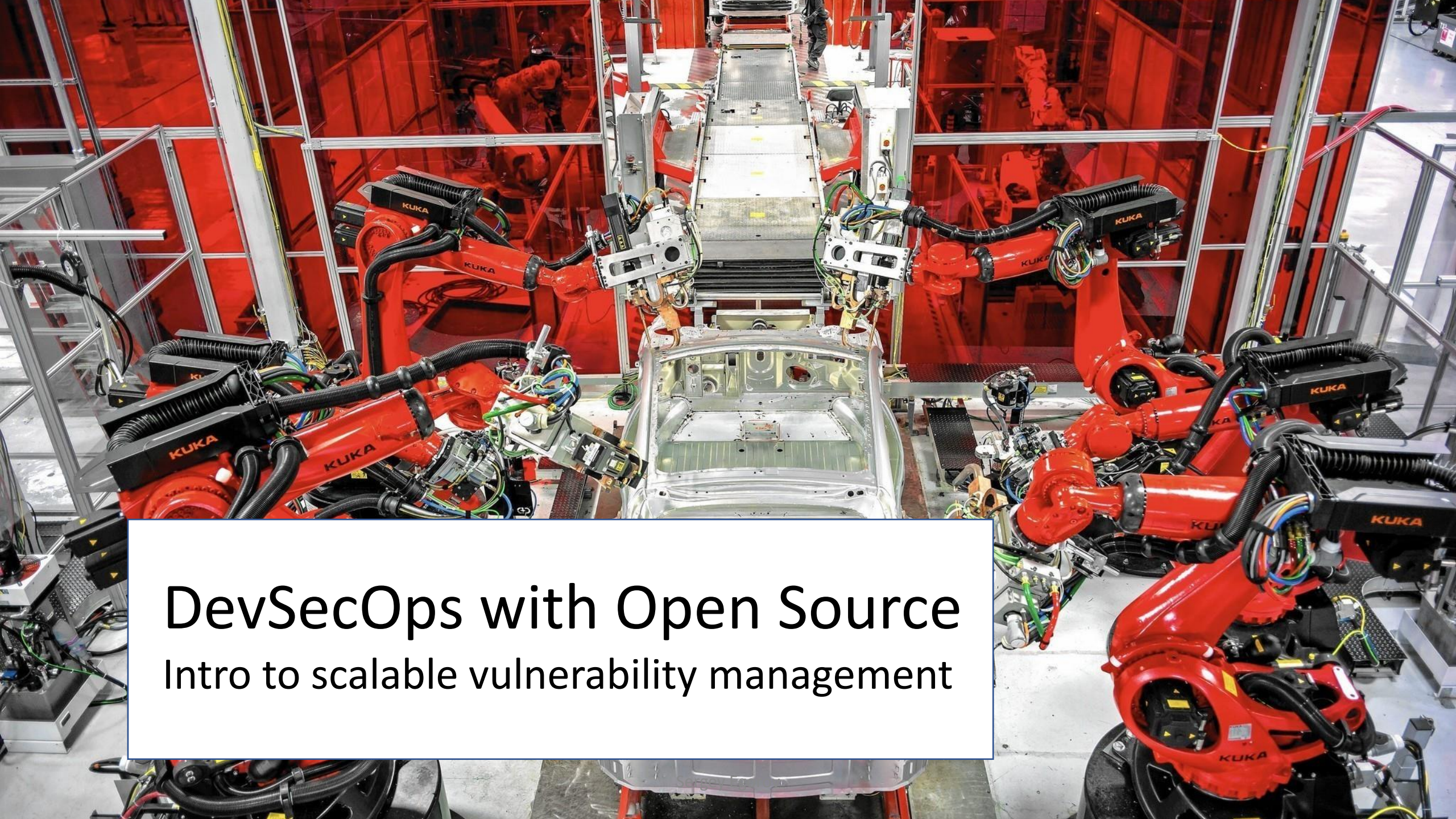


DevSecOps with Open Source

Intro to scalable vulnerability management

Solution Requirements

- Analyze vulnerabilities in applications (code, dependencies, websites)
- Check the infrastructure configuration against best practices and known vulnerabilities, including Docker / Kubernetes and Infra as Code
- Aggregate issues in one vulnerability management system
- On-prem, no cloud code submissions or findings exposure
- Scale with number of scans required (ad-hoc vs CI/CD)
- Reasonable price, but effective analysis


GitLab
RUNNER
scansuite
DEFECTDOJO
Jira
Vulnerability scanners

scansuite

- Vulnerability scanners orchestration software
- Supports ~30 open source and commercial scanners
- CI/CD and stand-alone checks
- Tasks spread via MQ to workers, scales to any number of scans, exports results to Defect Dojo
- Not open sourced, could be used for non-commercial purposes

Static Application Security Testing (SAST):

- Semgrep (+ GitLab edition)
- CodeQL

+ Language specific (FindSecBugs, Sec Code Scan, Bandit etc.)

Software Composition Analysis (SCA):

- Trivy
- OWASP Dependency Check
- Snyk

Mobile Application Security Testing (MAST):

- MobSF

Secrets scan

- GitLeaks
- TruffleHog

Dynamic Application Security Testing (DAST):

- ZAP
- PortSwigger Dastardly
- Nuclei
- Nikto by Netsparker
- Arachni
- DirSearch

+ CMS specific (WPScan etc)

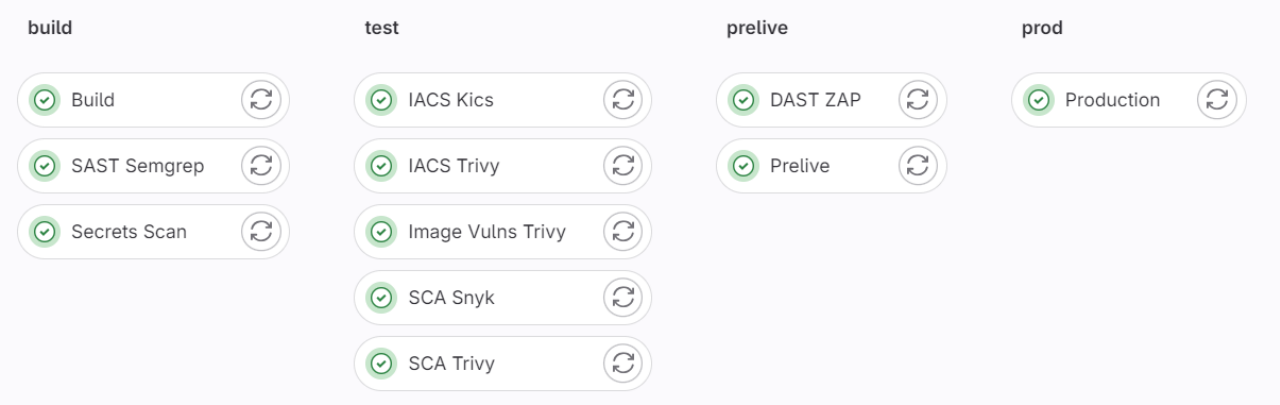
Infrastructure checks

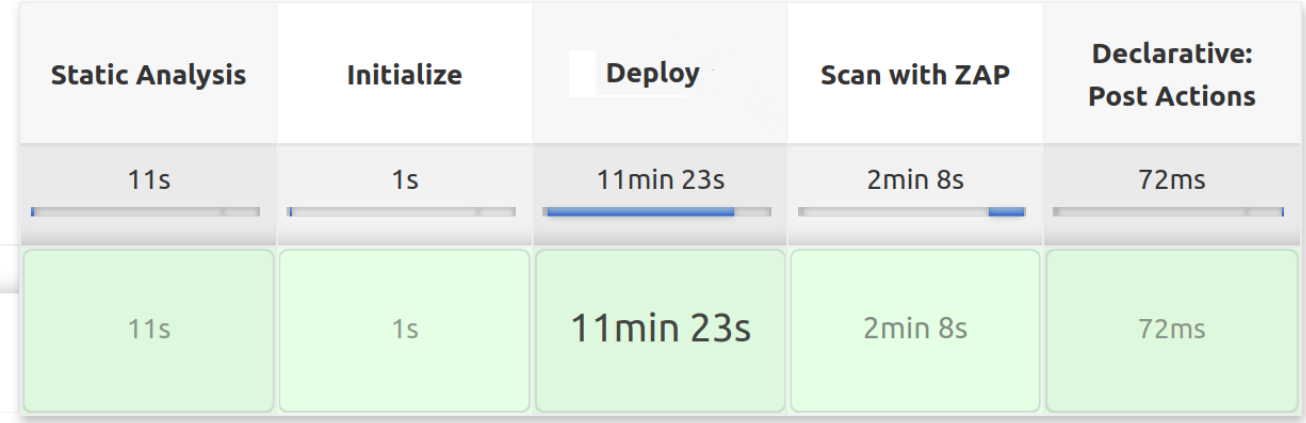
- **Local server patch level**: OpenScap with OVAL definitions
- **Linux CIS/STIG compliance**: OpenScap
- **Docker / Kubernetes**: Trivy, Snyk, Docker-Bench, Kube-Bench
- **Infrastructure as Code Scan (IACS):** Checkmarx KICS, Aqua Security Trivy
- **Remote scans:** OpenVAS, nmap, Nuclei, Netattaker

Scanning via GUI / cli

```
scanbot@scansuite:~$ sudo ./scansuite oscap_ubuntu 3 22

------ ScanSuite v2.0 -----
-- Author: Sergey Egorov --

Title   Package "prelink" Must not be Installed
Rule    xccdf_org.ssgproject.content_rule_package_prelink_removed
Result  pass

Title   Install AIDE
Rule    xccdf_org.ssgproject.content_rule_package_aide_installed
Result  fail

Title   Build and Test AIDE Database
Rule    xccdf_org.ssgproject.content_rule_aide_build_database
Result  fail
```

CI/CD pipeline integration






```yaml
SAST Semgrep:
  stage: build
  image:
  script:
    ~/scansuite semgrep $ENG

Secrets Scan:
  stage: build
  script:
    - ~/scansuite secrets $ENG

Dep Check OWASP:
  stage: build
  script:
    - ~/scansuite dep_owasp $ENG

Dep Check Trivy:
  stage: build
  script:
    - ~/scansuite dep_trivy $ENG

Image Vulns Trivy:
  stage: build
  script:
    - cd && ./scansuite image_trivy $ENG $IMAGE

IACS Trivy:
  stage: test
  script:
    - ~/scansuite iacs_trivy $ENG

IACS Kics:
  stage: test
  script:
    - ~/scansuite iacs_kics $ENG
```

```
17 Starting the scan ...
18 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ GitLab Find Security Bugs analyzer v2.28.4
19 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ Detecting project
20 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ Found project in /src
21 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ Running analyzer
22 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ Found Mvnw project in /src directory
23 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ Found 1 analyzable projects.
24 [INFO] [Find Security Bugs] [2022-01-03T07:00:13Z] ▶ Building Mvnw project at /src.
25 [INFO] [Find Security Bugs] [2022-01-03T07:00:26Z] ▶ Project built.
26 [INFO] [Find Security Bugs] [2022-01-03T07:00:56Z] ▶ SpotBugs analysis succeeded for /src!
27 [INFO] [Find Security Bugs] [2022-01-03T07:00:56Z] ▶ Creating report
28 Uploading Results to DefectDojo ...
29   % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
30                                  Dload  Upload   Total   Spent    Left  Speed
31 100 30589  100   234  100 30355    124  16172  0:00:01  0:00:01 --:--:-- 16288
32 {"scan_date":"2022-01-03","minimum_severity":"Low","active":true,"verified":true,"scan_type":"GitLa
   a":false,"test":54}
34 Cleaning up file based variables
36 Job succeeded
```

DEFECTDOJO

Vulnado

Overview | Components | Metrics | Engagements 1 | Findings 448

Description

Vulnado

Metrics

29	146	222
CRITICAL	HIGH	MEDIUM

Jira | Your work | Projects | Filters | Dashboards | People | Apps | Create

Java Vulnado
Software project

Back to project

Filters

All issues
My open issues
Reported by me
Open issues
Done issues
Viewed recently
Resolved recently
Updated recently

Projects / Java Vulnado

Issues

Search issues | Project: Java Vulnado | Type | Status | Assignee | More | Save filter

Type	Key	Summary	Assignee
	JV-6	Spring CSRF Unrestricted RequestMapping	Unassigned
	JV-5	CVE-2021-33574 Libc-Devtools 2.31-13+deb11u2	Sergey E
	JV-4	CVE-2020-27619 libpython3.9-minimal 3.9.2-1	Sergey E
	JV-3	Unsafe Hash Equals	Sergey E
	JV-2	Potential Command Injection	Sergey E
	JV-1	Spring CSRF Unrestricted RequestMapping	Sergey E

Open Findings

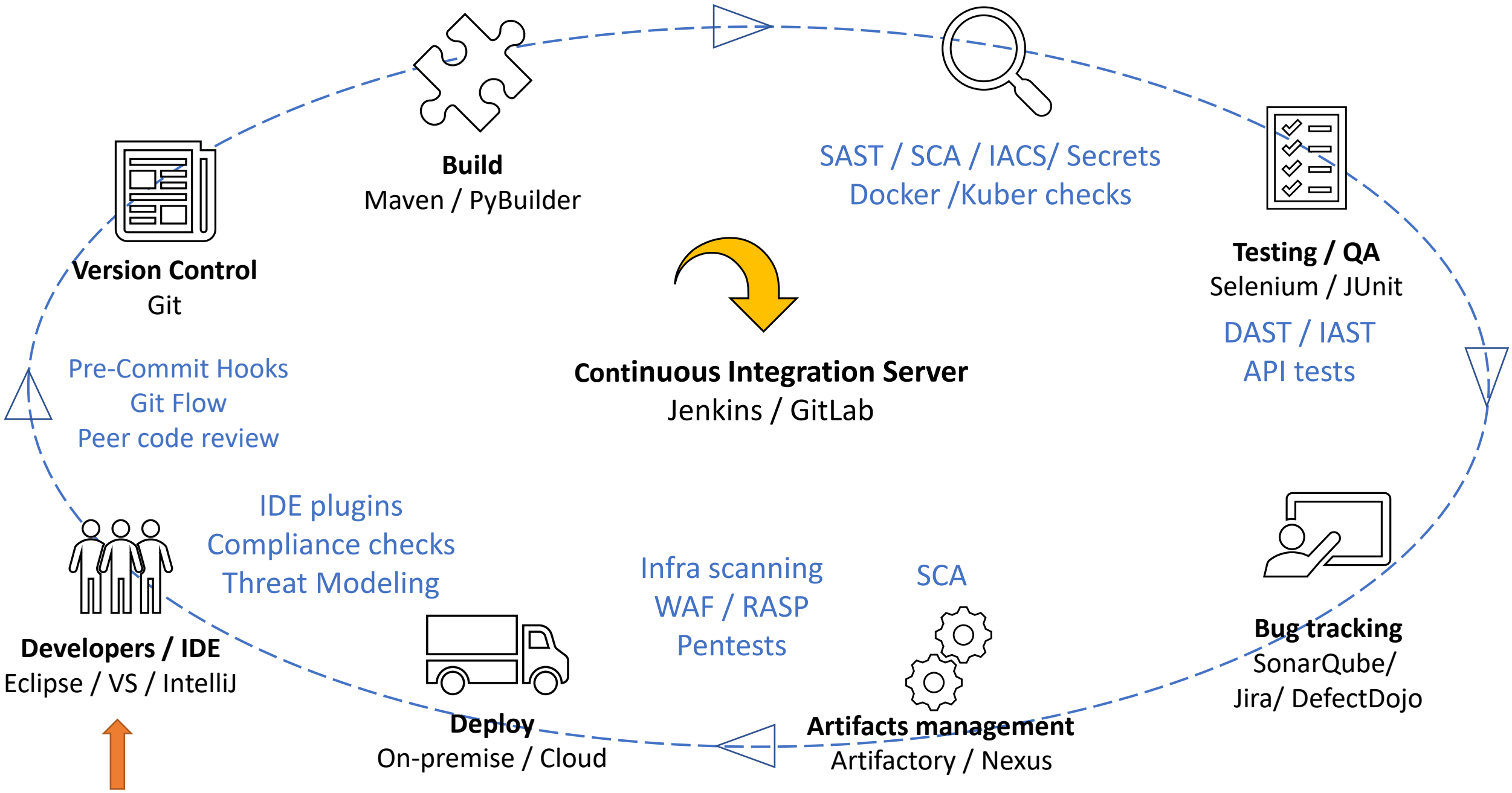
Showing entries 1 to 25 of 1450

1 2 3 4 5 6 7 8 9

Bulk Edit

Column visibility | Copy | PDF | Print

Severity	Name	CWE	Vulnerability Id	Date	Age	SLA	Reporter	Found By	Status
Critical	com.scalesec:vulnado@0.0.1-SNAPSHOT: Remote Code Execution target_file:pom.xml upgrade_to:org.springframework.boot:spring-boot-starter-web@2.6.13	94	CVE-2022-22965	Jan. 25, 2023	244	237	Admin User (admin)	Snyk Scan	Active, Verified
High	com.scalesec:vulnado@0.0.1-SNAPSHOT: Denial of Service (DoS) target_file:pom.xml upgrade_to:org.jsoup:jsoup@1.15.3	835	CVE-2021-37714	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified
High	Object Deserialization Is Used in {1}	502		Jan. 25, 2023	244	214	Admin User (admin)	SpotBugs Scan	Active, Verified
High	MD2, MD4 and MD5 Are Weak Hash Functions	328		Jan. 25, 2023	244	214	Admin User (admin)	SpotBugs Scan	Active, Verified
High	com.scalesec:vulnado@0.0.1-SNAPSHOT: Remote Code Execution ... target_file:pom.xml upgrade_to:org.postgresql:postgresql@42.3.3	94	CVE-2022-21724	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified
High	com.scalesec:vulnado@0.0.1-SNAPSHOT: Arbitrary Code Injecti... target_file:pom.xml upgrade_to:org.postgresql:postgresql@42.3.3	94	CVE-2022-26520	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified
High	com.scalesec:vulnado@0.0.1-SNAPSHOT: SQL Injection target_file:pom.xml upgrade_to:org.postgresql:postgresql@42.3.3	89	CVE-2022-31197	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified


Build
Maven / PyBuilder
SAST / SCA / IACS/ Secrets
Docker /Kuber checks
Testing / QA
Selenium / JUnit
DAST / IAST
API tests
Version Control
Git
Pre-Commit Hooks
Git Flow
Peer code review
Continuous Integration Server
Jenkins / GitLab
IDE plugins
Compliance checks
Threat Modeling
Developers / IDE
Eclipse / VS / IntelliJ
Infra scanning
WAF / RASP
Pentests
Deploy
On-premise / Cloud
SCA
Artifacts management
Artifactory / Nexus
Bug tracking
SonarQube/
Jira/ DefectDojo

This is just a beginning …

- Tools are just one piece of DevSecOps puzzle, will not help without clearly set vulnerability / risk management processes, requirements and metrics.
- Good vulnerability management system is the key for successful tracking and remediation.
- Scanners / rules need to be maintained and optimized, prefer flexible solutions to black boxes, write own rules.
- Scanners are not good for identifying business logic vulnerabilities.
- Requires AppSec skills and knowledge, do not expect IT to self manage this.

The Labs

- No prior knowledge is required, just follow the DevSecOps-with-OpenSource-workbook.pdf
- Download link: **http://bit.ly/3RqD6Tl**
- 2 VMWare VMs
  - ScanSuite + Scanners + DefectDojo + GitLab Worker
  - GitLab
- 2 vulnerable code repos
- For DAST target your GitLab host
- upgrade-scansuite.sh for Lab 4

Sergey Egorov

STR295ER