SYNOPSYS®

Intelligent Orchestration

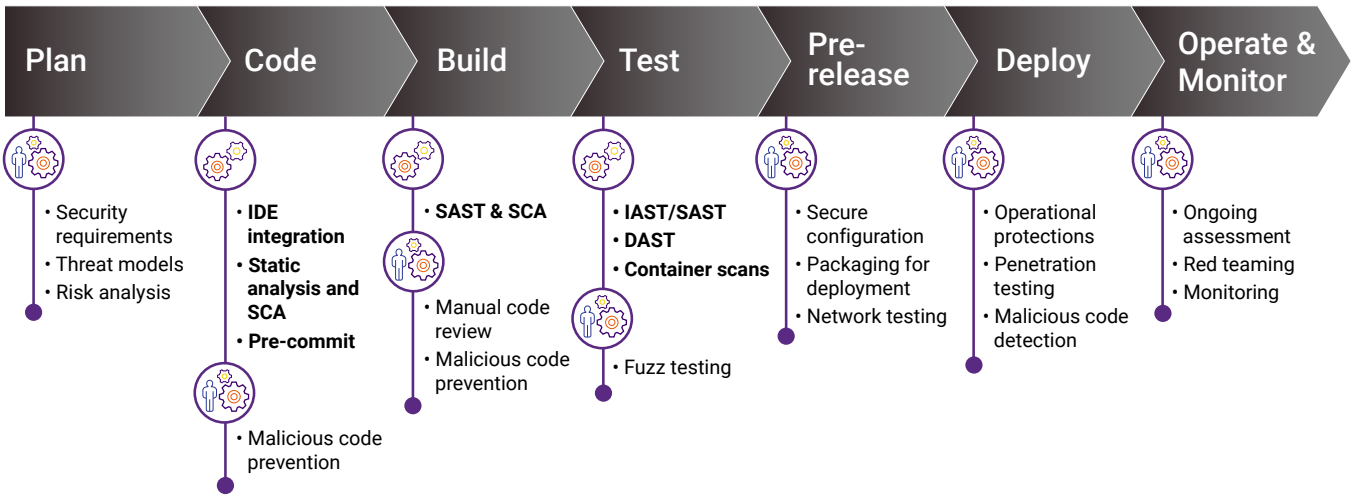
Define the rules for how your organization manages risks. Let Intelligent Orchestration manage test execution, policy enforcement, and issue prioritization and filtering.

Overview

Synopsys Intelligent Orchestration provides customized AppSec pipelines that not only automate security testing for a few stages, but throughout the entire software development life cycle (SDLC). It automatically runs the right security tools or triggers manual testing activities based on how significant the code changes are, the total risk score, and your company's own security policies. This enables security teams to easily implement security processes and policies for all applications across their organization, at enterprise scale.

Intelligent Orchestration works with Synopsys AppSec tools (Coverity®, Polaris Software Integrity Platform®, Black Duck®, Seeker®) and services, third-party commercial and open source tools, and also provides key integrations support for GitHub Actions, industry-standard source code management systems (SCMs), continuous integration (CI) build servers, issue trackers, and dashboarding systems. It supports on-premises deployment and can also be hosted on Amazon AWS and Microsoft Azure cloud pipelines.

Dedicated application security pipeline
Intelligent Orchestration



Key features

For development teams

- Intelligent Orchestration uses separate pipelines that don't get in the way of your main development pipelines. Simply merge the security analysis results into your main development pipeline, and get the right information delivered directly to the right teams within their own issue trackers and notification channels.

Benefits

- **Fast adoption and onboarding.** Intelligent Orchestration includes native Synopsys static application security testing (SAST), software composition analysis (SCA), and interactive application security testing (IAST) tools. Other commercial and open source tools can also be added. Quickly onboard new and existing applications in hours or minutes.
- **Improved visibility into security risk.** Intelligent Orchestration converts reports extracted from security tools into a uniform schema. Dashboarding tools display risk calculation, scores for different app risk factors, and security activities selected for the latest pipeline run.
- **Flexible configuration options.** Security and development teams can set:
  - Scan frequency and out-of-band activities based on risk score
  - Whether the tools are run asynchronously or synchronously
  - Notification types (Slack, email)
  - Criteria for pausing, breaking, or continuing the build and defect tracking
- **Accelerated development velocity.** Instead of spending time running all AppSec scans (e.g., SAST, SCA, IAST, dynamic application security testing [DAST]) for every build, run only the right tools at the right time—or not at all.
- **Earlier and more-efficient security testing.** Enable your teams to fix software defects quickly, easily, and correctly with fast analysis results and actionable remediation advice as they code. Issue tickets are automatically created in Jira for tracking and triage.
- **Developer training metrics and insights.** Data gathered on the type and frequency of security vulnerabilities found in individual developers' code can be leveraged for focused developer feedback and training.

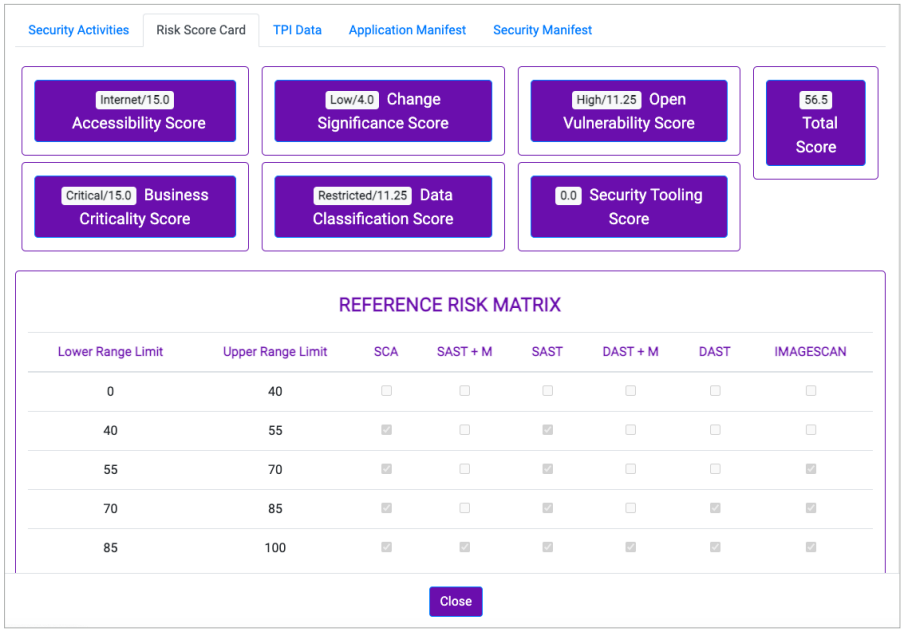
- With Intelligent Orchestration, developers aren't overwhelmed by analysis results—they get vulnerability information prioritized by their organization's security policies (e.g., only critical vulnerabilities or critical SQLi vulnerabilities). Intelligent Orchestration is smart enough to know when to run a specific scan and when not to, based on actual code changes, a dynamically calculated total risk score, and predetermined security policies.
- Development teams can specify that GitHub Actions will run any time a developer pushes a code change. Developers get all the information they need to fix identified issues and merge the fixed code into the main branch: detailed descriptions, actionable remediation advice, which file changed, the line number, and the commit ID.

For security teams

- Intelligent Orchestration enables users to configure post-scan feedback so that designated development, security, and DevOps leads are immediately notified of paused or failed builds, or critical security vulnerabilities or failures, so they can be remediated right away.
- Easily implement security or quality gates based on configurable failure criteria. Identified critical issues are then pushed automatically to issue-tracking systems like Jira. This provides development teams with continuous feedback and visibility into security findings.
- Security teams can easily configure governance and compliance requirements. The policies that determine the depth and breadth of security activities, define development workflows, and set scan compliance requirements can be configured for each individual business unit, product team, application, or the entire organization.

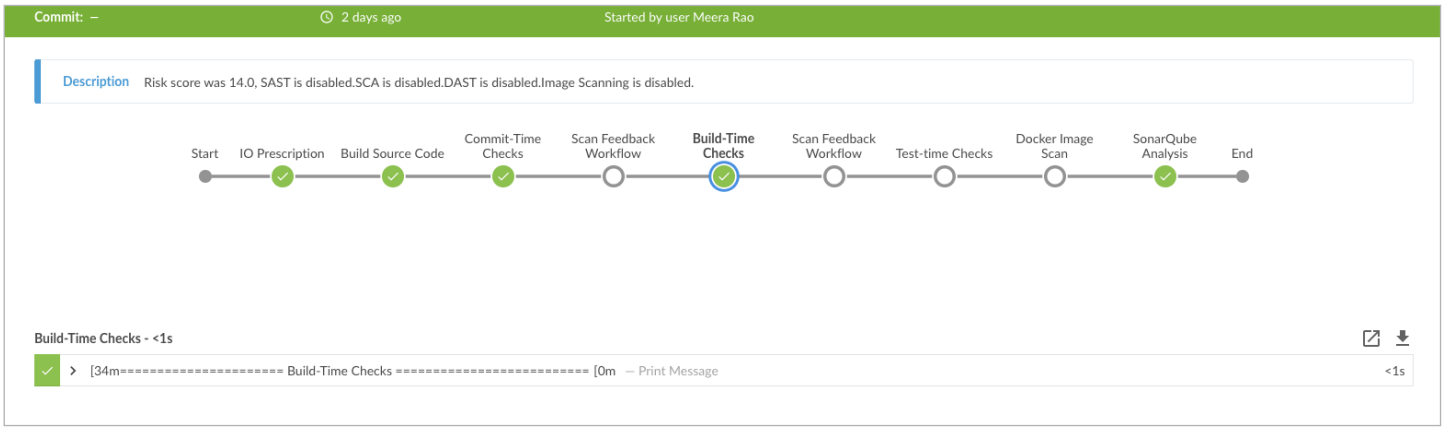
Customized policy management

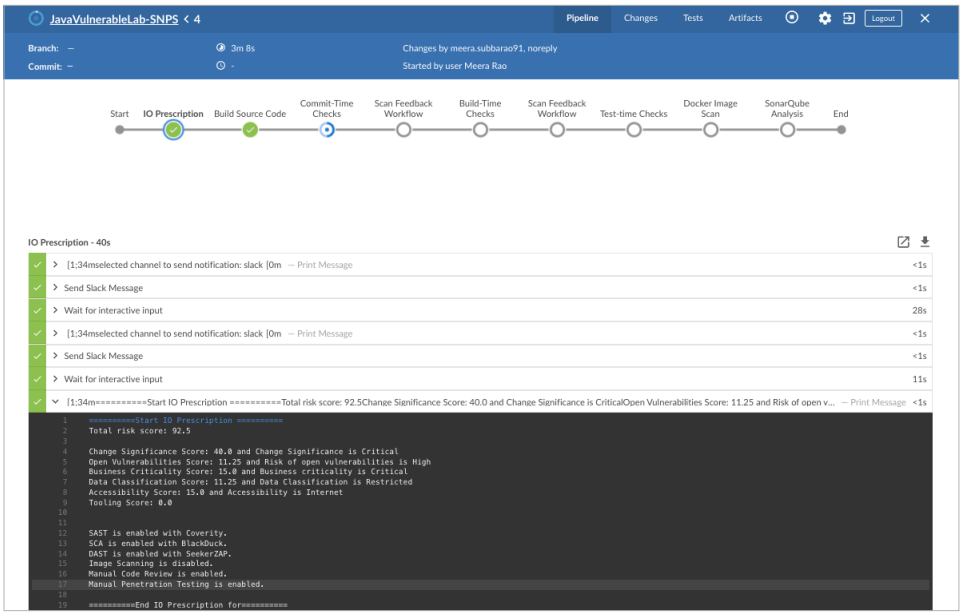
- With Intelligent Orchestration you can define and customize the weights assigned to the criteria used to calculate the total risk score. For example, you can set risk scores for criteria including whether the application is internet- facing, is business-critical, contains restricted data, includes critical open vulnerabilities, or has had significant code changes. You can customize the ranges for the scores and the types of security tools to run, based on your company's security policies, compliance, and governance requirements.



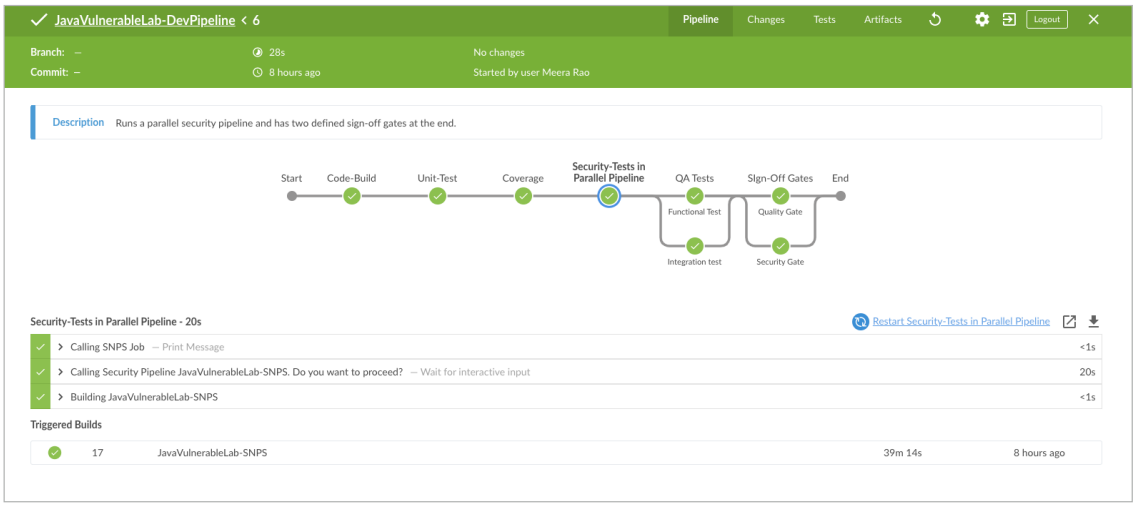
How Intelligent Orchestration works

Intelligent Orchestration is smart enough to determine which scans or manual testing are required, based on actual code changes, risk score, and corporate policies. If the code changes are minor, such as changing the font using CSS in an HTML file, the risk score would be low and no security scan would be run at all. This saves valuable time and resources.





However, if the code change is major and critical in nature, such as changing an authentication API, Intelligent Orchestration would assign a high risk score, and multiple security testing scans such as SAST, SCA, and DAST would be enabled. In addition, manual code review and manual penetration testing would be triggered as required actions.



Executing security tools and other tests in parallel is also possible with Intelligent Orchestration.

Intelligent Orchestration | Technical Specifications

SDLC native integrations

Source code management (SCM)

- GitHub
- GitLab
- Bitbucket
- Other Git-based SCMs

CI build servers / developer tool chains

- Jenkins
- GitLab CI
- Bitbucket Pipes
- GitHub Actions

Issue tracking

- Jira
- GitHub Code Scanning Alerts
- Bitbucket Code Insights

Security tools

- Synopsys Coverity/Polaris
- Synopsys Black Duck
- Synopsys Seeker
- Other commercial AppSec tools*
- Open source SAST, SCA, and image scanning tools*

Dashboarding tools

- Polaris reporting and Intelligent Orchestration
- Third party reporting and dashboarding tools*

Cloud and cloud pipelines

- Amazon Web Services / AWS Data Pipeline
- Azure / Azure Pipelines

Other development environments

- Docker (image scanning)
- Kubernetes

Notification channels

- Slack
- Teams
- Email

*Custom integrations are also available.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com