

Secure Code-to-Cloud: Key Discovery Questions

Topic 2: Managing and securing Secrets, Non-Human Identity and Bots?

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 API keys, tokens, and certificates stored today, and how often are they rotated?
- 2 Do you have an inventory of non-human identities (service accounts, workloads, automation) and clear ownership for each?
- 3 Can you distinguish good bots (search engines, partners) from bad bots, and how confident are you in your current controls?
- 4 Do you have visibility into secrets your teams may have accidentally exposed in source control (e.g., GitHub/GitLab/Bitbucket)?
- 5 If you could improve one outcome first, would it be fewer secret leaks, faster rotation, fewer bot-driven incidents/fraud, or better visibility?

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.