ZeroDay

ZeroDay Cloud-based AIAST Solution

By Alex

Agenda

ZeroDay

ZeroDay

01 About Zeroday Co.,Ltd

02 IAST & AIAST Overview

03 AIAST Features and Advantages

01

About ZeroDay Co.,Ltd

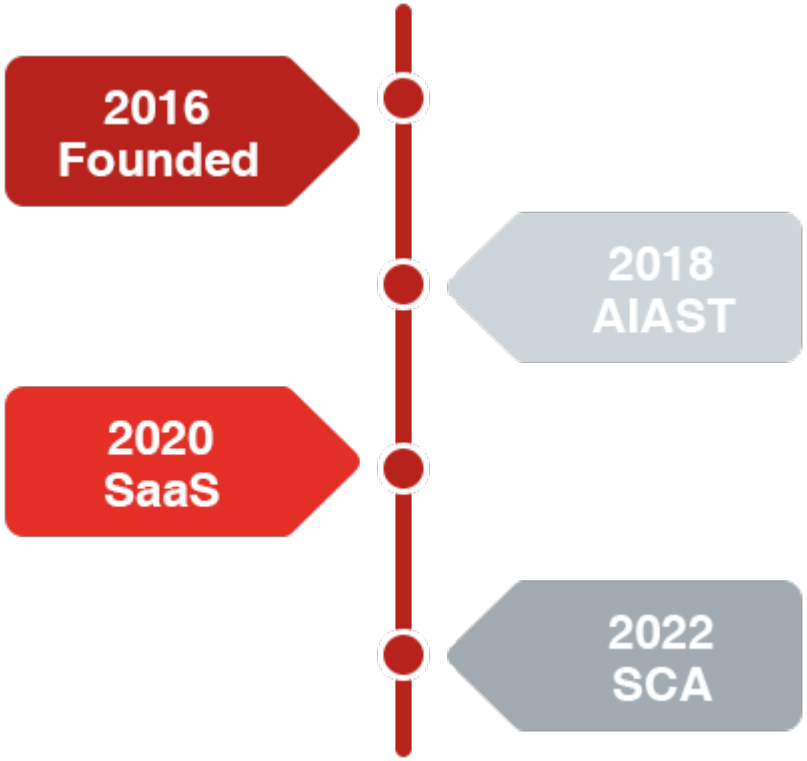
HQ in UK with international business

Headquartered in Manchester, U.K, ZeroDay has R&D offices and supporting centers in Canada, Singapore, and Hong Kong respectively, as well as representative offices and partners across the globe.

ZeroDay Strong team

With global vision from the start, our team embrace the variety of ethnics, background and expertise. Enterprising veterans from top IT companies as well as promising graduates from renowned colleges are the most valuable assets of our company, key to our cutting edge and innovative products.

ZeroDay History and Mission



Founded in 2016, ZeroDay aims to make software development more secure and application security work simpler, saving your precious time and work force.

Spearheaded by AIAST, our product portfolio will include software component analysis, static application security testing, dynamic application security testing, fuzz testing, and more in the coming days.

02

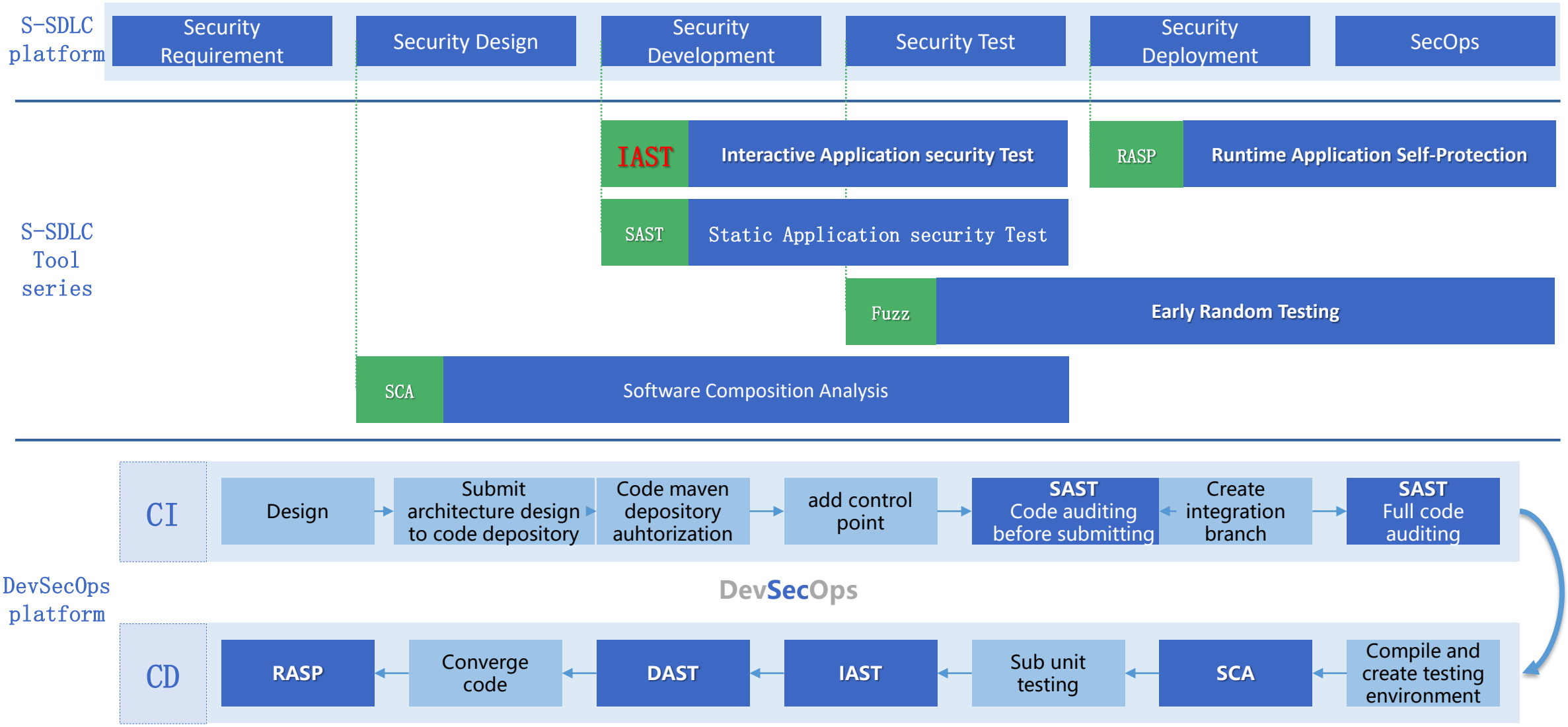
IAST & AIAST Overview

AppSec tools

ZeroDay

#	Category	technology	Description
1	SAST	Static AST	analyzes an application’ s source, bytecode or binary code for security vulnerabilities, typically at the programming and/or testing software life cycle (SLC) phases.
2	DAST	Dynamic AST	analyzes applications in their dynamic, running state during testing or operational phases. It simulates attacks against an application (typically web-enabled applications and services and APIs), analyzes the application’ s reactions and, thus, determines whether it is vulnerable.
3	IAST	Interactive AST	combines elements of DAST simultaneously with instrumentation of the application under test. It is typically implemented as an agent within the test runtime environment (for example, instrumenting the Java Virtual Machine [JVM] or .NET CLR) that observes operation or attacks and identifies vulnerabilities.
4	SCA	Software composition analysis	used to identify open-source and third-party components in use in an application, their known security vulnerabilities, and typically adversarial license restrictions.
5	FUZZ	Fuzz	Fuzz testing or fuzzing is an automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities.

CI/CD--Build software fast with AppSec tools



Tools comparison

ZeroDay

#	IAST	SAST	DAST	RASP
Working Mechanism	Interactive application security testing	Static application security testing	Dynamic application security testing	Runtime application self-protection
Integration Phase	Dev、Test、QA、Deploy	Dev	Test、Deploy	Deploy
Detection Speed	Fast	Medium	Slow	Fast
Continuous	✓	✗	✓	✓
CI/CD Integration	✓	✗	✓	✓
Accuracy	OWASP Benchmark Accurate Rate: 100% False Positive Rate: 0%	OWASP Benchmark Accurate rate: 80% False Positive: 50%	OWASP Benchmark Accurate Rate : 20% False Positive Rate 1%	High
Controllable	High Pinpoint specific code line of vulnerabilities	High Pinpoint specific code line of vulnerabilities	Low Hard to locate problem	High Detailed attacking information

ZeroDay AIAST Quick View

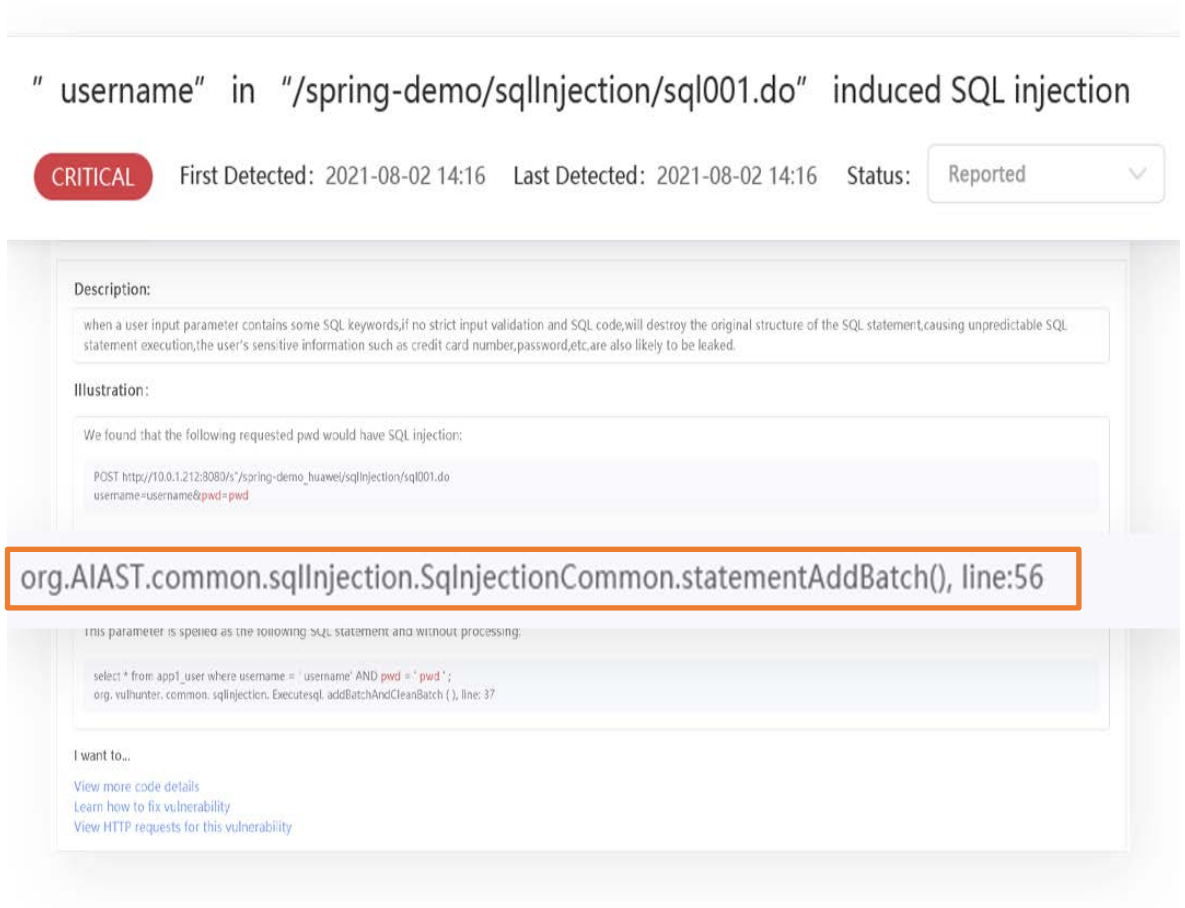
03

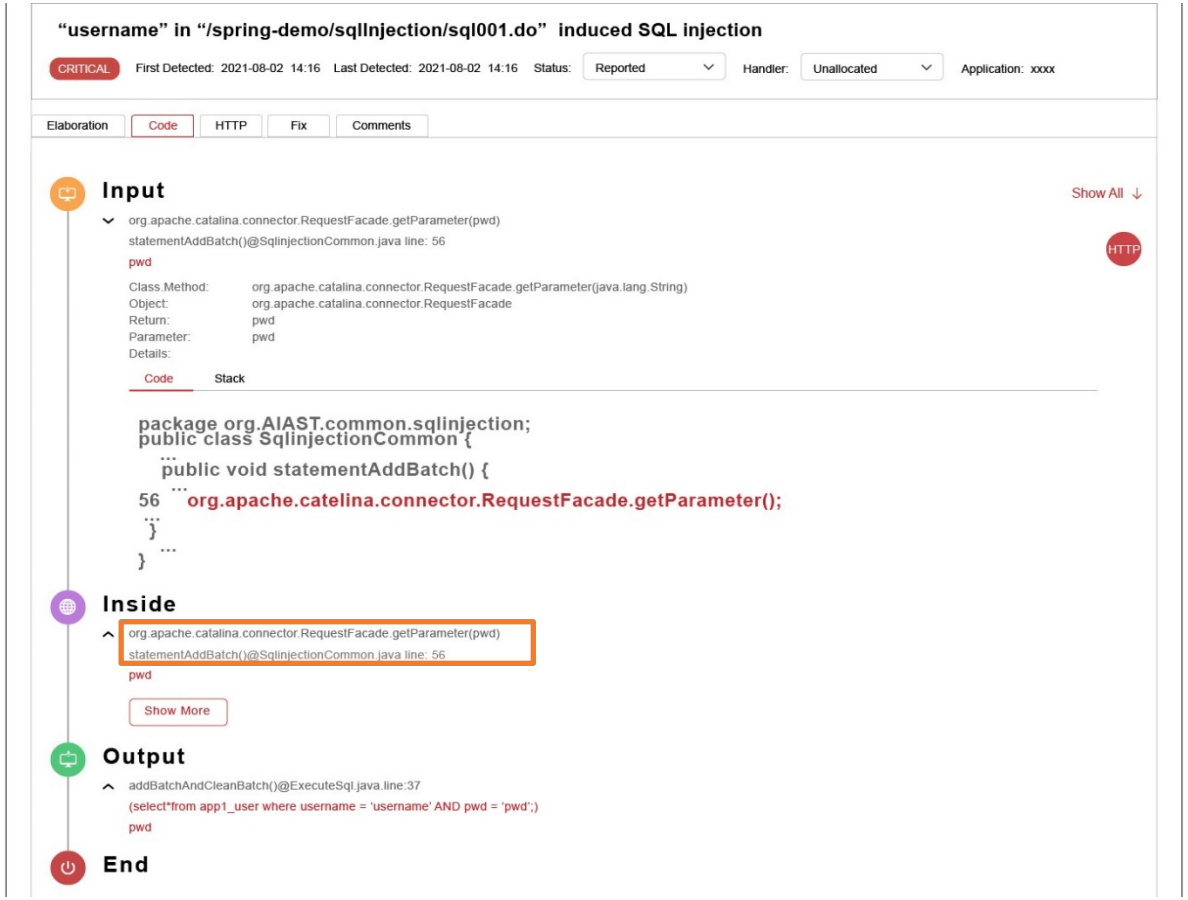
AIAST features and advantages

Seamless integration with functional test

Automatic scanning during the normal functional test introduces no extra phases in secure software development lifecycle, helping your DevOps team to meet the hard security requirement without involving additional delay for stringent time-to-market.

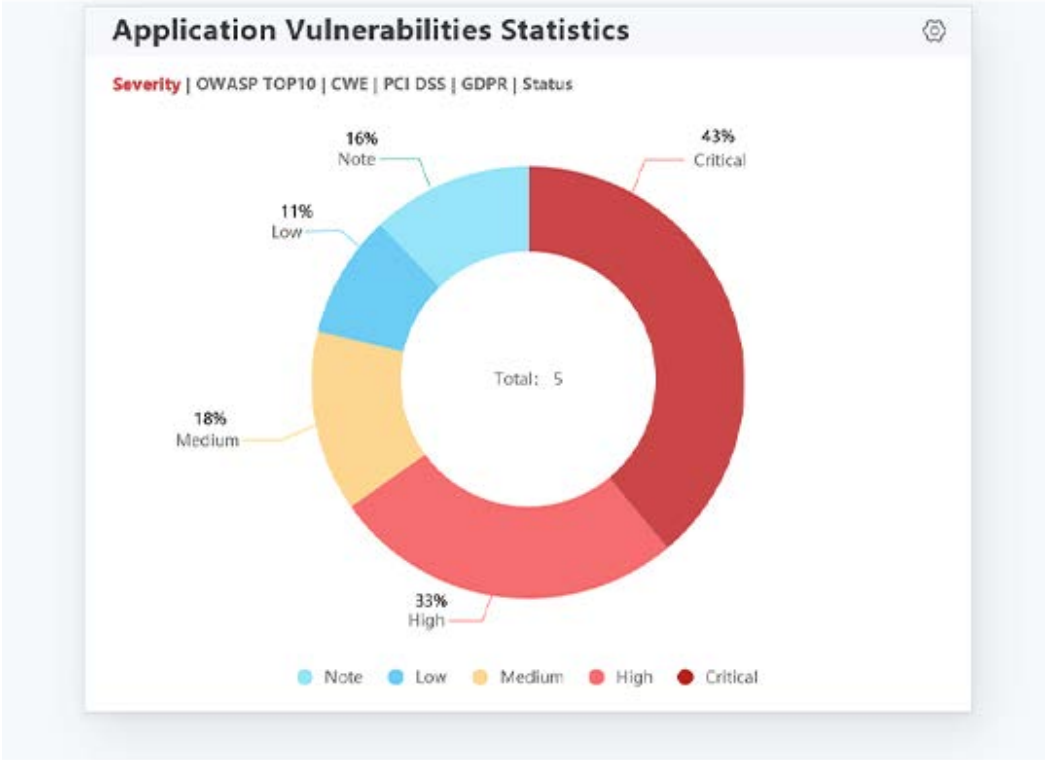
Correlates lines of code with vulnerabilities

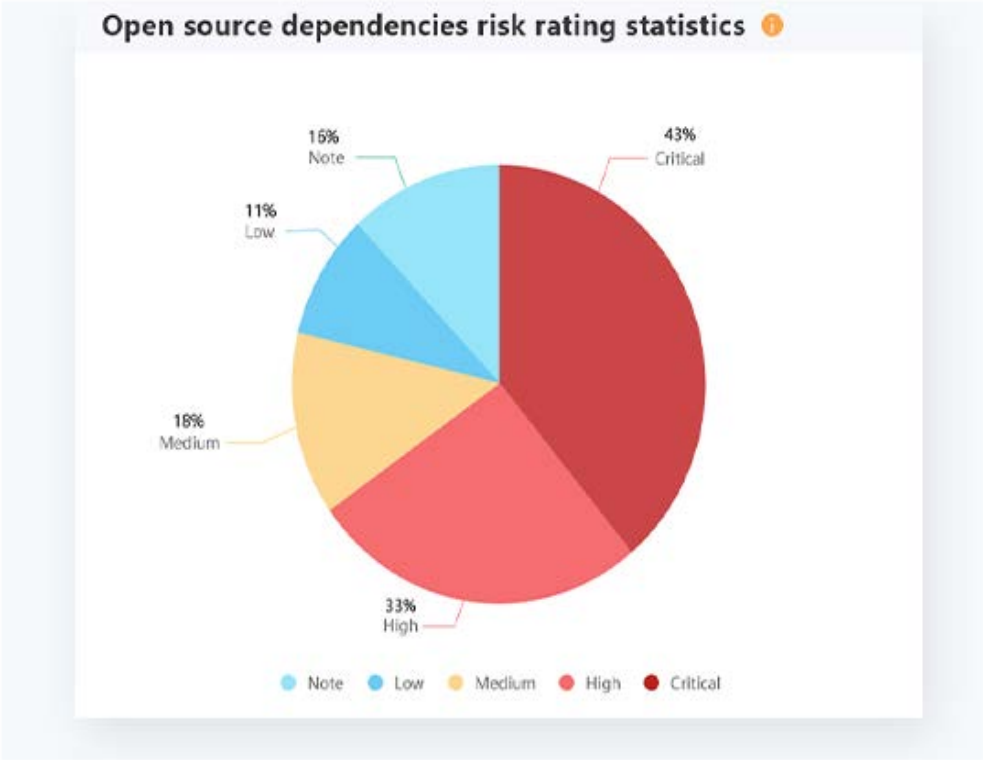




By taking advantage of instrumentation technique, AIAST pinpoint the lines of code where vulnerabilities are detected. Moreover, it provides full stack traces and data flow analysis.

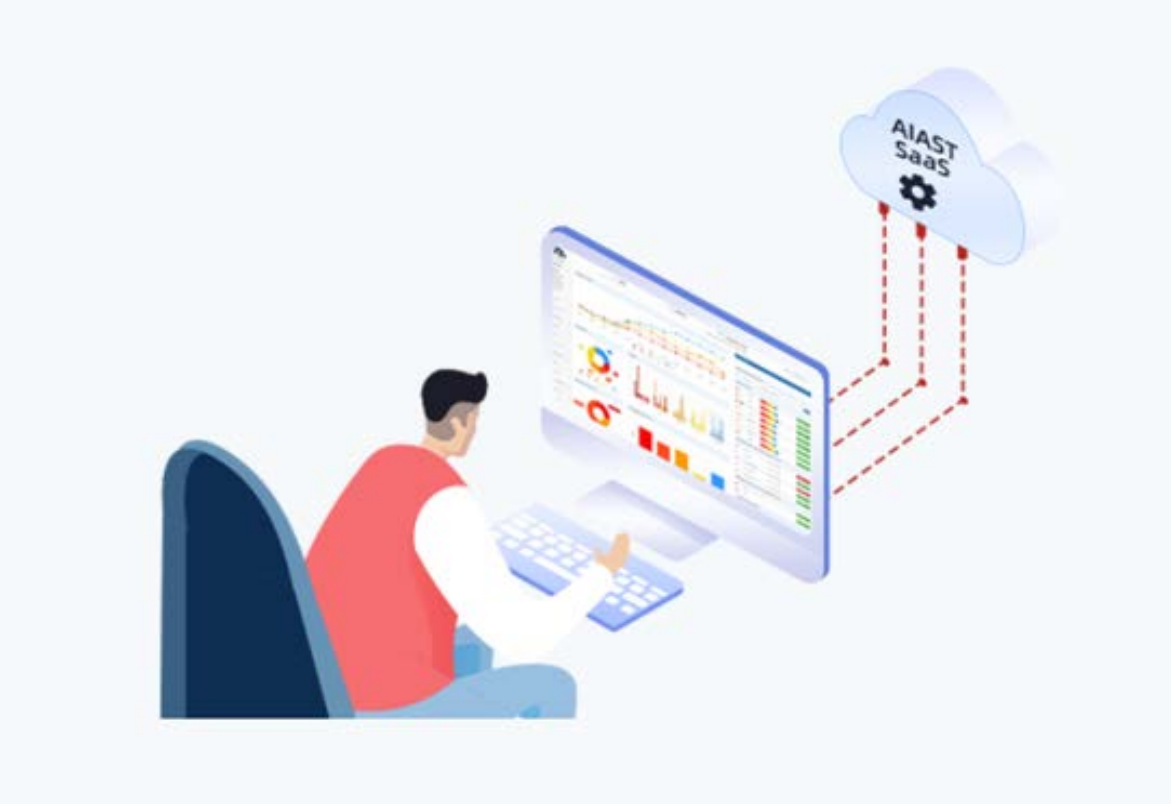
A holistic view of security





Reveals security posture of both custom code and open source dependencies, enjoying the privileges of Interactive Application Security Testing and Source Component Analysis with a single product.

Ready to go & Simple configuration

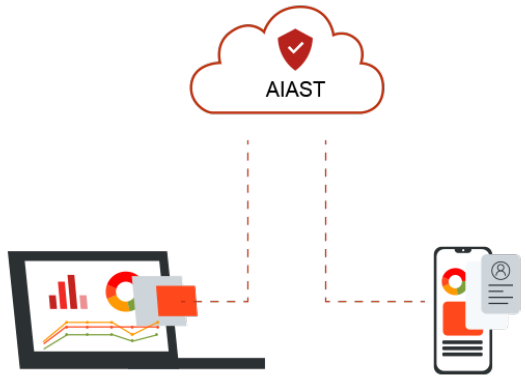


SaaS Solution: spare your hardware investment, no installation/tunning

Quick Start: : launch an app test with just a few commands

Advanced features: more configurations for deeper analysis and custom rules

Main application scenarios



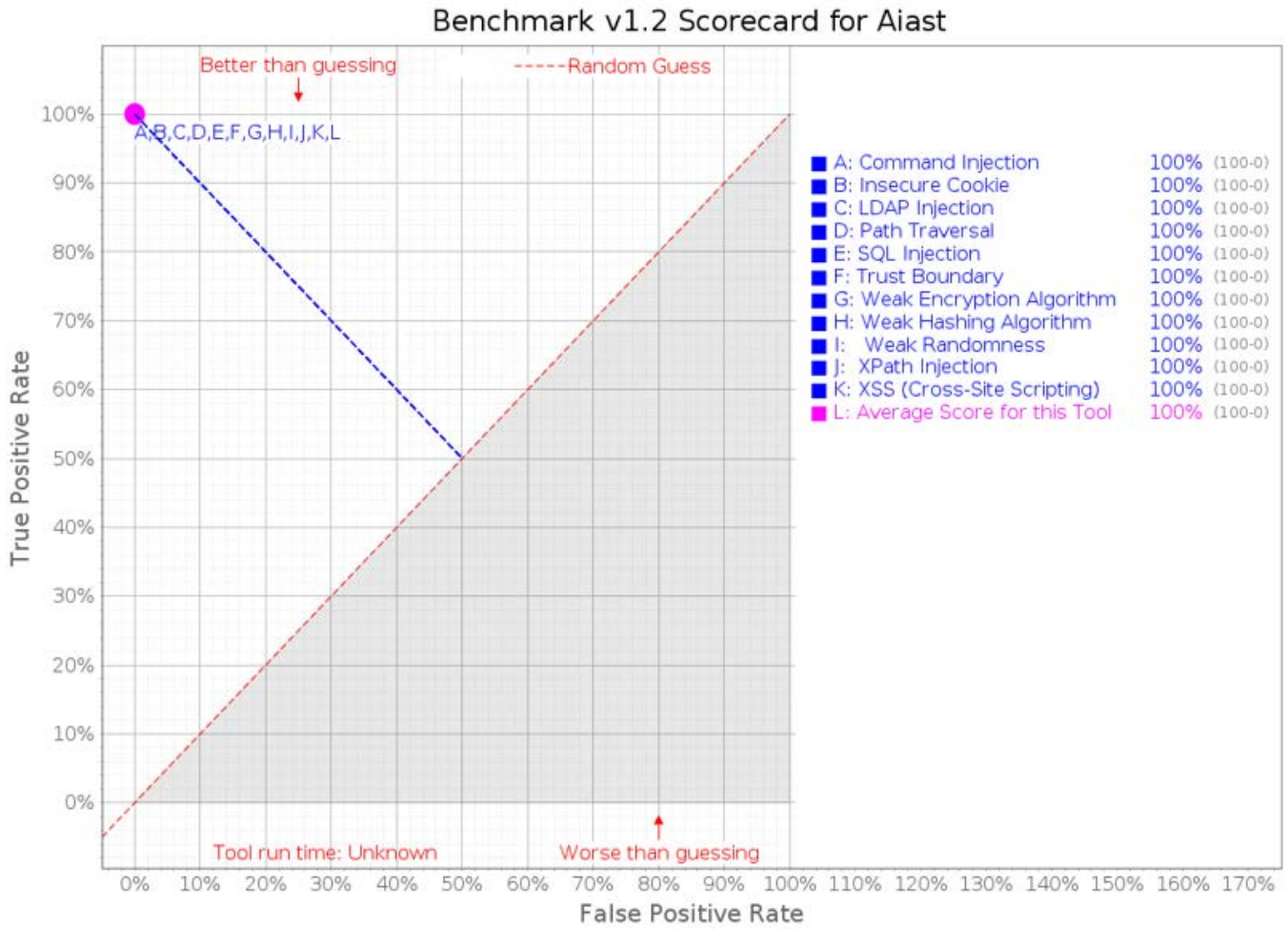
Development and QA Phase:

Shift security left to fix vulnerabilities before release

Regulation and manage software supply chain risk:

Quick issue discovery & supply chain security check

Industry-leading performance



Perfect score against OWASP Benchmark Project

Custom security rules further eliminate false positives

ZeroDay

Thank you very much!