Security Vulnerability Management:

OWASP DefectDojo

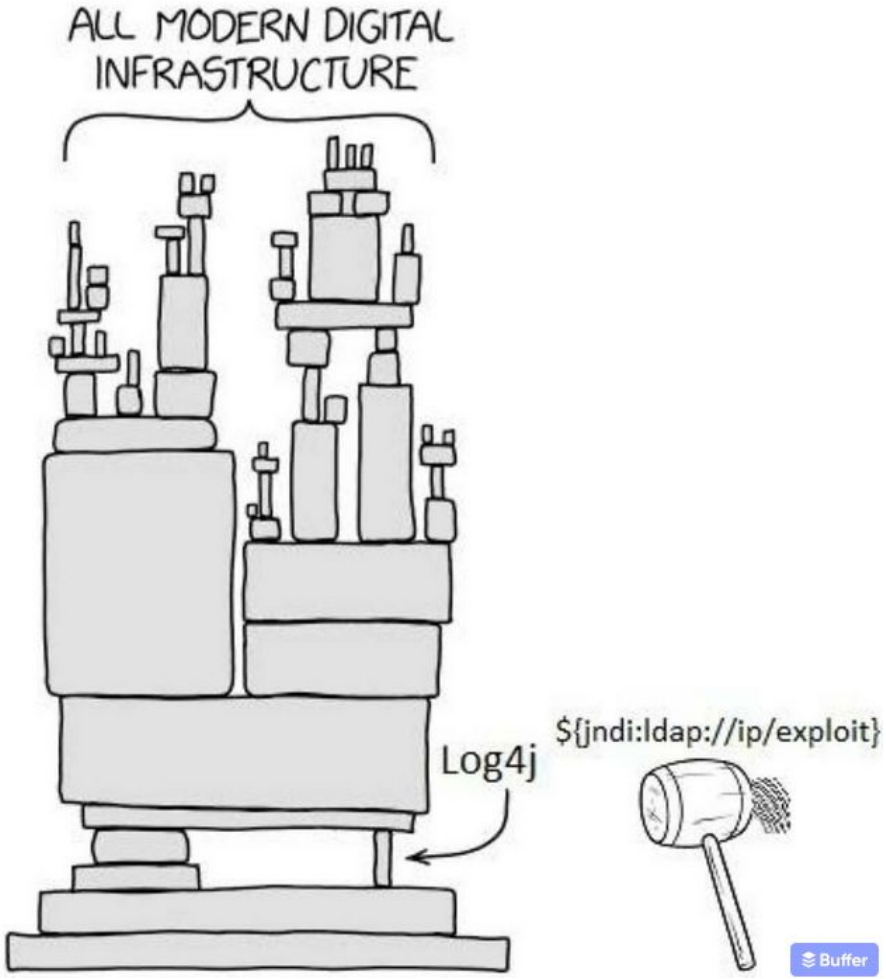
🥨 Augsburg 🥨 @Hackerkiste, 24.10.2025

Michael Wager

Intro

> Some of us stopped sleeping. We all felt that either we fix it right now in the next few days, or we close this project.
>
> – Christian Grobmeier

[Read the story behind Log2Shell]



About me

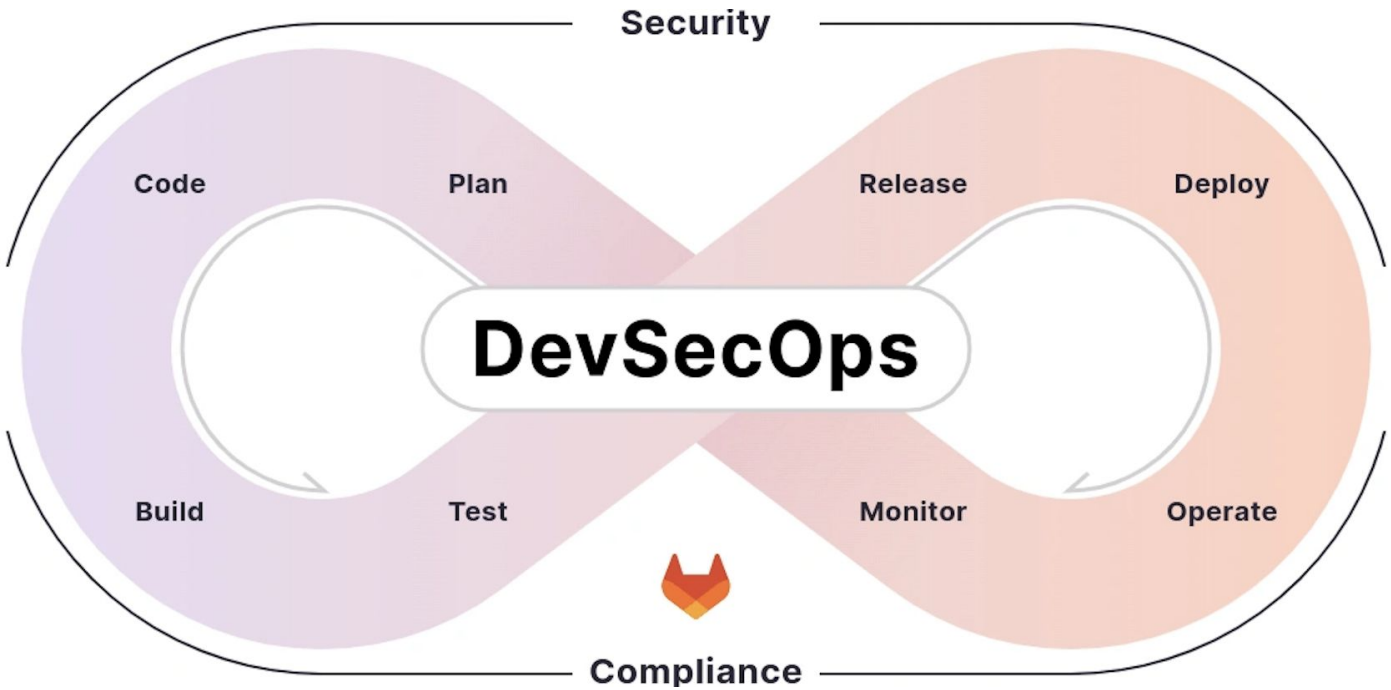
- Born in Augsburg 🥨 👍🏻, living in Nürnberg🥨 👎🏻
- Bachelor 2011 & Master 2024 at TH Augsburg
- Software Engineer for 10 years (freelance)
- AppSec Consultant at secureIO (May 2022- Sep 2025)
- Since October 2025:

  Senior Professional Services Engineer @ GitLab
- Website: https://mwager.de/

Agenda

- Intro: SSDLC, AppSec-Programs, Regulations & DevSecOps
- Why Vulnerability Management?
- What is OWASP DefectDojo?
- Demo
- Architecture & Challenges

The Problem: Scanner Overload



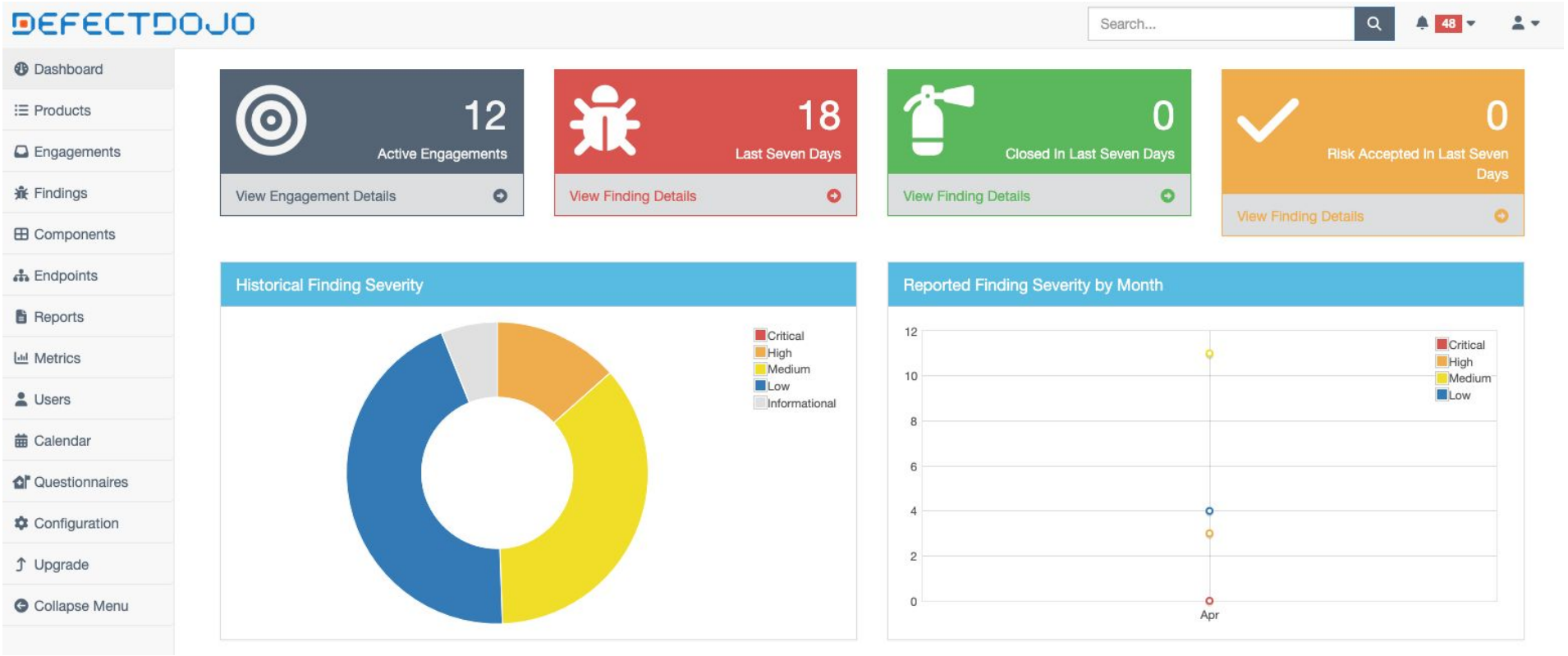
GitLab: What is DevSecOps?

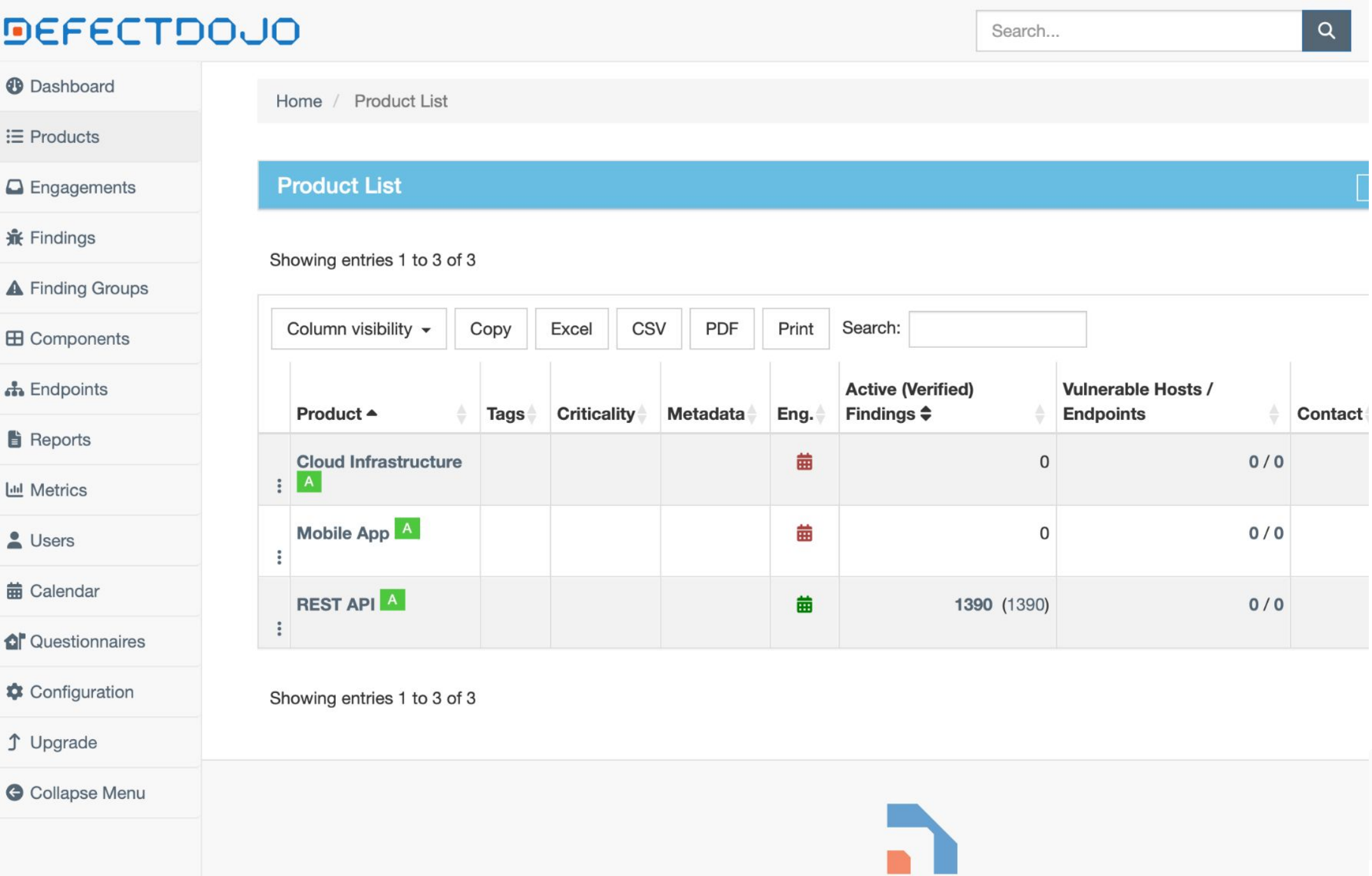
OWASP DefectDojo

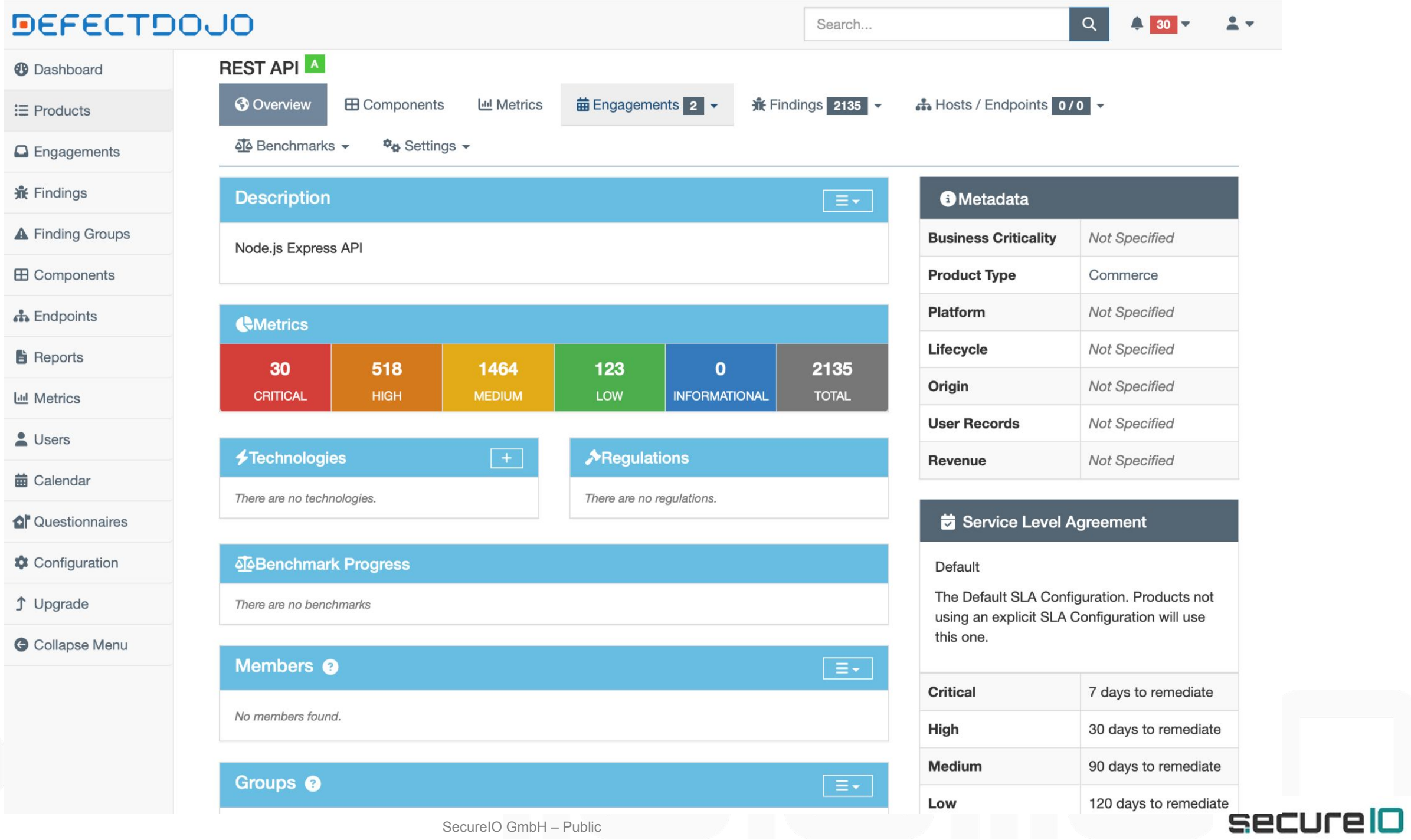
- OWASP
  - *Open Web Application Security Project*
  - OWASP Top 10 (E.g. Injection, supply chain, Broken Access control, etc)
  - But there is more! Tools, Projects, Standards, Chapters (e.g. OWASP Augsburg Stammtisch)
  - Community-driven & free
- DefectDojo
  - Open-source vulnerability management tool by OWASP (“ASPM” -> application security posture management)
  - Central platform to track, deduplicate, and triage findings across multiple applications, teams, and scan types
  - Supports automation, reporting, and integrations (Jira, CI/CD, API) to streamline AppSec programs

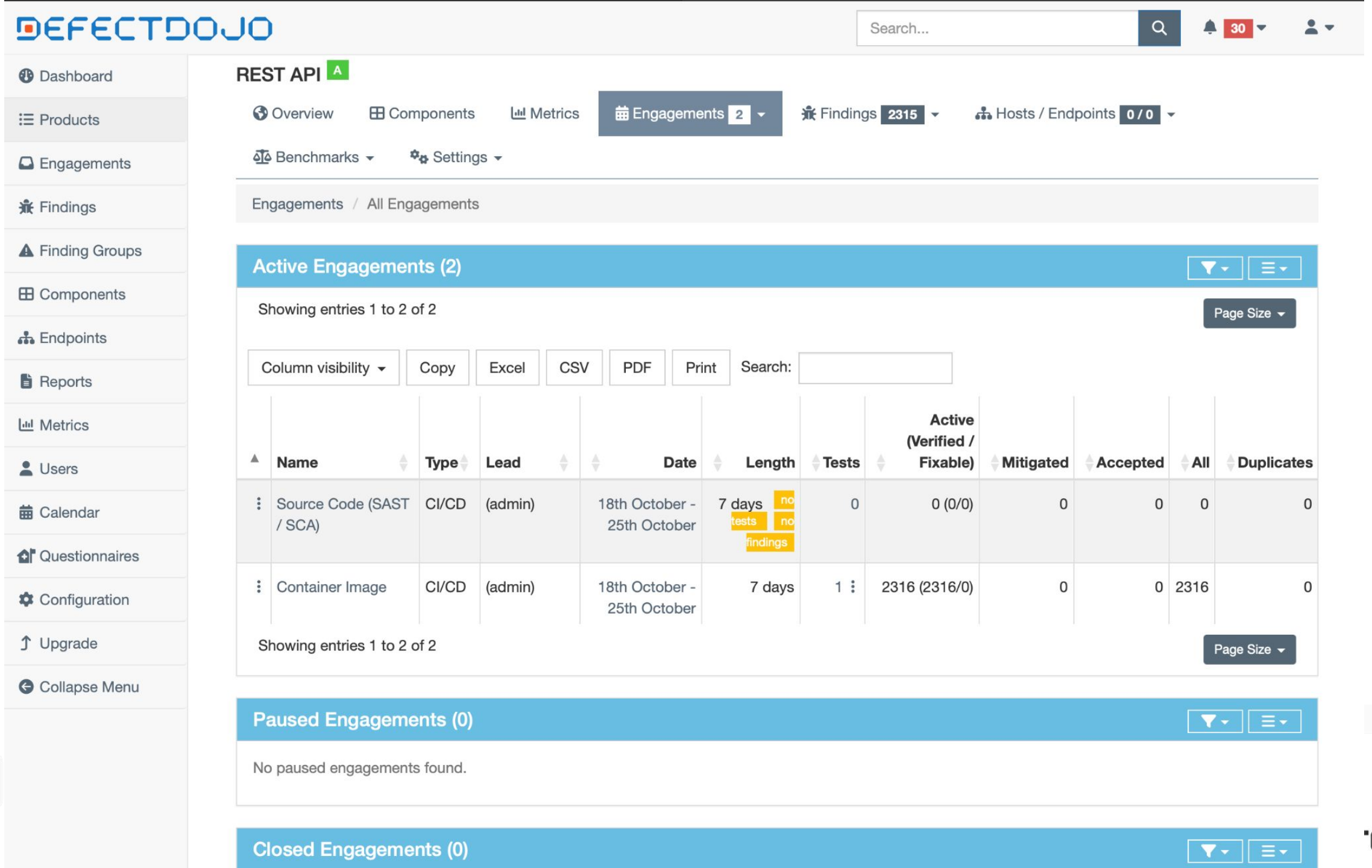
Demo

https://demo.defectdojo.org/ -> Log in with admin / 1Defectdojo@demo#appsec




DEFECTDOJO
Search...
Dashboard
Products
Engagements
Findings
Finding Groups
Components
Endpoints
Reports
Metrics
Users
Calendar
Questionnaires
Configuration
Upgrade
Collapse Menu
Home / Product List
Product List
Showing entries 1 to 3 of 3
Column visibility
Copy
Excel
CSV
PDF
Print
Search:
Product
Tags
Criticality
Metadata
Eng.
Active (Verified) Findings
Vulnerable Hosts / Endpoints
Contact
Cloud Infrastructure A 0 0 / 0
Mobile App A 0 0 / 0
REST API A 1390 (1390) 0 / 0
Showing entries 1 to 3 of 3


DEFECTDOJO
Search...
30
Dashboard
Products
Engagements
Findings
Finding Groups
Components
Endpoints
Reports
Metrics
Users
Calendar
Questionnaires
Configuration
Upgrade
Collapse Menu
REST API
A
Overview
Components
Metrics
Engagements 2
Findings 2135
Hosts / Endpoints 0 / 0
Benchmarks
Settings
Description
Node.js Express API
Metrics
30 CRITICAL
518 HIGH
1464 MEDIUM
123 LOW
0 INFORMATIONAL
2135 TOTAL
Technologies
There are no technologies.
Regulations
There are no regulations.
Benchmark Progress
There are no benchmarks
Members
No members found.
Groups
Metadata
Business Criticality Not Specified
Product Type Commerce
Platform Not Specified
Lifecycle Not Specified
Origin Not Specified
User Records Not Specified
Revenue Not Specified
Service Level Agreement
Default
The Default SLA Configuration. Products not using an explicit SLA Configuration will use this one.
Critical 7 days to remediate
High 30 days to remediate
Medium 90 days to remediate
Low 120 days to remediate


DEFECTDOJO
Search...
30
Dashboard
Products
Engagements
Findings
Finding Groups
Components
Endpoints
Reports
Metrics
Users
Calendar
Questionnaires
Configuration
Upgrade
Collapse Menu
REST API
A
Overview
Components
Metrics
Engagements 2
Findings 2315
Hosts / Endpoints 0 / 0
Benchmarks
Settings
Engagements / All Engagements
Active Engagements (2)
Showing entries 1 to 2 of 2
Page Size
Column visibility
Copy
Excel
CSV
PDF
Print
Search:
Name
Type
Lead
Date
Length
Tests
Active (Verified / Fixable)
Mitigated
Accepted
All
Duplicates
Source Code (SAST / SCA)
CI/CD
(admin)
18th October - 25th October
7 days
no tests
no findings
0
0 (0/0)
0
0
0
0
Container Image
CI/CD
(admin)
18th October - 25th October
7 days
1
2316 (2316/0)
0
0
2316
0
Showing entries 1 to 2 of 2
Page Size
Paused Engagements (0)
No paused engagements found.
Closed Engagements (0)

DEFECTDOJO

Search... 30

- Dashboard
- Products
- Engagements
- Findings
- Finding Groups
- Components
- Endpoints
- Reports
- Metrics
- Users
- Calendar
- Questionnaires
- Configuration
- Upgrade
- Collapse Menu

REST API A

Overview | Components | Metrics | Engagements 2 | Findings 2515 | Hosts / Endpoints 0 / 0 | Benchmarks | Settings

Engagements / Container Image / Trivy Scan (Trivy Scan) / Test

Trivy Scan (Trivy Scan) Updated 4 minutes ago, Created 4 minutes ago

Engagement	Environment	Dates	Updated	Fix Available	Version
Container Image	Test	Oct. 18, 2025 - Oct. 25, 2025	Oct. 18, 2025	0	None

Groups (0)

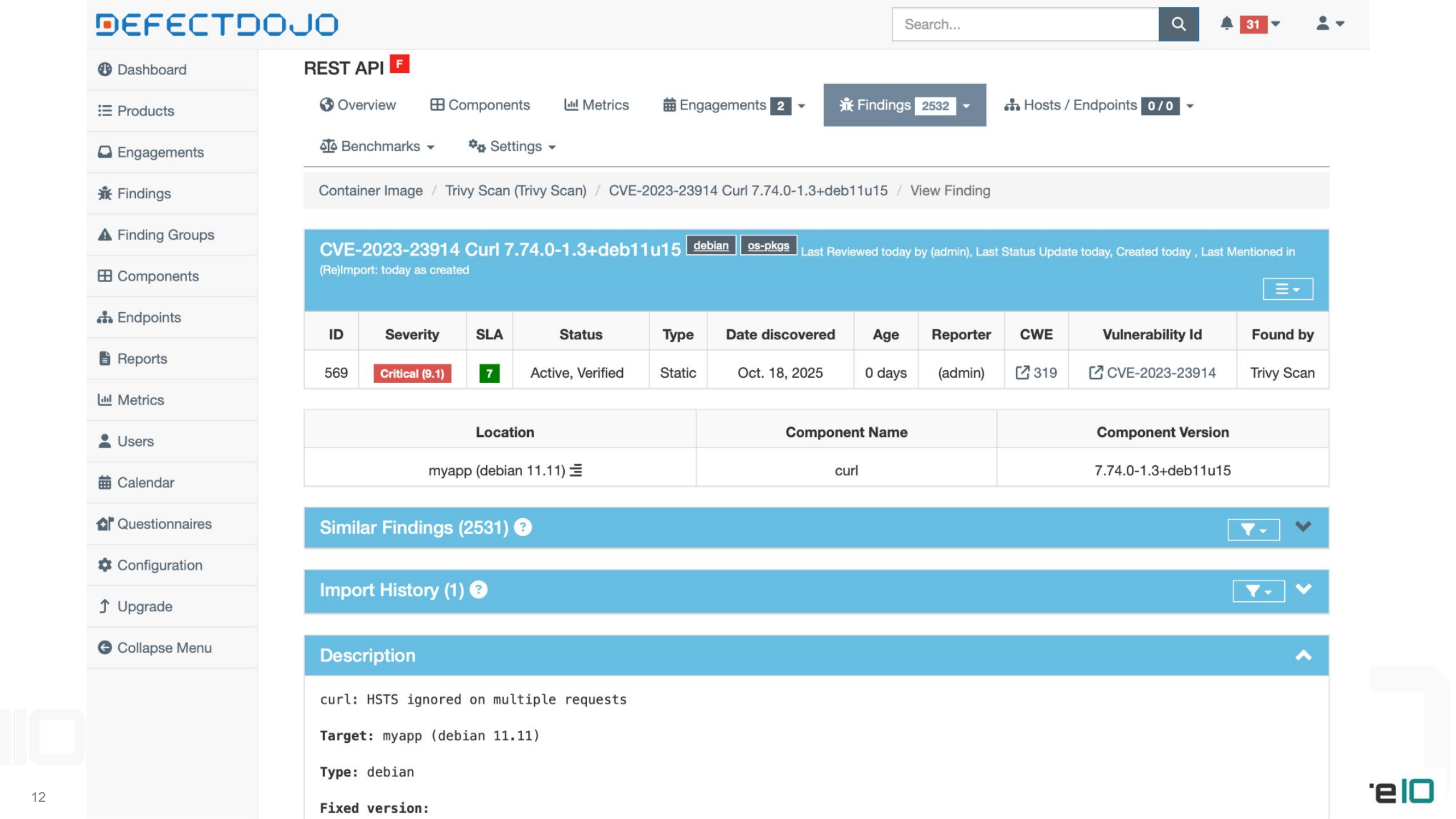
Findings (2515) Critical: 33, High: 545, Medium: 1775, Low: 162, Info: 1, Total: 2516 Findings

Showing entries 1 to 25 of 2515

1 2 3 4 5 6 7 8 9 10 ... 101 Next Page Size

Column visibility | Copy | Excel | CSV | PDF | Print | Search:

Severity	Name	CWE	Vulnerability Id	EPSS Score	EPSS Percentile	Date	Age	SLA	Reporter	Stat
Critical	CVE-2023-23914 Curl 7.74.0-1.3+deb11u15 debian os-pkgs	319	CVE-2023-23914	N.A.	N.A.	Oct. 18, 2025	0	7	(admin)	Activ
Critical	CVE-2023-34152 Imagemagick 8:6.9.11.60+dfsg-	20	CVE-2023-34152	N.A.	N.A.	Oct. 18, 2025	0	7	(admin)	Activ


DEFECTDOJO
Search...
31
Dashboard
Products
Engagements
Findings
Finding Groups
Components
Endpoints
Reports
Metrics
Users
Calendar
Questionnaires
Configuration
Upgrade
Collapse Menu
REST API
F
Overview
Components
Metrics
Engagements 2
Findings 2532
Hosts / Endpoints 0 / 0
Benchmarks
Settings
Container Image / Trivy Scan (Trivy Scan) / CVE-2023-23914 Curl 7.74.0-1.3+deb11u15 / View Finding
CVE-2023-23914 Curl 7.74.0-1.3+deb11u15
debian
os-pkgs
Last Reviewed today by (admin), Last Status Update today, Created today , Last Mentioned in
(Re)Import: today as created
ID
Severity
SLA
Status
Type
Date discovered
Age
Reporter
CWE
Vulnerability Id
Found by
569
Critical (9.1)
7
Active, Verified
Static
Oct. 18, 2025
0 days
(admin)
319
CVE-2023-23914
Trivy Scan
Location
Component Name
Component Version
myapp (debian 11.11)
curl
7.74.0-1.3+deb11u15
Similar Findings (2531)
Import History (1)
Description
curl: HSTS ignored on multiple requests
Target: myapp (debian 11.11)
Type: debian
Fixed version:

DefectDojo API v2

2.51.1 OAS 3.0

/api/v2/oa3/schema/?format=json

DefectDojo - Open Source vulnerability Management made easy. Prefetch related parameters/responses not yet in the schema.

Authorize

findings

GET /api/v2/findings/

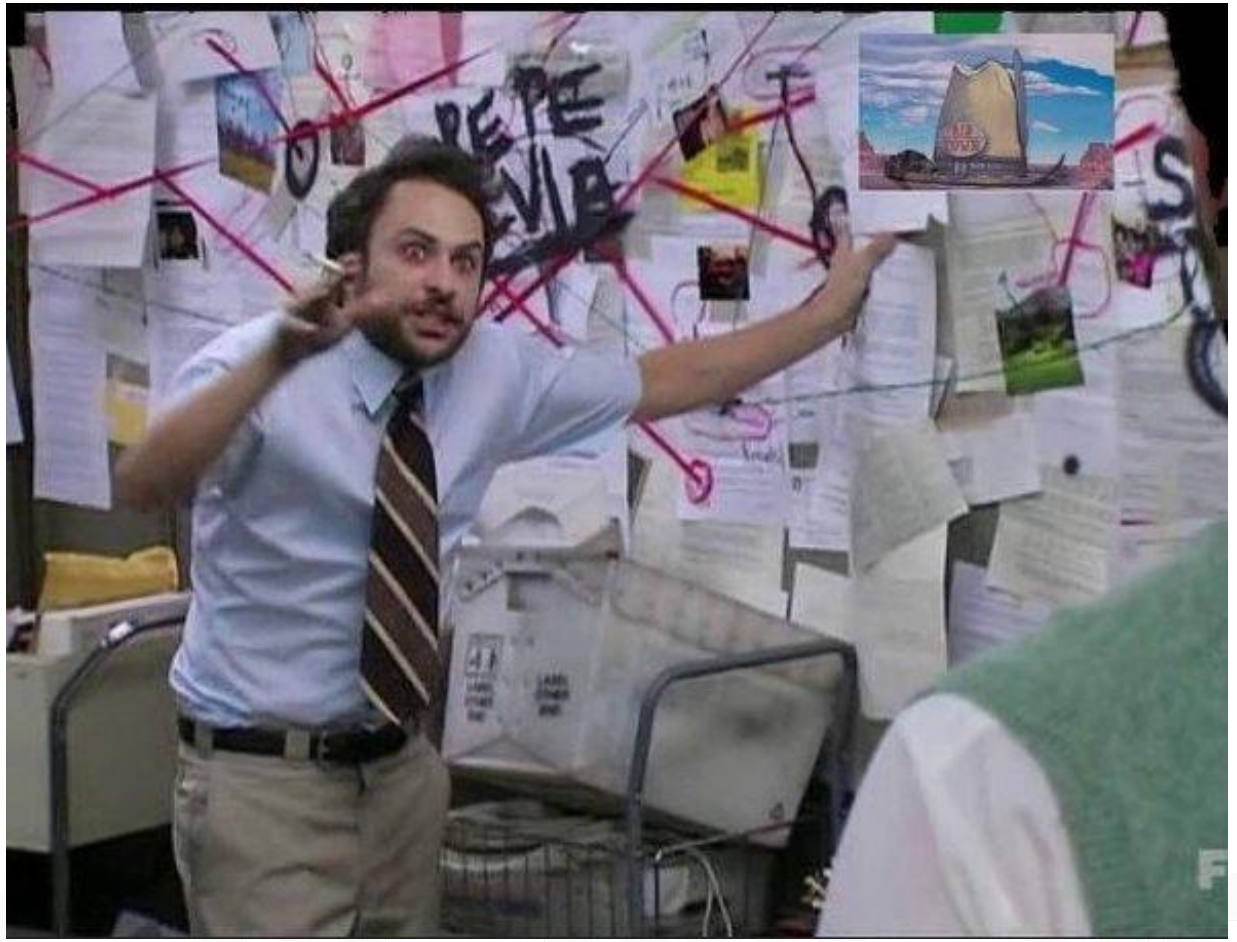
Parameters

Try it out

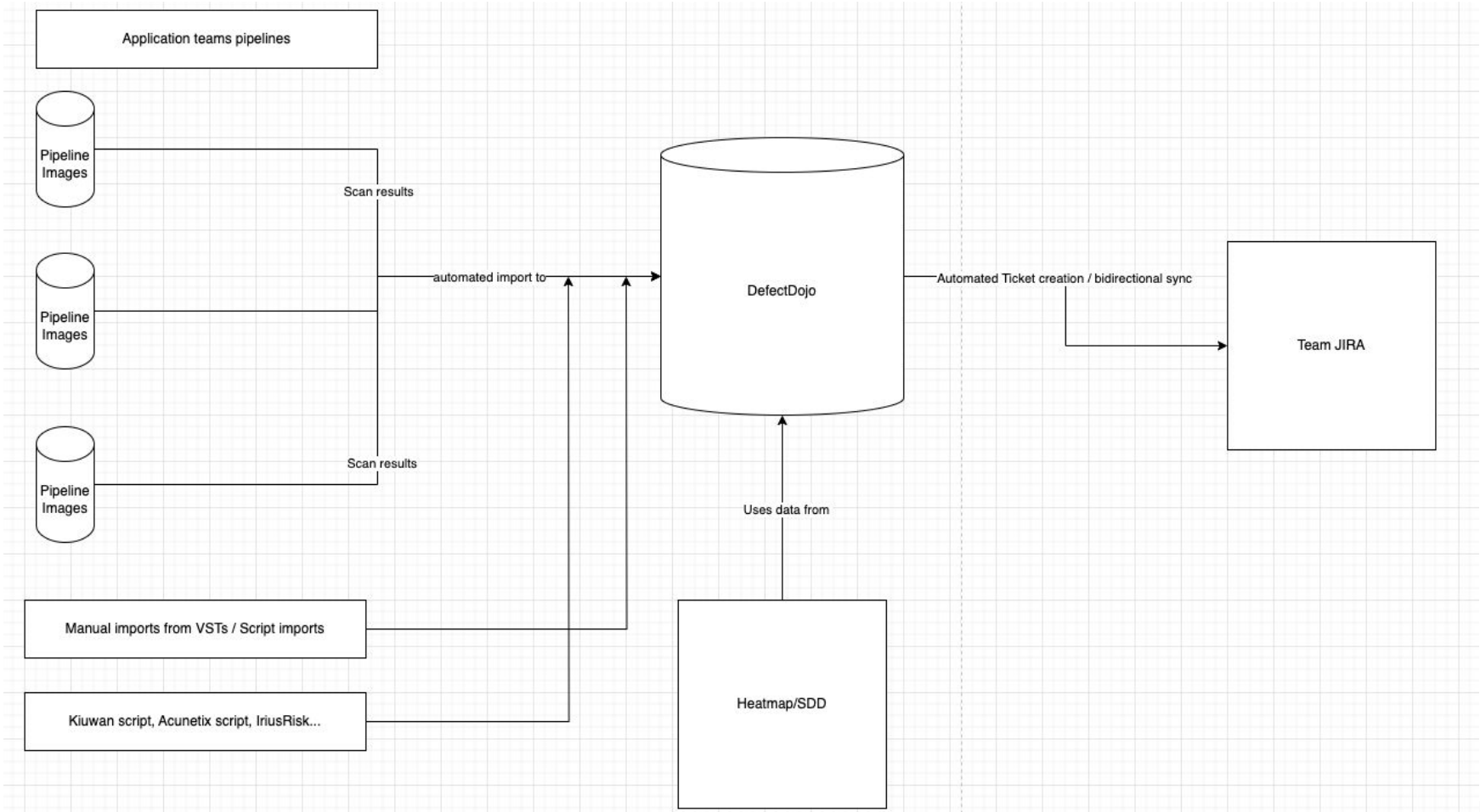
Name	Description
active **boolean** *(query)*	--
component_name **string** *(query)*	component_name
component_version **string** *(query)*	component_version
created **string($date-time)** *(query)*	The date the finding was created inside DefectDojo. • None - Any date • 1 - Today • 2 - Past 7 days • 3 - Past 30 days • 4 - Past 90 days • 5 - Current month • 6 - Current year • 7 - Past year

Vulnerability Management Architecture

- Centralized Management with DefectDojo
- Standardization of Scanning in CI/CD Pipelines
- Automation of Ticket Creation

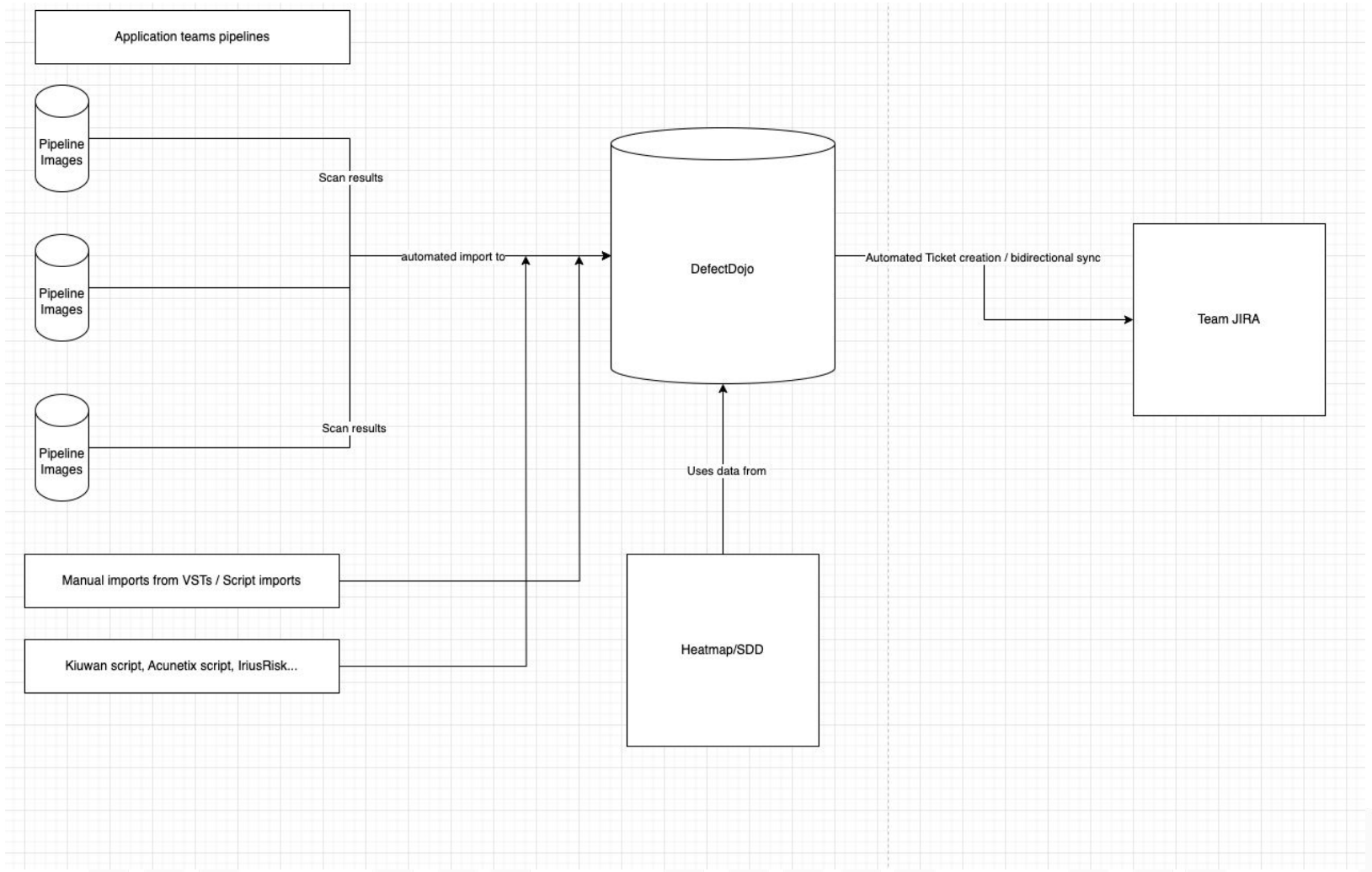


Vulnerability Management Architecture



Challenges we faced

- Maintenance of scan tools
- Maintenance of DefectDojo (Upgrades, DB Migration)
- False Positives and JIRA Spam



Discussion

Connect?

LinkedIn

https://mwager.de

Support

secureIO GmbH - > secure-io.de

GitLab AppSec -> about.gitlab.com