







SAST

Quickly Detect Code Vulnerabilities with Static Application Security Testing



OpsMx Delivery Shield includes Static Application Security Testing (SAST) as part of its comprehensive application security solution. OpsMx SAST leverages open source Semgrep and Sonarqube to provide lightweight, fast, and customizable static analysis designed for developers and security professionals. OpsMx SAST bridges the gap between traditional SAST tools and developer-friendly workflows, enabling efficient code analysis for vulnerabilities and coding best practices.

SAST Key Features

-  **Lightweight and Fast**
 - Low Overhead:** No need for complex setup or heavyweight integrations.
 - Quick Scans:** Analyze code in seconds, suitable for CI/CD pipelines.
-  **Developer-Centric**
 - Intuitive Rules:** Write rules in YAML or use pre-built rules from the Semgrep Registry.
 - Actionable Feedback:** Provides clear, contextual remediation guidance.
-  **Language and Framework Support**
 - Multi-Language Coverage:** Supports 20+ programming languages, including Python, JavaScript, Java, Go, Ruby, and more.
 - Framework-Specific Rules:** Tailored checks for popular frameworks like React, Flask, and Django.
-  **Open Source and Extensible**
 - Community-Driven Rules:** Access a rich library of rules from the open-source community.
 - Custom Rule Creation:** Write and adapt rules for specific use cases.
-  **CI/CD Integration**
 - Seamless Integration:** Works with GitHub Actions, GitLab CI, Jenkins, CircleCI, and other CI/CD tools.
 - Shift-Left Security:** Catch issues early in the development lifecycle.
-  **Security and Code Quality**
 - Vulnerability Detection:** Identify common security flaws like SQL injection, XSS, and insecure configurations.
 - Coding Standards:** Ensure adherence to organization-specific coding guidelines.



Benefits

- Developer-Friendly:** Minimal learning curve, making it easy for developers to adopt.
- Customizable:** Tailor rules to meet your organization's unique requirements.
- Transparent:** Open-source transparency ensures trust and adaptability.

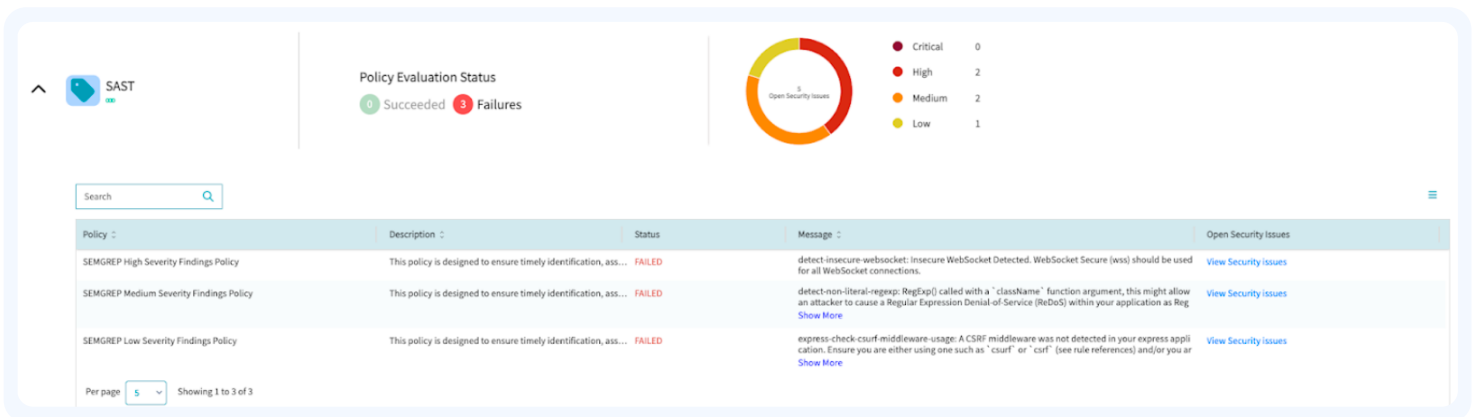
Use Cases

OpsMx Delivery Shield SAST simplifies application security without sacrificing speed. Backed by an active and supportive open-source community, OpsMx SAST aligns security with agile development practices to enable organizations to deliver more security applications faster.

OpsMx Delivery Shield SAST simplifies application

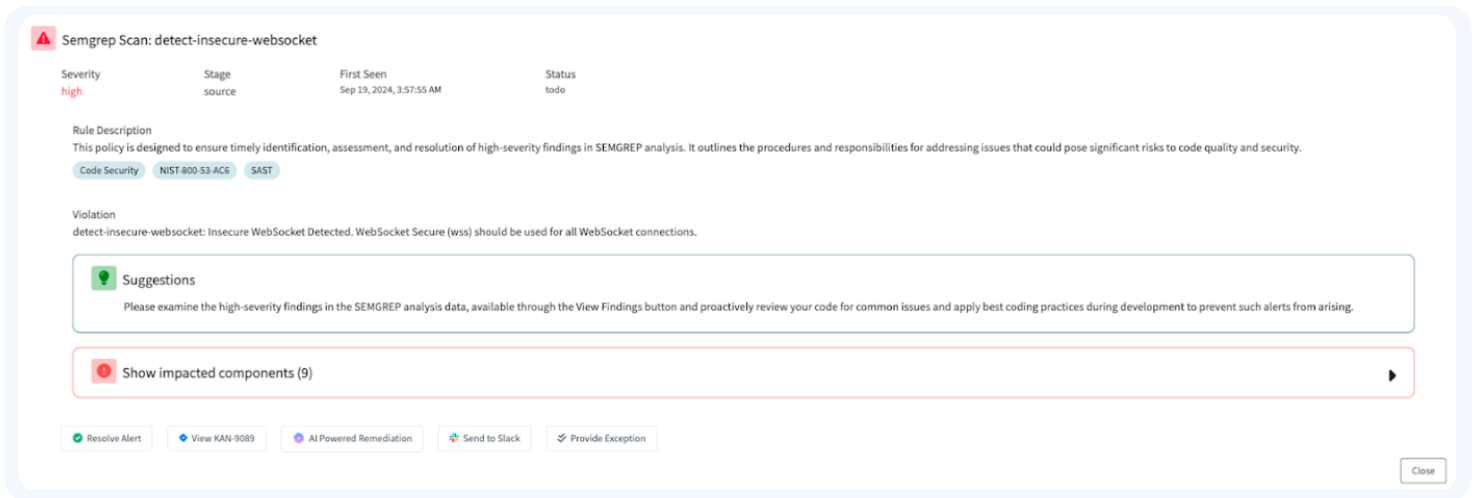
-  security without sacrificing speed.
-  Backed by an active and supportive open-source community, OpsMx SAST aligns security with agile development practices to enable organizations to deliver more security applications faster.

Screenshots



The dashboard shows a 'Policy Evaluation Status' section with 1 Succeeded and 3 Failures. A donut chart displays the distribution of security issues: 0 Critical, 2 High, 2 Medium, and 1 Low. Below is a table of findings:

Policy	Description	Status	Message	Open Security Issues
SEMGREP High Severity Findings Policy	This policy is designed to ensure timely identification, ass...	FAILED	detect-insecure-websocket: Insecure WebSocket Detected. WebSocket Secure (wss) should be used for all WebSocket connections.	View Security issues
SEMGREP Medium Severity Findings Policy	This policy is designed to ensure timely identification, ass...	FAILED	detect-non-literal-regexp: RegExp() called with a "className" function argument, this might allow an attacker to cause a Regular Expression Denial-of-Service (ReDoS) within your application as Reg... Show More	View Security issues
SEMGREP Low Severity Findings Policy	This policy is designed to ensure timely identification, ass...	FAILED	express-check-csrf-middleware-usage: A CSRF middleware was not detected in your express application. Ensure you are either using one such as "csrf" or "csrf" (see rule references) and/or you ar... Show More	View Security issues



Semgrep Scan: detect-insecure-websocket

Severity: **high** | Stage: source | First Seen: Sep 19, 2024, 3:57:55 AM | Status: todo

Rule Description
This policy is designed to ensure timely identification, assessment, and resolution of high-severity findings in SEMGREP analysis. It outlines the procedures and responsibilities for addressing issues that could pose significant risks to code quality and security.

Violation
detect-insecure-websocket: Insecure WebSocket Detected. WebSocket Secure (wss) should be used for all WebSocket connections.

Suggestions
Please examine the high-severity findings in the SEMGREP analysis data, available through the View Findings button and proactively review your code for common issues and apply best coding practices during development to prevent such alerts from arising.

Show impacted components (9)

Resolve Alert | View KAN-9089 | AI Powered Remediation | Send to Slack | Provide Exception

ABOUT US

OpsMx secures and intelligently automates software delivery from developer to deployment, building on an Open Software Delivery architecture and AI/ML-powered DevSecOps. OpsMx products and services enable hundreds of thousands of developers at Google, Cisco, Western Union, and other leading global enterprises to ship better software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085 | INFO@OPSMX.COM
WWW.OPSMX.COM/SECURE SOFTWARE DELIVERY