WEBINAR SERIES

Webinar topic

WEBINAR 1: UNLOCKING THE POWER OF DEVSECOPS: WHAT IT IS - HOW IT WORKS - WHY IT MATTERS?
WEBINAR 2: SOFTWARE SUPPLY CHAIN RISKS & SBOM
WEBINAR 3: MASTERING DEVSECOPS WITH ASPM/SRM: ELEVATING YOUR APPLICATION SECURITY SKILL

Webinar #3

Mastering DevSecOps with ASPM/SRM

Son Nguyen
Email: SonNV@mi2.com.vn
Mobile: +84977585651

Agenda


DEVSECOPS & ORCHESTRATION ISSUE
APPLICATION SECURITY POSTURE MANAGEMENT
SYNOPSYS APPLICATION SECURITY RISK MANAGEMENT
DISCUSSION

Despite AppSec Investment, Security is Failing at the SDLC

64%

are using at least 6 AST tools or more

35%

push production-level code with known vulnerabilities

45%

release software without testing or security checks

Presentation content source: Synopsys

Why do Current AppSec Initiatives Fall Short?

Poor AppSec ROI

Unable to adequately secure software despite high cost of tooling, staff, and maintenance.

Inaccurate view of software risk

Cannot audit and pinpoint most vulnerable software, making compliance difficult.

Inconsistent AppSec checks

Difficult to standardize quality standards for all production-level code, in-house & contracted.

Cannot prioritize critical work

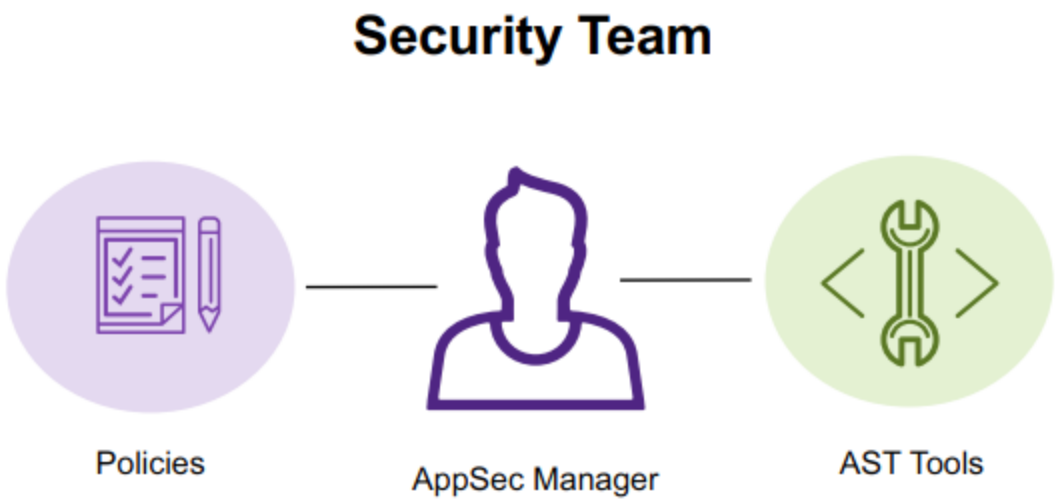
Too many false positives and redundant activities are slowing down productivity.

Cannot test at speed required

Security is holding up shipping product, meeting customer SLAs. Unable to maintain business continuity.

Presentation content source: Synopsys

To Achieve AppSec ROI, Security Teams Need to Answer...



How do I get my developers to adopt my tools and workflows?

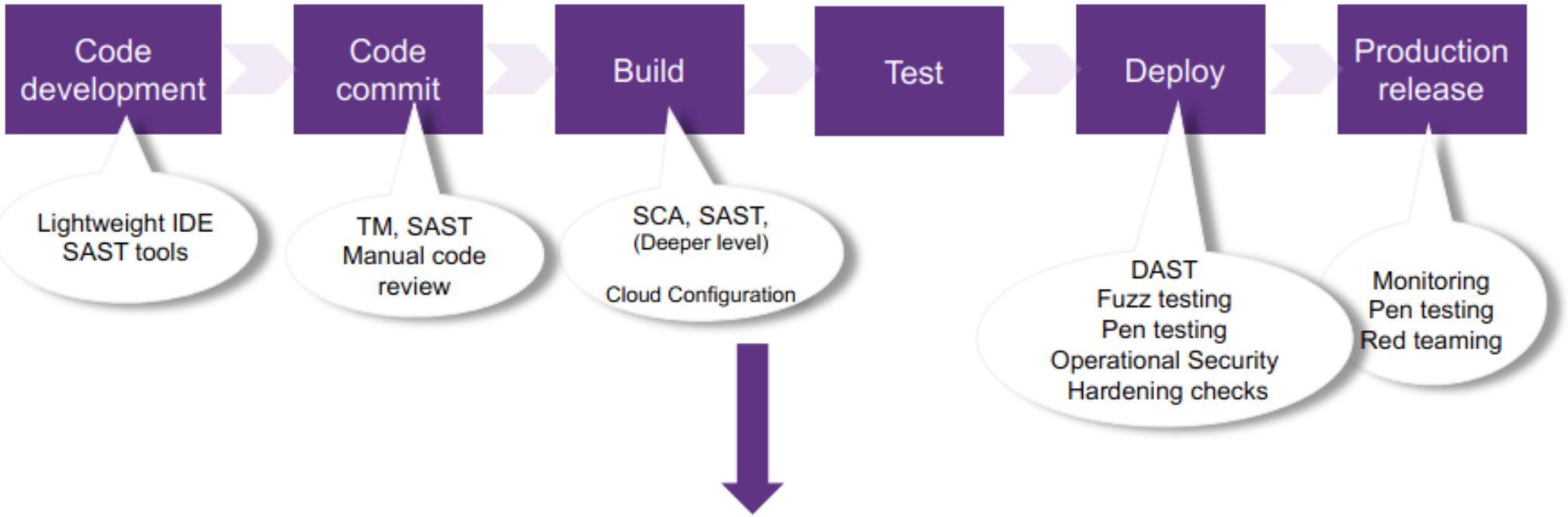
How do I know that my security policy is being adhered to?

What is my application security risk?

How do I scale my AST investments?

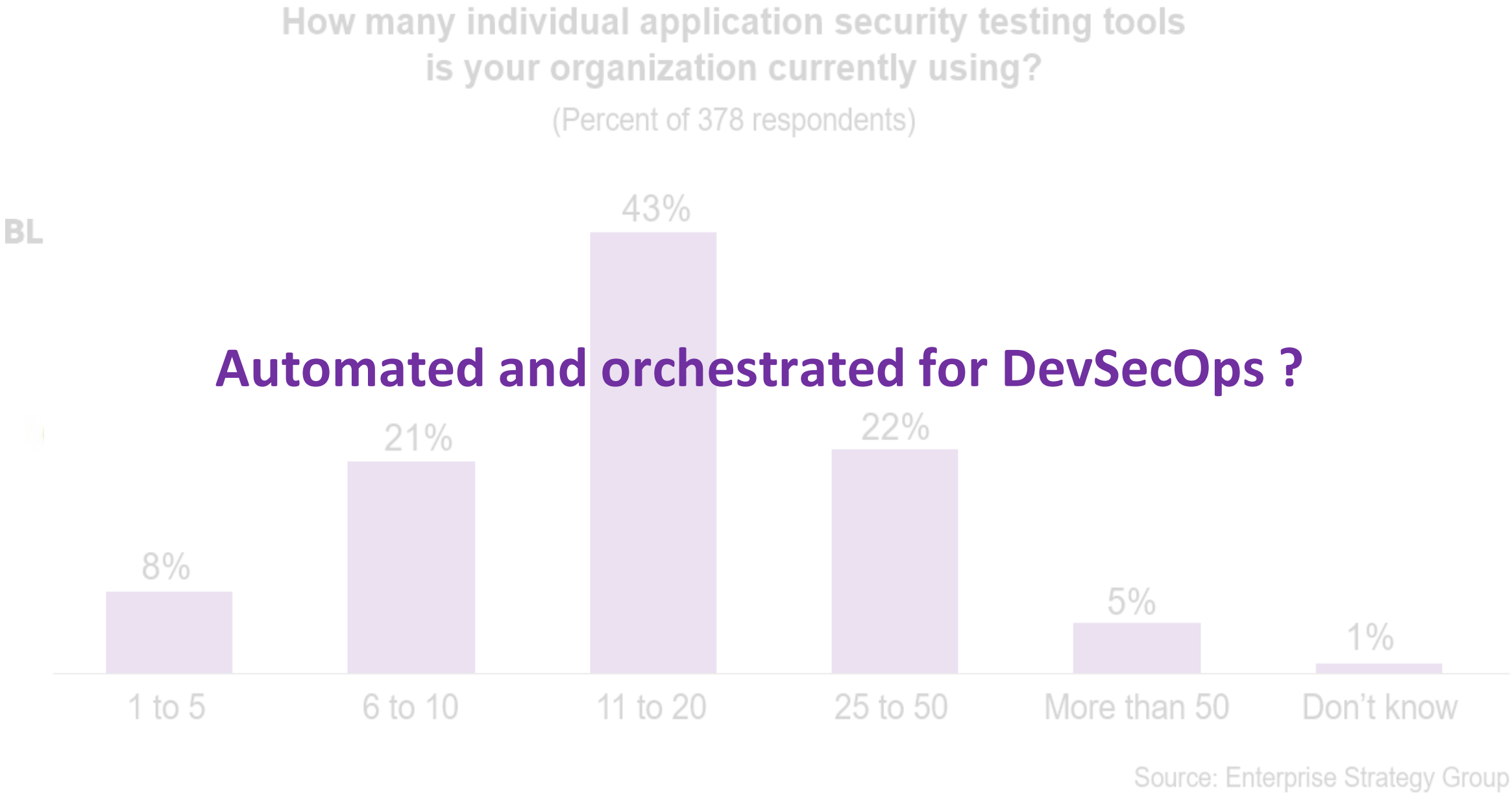
Presentation content source: Synopsys

Managing security posture requires a comprehensive view



What makes up my software? What/when was it tested? What was fixed? What was found?
What is the extent of my exposure/exploitability? Is my software compliant?

Presentation content source: Synopsys



Automated and orchestrated for DevSecOps ?

Presentation content source: Synopsys

Application Security Posture Management (ASPM)

Gartner defines the evolution of the Application Security Posture Management (ASPM) market.

According to Gartner:

"*Application security posture management **(ASPM)** analyzes security signals across software development, deployment, and operation to **improve visibility**, **better manage** vulnerabilities, and **enforce controls**. Security leaders can use ASPM to improve application security efficacy and better manage risk.*"

Presentation content source: Synopsys

What Does an ASPM Solution Need to Be Able To Do?

Integrate across a heterogenous environment

Synthesizes data across all security testing, developer tools, issue trackers

Prioritize issues and accelerate triage

Reduces number of findings and understands security work that matters most

Centralize policy management

Defines and enforces pre and post scan activities

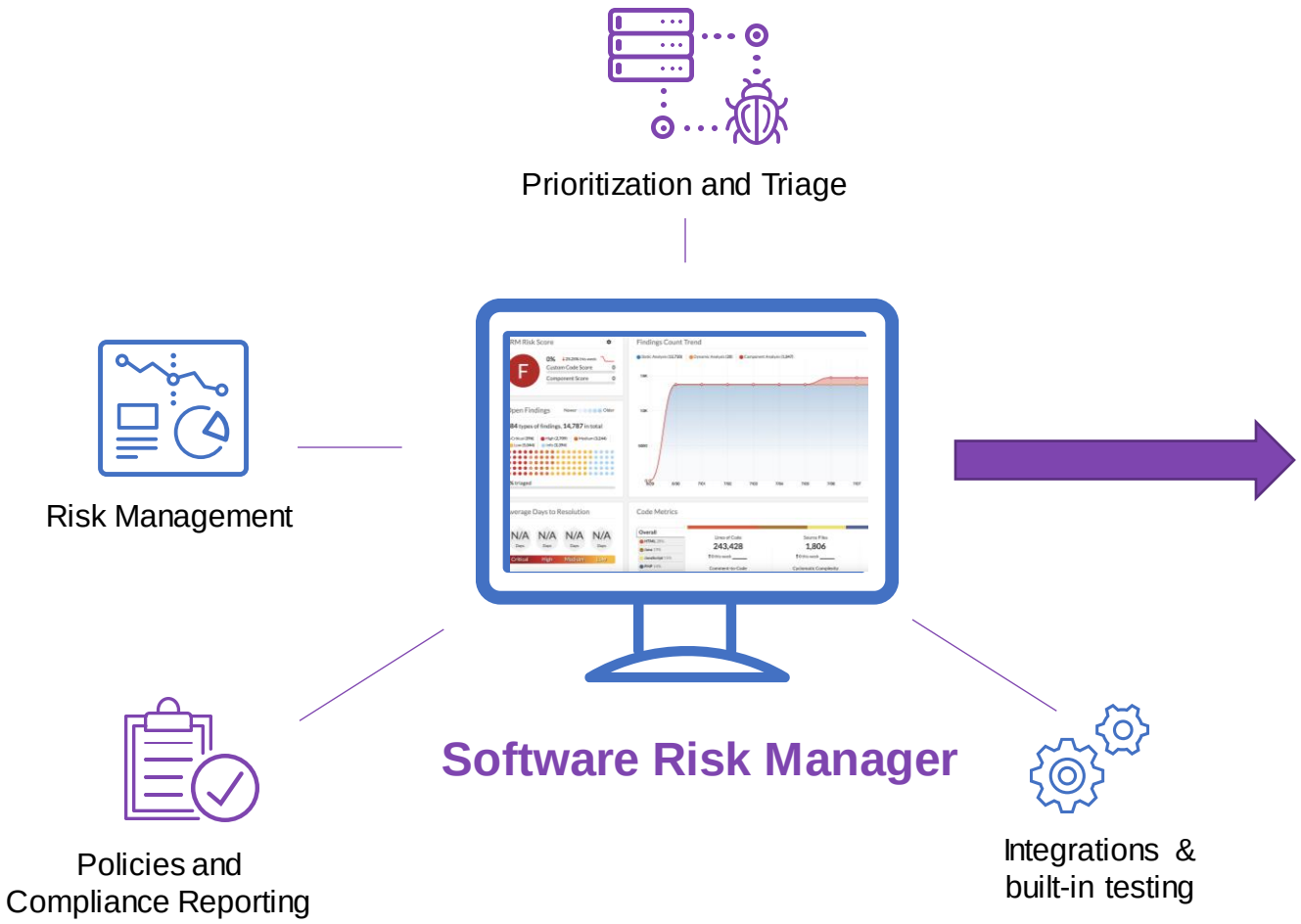
Provide an accurate view of software risk

Summarizes compliance posture across the software footprint

Presentation content source: Synopsys

Synopsys Software Risk Manager

Application Security Posture Management (ASPM)



Risk management

- Overall risk posture
- Audit capability

Policy – orchestrate testing and remediation

- Pre-scan
- Post-scan

Prioritization and triage

- Normalization / De-duplication
- Risk scoring

Integrations – 135+ and growing

- Manual and automated AST
- Development, deployment, and operations

Built-in testing – only ASPM solution that includes market-leading scan engines

- SAST
- SCA

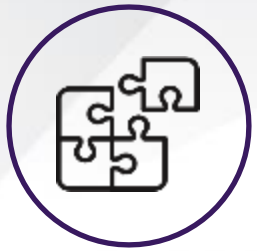
Presentation content source: Synopsys

Synopsys Software Risk Manager

Application Security Posture Management (ASPM)

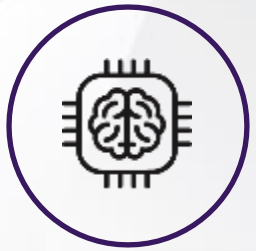
Execute tests

Automatically & intelligently run AppSec tools



Correlate results

Combine issues found by security tools



Prioritize vulnerabilities

Filter out noise using machine learning to determine what to fix first

Track remediation

Track all testing and remediation activities in a system of record

Centralize risk visibility

Provide continuous situational awareness through a single pane of glass

Fits seamlessly into the CI/CD pipeline

Presentation content source: Synopsys

AppSec Program
Objectives & Metrics

Policies

Intelligent Orchestration

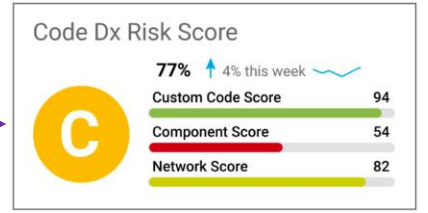
Executes the right tests, at the right time, at the right level; triggers manual tests

Insight Risk Management

Correlates, prioritizes, and tracks remediation.
Centralizes risk visibility

Secure Development

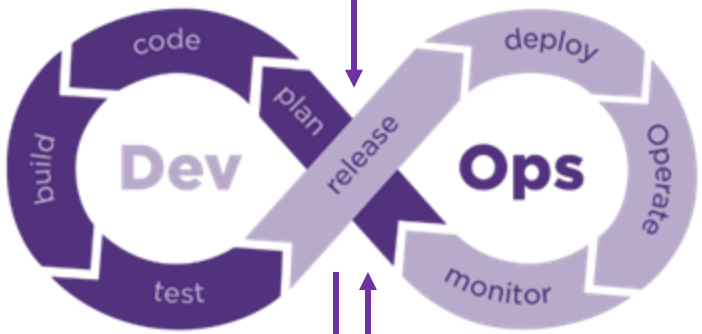
Deliver actionable risk insight and remediation guidance to developers in their workflow



Actionable insights into software risk

Prioritized tickets for remediation

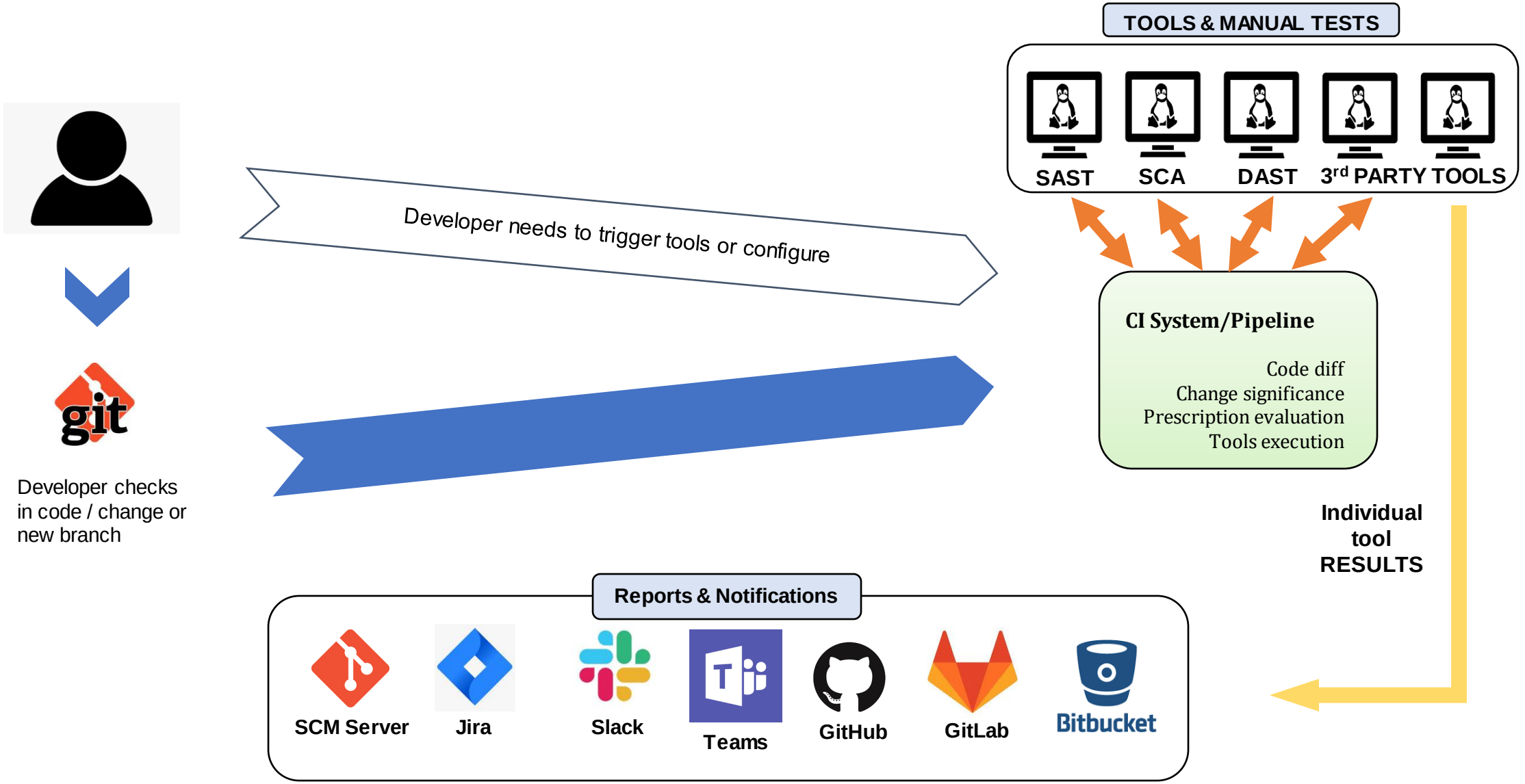
Jira



Presentation content source: Synopsys

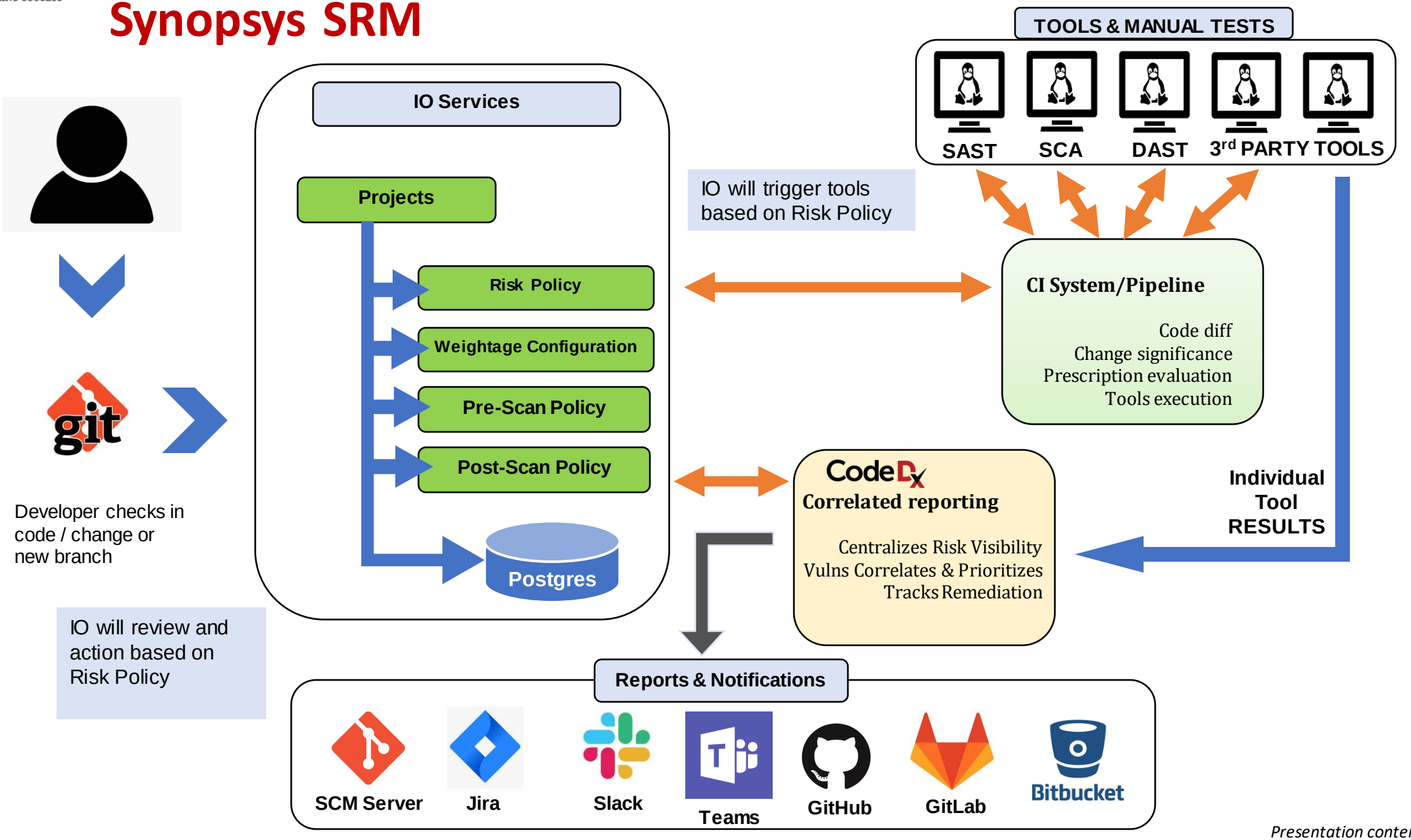
Threat Model | Code Review | SAST | SCA | IAST | DAST | Pen Test | Risk Analysis

Typical current process



Presentation content source: Synopsys

Synopsys SRM



Presentation content source: Synopsys

Unify Policy, Test Orchestration, Issue Correlation

Right tests, right time, right level

Simplify AST Integration

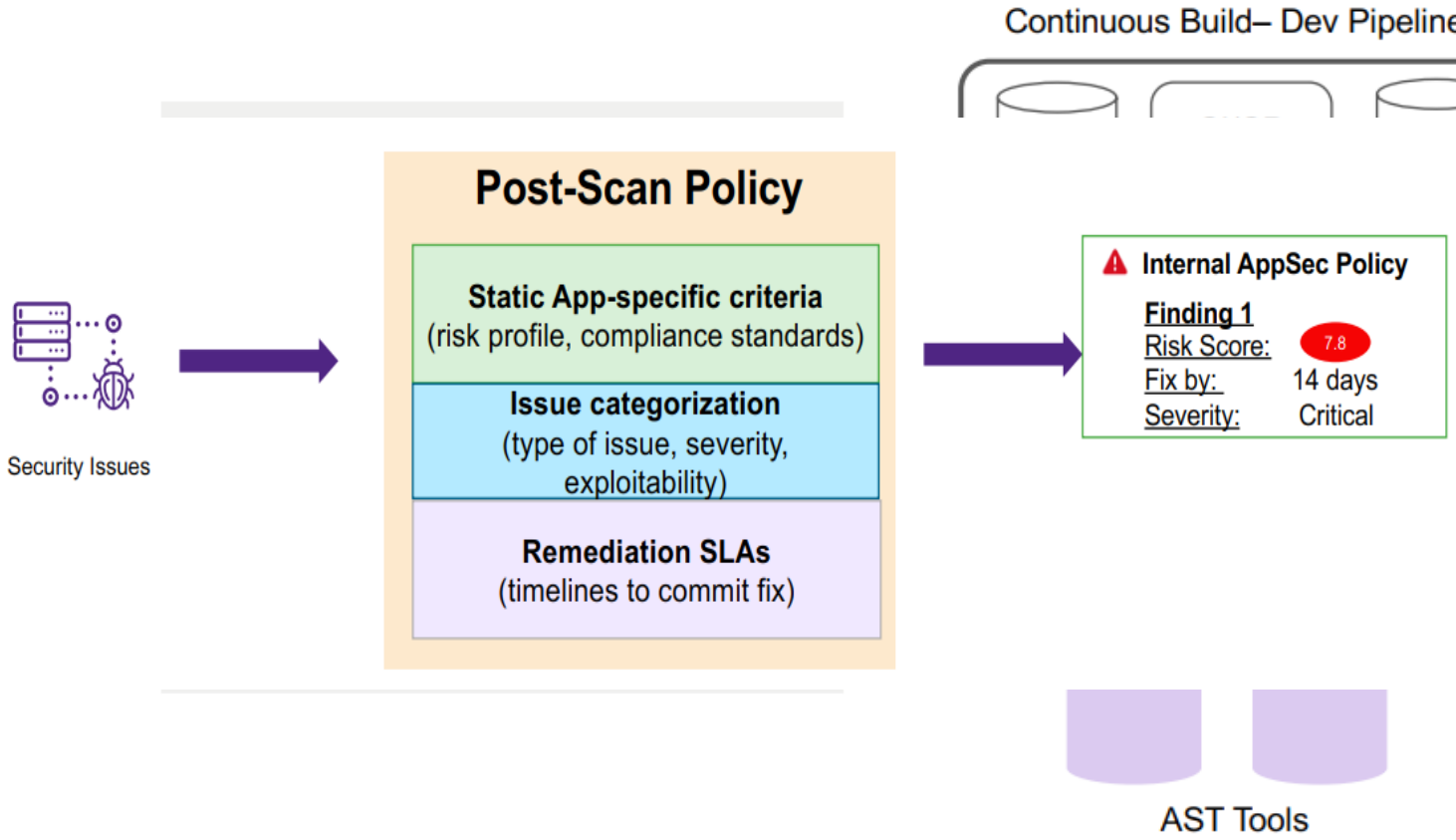
- Orchestrates in- and out-of-band tests from commercial, third-party, and open source tools
- Integrate into dev pipelines with a small connector

Optimize Test Execution

- Runs the right test at the right time based on:
  - AppSec Policy-as-code
  - Application risk profile
  - Code changes
  - SDLC events

Maintain Pipeline Velocity

- Is a separate purpose-build pipeline, optimized for security policy



Presentation content source: Synopsys

Insight Management

Actionable insights into AppSec risks across the organization

Correlation and Prioritization

- Identify and focus on issues with the highest business risk

Consolidated Dashboard

- View of AppSec activities and software risks across your entire organization

AppSec System of Record

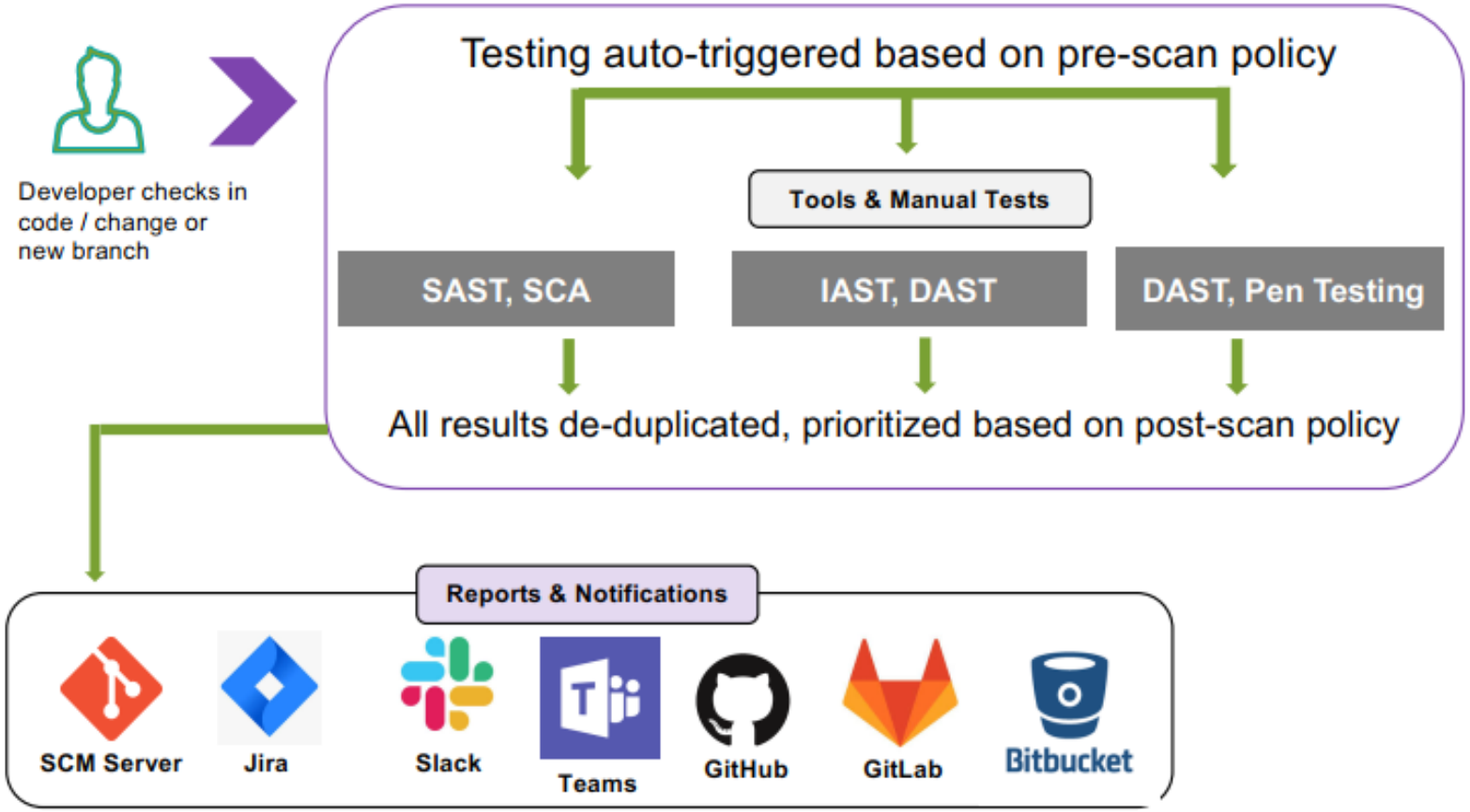
- Track when software was tested, what was found, and when/if it was fixed

Presentation content source: Synopsys

Drive Governance at Scale

Enforce your security runbook from a central point of control

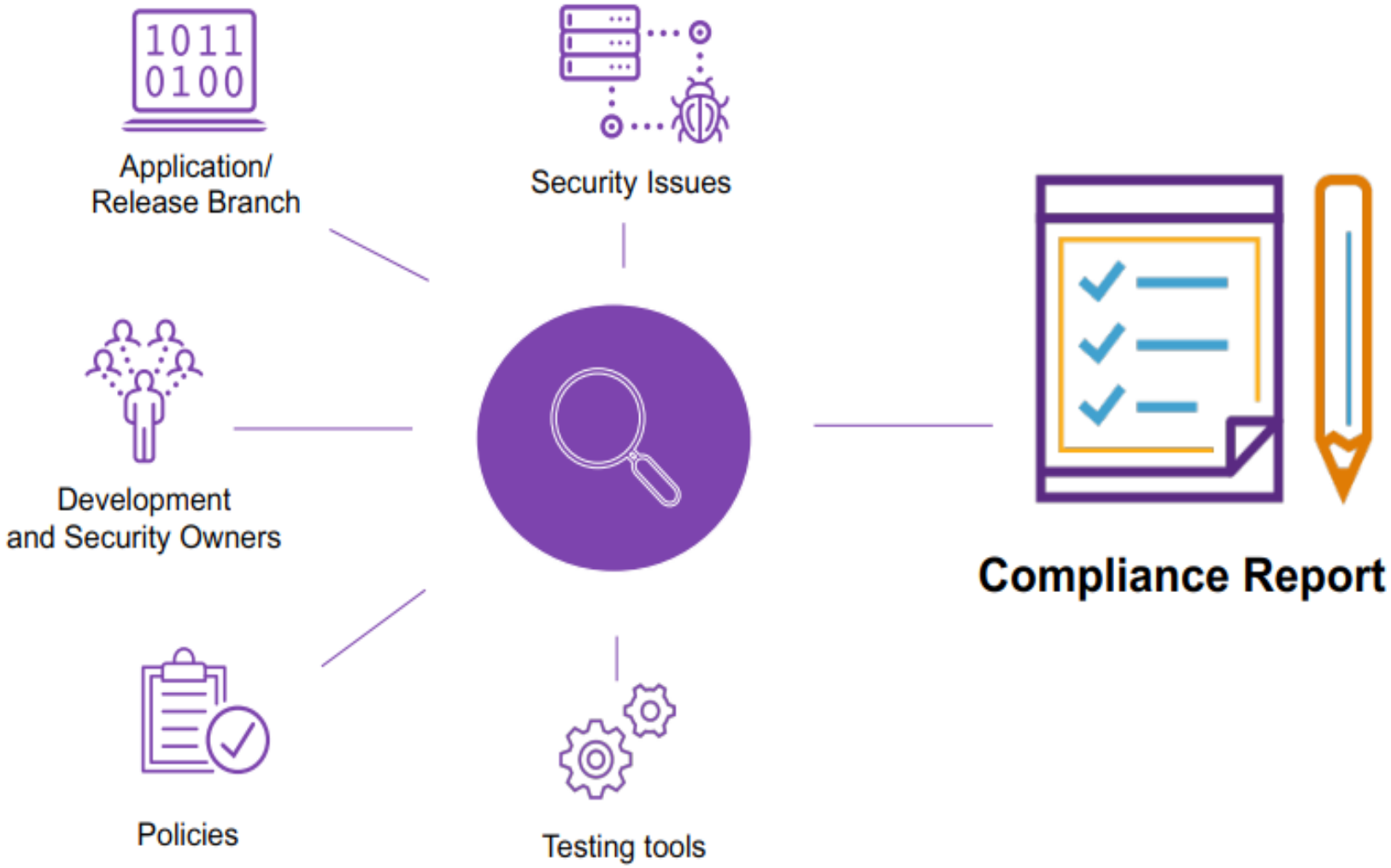
Orchestrate consistent testing and remediation through pushing policies and actions from one place.



Presentation content source: Synopsys

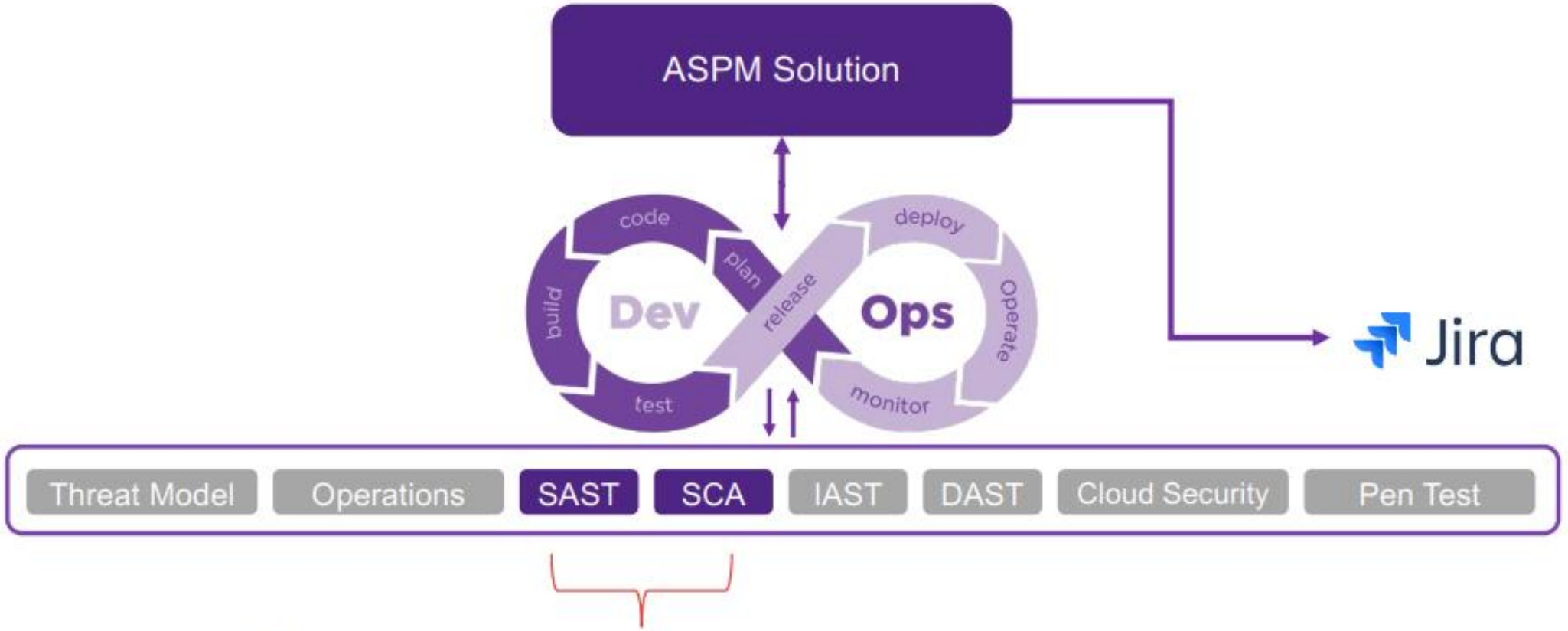
Continuous Compliance Monitoring

Map and audit findings per regulatory compliance violations



Presentation content source: Synopsys

Built-in security testing, accelerate risk attestation

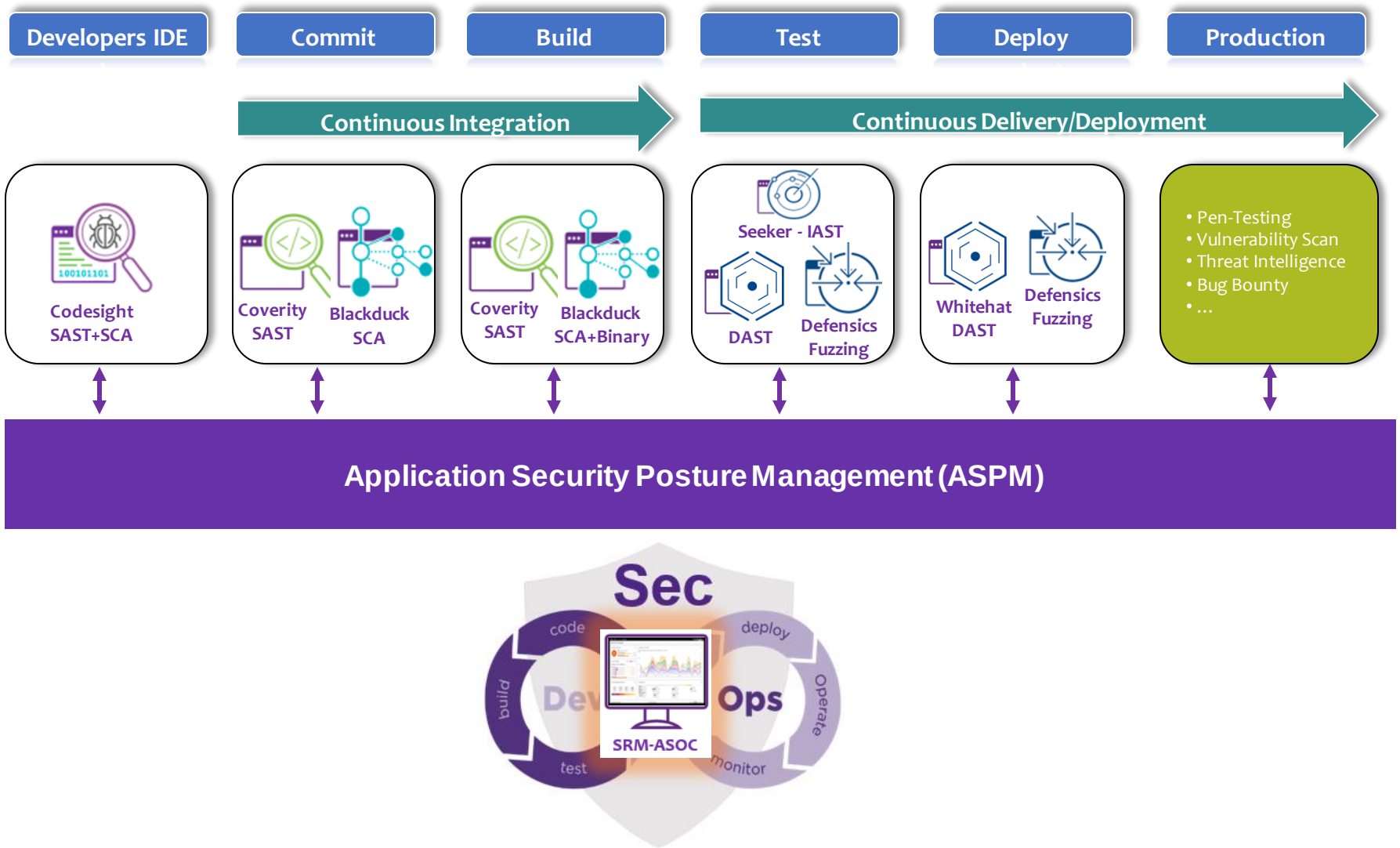


Accomplish 80% of your testing needs, and dynamically discover issues and software assets

Presentation content source: Synopsys

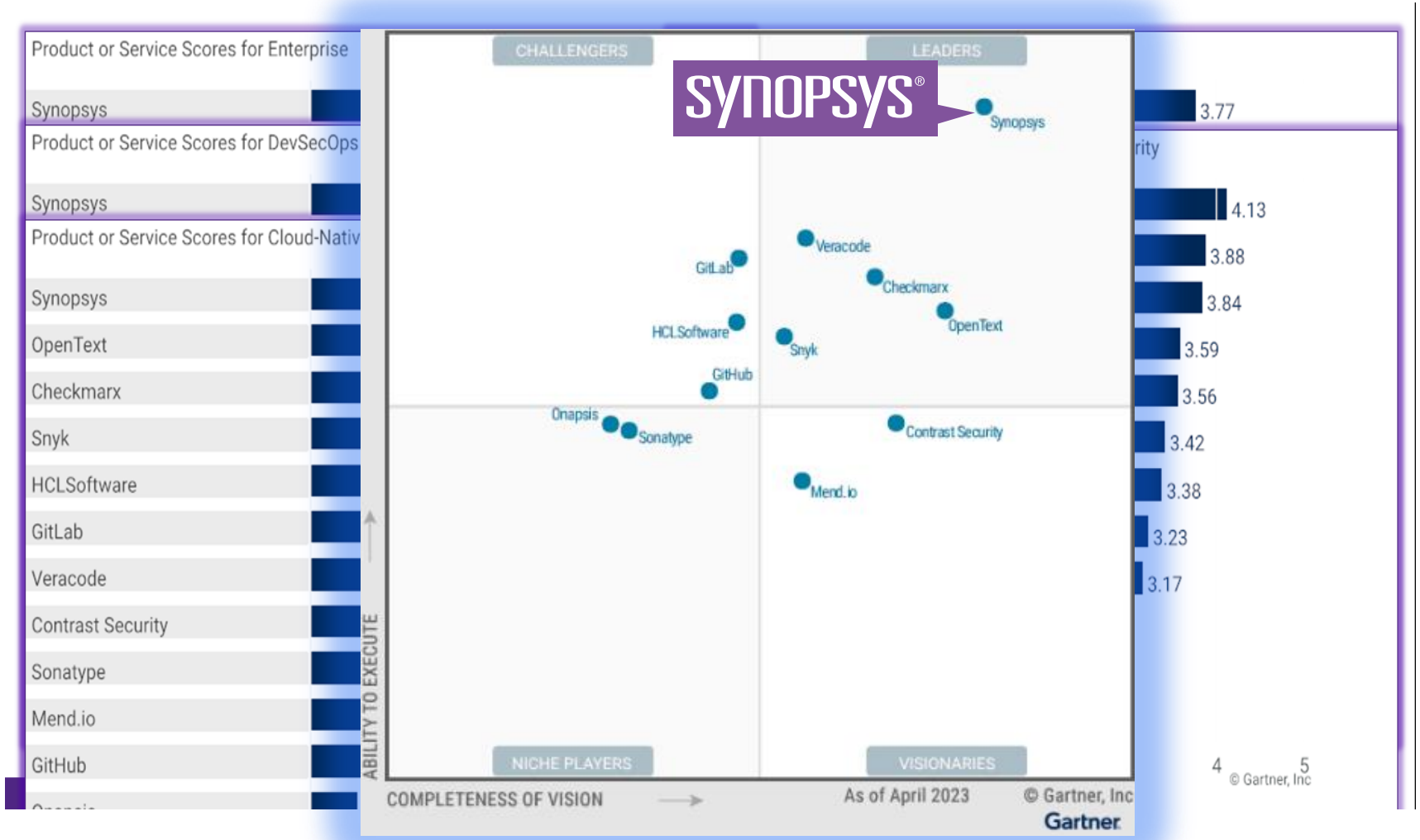
SYNOPSYS SRM QUICK DEMO

Synopsys SRM In DevSecOps Pipeline



Presentation content source: Synops

The Recognized Lead In End-to-End Application Security



Presentation content source: Synopsys

Application security testing is about outcomes, not tools

Build security into DevOps

- Enable developers to build better software
- Maintain velocity while ensuring security
- Focus teams on the issues that matter most

Secure your software supply chain

- Secure and manage OSS dependencies
- Comprehensively test any type of software
- Immediate respond to supply chain attacks

Manage AppSec at Enterprise Scale

- Align people, processes, and technology
- Consolidate AST processes to lower TCO
- Deliver an organizational view of software risk

Presentation content source: Synopsys

Thank you

mi2jsc@mi2.com.vn www.mi2.com.vn

WEBINAR SERIES

Webinar topic

WEBINAR 1: UNLOCKING THE POWER OF DEVSECOPS: WHAT IT IS - HOW IT WORKS - WHY IT MATTERS?
WEBINAR 2: SOFTWARE SUPPLY CHAIN RISKS & SBOM
WEBINAR 3: MASTERING DEVSECOPS WITH ASPM/SRM: ELEVATING YOUR APPLICATION SECURITY SKILL