Threat ID	QUALTRICS ID	Threat Description	Assumptions	STRIDE Threat	Affected Components
1	LEAKED-PRIVILEGE-REMOTE	An attacker uses leaked (e.g. on Github) cluster configuration file (e.g. /etc/kubernetes/admin.conf) to interact with the cluster, potentially jeopardize running workloads and creating malicious pods.	- The attacker finds the leaked information; - The attacker can (remotely) interact with the cluster.	Elevation of privilege Information Disclosure	- Cluster secrets/credentials
2	SPOOFING-AUTH-WORKLOAD	Spoofing a cluster admin by stealing the authentication credentials via a social engineering attack.	- The attacker carries out a successful spoofing attack; - The credentials are valid.	Spoofing	- Cluster configuration - Running workloads (pods, container, etc.) - Access control (of users and services) In general, he/she can take over the all cluster.
3	DOS-WORKERNODE	An attacker with shell access to only one pod which has no resource limits applied (e.g. max memory and cpus usage) can crash the worker node on which that pod is running, causing a Denial of Service (DoS).	- The attacker got a remote shell on a pod.	DoS	- Compromised pod, worker node, and all the other pods running on the same node.
4	ELEVATION-PRIVILEGE-MALICIOUS-IMG	An attacker able to upload images to a container registry from which a Kubernetes cluster retrieves pods images, he or she can potentially execute a malicious pod inside the cluster and get a shell from the malicious container.	- The attacker has permissions to upload or modify images in the registry used by the Kubernetes cluster;	Elevation of privilege	- Images Registry - Running pod
5	EXPLOIT-PRIVILEGED-CONTAINER	Privileged containers run as root on the host, thus an attacker compromising one of such containers, gets automatically root access on the host.	- The attacker get acccess to a privileged container running in the cluster; - The attacker escapes the container.	Elevation of privilege	- Pod - Worker node
6	PORT-JAMMING-NETWORK-POLICIES	If an attacker deploys a malicious pod into a namespace of the cluster with network policies in place, the attacker can use such a pod to send bogus network packages to pods in different namespaces to jam the exposed ports, causing a disruption in the cluster performance.	- The network policies are implemented correctly to segment the namespaces.	DoS	- Pods in different namespaces.
7	LEAKED-SECRET-DOCKERFILE	If a developer embeds a secret in a Dockerfile A and then builds an image (image A), an attacker with access to image A can reverse the image's layers to not only observe the embedded secret in Dockerfile A but also from other images that were built from different Dockerfiles.	- The attacker has access to the image	Information Disclosure	- Cluster secrets/credentials
8	CHAIN-ATTACK-MALICIOUS-INPUTS	If an attacker compromises a running container, he/she can only continue exploiting the container by running the software specified in Dockerfile (by the developers) with malicious inputs.	- The attacker got access to a running container.	Elevation of privilege Tampering	- Running pod/container
9	UNAUTH-CONFIG-TAMPERING	An unauthenticated and non privileged attacker can still upload custom pod configuration into the cluster to prepare the first step of another attack, e.g. turning off logging service or cause a denial of service.	- The attacker can reach the cluster API server (e.g. through internet)	Elevation of privilege Tampering	- New pods
10	SPOOFING-LAYER-3	If an attacker compromises a pod in a Kubernetes cluster using a Layer 3 network solution, he/she can steal other pod's identities and laterally move within the cluster using the network bridge.	- The attacker exploits one container - The CNI works at layer 3	Spoofing	- Lateral movement between pods