Static App Security Testing (SAST)

Decision Matrix Worksheet

clarify360.com

Static Application Security Testing (SAST) has become an essential tool for increasing code security and reducing cyber risk. Static AST (SAST) analyzes an application's source, bytecode or binary code for security vulnerabilities, typically during the programming and/or testing phases of the software development life cycle (SDLC).

TECHNICAL CONSIDERATIONS	Vendor:	Vendor:	Vendor:
Supports a number of languages			
Comprehensive testing of APIs, applications deployed in containers, and other aspects of modern development to support those use cases			
Ability to pinpoint the line in code where the security vulnerability is identified			
Offers a set of pre-defined industrial standard secure coding rules like OWASP Top 10, OWASP Top 10 for Mobile			
Offers a set of pre-defined industrial standard and secure coding rules: ISO/IEC TS 17961:2013/C or 1:2016 C Secure Coding Rules, DISA STIG, SANS/CWE Top 25, SEI CERT Coding Standards			
Provides a default prioritization of vulnerabilities according to severity and risk but offers the flexibility to change prioritization according to organizational needs.			

SAST
Vendor Comparison Worksheet

TECHNICAL CONSIDERATIONS
(continued)

	Vendor:	Vendor:	Vendor:
Provides real time or regular updates to its vulnerability/rule's knowledge base			
Provides the option of "incremental scanning", where only the portion of new or changed code is scanned			
Ability to to mark a particular observation as false positive in less than 2 minutes			
Compares between multiple scans for the same application and tags fixed, recurring & new vulnerabilities observed between the scans			
Automatically retains the status of existing false positive in the next scan			
Capability to create custom policies			
Provides detailed reporting of vulnerabilities found			
Supports a variety of Operating Systems Provides security tips while developers are coding			
Tool allows Developer to do a private scan, retrieve results & remediate the vulnerabilities within the IDE			
Scans the source code locally developed by the developer in run-time environment without requiring connection to a centralized server			
Capability to schedule scanning activity			

SAST
Vendor Comparison Worksheet

	Vendor:	Vendor:	Vendor:
DASHBOARD			
Displays trend graphs of project / application security health			
Maps scan results to compliance standards			
Offers a common dashboard for a project with all application vulnerabilities			
INTEGRATION/ADMINISTRATION			
Integration with a comprehensive selection of vulnerability databases			
Integration with threat intelligence feeds			
Ability to sort results by the priority of the vulnerability			
Integrates with a defect-tracking system (HP ALM, JIRA, Bugzilla etc) for easy creation of defects for vulnerabilities found from within the solution itself			
Able to integrate with automatic build and deployment			
Able to integrate with free and open source automation server like Jenkins			
Ability to integrate with developer environment Via IDE (Eclipse, Visual Studio)			
Able to integrate with automatic build and deployment			
Supports CI/CD integration			
Able to integrate with common code repository (GITHUB, SVN)			
Supports integration with build management solutions			

SAST
Vendor Comparison Worksheet

REPORTING	Vendor:	Vendor:	Vendor:
Capability to generate out-of-the-box reports such as high- level executive summary and low-level (detailed) technical reports for developers			
Ability to create custom reports			
Export reports in different formats: csv, pdf, xls, text, HTML, XML			
Provides integration with SMTP for email notification			
ACCESS CONTROL			
Provides role based access controls			
Provides integration with Active directory and SAML integration for SSO implementation			

If you want to talk about SAST solutions more in depth, reach out at clarify360.com!

About Clarify360

Clarify360 is a technology sourcing and consulting provider specializing in the discovery, planning, and migration of cloud/colocation, connectivity, collaboration, and security deployments globally. Our key goal is to shorten the IT procurement process for our clients while optimizing costs and ROI. With roots in network connectivity and telecommunications dating back more than two decades, reducing complexity and leveraging IT savings for our clients is part of our DNA. Visit clarify360.com for more information.