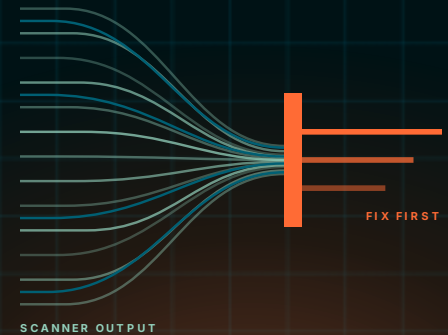


WHAT IS DEFECTDOJO

Every security finding in one place, **ranked by real risk.**

DefectDojo is the open source unified vulnerability management platform that remediates at the speed of AI, enabling security teams to focus on fixing the most critical vulnerabilities first. Parse any security finding, aggregate across your stack, prioritize what matters, and report on your security posture and compliance.



500+

INTEGRATIONS IN
DEFECTDOJO PRO

360+

PARSERS IN
COMMUNITY EDITION

3

WAYS TO DEPLOY PRO,
INCLUDING AIR-GAPPED

OWASP

FLAGSHIP PROJECT, OPEN
SOURCE SINCE 2014

THE PROBLEM

Your scanners don't agree with each other.

SAST, SCA, container, DAST, and cloud scanners each report in their own format, on their own severity scale. The same vulnerability shows up three times under three names. Nobody can say how many findings are actually open, or which of them attackers are exploiting right now.

WHAT DEFECTDOJO DOES

One system of action on top of every tool.

DefectDojo ingests the output of the tools you already run, collapses the duplicates, adds threat intelligence and business context, and sends what's left to the people who fix it. Findings follow the structure of your organization, and every metric, SLA, and Jira project hangs off it:

[Organization](#) > [Asset](#) > [Engagement](#) > [Test](#) > [Finding](#)

HOW IT WORKS From raw scan output to a merged fix

01

AGGREGATE

Import scan results through parsers, the REST API, or your CI/CD pipeline. DefectDojo Pro adds connectors that sync with your tools on a schedule.

02

DISTILL

Deduplication tracks each vulnerability once, with its full history. Reimporting a scan closes the findings that no longer appear.

03

ENRICH

DefectDojo Pro adds daily EPSS scores and CISA KEV status to findings with a CVE, weighed against each Asset's business criticality.

04

REMEDiate

Route findings to Jira, hold teams to SLAs, and track mean time to remediate. Sensei opens the pull request that fixes the code.

SECURITY ENGINEERS

Stop reformatting scanner output by hand. Import from CI/CD, triage a finding once, and let deduplication handle the repeats.

APPSEC LEADERS

Track open findings, SLA compliance, and mean time to remediate for every Asset, and show leadership the trend over time.

PEN TESTERS

Run each assessment as an Engagement, log manual findings next to scanner results, and build the report from the same data.

COMPLIANCE

Report on security posture and compliance across frameworks including SOC 2, PCI-DSS, and the EU Cyber Resilience Act.



CAPABILITIES What the platform does

Import from any tool

Parsers for the scanners teams already run, plus the REST API and CI/CD imports. Pro adds Upstream Connectors, background imports, and a Universal Parser that turns any JSON or CSV file into findings.

Deduplication

Matches repeat findings from the same tool within each Asset. Pro adds tuning for same-tool, cross-tool, and reimport matching, so an issue two scanners report can be worked as one finding.

Priority and Risk

PRO

Every active finding gets a calculated Priority and Risk based on EPSS, CISA KEV, and the Asset's business criticality and exposure. Set SLAs by severity or by Risk.

Triage Engine

PRO

Build no-code rules that apply bulk actions to findings and other objects, then run them on a schedule. Preview a rule against your real data before it changes anything.

Issue tracking

Jira integration in both editions. Pro adds Downstream Connectors for Azure DevOps, GitHub, GitLab, ServiceNow, Bitbucket, PagerDuty, Zendesk, and more.

Metrics and reporting

Per-Asset metrics for open findings, SLA compliance, and mean time to remediate. Pro adds custom dashboards, executive reporting, and MCP support so your AI client can query findings.

SENSEI

From finding to pull request, without leaving DefectDojo.

Sensei is DefectDojo's AI. It scans your repositories, brings the results in as findings, and opens pull requests that fix them. Every fix is a preview first, and nothing runs until you approve it.

Sensei is available to DefectDojo Pro customers.

EDITIONS Two editions, one data model

Community Edition

FREE

The OWASP Flagship project, built in the open on GitHub.

- Self-hosted and BSD-3 licensed
- 360+ parsers, a full REST API, and CI/CD imports
- Deduplication, SLA configuration, and per-Asset metrics
- Jira integration
- Community support on GitHub and Slack

DefectDojo Pro

CONTACT US

Everything in Community Edition, optimized for scale.

- 500+ integrations, including API connectors
- Priority and Risk with daily EPSS and CISA KEV enrichment
- Triage Engine and deduplication tuning
- SSO (SAML, OIDC, OAuth), LDAP, MFA, and RBAC
- Cloud or self-hosted, including air-gapped
- Commercial support with SLAs

MANAGED APPSEC Want it run for you? DefectDojo Managed AppSec pairs Sensei with hands-on supervision from our security team.

DEPLOY

Pro runs on DefectDojo Cloud, or self-hosted on Kubernetes, Docker Compose, or OpenShift.

INTEGRATE

REST API v2 with an OpenAPI spec. Pro CLI tools run on Windows, macOS, and Linux.

HARDEN

FIPS 140-3 mode and forward HTTPS proxy support for self-hosted Pro.

EXPORT

SBOM, VEX, and AIBOM export from DefectDojo Pro.

See your own findings
in DefectDojo.

Start a DefectDojo Pro
trial
defectdojo.com

Run Community
Edition
[github.com/DefectDojo/
django-DefectDojo](https://github.com/DefectDojo/django-DefectDojo)

Read the docs
docs.defectdojo.com