

A high-angle, wide shot of a modern automotive manufacturing plant. In the center, a silver car chassis is positioned on a conveyor belt. Several red KUKA industrial robotic arms are visible, some with black and yellow accents, working on the chassis. The background shows a complex network of metal frames, pipes, and other industrial equipment, all illuminated by bright overhead lights. The overall scene conveys a sense of precision and automation in manufacturing.

# 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
- Triage and track findings, push them to IT bug tracking
- On-prem, no cloud code submissions or findings exposure
- Scale with the number of scans required (ad-hoc vs CI/CD)
- Reasonable price, but effective analysis

# Application scanners

## Static Application Security Testing (SAST):

- Semgrep (+ GitLab edition)
  - CodeQL
  - Snyk
- + Language specific (FindSecBugs, Sec Code Scan, Bandit etc.)

## Software Composition Analysis (SCA):

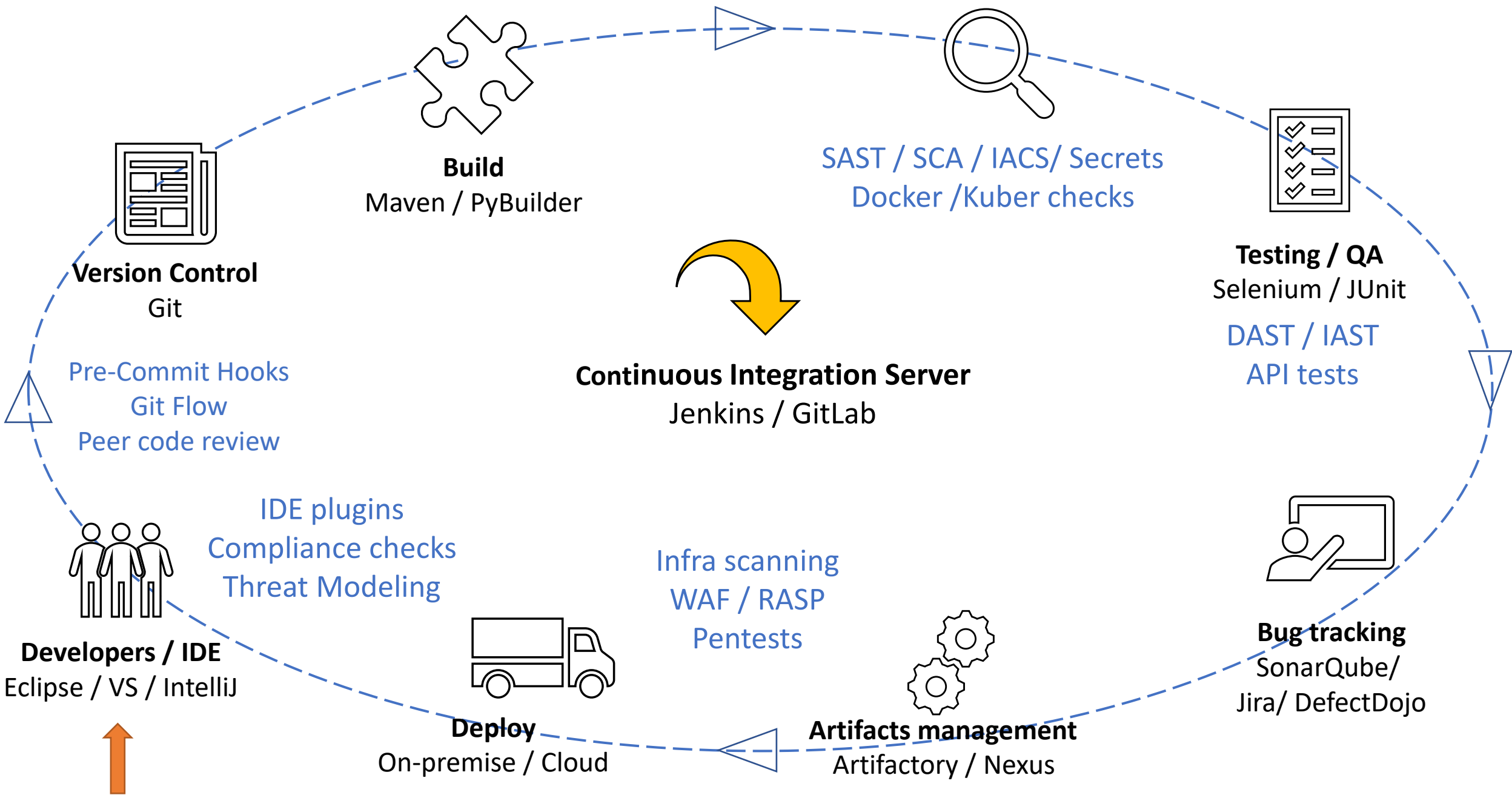
- Trivy
- OWASP Dependency Check
- Snyk

## Dynamic Application Security Testing (DAST):

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





# 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
- Not open sourced, could be used for non-commercial purposes

## 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
```

## Upload the source code



Choose a ZIP file...

No file uploaded

### Main Language

python

☒ Semgrep SAST☐ Semgrep with GitLab rules☒ GitLeaks Secrets Scan☒ CodeQL SAST☐ Snyk SAST☒ Trivy Dependency Check☐ Snyk Dependency Check☐ KICS Infra as Code Scan

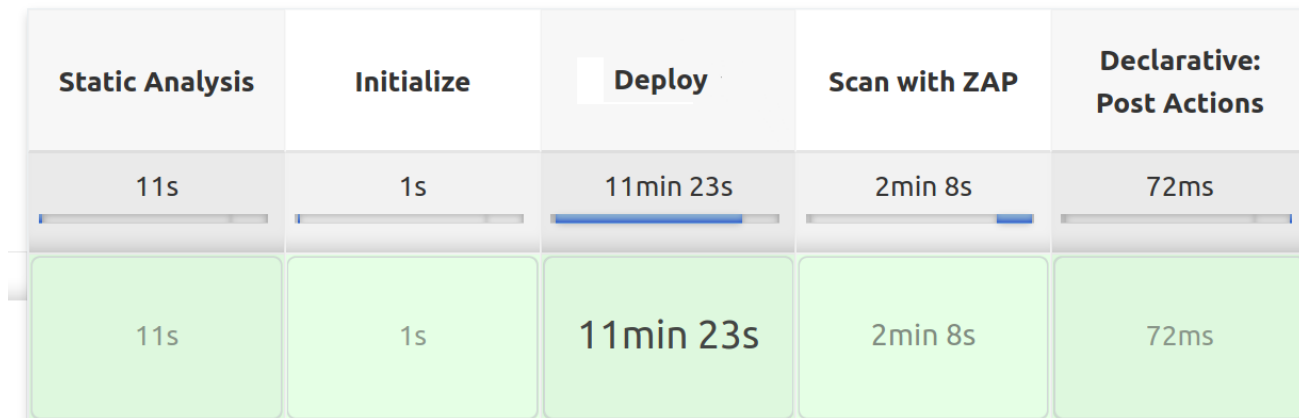
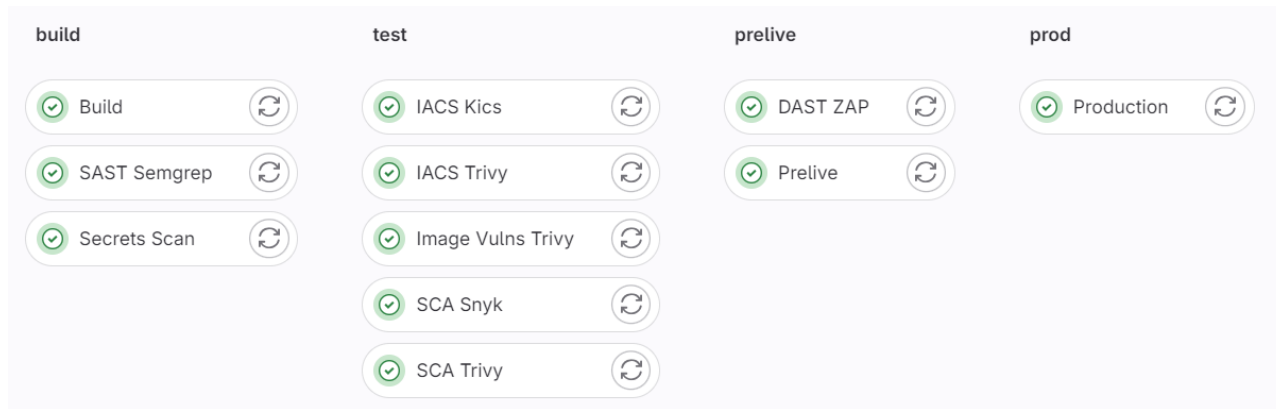
### Engagement ID

123

Upload



# CI/CD pipeline integration



```
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":"GitLab
33 a":false,"test":54}
34 Cleaning up file based variables
36 Job succeeded
```



OverviewComponentsMetricsEngagements1Findings448

Description

Vulnado

Metrics

29CRITICAL

146HIGH

222MEDIUM



JiraYour work▼Projects▼Filters▼Dashboards▼People▼Apps▼Create

Java VulnadoSoftware project

Back to project

Filters

All issuesMy open issuesReported by meOpen issuesDone issuesViewed recentlyResolved recentlyUpdated recently

Projects / Java Vulnado

Issues

Search issuesProject: Java VulnadoTypeStatusAssigneeMore+Save filter

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

Give feedback



Open Findings											
Showing entries 1 to 25 of 1450											
Bulk Edit✎✖											
Column visibilityCopyPDFPrint											
<input checked="" type="checkbox"/>	Severity	Name	CWE	Vulnerability Id	Date	Age	SLA	Reporter	Found By	Status	G
<input checked="" type="checkbox"/>	Critical	com.scaleshsec:vulnado@0.0.1-SNAPSHOT: Remote Code Execution   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	
<input checked="" type="checkbox"/>	High	com.scaleshsec:vulnado@0.0.1-SNAPSHOT: Denial of Service (DoS)  upgrade_to org.jsoup:jsoup@1.15.3	835	CVE-2021-37714	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified	
<input checked="" type="checkbox"/>	High	Object Deserialization Is Used in {1}	502		Jan. 25, 2023	244	214	Admin User (admin)	SpotBugs Scan	Active, Verified	
<input checked="" type="checkbox"/>	High	MD2, MD4 and MD5 Are Weak Hash Functions	328		Jan. 25, 2023	244	214	Admin User (admin)	SpotBugs Scan	Active, Verified	
<input checked="" type="checkbox"/>	High	com.scaleshsec:vulnado@0.0.1-SNAPSHOT: Remote Code Execution   upgrade_to org.postgresql:postgresql@42.3.3	94	CVE-2022-21724	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified	
<input checked="" type="checkbox"/>	High	com.scaleshsec:vulnado@0.0.1-SNAPSHOT: Arbitrary Code Injection   upgrade_to org.postgresql:postgresql@42.3.3	94	CVE-2022-26520	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified	
<input checked="" type="checkbox"/>	High	com.scaleshsec:vulnado@0.0.1-SNAPSHOT: SQL Injection   upgrade_to org.postgresql:postgresql@42.3.3	89	CVE-2022-31197	Jan. 25, 2023	244	214	Admin User (admin)	Snyk Scan	Active, Verified	

- Good vulnerability management system is the key for successful tracking and remediation
- Scanners / rules need to be maintained and optimized
- Scanners are not good for identifying business logic vulnerabilities
- Vulnerability management requires solid AppSec / DevSecOps skills and knowledge, do not expect IT to self manage this
- Tools are just one piece of DevSecOps puzzle, will not help without clearly set processes, requirements, guidelines and checklists

## The Labs

- No prior knowledge is required, just follow the DevSecOps-with-OpenSource-workbook.pdf
- Download link: <http://bit.ly/3RqD6TI>
- 2 VMWare VMs
  - ScanSuite + Scanners + DefectDojo + GitLab Worker
  - GitLab
- 2 vulnerable code repos
- upgrade-scansuite.sh for Lab 4

Sergey Egorov  
STR295ER