SYNOPSYS®

Intelligent Orchestration for Financial Services

The Right Security Testing at the Right Time

The customer

The company is a major financial services enterprise and Fortune 500 member with over $2 trillion in assets under management. Its databases hold sensitive personal information on millions of U.S. citizens. As with all members of the financial services industry, application security testing is critical for this organization—as is ensuring that developers aren't slowed by the testing process.

The continuous integration / continuous deployment (CI/CD) environment includes:

- Synopsys Black Duck® SCA to detect vulnerabilities in open source dependencies
- Amazon Web Services cloud computing platform
- Jenkins automation server for CI/CD builds, testing, and deployment
- Micro Focus Fortify Static Analysis to detect security defects in proprietary code
- Contrast Assess interactive application security testing for runtime security analysis
- Prisma Cloud from Palo Alto Networks for preproduction container security image assessment
- OWASP ZAP for dynamic security testing
- Java, JavaScript, and Python coding languages

The challenge

Integrate application security analysis from multiple tools into the DevOps pipeline while maintaining development velocity. Develop a purpose-built, cloud-based CI/CD pipeline that automatically performs the right security tests at the right time based on software development life cycle events and defined policies.

The solution

Intelligent Orchestration from Synopsys is a risk-based and adaptive application security test orchestration solution optimized to match the speed of development teams while ensuring that governance, compliance, regulatory, and other policies are applied as required.

Imagine an automated application security test orchestration solution in which you configure the rules for the security testing applications you use, ensuring that you get the right analysis at the right time. An intelligent solution that understands code change significance, the risk profile of an application, and which security testing policies to apply for that application. An orchestration solution that automates the decision-making process on whether specific security testing should be skipped or applied—and that provides continuous feedback to your DevSecOps teams through notifications on Slack, Teams, Jira, or whatever platform you use.

This ideal application security test orchestration solution would be tool-agnostic and work with all commercial static, dynamic, interactive, and software composition analysis tools, as well as with open source tools such as OWASP ZAP, SpotBugs, and OWASP Dependency Check. And it's extensible, scalable, and very adaptable.

That solution is here today: Intelligent Orchestration from Synopsys.

Intelligent Orchestration: Experience guided by intelligence

"Application testing has to be fast, and it can't be intrusive," notes the senior technical lead of the application security initiative at a financial services enterprise, who asked that the organization not be named because of the sensitivity of the personal data it stores. "Most of all, developers don't want time wasted on more security testing than needed."

"What we need is the right test performed at the right time, getting the right amount of data, and getting that data at the right time," he continues. "If you've made a trivial change to a web application—modified a CSS page, for example—another static analysis test probably isn't needed at that time. If an open source dependency hasn't changed, there's probably no need to do an SCA (software composition analysis) scan."

"We commissioned Synopsys consultants to help us develop an application security test orchestration solution that looks at the significance of code changes our developers make and the risk profile of the application they're working on. In essence, we wanted to build an automated traffic cop to direct our security activities. What we now call Intelligent Orchestration moves those activities in the right direction without causing traffic snarls."

"Moreover, Intelligent Orchestration is prescriptive. Think of a doctor visit. Rather than conducting an MRI scan each time you visit, a doctor evaluates your current state of health and then applies whatever treatment is needed. Maybe an MRI is in order; maybe a less dramatic solution is called for. The decision is based on the doctor's experience guided by their intelligence. With IO, 'experience' equates to 'policy' and 'intelligence' to 'code'."

Security policy as code

All organizations have security policies that define rules. For example, "externally facing critical applications require a manual penetration test every 90 days." In most organizations, those policies are enforced by a security group—sometimes one person—and it often tends to disrupt production schedules. Unless someone is keeping a close eye on the policies and is carefully synched with the DevOps team's production pipeline, there's often a last-minute scramble to meet the security requirements. "We only have four days to production. Who's going to do a penetration test? Who's going to do a manual code review within the next four days?"

With Intelligent Orchestration, security policy is translated into code and applied into a dedicated CI pipeline that runs in parallel with your existing build and release pipeline. For example, if the security policy requires a pen test for an application every 90 days, Intelligent Orchestration triggers a heads-up notification to the team after 80 days, or whatever time frame the policy indicates. Most organizations have some internal technology where they store their policies. Synopsys helps the client's security team transform those manual policies into code that is enforced by the automated Intelligent Orchestration solution.

Results: Less confusion, less stress on resources

"Every time we have a release candidate or a pull request, it's run through our application security test orchestration pipeline," notes the senior technical lead of Synopsys' FSI client. "The net benefit we've found is less extraneous testing, which translates into less data to manage, less confusion trying to reconcile data from duplicate tests, [and] ultimately less stress on our resources. Like most organizations, our resources are already stretched. Intelligent Orchestration has allowed us to focus on higher-value tasks."

"When we onboard an application, we include its risk profile into Intelligent Orchestration. Things like: What data does it manage? Is it a long-running app or something that runs for a few milliseconds? What's the attack surface? A low-risk application may not need to be run through frequent security checks. Intelligent Orchestration risk profiling also has become a big factor in our relationship with our auditors. It's hard to defend decisions to an auditor without documentation on how those decisions were made. Intelligent Orchestration provides detailed application risk profile information, logs when and why a testing decision was made, and shows the outcome from that decision. It's all documented—and that documentation sometimes almost gets us a smile from the auditor."

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