tufin

SecureCloud™

Security Posture Report

SecureCloud account: generic-bank

04 Jan 2021, 09:24 AM

Table of Contents

Public Cloud Summary

5	37	48	4
CLOUD ACCOUNTS	ASSETS IN VIOLATION	TOTAL ASSETS	ACCOUNTS FAIL CIS BENCHMARK

Risky Ports

3 out of 48 assets
have high-risk ports

Overly Permissive Access

31 out of 48 assets
have overly permissive access

Policy Violations

0 out of 48 assets
have cloud vendor settings that don't comply with your policy

Tag Usage

15 out of 48 assets
without tags

CIS Benchmark Public Cloud

47 out of 82 tests
fail the CIS benchmark

Kubernetes Summary

3	68	68	1
CLUSTERS	WORKLOADS IN VIOLATION	TOTAL WORKLOADS	CLUSTERS FAIL CIS BENCHMARK

Workload Security

68 out of 68 workloads
have a security context that violates your risk configuration

Kubernetes Vulnerabilities

0 out of 3 clusters
have known vulnerabilities

Container Vulnerabilities

68 out of 68 workloads
have containers with score B and lower

Permissive Network Policies

3 out of 3 clusters
have permissive Kubernetes network policies

CIS Benchmark Kubernetes

16 out of 39 tests
fail the CIS benchmark

Public Cloud Account Details

demo-iris

2	3	Failed
ASSETS IN VIOLATION	TOTAL ASSETS	CIS BENCHMARK

Violation Type	Assets	Violation Details
Risky Ports	--	--
Permissive Source	1	Any (1 assets)
Permissive Service	--	--
Policy Violations	--	--
Tag Usage	1	Without tags
CIS benchmark	--	13 out of 22 tests fail

dev-iris

3	4	Failed
ASSETS IN VIOLATION	TOTAL ASSETS	CIS BENCHMARK

Violation Type	Assets	Violation Details
Risky Ports	--	--
Permissive Source	2	Any (2 assets)
Permissive Service	1	TCP: 0-65535 (1 assets)
Policy Violations	--	--
Tag Usage	2	Without tags
CIS benchmark	--	15 out of 22 tests fail

iris-demo

5	9	Failed
ASSETS IN VIOLATION	TOTAL ASSETS	CIS BENCHMARK

Violation Type	Assets	Violation Details
Risky Ports	--	--
Permissive Source	4	Any (3 assets) 10.0.0.0/8 (1 assets)
Permissive Service	--	--
Policy Violations	--	--
Tag Usage	2	Without tags
CIS benchmark	--	16 out of 19 tests fail

iris-dev

19	24	Failed
ASSETS IN VIOLATION	TOTAL ASSETS	CIS BENCHMARK

Violation Type	Assets	Violation Details
Risky Ports	2	RDP (TCP:3389) (2 assets) POP3 (TCP:110) (2 assets) Microsoft-DS (TCP:445) (2 assets) Telnet (TCP:23) (2 assets) Net-Bios (TCP:137-139) (2 assets)
Permissive Source	16	Any (16 assets)
Permissive Service	5	Any (5 assets)
Policy Violations	--	--
Tag Usage	10	Without tags
CIS benchmark	--	3 out of 19 tests fail

securecloud-demo

8	8	Passed
ASSETS IN VIOLATION	TOTAL ASSETS	CIS BENCHMARK

Violation Type	Assets	Violation Details
Risky Ports	1	RDP (TCP:3389) (1 assets) Telnet (TCP:23) (1 assets)
Permissive Source	5	Any (5 assets)
Permissive Service	6	Any (6 assets)
Policy Violations	--	--
Tag Usage	--	--
CIS benchmark	--	--

Kubernetes Cluster Details

eks

6	6	0	Failed
WORKLOADS IN VIOLATION	TOTAL WORKLOADS	KUBERNETES VULNERABILITIES	CIS BENCHMARK

Violation Type	Workloads	Violation Details
Workload Security	6	Capability NET_RAW (5 workloads) Memory unlimited (6 workloads) Writable root filesystem (5 workloads) Privileged (3 workloads) Privileged escalation (5 workloads) Writable OS mount (3 workloads) hostNetwork (2 workloads) CPU unlimited (6 workloads) Root allowed (6 workloads)
Container Vulnerabilities	6	Score NA (6 workloads)
Kubernetes Vulnerabilities	--	--
Permissive Network Policies	--	6 Namespaces
CIS Benchmark Kubernetes	--	4 out of 13 tests fail

retail

32	32	0	Failed
WORKLOADS IN VIOLATION	TOTAL WORKLOADS	KUBERNETES VULNERABILITIES	CIS BENCHMARK

Violation Type	Workloads	Violation Details
Workload Security	32	Privileged escalation (29 workloads) Memory unlimited (23 workloads) hostNetwork (9 workloads) Privileged (7 workloads) Writable root filesystem (32 workloads) CPU unlimited (28 workloads) Root allowed (31 workloads) Writable OS mount (7 workloads) Read-only OS mount (2 workloads) hostPID (1 workloads) Capability NET_RAW (29 workloads)
Container Vulnerabilities	32	Score NA (32 workloads)
Kubernetes Vulnerabilities	--	--
Permissive Network Policies	--	7 Namespaces
CIS Benchmark Kubernetes	--	6 out of 13 tests fail

my-project

30	30	0	Failed
WORKLOADS IN VIOLATION	TOTAL WORKLOADS	KUBERNETES VULNERABILITIES	CIS BENCHMARK

Violation Type	Workloads	Violation Details
Workload Security	30	Privileged escalation (27 workloads) Memory unlimited (21 workloads) Root allowed (29 workloads) Writable OS mount (5 workloads) Privileged (5 workloads) Read-only OS mount (2 workloads) Writable root filesystem (30 workloads) Capability NET_RAW (27 workloads) CPU unlimited (26 workloads) hostNetwork (8 workloads)
Container Vulnerabilities	30	Score NA (30 workloads)

Violation Type	Workloads	Violation Details
Kubernetes Vulnerabilities	--	--
Permissive Network Policies	--	7 Namespaces
CIS Benchmark Kubernetes	--	6 out of 13 tests fail

Terms

Public Cloud

Term / Phrase	Description
Assets	An asset in SecureCloud is a server or cloud service in your cloud account such as a virtual machine or bucket storage.
CIS Benchmark Public Cloud	The CIS Benchmark for Public Cloud is a subset of the security controls developed by the Center for Internet Security (CIS) and adapted for Microsoft Azure and Amazon AWS. These controls have gained widespread acceptance as a baseline for public cloud security and can be downloaded from the CIS website.
Permissive service	Permissive service is where UDP or TCP ingress is allowed from any port (Min=0, Max=65535). This is configured in Risk Configuration.
Permissive source	Permissive source is where the access allowes unlimited range of IPs (class A subnet mask e.g. 10.0.0.0/8) or any source (Source=ANY). This is configured in the "Risk Configuration" section of the "Configuration" area.
Policy Violations	A policy violation is a case where access is allowed while going against the Cloud Policy.
Risky ports	List of ports that expose your environment to risk. the list is configured in the "Risk Configuration" section of the "Configuration" area.

Kubernetes

Term / Phrase	Description
Capability NET_ADMIN	Allows various network-related operations including interface configuration, administration of IP firewall, modifying routing tables and more.
Capability NET_RAW	Any kind of packet can be forged, which includes faking senders, sending malformed packets, etc., this also allows to bind to any address (associated to the ability to fake a sender this allows to impersonate a device, legitimately used for \"transparent proxying\" as per the manpage but from an attacker point-of-view this term is a synonym for Man-in-The-Middle). This should be prevented by dropping the NET_RAW capability.
Capability SYS_ADMIN	Never enable this capability - it is equivalent to root.
CIS Benchmark Kubernets	The CIS Benchmark for Kubernetesis a subset of the security controls developed by the Center for Internet Security (CIS) and adapted for Kubernetes . These controls have gained widespread acceptance as a baseline for public cloud security and can be downloaded from the CIS website.
Container vulnerabilities	SecureCloud scans your containers and gives each one a security score from A to F, according to the number and type of software vulnerabilities found, where A - the best score - represents

Term / Phrase	Description
	the lowest risk and F - the worst score - represents the highest risk.
CPU unlimited	The Container has no upper bound on the CPU resources it can use. The Container could use all of the CPU resources available on the Node where it is running. This should be prevented by setting the CPU limit at the container level or through a LimitRange at the namespace level.
hostIPC	Pod can share the host's IPC namespace.
hostNetwork	Pod can use the host's network namespace. This gives the pod access to the loopback device, services listening on localhost, and could be used to snoop on network activity of other pods on the same node
Kubernetes vulnerabilities	Kubernetes Vulnerabilities are known vulnerabilities in Kubernetes implementations. The full list of vulnerabilities can be seen here on GitHub.
Memory unlimited	The Container has no upper bound on the amount of memory it uses. The Container could use all of the memory available on the Node where it is running which in turn could invoke the OOM Killer. Further, in case of an OOM Kill, a container with no resource limits will have a greater chance of being killed. This should be prevented by setting the memory limit at the container level or through a LimitRange at the namespace level.
Privileged	Container is privileged. Process in privileged containers are essentially equivalent to root on the host.
Privileged escalation	Process in this container can gain more privileges than their parent process. This should be prevented by setting 'allowPrivilegeEscalation: false'
Read-only OS mount	Container can read from a host OS volume.
Root allowed	Process in this container can run as root. This should be prevented by setting 'runAsNonRoot: true' and providing a non-zero runAsUser value or a USER value in the Dockerfile. It is advisable to select a value greater than 10000, as this reduces the likelihood that this value is already taken on the host system.
Running as root	Process in this container are running with UID 0 (root).
Unmasked ProcMount	Container has full access to host's /proc.
Unsafe sysctls	Pod can use unsafe sysctls. You should only allow unsafe sysctls for very special situations such as high-performance or real-time application tuning.
Security context	A security context defines privilege and access control settings for pods and containers.
Workload	Workloads are objects that set deployment rules for pods. Based on these rules, Kubernetes performs the deployment and updates the workload with the current state of the application. Workloads let you define the rules for application scheduling, scaling and upgrade.
Workload security	Workload security refers to a pod or container having a security context that doesn't comply with

Term / Phrase	Description
	your policy
Writable OS mount	Container can read and write to a host OS volume.
Writable root filesystem	Container has a writable root filesystem. An immutable root filesystem can prevent malicious binaries being added to PATH and increase attack cost. This should be prevented by setting 'readOnlyRootFilesystem: true'.

Legend

Term / Phrase	Description
	Any
	Service
	Subnet
	Kubernetes Cluster
	AWS
	Azure
	Google Cloud