

Application Security in the Age of Coding Agents

Where Black Duck Signal fits — and why the broader AppSec portfolio still matters in an AI-assisted SDLC.

Signal provides the first fast feedback loop. Coverity, SCA, Seeker, DAST and Polaris add depth, validation and governance.

Why AI-assisted development changes the AppSec landscape

Teams are not only writing code faster. They are compressing security decisions across the SDLC.



Speed

The same team can now produce much more code in much less time.



Risk

Defects, unsafe patterns and problematic dependencies can spread earlier and further.



Reaction

Security must move closer to code generation without losing depth later in the pipeline.

In AI-assisted development, the biggest challenge is not running scans. It is getting useful feedback to the right team quickly enough.

AI coding agents compress the SDLC — and amplify software risk

What changes when code is generated faster?

- Human review time per change shrinks, while code volume grows.
- Security defects, unsafe patterns, and bad dependencies can be introduced earlier and more often.
- License and copyright exposure becomes harder to spot when generated snippets move quickly into repos.
- Traditional AppSec gates still matter — but they must keep pace with AI-assisted delivery.

Speed

Code lands faster than security review cycles can traditionally handle.

Noise

Generic AI guidance often produces too many low-value findings and weak prioritization.

Context

Teams need issue context, exploitability signal, and remediation guidance in workflow.

Governance

Portfolio controls still need SAST, SCA, DAST, IAST, fuzzing, and policy-based orchestration.

Black Duck positions Signal as the new AI-native front line, with the established portfolio enforcing depth across the SDLC.



Black Duck Signal™

Agentic AI AppSec for AI-powered software development

Signal combines ContextAI™ with 20+ years of human-curated AppSec intelligence to help teams find and fix issues without the usual noise or AI hallucinations.

**MCP + coding
assistant**

Real-time analysis

- Analyze new code instantly and fix issues before code is committed.

AI-powered development fit

- Run security scans with natural language prompts in coding assistants and IDEs.

Agentic investigation

- Route and prioritize issues so teams focus on the code that matters most.

Language coverage

- Built for modern languages, frameworks, and AI-assisted development workflows.

Operational role

- Signal secures the earliest AI-generated code path; the broader Black Duck portfolio validates, governs, and scales trust across the rest of the SDLC.

Polaris Assist

AI Application Security Assistant

Polaris

Integrated SaaS AppSec Platform

fAST Static

fAST SCA

fAST Dynamic

Software Risk Manager

ASPM

Coverity
SAST

Black Duck
SCA &
Supply Chain

Seeker
IAST

Continuous
Dynamic
DAST

Defensics
Fuzzing

Integrations

IDE

SCM

Build/CI

Workflow

3rd Party AST

Container/Cloud

Services

Program Consulting

Testing

Training

Audits

Customer Success

Polaris Assist
AI Application Security Assistant

Polaris
Integrated SaaS AppSec Platform

fAST Static

fAST SCA

fAST Dynamic

Software Risk Manager
ASPM

Coverity
SAST

Black Duck
*SCA &
Supply Chain*

Seeker
IAST

**Continuous
Dynamic**
DAST

Defensics
Fuzzing

Integrations

IDE

SCM

Build/CI

Workflow

3rd Party AST

Container/Cloud

Services

Program Consulting

Testing

Training

Audits

Customer Success



SAST - Coverity

In-depth static analysis for secure code that's free of defects



Comprehensive Analysis

- Identifies both code quality and security issues
- Uncovers complex issues that span files and libraries
- Broad and deep language and framework support



Developer Velocity

- Accurate results let developers focus on business value
- Fast scans on PR/MR to find defects early in the SDLC
- Easy triage and prioritization of results



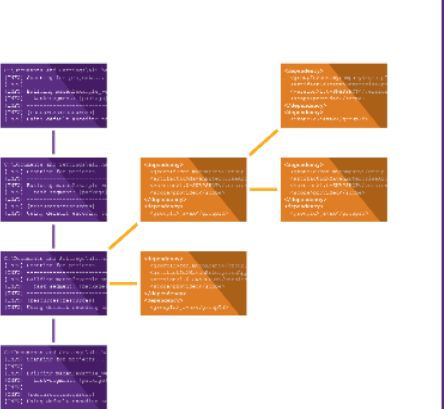
Enterprise Scale

- Thousands of developers
- Thousands of projects
- Apps with millions of lines of code

Black Duck SCA - multi-factor scanning ensures complete discovery

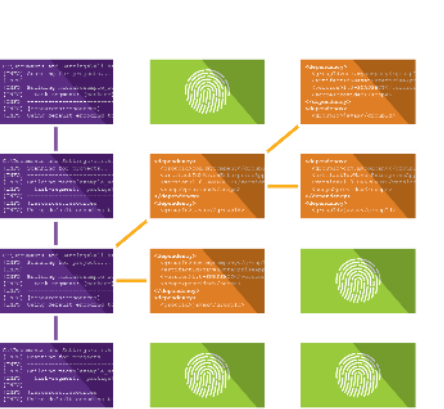


Dependency analysis



- Fast and shallow
- Package managers

Codeprint analysis



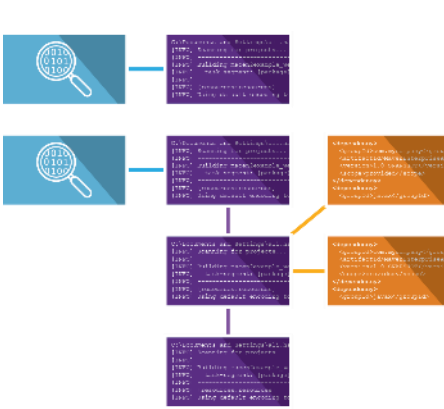
- Catches modified open source
- C/C++

Snippet matching



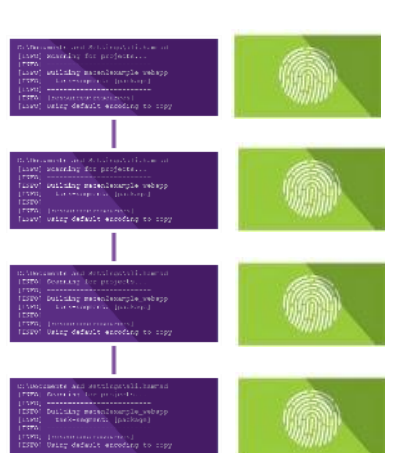
- Scans compiled code
- Containers

Binary analysis



- Identifies snippets of open source

Custom component detection



- Non-OSS, internal, or third-party components

Complete Software Bill of Materials (SBOM)

DAST - Continuous Dynamic

Continuous Dynamic provides industry-proven web application security testing for modern and traditional websites, web applications, and frameworks.



Full Visibility

Delivers full visibility and the front line of defense for secure DevSecOps



Intelligent Prioritization

Automates the prioritization of results based on machine learning



Continuous and On-Demand Risk Assessments

Provides continuous and on-demand scanning to automatically check for vulnerabilities



Production-Safe

Scans production servers safely and without causing any downtime - saving valuable time, resources, and cost

Polaris Assist
AI Application Security Assistant

Polaris
Integrated SaaS AppSec Platform

fAST Static

fAST SCA

fAST Dynamic

Software Risk Manager
ASPM

Coverity
SAST

Black Duck
*SCA &
Supply Chain*

Seeker
IAST

**Continuous
Dynamic**
DAST

Defensics
Fuzzing

Integrations

IDE

SCM

Build/CI

Workflow

3rd Party AST

Container/Cloud

Services

Program Consulting

Testing

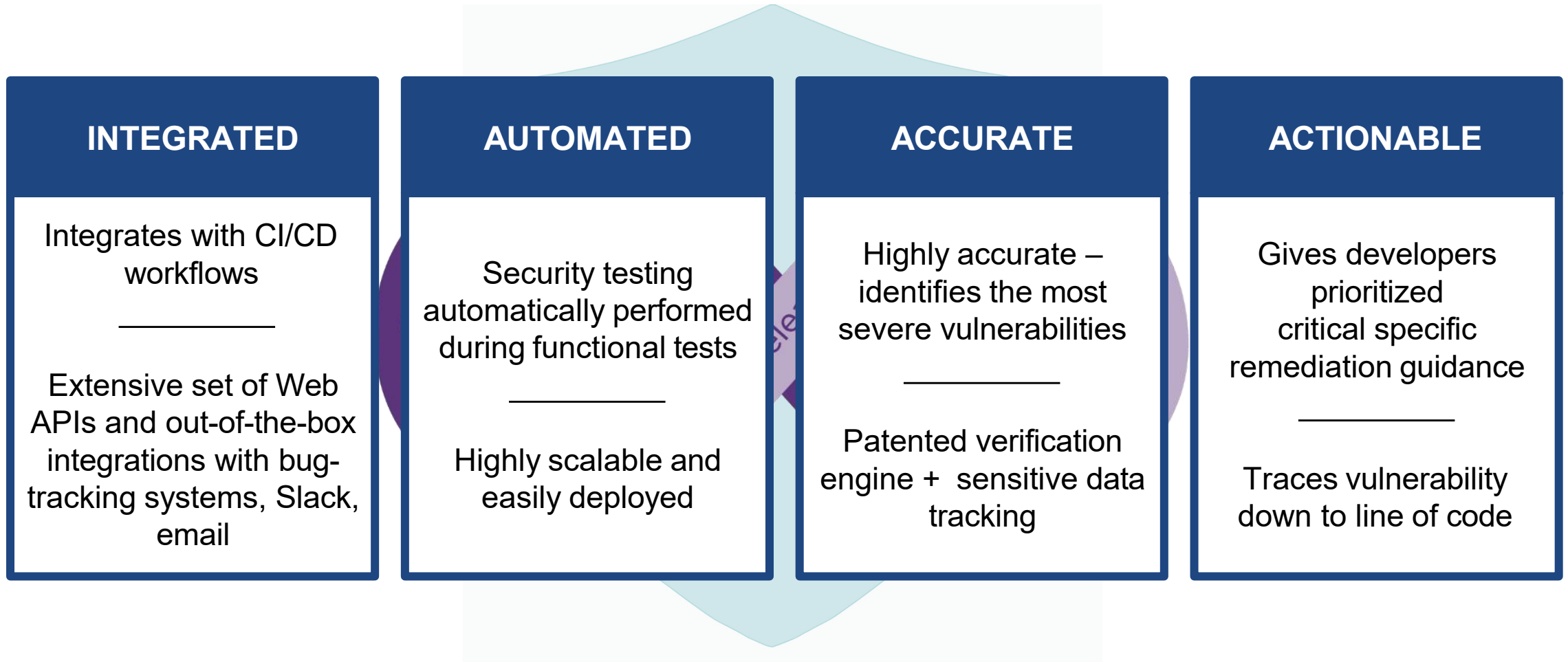
Training

Audits

Customer Success

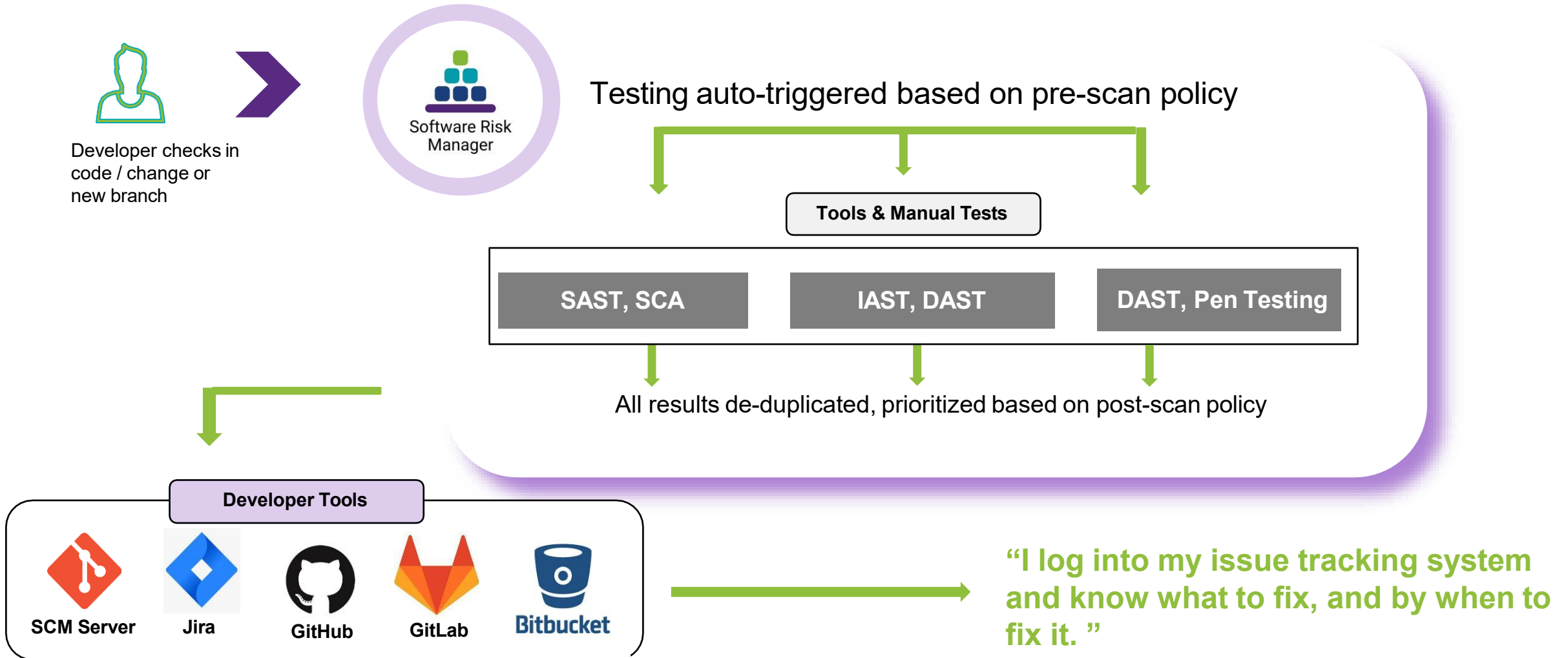
Seeker – IAST, Interactive Application Security Testing

*Accurate, easy-to-use enterprise-scale IAST that identifies **and** verifies web application vulnerabilities in real time*





The Developer Dream with **Software Risk Manager**



Uncover vulnerabilities across all your languages

Broad and deep support for more than 20 languages

Language Coverage



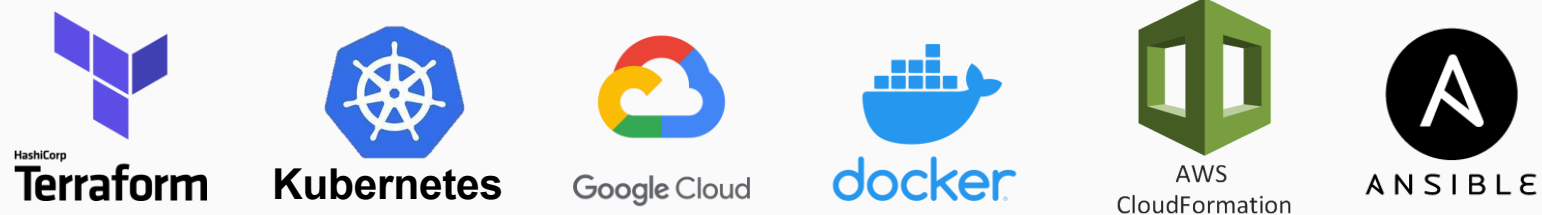
Support for Popular Compilers

- ☐ ARM C/C++
- ☐ Clang
- ☐ GNU GCC/G++
- ☐ Intel C++ for Windows
- ☐ JDK for Mac OS X
- ☐ Microsoft Visual C++
- ☐ Nvidia CUDA (NVCC)
- ☐ Renesas C/C++
- ☐ SONY PS4 SDK
- ☐ Sun (Oracle) CC
- ☐ Sun/Oracle JDK
- ☐ Wind River C/C++

Deploy cloud environments with confidence

IaC scans identify misconfigurations to prevent vulnerabilities in cloud environments

Infrastructure-as-Code



File formats:

JSON	YAML	HCL	HTML	XML	plist
TOML	Properties	Vue template	JSX	TSX	

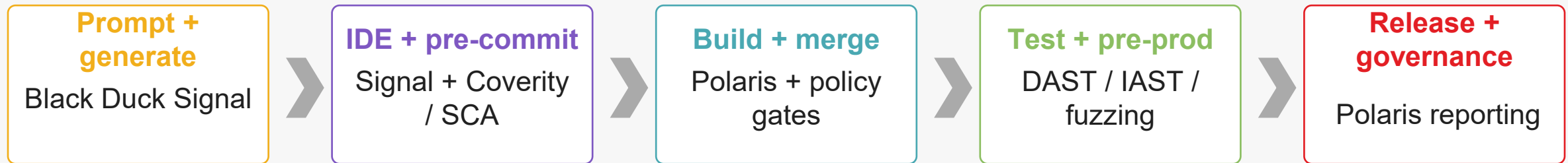
Supports CIS Benchmarks for Cloud Environment

- Access controls
- Data protection
- Hardcoded secrets
- Network settings
- Infrastructure configuration
- Software settings



Securing the AI-assisted SDLC with Black Duck

End-to-end coverage



Developer outcome

- Faster feedback, earlier remediation, less late-stage rework.

Security outcome

- Better prioritization, deeper validation, and clearer policy enforcement.

Business outcome

- AI adoption without surrendering AppSec depth, auditability, or governance.

Köszönöm a figyelmet!

blackduck@clico.hu