Attack Vectors Overview

From public www
Kubernetes dashboard(s)
Kubernetes control plane (apiserver, kubelets)
Infrastructure components that shouln't be accessible from this POV (image repository, etcd…)
Application components that shouldn't be accessible from this POV
cloud provider management console / api
supply compromised container (base) image
supply compromised Kubernetes configuration
supply compromised dependencies (i.e. npm packages)
on (underlying) infrastructure
on application logic

information gathering

= Out of scope

From company network
Kubernetes dashboard(s)
Kubernetes control plane (apiserver, kubelets)
Infrastructure components that shouln't be accessible from this POV (internal image repository, etcd…)
Application components that shouldn't be accessible from this POV
cloud provider management console / api
on (underlying) infrastructure
on application logic

information gathering
circumvent detection / logging / monitoring
compromise orchestration-external resources

From within container
Kubernetes dashboard(s)
Kubernetes control plane (apiserver, kubelets)
Infrastructure components that shouln't be accessible from this POV (internal image repository, etcd…)
Application components that shouldn't be accessible from this POV
cloud provider management console / api (i.e. azure subscription file)
breakout to host / Priviledge Escalation
compromise local image cache
R/W on host file systems
modify existing container
hoard node resources (DOS)
misuse node resources (cryptojacking)
on (underlying) infrastructure
on application logic
information gathering
circumvent detection / logging / monitoring
cross-tenancy influcence
gain persistence
compromise orchestration-external resources

From Node	From management interfaces (api's & webinterfaces of cloud & k8s)
	add new node
add new container	add new container
manipulate cluster configuration	manipulate cluster configuration
hoard node resources (DOS)	hoard orchestration resources (DOS)
misuse node resources (cryptojacking)	misuse orchestration resources (cryptojacking)
information gathering	information gathering
circumvent detection / logging / monitoring	circumvent detection / logging / monitoring
cross-tenancy influcence	cross-tenancy influcence
gain persistence	gain persistence
compromise orchestration-external resources	compromise orchestration-external resources

Criteria:

Required Acess Level	Auffindbarkeit	Ausnutzbarkeit (Komplexität)
any (5)	Einfach (5)	Sehr einfach (5)
read access (4)	Durchschnittlich (3)	Einfach (4)
cluster user (3)	Schwierig (1)	Durchschnittlich (3)
cluster admin (2)		Schwierig (2)
cloud admin (1)		Theoretisch (1)

Formel Possibility: RAL + Auffindbarkeit + Ausnutzbarkeit
-> Theoretische Range: 1 bis 15

Formel Risk: ((Possibility/3) * Impact)
-> Produkt aus Eintrittswahrscheinlichkeit (1-5) und Auswirkung (1-5)

TODO: Possibility-Faktoren miteinander addieren oder multiplizieren?

Quellen:
https://www.owasp.org/images/0/0b/Threat_Modeling_Using_STRIDE_v1.1.pdf

Impact	App specific criticality
Schwerwiegend (5)	out of scope
Mittel (3)	
Gering (1)	
keine (0)	