8: Security Framework

WHY THIS FRAMEWORK IS IMPORTANT	EXERCISE
A new environment and new application deployment necessitates security changes in policy and processes. This framework focuses on the 4 C's of Kubernetes Security: Cloud, Clusters, Containers, Code. Pay attention to how secrets, data clusters, authentication, and authorization are handled.	2 Hours Medium Difficulty Enterprise Architect Head of Operations Security Manager

Is there a defined process where clusters are being scanned and certified?

□ Yes
□ No

Are clusters being scanned/rescanned?

□ Yes
□ No

Is there a process for handling clusters that fail a compliance/vulnerability scan?

□ Yes
□ No

Do authentication mechanisms vary from cluster to cluster?

□ Yes
□ No

If a backend authentication issue occurs, are local accounts available to access a cluster?

□ Yes
□ No

Does the initial kubeadmin account still exist? If so, is it active?

□ Yes - Exist
□ Yes - Active
□ No

Is there a process for provisioning accounts to each cluster?

□ Yes
□ No

Are access rights different across clusters (dev/test, QA, production)?

□ Yes
□ No

What networking subsystem is being used to provide underlying SDN for clusters?

□ Calico
□ Flannel
□ OpenShift SDN
□ Other______________________________

Is there a default network policy used when provisioning new namespaces?

□ Yes
□ No

Is there a policy or practice in place limiting access between pods that should be restricted from communicating?

□ Yes
□ No

Is there a central management system in place to store secrets?

□ Yes
□ No

Is there a process in place to enforce the access of secrets across deployments?

□ Yes
□ No

Is there a requirement for data to be encrypted at rest?

□ Yes
□ No

Is there a requirement for data to be encrypted in transit?

□ Yes
□ No

Do you have an intrusion detection system in place?

- □ Yes
- □ No

If yes, is your intrusion detection solution able to automatically respond to threats?

- □ Yes
- □ No

Are you using a Web Application Firewall?

- □ Yes
- □ No

NEXT STEPS

Count the number of times you answered “Yes” and compare it to the number of times you answered “No.” This will give you a sense of how secure you are today.

Now, look at your “No” answers. Rank order them from the highest risk to the lowest risk. (even though the lowest risk might make you very vulnerable.) This ranking will give you a roadmap on what to tackle first.