path/scenarios/health-check/deployment.yaml:4

Expected: metadata.name={{health-check-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/hidden-in-layers/deployment.yaml:4

Expected: metadata.name={{hidden-in-layers}} has a 'ResourceQuota' policy associated

../../path/scenarios/system-monitor/deployment.yaml:15

Expected: metadata.name={{system-monitor-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/poor-registry/deployment.yaml:5

Expected: metadata.name={{poor-registry-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/kube-bench-security/node-job.yaml:5

Expected: metadata.name={{kube-bench-node}} has a 'ResourceQuota' policy associated

../../path/scenarios/docker-bench-security/deployment.yaml:15

Expected: metadata.name={{docker-bench-security}} has a 'ResourceQuota' policy associated

../../path/scenarios/hunger-check/deployment.yaml:59

Expected: metadata.name={{hunger-check-deployment}} has a 'ResourceQuota' policy associated

../../path/scenarios/build-code/deployment.yaml:5

Expected: metadata.name={{build-code-deployment}} has a 'ResourceQuota' policy associated

Pod or Container Without Security Context

Results **11**

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

A security context defines privilege and access control settings for a Pod or Container

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: spec.template.spec.containers.name=poor-registry has a security context

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: spec.template.spec.containers.name=hidden-in-layers has a security context

../../path/scenarios/batch-check/job.yaml:11

Expected: spec.template.spec.containers.name=batch-check has a security context

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: spec.template.spec.containers.name=hunger-check has a security context

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: spec.template.spec.containers.name=kubernetes-goat-home has a security context

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: spec.template.spec.containers.name=info-app has a security context

Checkmarx

KICS REPORT v2.1.1

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: spec.template.spec.containers.name=internal-api has a security context

../../path/scenarios/build-code/deployment.yaml:16

Expected: spec.template.spec.containers.name=build-code has a security context

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: spec.template.spec.containers.name=kube-bench has a security context

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: spec.template.spec.containers.name=kube-bench has a security context

../../path/scenarios/cache-store/deployment.yaml:36

Expected: spec.template.spec.containers.name=cache-store has a security context

Root Container Not Mounted Read-only

Results **14**

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Build Process

Description

Check if the root container filesystem is not being mounted read-only.

../../path/scenarios/health-check/deployment.yaml:24

Expected: metadata.name={{health-check-deployment}}.spec.template.spec.containers.name={{health-check}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.template.spec.containers.name={{poor-registry}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.template.spec.containers.name={{kubernetes-goat-home}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/hidden-in-layers/deployment.yaml:11

Expected: metadata.name={{hidden-in-layers}}.spec.template.spec.containers.name={{hidden-in-layers}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.template.spec.containers.name={{hunger-check}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/kube-bench-security/node-job.yaml:11

Expected: metadata.name={{kube-bench-node}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/docker-bench-security/deployment.yaml:44

Expected: metadata.name={{docker-bench-security}}.spec.template.spec.containers.name={{docker-bench}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{info-app}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/system-monitor/deployment.yaml:39

Expected: metadata.name={{system-monitor-deployment}}.spec.template.spec.containers.name={{system-monitor}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.template.spec.containers.name={{internal-api}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.template.spec.containers.name={{build-code}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/kube-bench-security/master-job.yaml:28

Expected: metadata.name={{kube-bench-master}}.spec.template.spec.containers.name={{kube-bench}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.template.spec.containers.name={{cache-store}}.securityContext.readOnlyRootFilesystem should be set to true

../../path/scenarios/batch-check/job.yaml:11

Checkmarx

KICS REPORT v2.1.1

Expected: metadata.name={{batch-check-job}}.spec.template.spec.containers.name={{batch-check}}.securityContext.readOnlyRootFilesystem should be set to true

Run Using apt

Results 3

Severity	LOW
Platform	Dockerfile
Cwe	758
Category	Supply-Chain

Description

apt is discouraged by the linux distributions as an unattended tool as its interface may suffer changes between versions. Better use the more stable apt-get and apt-cache

../../path/infrastructure/hunger-check/Dockerfile:4

Expected: RUN instructions should not use the 'apt' program

../../path/infrastructure/helm-tiller/Dockerfile:9

Expected: RUN instructions should not use the 'apt' program

../../path/infrastructure/health-check/Dockerfile:12

Expected: RUN instructions should not use the 'apt' program

Secrets As Environment Variables

Results 1

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Secret Management

Description

Container should not use secrets as environment variables

../../path/scenarios/system-monitor/deployment.yaml:50

Expected: 'spec.template.spec.containers.name={{system-monitor}}.env.name={{K8S_GOAT_VAULT_KEY}}.valueFrom.secretKeyRef' should be undefined

Service Does Not Target Pod

Results 1

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Insecure Configurations

Description

Service should Target a Pod

../../path/scenarios/metadata-db/templates/service.yaml:3

Expected: metadata.name={{{}}}.spec.selector label refers to a Pod label

Service Type is NodePort

Results 1

Severity	LOW
Platform	Kubernetes
Cwe	
Category	Networking and Firewall

Description

Service type should not be NodePort

../../path/scenarios/internal-proxy/deployment.yaml:60

Expected: spec.type should not be 'NodePort'

Checkmarx

KICS REPORT v2.1.1

APT-GET Not Avoiding Additional Packages

Results 1

Severity	INFO
Platform	Dockerfile
Cwe	710
Category	Supply-Chain

Description

Check if any apt-get installs don't use '--no-install-recommends' flag to avoid installing additional packages.

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: 'RUN apt-get update && apt-get install -y htop libcap2-bin curl wget && cd /tmp; arch=`uname -m` && if [$arch = "aarch64"] || [$arch = "arm64"]; then GOTTY="gotty_2.0.0-alpha.3_linux_arm.tar.gz"; else GOTTY="gotty_2.0.0-alpha.3_linux_amd64.tar.gz"; fi; wget https://github.com/yudai/gotty/releases/download/v2.0.0-alpha.3/${GOTTY} && tar -xvzf ${GOTTY}; mv gotty /usr/local/bin/gotty' uses '--no-install-recommends' flag to avoid installing additional packages

Apk Add Using Local Cache Path

Results 1

Severity	INFO
Platform	Dockerfile
Cwe	459
Category	Supply-Chain

Description

When installing packages, use the '--no-cache' switch to avoid the need to use '--update' and remove '/var/cache/apk/*'

../../path/infrastructure/goat-home/Dockerfile:7

Expected: 'RUN' should not contain 'apk add' command without '--no-cache' switch

Apt Get Install Lists Were Not Deleted

Results 1

Severity	INFO
Platform	Dockerfile
Cwe	459
Category	Supply-Chain

Description

After using apt-get install, it is needed to delete apt-get lists

../../path/infrastructure/system-monitor/Dockerfile:4

Expected: After using apt-get install, the apt-get lists should be deleted

Ensure Administrative Boundaries Between Resources

Results 1

Severity	INFO
Platform	Kubernetes
Cwe	
Category	Access Control

Description

As a best practice, ensure that is made the correct use of namespaces to adequately administer your resources. Kubernetes Authorization plugins can also be used to create policies that segregate user access to namespaces.

../../path/scenarios/build-code/deployment.yaml:5

Expected: ensure that these namespaces are the ones you need and are adequately administered as per your requirements.

Liveness Probe Is Not Defined

Results 10

Severity	INFO
Platform	Kubernetes
Cwe	

Checkmarx

KICS REPORT v2.1.1

Category Availability

Description

In case of an unresponsive container, a Liveness Probe can help your application become more available since it restarts the container. However, it can lead to cascading failures. Define one if you really need it

../../path/scenarios/internal-proxy/deployment.yaml:18

Expected: metadata.name={{internal-proxy-deployment}}.spec.containers.name={{internal-api}}.livenessProbe should be defined

../../path/scenarios/health-check/deployment.yaml:15

Expected: metadata.name={{health-check-deployment}}.spec.containers.name={{health-check}}.livenessProbe should be defined

../../path/scenarios/poor-registry/deployment.yaml:16

Expected: metadata.name={{poor-registry-deployment}}.spec.containers.name={{poor-registry}}.livenessProbe should be defined

../../path/scenarios/hunger-check/deployment.yaml:71

Expected: metadata.name={{hunger-check-deployment}}.spec.containers.name={{hunger-check}}.livenessProbe should be defined

../../path/scenarios/internal-proxy/deployment.yaml:29

Expected: metadata.name={{internal-proxy-deployment}}.spec.containers.name={{info-app}}.livenessProbe should be defined

../../path/scenarios/kubernetes-goat-home/deployment.yaml:16

Expected: metadata.name={{kubernetes-goat-home-deployment}}.spec.containers.name={{kubernetes-goat-home}}.livenessProbe should be defined

../../path/scenarios/cache-store/deployment.yaml:36

Expected: metadata.name={{cache-store-deployment}}.spec.containers.name={{cache-store}}.livenessProbe should be defined

../../path/scenarios/docker-bench-security/deployment.yaml:33

Expected: metadata.name={{docker-bench-security}}.spec.containers.name={{docker-bench}}.livenessProbe should be defined

../../path/scenarios/system-monitor/deployment.yaml:33

Expected: metadata.name={{system-monitor-deployment}}.spec.containers.name={{system-monitor}}.livenessProbe should be defined

../../path/scenarios/build-code/deployment.yaml:16

Expected: metadata.name={{build-code-deployment}}.spec.containers.name={{build-code}}.livenessProbe should be defined

Using Kubernetes Native Secret Management

Results **3**

Severity INFO
Platform Kubernetes
Cwe
Category Secret Management

Description

Kubernetes External Secret Storage and Management System usage should be considered if you have more complex secret management needs, rather than using Kubernetes Secrets directly. Additionally, ensure that access to secrets is carefully limited

../../path/scenarios/hunger-check/deployment.yaml:49

Expected: External secret storage should be used

../../path/scenarios/system-monitor/deployment.yaml:4

Expected: External secret storage should be used

../../path/scenarios/hunger-check/deployment.yaml:40

Expected: External secret storage should be used