DevSecOps Best Practices

Friday, November 18, 2022

8:23 AM

1. Maintain cordial relationships with Developers/QA and Operation teams.

2. Do not fail builds unless you are at maturity level 3 or 4.

3. Do not run any tool which takes more than 10 minutes in CI/CD pipelines.

4. Create separate jobs for each tool/scan.

5. Roll out tools/scans in phases (iteratively) even when critical/high severity issues are found.

6. Do not buy tools that does not provide APIs or CLIs.

7. Love the vendor who does per-use licensing model with all your heart, soul, mind and strength.

8. Verify if the tool vendors support incremental/baseline scans

9. Create SAST/DAST custom rule sets. Tools are of no use without creating custom rules/tweaks down the line

10. Do Everything as Code (EaC) to provide the audit-ability, measurability, and security.

11. Do False Positives as Code to control scope of the scans.

12. Link tool wiki in the pipeline as a comment for sharing your team’s expertise with others.