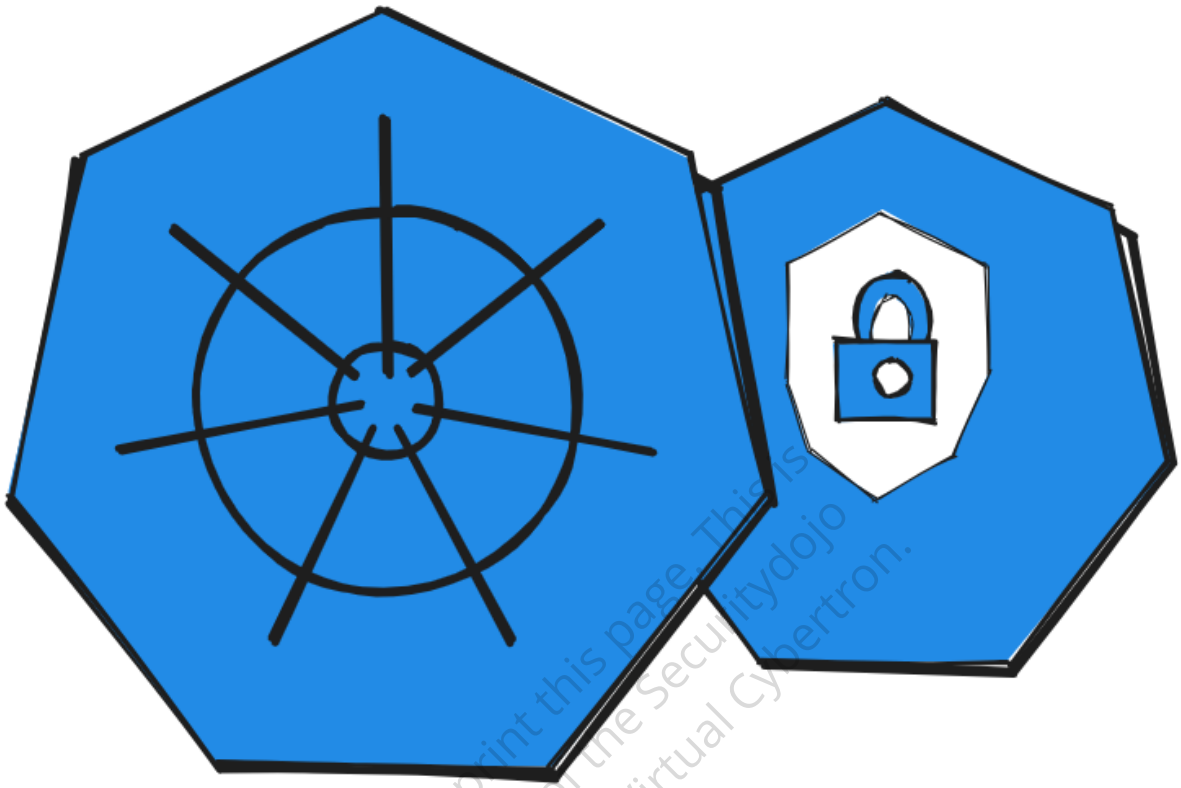
Hardening Kubernetes



Hardening Kubernetes refers to the practice of enhancing the security posture of your Kubernetes cluster by reducing potential attack surfaces and implementing stricter access controls.

- Security Context:
    - In Kubernetes, a Security Context is an attribute that can be associated with a Pod or a specific container within the Pod to manage security aspects. These aspects include running a pod or container as a non-root user, enforcing read-only root file system, and controlling Linux capabilities.
- Discretionary Access Control (DAC):
    - Kubernetes employs Role-Based Access Control (RBAC), which is a form of DAC. It allows cluster administrators to define roles with specific permissions (like reading secrets, listing pods, etc.), and bind these roles to users or groups of users. The user's permissions can be passed to the applications and services that

they deploy.

- Security Enhanced Linux (SELinux):
    - When running on a host that has SELinux enabled, Kubernetes can utilize its features to provide additional isolation and protection between pods. It allows further restrictions on what processes can do and what resources they can access.
- Linux Capabilities:
    - In Kubernetes, capabilities can be dropped or added to containers via the Security Context to provide a more granular level of access control and to minimize potential risks. This can help to ensure that containers have only the privileges they need to function, and no more.
- AppArmor:
    - AppArmor can be used with Kubernetes to confine containerized applications more securely using application-specific profiles. These profiles can help to reduce the potential impact of a container compromise by limiting what the container process can do and access.
- Seccomp:
    - Kubernetes supports the use of seccomp profiles for containers. A seccomp profile can be associated with a container to restrict the system calls it's able to make, thereby reducing the attack surface of the Linux kernel.
- Pod Security Policies (PSP):
    - Pod Security Policies (PSP) are a cluster-level resource that controls the actions that a pod can perform and what it has access to. PSPs are used to enforce security best practices and policies for pods in a cluster. **Now deprecated, PSPs are being replaced by the more flexible Pod Security Admission Controllers.**