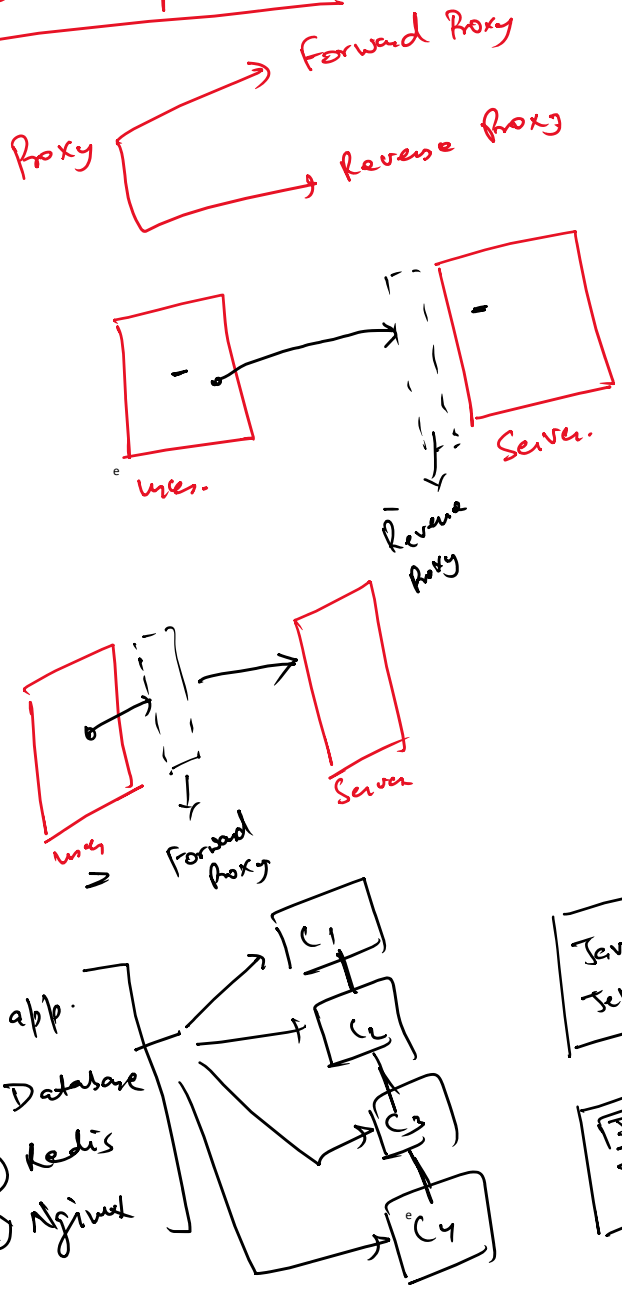
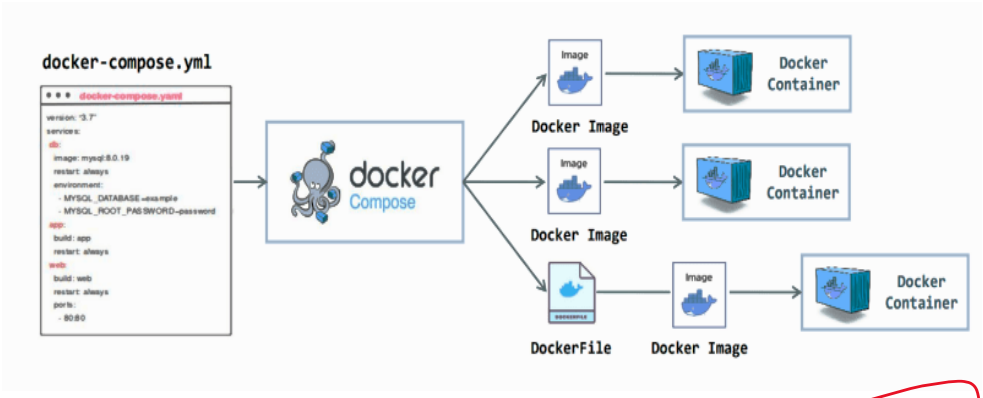
Day - 3

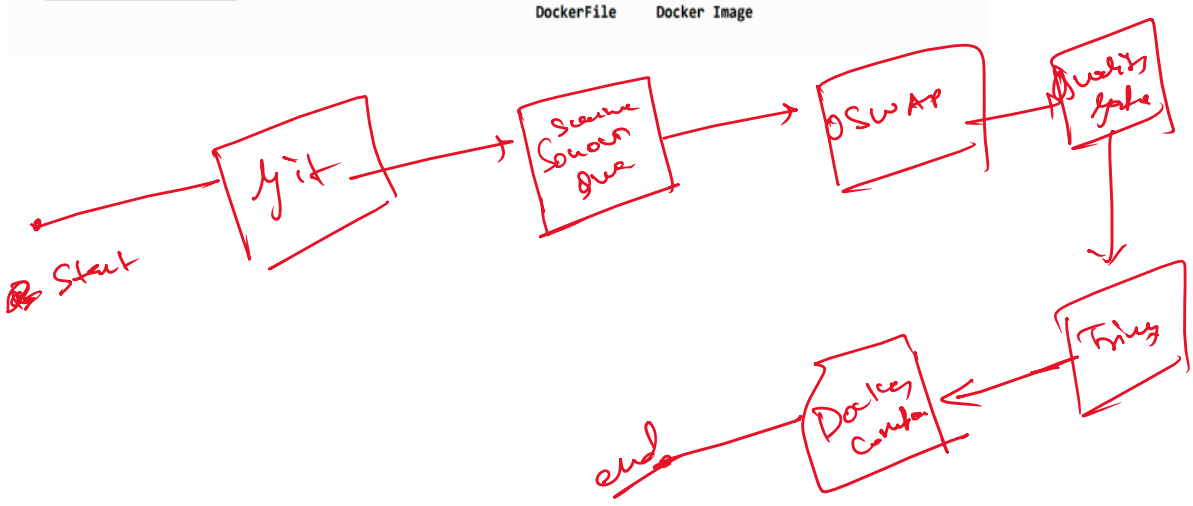
27 November 2025 10:23

1. Docker Compose ✓
2. Complete pipeline. ✓
3.
   - Automating compliance checks (e.g., GDPR)
   - Introduction to threat modeling

1. Docker Compose :-







GDPR (General Data Protection Regulation)

↓

law in European Union

↓

Protect & maintain privacy of user.

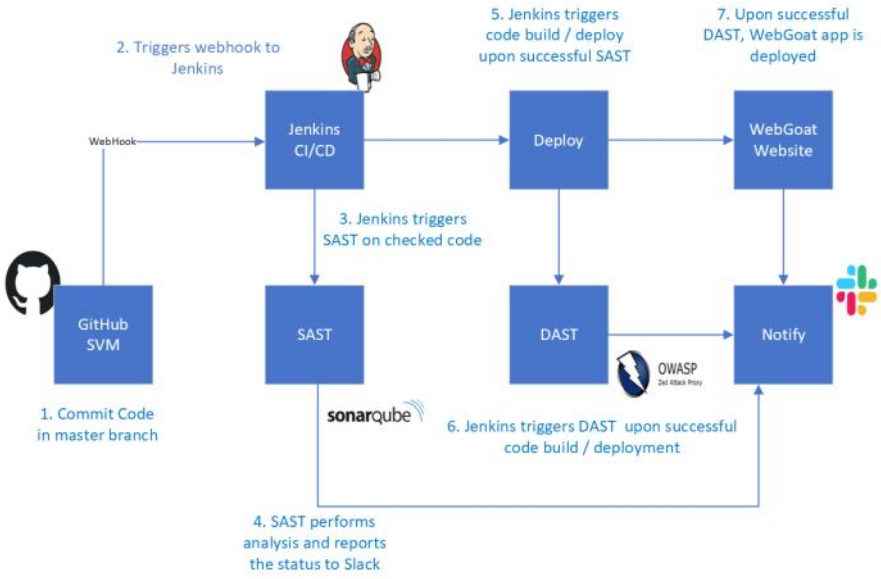
↓

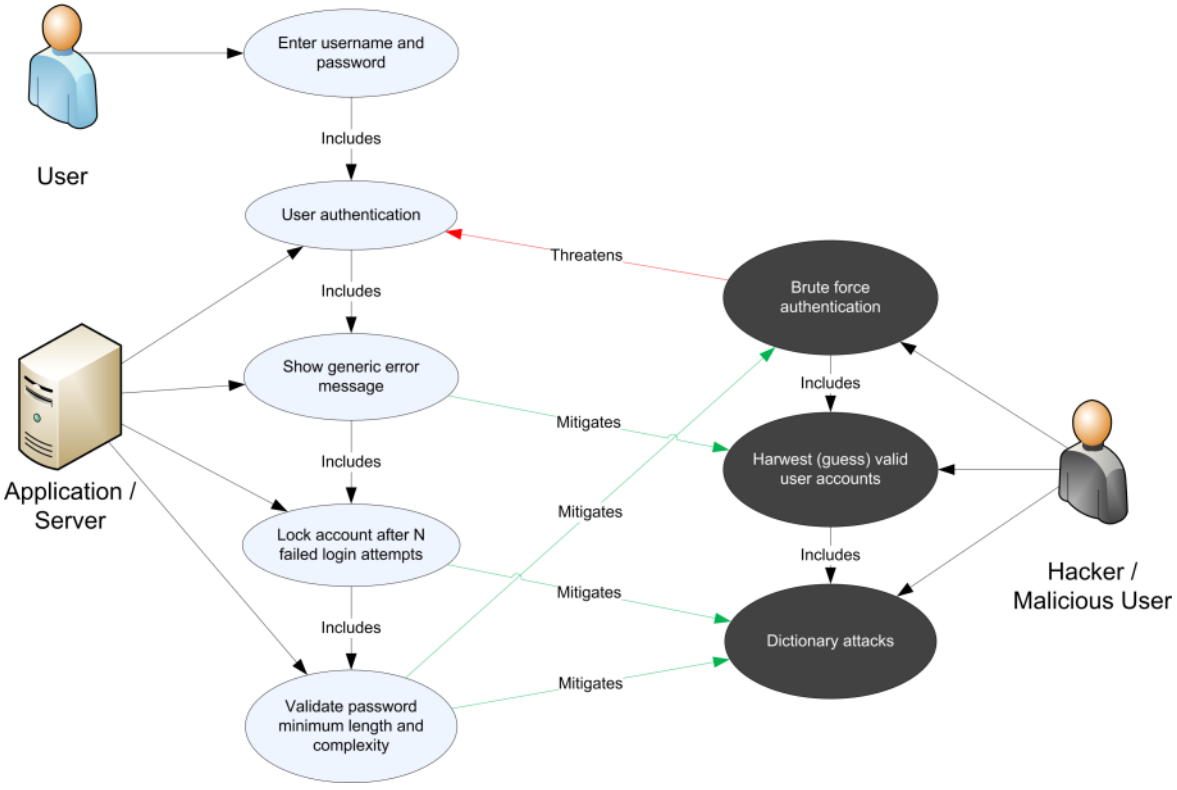
Company in EU

Company → Handle the EU citizen data

Data Protection law that govern in EU Region, & add the compliance to the Companies to how to store, collect, process, secure & retain your data.

DAST – Dynamic Application Security Tool


2. Triggers webhook to Jenkins
5. Jenkins triggers code build / deploy upon successful SAST
7. Upon successful DAST, WebGoat app is deployed
WebHook
Jenkins CI/CD
Deploy
WebGoat Website
3. Jenkins triggers SAST on checked code
GitHub SVM
SAST
DAST
Notify
OWASP
1. Commit Code in master branch
sonarqube
6. Jenkins triggers DAST upon successful code build / deployment
4. SAST performs analysis and reports the status to Slack


Enter username and password
User
Includes
User authentication
Threatens
Brute force authentication
Includes
Includes
Show generic error message
Mitigates
Harwest (guess) valid user accounts
Includes
Application / Server
Includes
Lock account after N failed login attempts
Mitigates
Includes
Mitigates
Hacker / Malicious User
Includes
Dictionary attacks
Validate password minimum length and complexity
Mitigates

TOOLBOX™

5 KEY STEPS OF THREAT MODELING PROCESS