nuaware
An Exclusive Networks Company

Secure Code-to-Cloud: Key Discovery Questions

Topic 9: Kubernetes Visibility & Troubleshooting

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. How many Kubernetes clusters/environments do you operate today, and who is responsible for supporting them day to day?
2. When an incident happens, what's your typical workflow to diagnose the issue (kubectl, dashboards, log tools, observability), and how long does it usually take to reach root cause?
3. Do teams struggle with context switching across clusters/namespaces, or is troubleshooting mostly handled by a small group of Kubernetes experts?
4. Do developers have safe, role based visibility into what's running in Kubernetes, or do they rely on Ops/SRE to pull logs and status?
5. What are the most common "release blockers" you see in Kubernetes?

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.