Secure Code-to-Cloud:
Key Discovery Questions

Topic 6: Securing Containers, Kubernetes & Data

Modern development moves fast, but security must keep pace. These questions help identify gaps in governance, tooling, and visibility across your pipelines.

Question List

Use these questions to assess your software supply chain security and DevSecOps readiness.

1 Where are you running containers and Kubernetes today (managed cloud, on prem, hybrid), and what are your biggest security concerns in production?

2 How do you control which images developers and pipelines can use (approved registries, curated images, signing/scanning)?

3 Do you have runtime threat detection and response for Kubernetes workloads and how quickly can you investigate what happened?

4 How do you measure and enforce Kubernetes security posture (RBAC, policies, misconfigurations, compliance reporting) across clusters?

5 What is your current approach to protecting sensitive data in container platforms (access controls, secrets, and audit visibility), and where are the gaps?

Why These Questions Matter?

Answering these questions helps uncover risks and align your strategy with best practices in DevSecOps.

✉ Contact Us

Want to strengthen your security posture? Contact our global team today.