| Qualtrics ID | To be copied on ChatGPT-Threat description, assumptions, STRIDE threat type, and Affected components |
|---|---|
| LEAKED-PRIVILEGE-REMOTE | **Scenario:** deploying a pod on kubernetes,<br>**Threat Description:** 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.<br>**Assumptions:** The attacker finds the leaked information. The attacker can (remotely) interact with the cluster<br>**STRIDE threat type:** Elevation of privilege and/or Information Disclosure<br>**Affected components:** Cluster secrets/credentials |
| SPOOFING-AUTH-WORKLOAD | **Scenario:** deploying a pod on kubernetes<br>**Threat Description:** 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<br>**Assumptions**: The attacker exploits one container, The CNI works at layer 3<br>**STRIDE threat type**: Spoofing<br>**Affected components**: Lateral movement between pods |
| DOS-WORKERNODE | **Scenario:** deploying a pod on kubernetes<br>**Threat Description:** 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)<br>**Assumptions**: The attacker got a remote shell on a pod<br>**STRIDE threat type**: Denial of Service<br>**Affected components:** Compromised pod, worker node, and all the other pods running on the same node. |
| ELEVATION-PRIVILEGE-MALICIOUS-IMG | **Scenario:** deploying a pod on kubernetes<br>**Threat Description:** 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<br>**Assumptions:** The attacker has permissions to upload or modify images in the registry used by the Kubernetes cluster<br>**STRIDE threat type:** Elevation of privilege<br>**Affected components**: Images Registry, Running pod |
| EXPLOIT-PRIVILEGED-CONTAINER | **Scenario:** deploying a pod on kubernetes<br>**Threat description:** Privileged containers run as root on the host, thus an attacker compromising one of such containers, gets automatically root access on the host.<br>**Assumptions:** The attacker get access to a privileged container |

| | |
|---|---|
| | running in the cluster, The attacker escapes the container<br>**STRIDE threat type**: Elevation of privilege<br>**Affected components:** Pod, Worker node |
| PORT-JAMMING-NETWORK-POLICIES | **Scenario:** deploying a pod on kubernetes<br>**Threat Description**: 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<br>**Assumptions:** The network policies are implemented correctly to segment the namespaces<br>**STRIDE threat type**: Denial of service<br>**Affected components:** Pods in different namespaces. |
| LEAKED-SECRET-DOCKERFILE | **Scenario:** deploying a pod on kubernetes<br>**Threat description:** 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<br>**Assumptions:** The attacker has access to the image<br>**STRIDE threat type:** Information Disclosure<br>**Affected components**: Cluster secrets/credentials |
| CHAIN-ATTACK-MALICIOUS-INPUTS | **Scenario:** deploying a pod on kubernetes<br>**Threat Description:** 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<br>**Assumptions:** The attacker got access to a running container<br>**STRIDE threat type**: Elevation of privilege and or Tampering<br>**Affected components**: running pod/container |
| UNAUTH-CONFIG-TAMPERING | **Scenario:** deploying a pod on kubernetes<br>**Threat description:** 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<br>**Assumptions:** The attacker can reach the cluster API server (e.g. through the Internet)<br>**STRIDE threat type:** Elevation of privilege and tampering<br>**Affected components**: New pods |
| SPOOFING-LAYER-3 | **Scenario:** deploying a pod on kubernetes<br>**Threat description:** Spoofing a cluster admin by stealing the authentication credentials via a social engineering attack<br>**Assumptions:** The attacker carries out a successful spoofing attack, The credentials are valid.<br>**STRIDE threat type:** Spoofing |

| | |
|---|---|
| | **Affected components:** Cluster configuration, Running workloads (pods, container, etc.),  Access control (of users and services) |