**SBOM integration with Jenkins CI/CD**

SBOM stands for Software Bill of Materials. It's a list of the components in a piece of software, including all its dependencies, libraries, modules, and their versions. SBOMs are essential for understanding the makeup of software, tracking known vulnerabilities, ensuring compliance with licensing requirements, and facilitating supply chain security. They provide transparency and visibility into the software supply chain, aiding in risk management and cybersecurity efforts. SBOMs are increasingly important in industries such as software development, cybersecurity, and regulatory compliance.

**Pipeline script including SBOM steps:**

pipeline {

agent any

tools {nodejs 'node'}

stages {

stage('Checkout from GitHub') {

steps {

checkout scmGit(branches: [[name: '\*/development']], extensions: [], userRemoteConfigs: [[url: 'https://github.com/Vikx001/Studio-Ghibli.git']])

}

}

stage('Install dependencies'){

steps{

dir('frontend/studio-ghibli'){

sh ('npm install')

}

}

}

stage('Build'){

steps{

dir('frontend/studio-ghibli'){

sh ('npm install -g license-checker && npm install --save-dev nyc && npm install istanbul --save-dev && npm install --save-dev @babel/plugin-proposal-private-property-in-object && npm run build')

}

}

}

stage('Static Code Analysis') {

environment {

SONAR\_URL = "http://44.204.44.47:9000"

}

steps {

dir('frontend/studio-ghibli'){

script{

withCredentials([string(credentialsId: 'sonarqube', variable: 'SONAR\_AUTH\_TOKEN')]) {

withSonarQubeEnv('sonar') {

//sh "npm install --save-dev mocha chai"

//sh "npm test -- --coverage"

// sh "npm run sonartest"

//sh "npm run coverage"

sh "npm install sonar-scanner"

sh "npm run sonar"

}

}

}

}

}

}

stage('Sonarqube quality gate check') {

steps{

timeout(time: 1, unit: 'HOURS'){

waitForQualityGate abortPipeline: true

}

}

}

stage('Generating SBOM'){

steps{

dir('frontend/studio-ghibli'){

sh ('license-checker --json --out sbom.json')}

}

}

}

}

**Output:**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**