DEFECTDOJO

Taking Control of Enterprise Vulnerability Management with DefectDojo

DEFECTDOJO.COM

Table of Contents

03 Executive Summary

04 Operating without a Centralized Vulnerability Management Platform

05 Centralizing with DefectDojo Open Source

06 Operating with a Centralized Vulnerability Management Platform like DefectDojo Pro

08 Strategic Prioritization with Environmental Context

09 Getting Started

Executive Summary

In today's complex business environment, enterprise security teams rely on a plethora of security findings from siloed tools to assess risk. Yet according to a SANS 2025 Survey, 69% of security teams surveyed still rely on manual or mostly manual processes to report metrics.

In 2026, manual vulnerability management is simply unsustainable, as the time to exploit vulnerabilities decreased from 63 days in 2018 to just 5 days now. To manage risk effectively, security teams need a centralized, automated vulnerability management platform, so they can focus on testing and remediation, instead of inefficient data collection.

This eBook explores three states of enterprise vulnerability management:

- Operating without a centralized vulnerability management platform.
- Operating with a centralized vulnerability management platform like DefectDojo Open Source that provides total visibility across your entire threat landscape.
- Operating with a centralized vulnerability management platform like DefectDojo Pro that automates remediation and reporting across your entire software development life cycle (SDLC).

Learn how centralized and automated vulnerability management will allow your teams to import, analyze, and report on risks across your SDLC — enabling you to reduce noise, focus on real risks, and scale security intelligently.

Operating without a Centralized Vulnerability Management Platform

OPERATING WITHOUT A CENTRALIZED VULNERABILITY MANAGEMENT PLATFORM CREATES A CHAOTIC ENVIRONMENT CHARACTERIZED BY THREE PRIMARY FAILURES:

Data duplication

Without a central tool, findings from SAST, SCA, DAST, and other scanners often overlap. For example, DAST may reveal a weakness already identified by an SCA scan, leading to duplicate findings that force developers to investigate the same issue multiple times.

Lack of focus on strategic testing

When a team is bogged down by manual results compilation and administrative overhead, they cannot focus on high-priority actionable vulnerabilities. According to Help Net Security, 57% of security teams dedicate 25–50% of their time to vulnerability management operations.

Manual processes

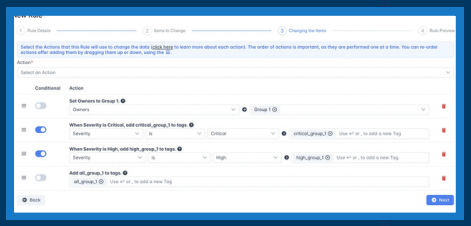
Before adopting automation, teams like global education company, Pearson, spent over 60% of their time on manual reports and metrics rather than actual security testing. This red tape and reliance on manual review limit an organization's ability to scale.

Centralizing with DefectDojo Open Source

DefectDojo Open Source serves as a unified vulnerability management platform that imports security data throughout the SDLC from nearly 200 different scanning tools. It provides a strong foundation to manage, analyze, and report on all security risks.

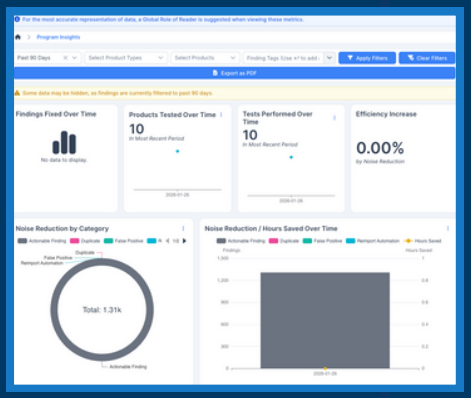
CUSTOMIZABLE API-DRIVEN AUTOMATION

Robust REST APIs and Swagger UI enable security teams to build customized automation workflows. Organizations like SAS use these APIs to create automated JIRA ticketing systems that deliver only verified, triaged findings to developers and auto-close tickets after remediation.



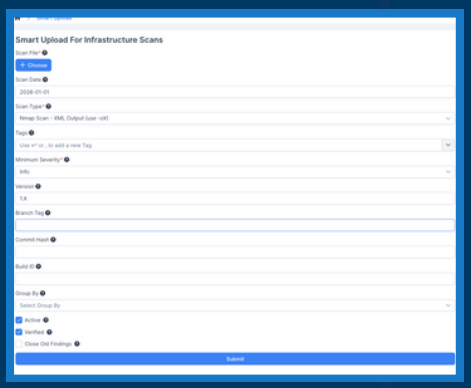
CORE REPORTING AND VISUALIZATION

The platform includes functional report builder capabilities and standard dashboards to track active engagements and historical severity — providing the essential metrics needed to manage a centralized vulnerability inventory.



STANDARDIZED DATA INGESTION

Findings are easily added via the UI or API, supporting 200+ tool parsers. Open Source acts as a versatile command center for data correlation and deduplication across the SDLC, while Pro further streamlines this with background processing and dedicated CLI tools.



Operating with a Centralized Vulnerability Management Platform like DefectDojo Pro

While the open source version of DefectDojo provides a powerful single pane of glass for vulnerability management, the Pro version is engineered to transform security from a manual bottleneck into a streamlined, high-velocity operation.

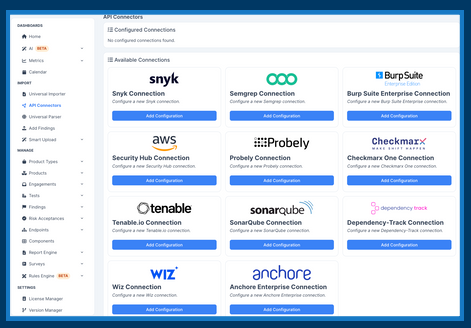
For organizations scaling their AppSec programs, the transition to Pro represents a shift from simply centralizing data to actively automating the entire security lifecycle.

Automated Data Ingestion & Workflow

To eliminate the manual effort of data entry and report merging, Pro offers advanced ingestion tools:

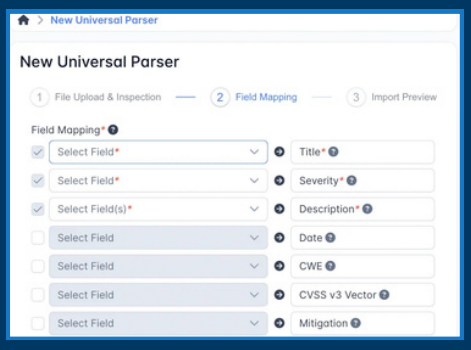
API CONNECTORS

Automated "out-of-the-box" pipelines that pull data from major enterprise tools like Snyk, Tenable, and SonarQube every 24 hours.



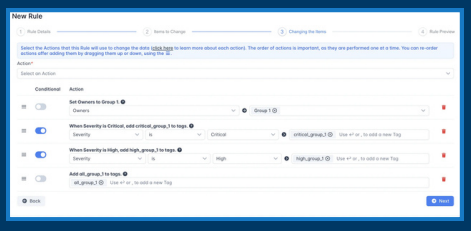
THE UNIVERSAL PARSER

Enables teams to import any JSON, CSV, or XML report, ensuring the platform remains resilient even if a vendor changes their export format.



RULES ENGINE

Allows for the creation of automated bulk actions — such as assigning reviewers or escalating high-risk findings — without requiring any programming experience.

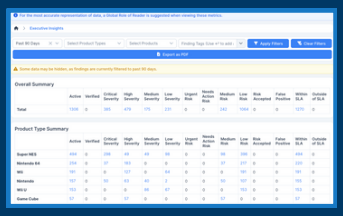


DEDUPLICATION TUNING

Provides fine-grained control to adjust how findings are matched across different tools, significantly reducing redundant work for developers.

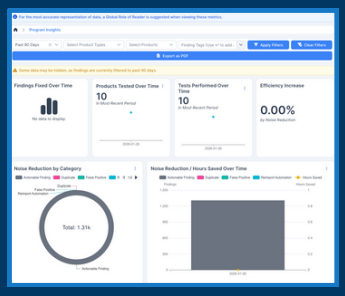
Enterprise-Grade Visibility & UX

The Pro version introduces an upgraded user interface specifically designed to easily showcase program metrics required in enterprise environments. Pro provides four distinct dashboards for various stakeholders:



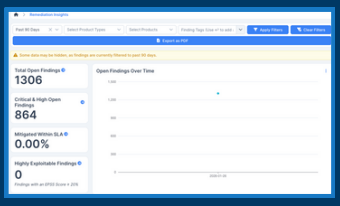
EXECUTIVE INSIGHTS

High-level metrics designed for management visibility and last-minute reporting.



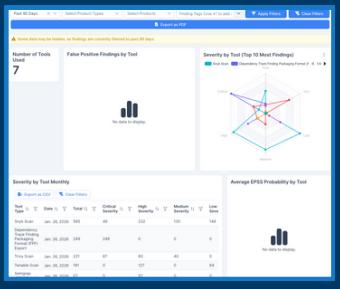
PROGRAM INSIGHTS

Quantifies the efficiency of the security program by tracking hours and cost savings gained through automation.



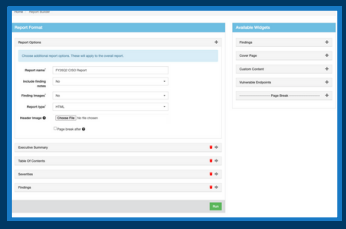
REMEDIATION INSIGHTS

Automates SLA tracking, helping teams monitor mitigation speed across different products.



TOOL INSIGHTS

Identifies the performance of security scanners, helping organizations manage "tool sprawl" by highlighting the most effective (and the noisiest) tools.



CUSTOMIZABLE REPORTING

All graphics can be exported as SVG files, and raw data can be exported as tables for external analysis.

CUSTOMER STORY SUMMARY

Pearson

By automating testing queues through CI/CD and using DefectDojo to centrally manage results, Pearson managed to scale their global testing coverage even as their security team decreased in size.

KEY RESULTS

- **840% increase** in number of security assessments performed.
- **60% reduction** in time spent on reporting.
- Dramatic improvement in resource efficiency.
- Company-wide coverage of security testing and standard enforcement, rather than just being able to protect the company crown jewels.

Strategic Prioritization with Environmental Context

Pro moves beyond standard severity scores to help teams fix what matters most.

EPSS INTEGRATION

Findings are automatically augmented with the Exploit Prediction Scoring System (EPSS) to prioritize vulnerabilities with the highest risk of real-world exploitation.

PRIORITY INSIGHTS

A customizable engine that calculates a finding's "true" priority by considering environmental factors such as business criticality, internet accessibility, and estimated revenue impact.

ENTERPRISE SUPPORT AND SECURITY

Upgrading to Pro ensures your infrastructure is backed by a dedicated support team, and includes unlimited tickets and seats, and a priority review process for feature requests.

For those on the SaaS platform, it includes comprehensive monitoring, maintenance, and backups, alongside support for enterprise authentication like Azure AD, GitHub, and GitLab.

Getting Started

MIGRATING FROM OPEN SOURCE TO PRO

To begin their transition to DefectDojo Pro, organizations can sign up for a free, full-featured 2-week trial, including the integration of 200+ security tools into a unified view.

Pro subscriptions include unlimited users and tool integrations, as well as priority support for troubleshooting and feature requests.

Organizations can move their existing data to a cloud-hosted environment that includes monitoring, maintenance, and backups.

CONCLUSION

Organizations can no longer rely on phased, manual testing cycles. Enterprise security requires continuous deployment where automated, pipeline-integrated scanning provides a holistic view of the organization's security posture.

DefectDojo Open Source is used by thousands of organizations worldwide, and has been downloaded more than 35 million times. It provides for centralized vulnerability management across your enterprise security landscape.

DefectDojo Pro automates remediation across your SDLC. Leveraging business criticality and exploit probability, Pro ensures teams fix the most dangerous risks first, rather than drowning in noisy data from tool sprawl.

DefectDojo Pro allows an organization to function as a security command center, enabling a culture where security enhances rather than impedes development velocity. In this rapidly evolving landscape, Pro provides the enterprise support, intelligence, and automation required to protect an enterprise organization at scale.

DEFECTDOJO

Visit our website for more information about Enterprise Vulnerability Management

DEFECTDOJO.COM