SYNOPSYS®

GUIDE

Faster IV&V and acceptance testing in defense programs

Best practices checklist

The complexity and high-stakes nature of U.S. Department of Defense (DOD) networks and weapons systems demands robust and strategic handling of application security. The multitude of departments across the government each have their own way of performing evaluation and testing activities. A general mandate that reaches across all departments, however, is independent verification and validation (IV&V). IV&V entails an independent assessment of a system and encompasses three key testing criteria. The first is an analysis to ensure the system is performing its intended functions correctly, the second is an analysis to ensure it does not perform any unintended functions, and the third is a general analysis of its quality and reliability. The multifaceted nature of this testing necessitates that auditors and testers be armed with proven application security tools integrated within their supporting test regimes and processes, in order to help reduce the time and effort needed to address risks attributable to exploitable software.

IV&V and acceptance testing challenges

The complexity of modern applications complicates the associated testing requirements and increases the difficulty for security teams. Modern applications are composed of a variety of elements, from custom/proprietary code to open source components and application configuration. This complexity poses key challenges for IV&V and audit and testing teams:

1. Scanners find bugs but don't prevent them.
2. Test criteria primarily focus on functional correctness, not actual exploitability of applications.
3. Auditors are rarely experts.

The result is a constant tradeoff between prioritizing security, risk, functionality, and schedule.

Further compounding these challenges are the key performance parameters (KPPs) that apply to defense programs. A team's success lies in its ability to actively manage a system's configuration to counter vulnerabilities at tactically relevant speeds. As soon as a system is fielded, teams are expected to fully understand the level of risk being accepted; teams must actively prioritize and buy down mission risks and test/audit.

The solution: Application security testing at the speed of IV&V

Application security tools are critical allies to any security team, enabling automated identification of vulnerabilities and compliance to security standards. Tools including static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), and interactive application security testing (IAST) should all be considered when addressing IV&V challenges. With its robust AppSec portfolio, Synopsys helps IV&V and audit teams streamline and pinpoint their AppSec activities, improving overall security stance and ensuring that stringent DOD requirements are met.

Using multiple AppSec solutions is an application security best practice. By employing a variety of methods that each involve separate activities and different phases of the software development life cycle (SDLC), AppSec testers can be sure they have the most comprehensive view of their security posture. Since each solution specializes in expertly identifying potential vulnerabilities through alternate methods, a combined testing approach offers the most comprehensive AppSec security methodology.

Using a combination of Synopsys tools and professional and managed services can help testers easily overcome the aforementioned challenges.

Coverity® SAST helps development teams ensure compliance to a wide range of quality and security standards. Coverity provides best-in-class identification of code quality issues, and the most comprehensive coverage of standards related to safety, security, and reliability (e.g., MISRA, CERT C/C++, CERT Java, DISA STIG, ISO 26262, ISO/IEC TS 17961, and AUTOSAR), as well as security standards (OWASP Top 10, CWE Top 25, and PCI DSS). Developers get high-fidelity incremental analysis in seconds as they code, allowing them to fix any issues prior to the build-test phase. Coverity enables teams to fix software defects quickly, easily, and correctly by supplying all the context, technical details, and remediation advice to fix risk-prioritized code issues and prevent potential vulnerabilities (addressing challenge 1 above). Context-specific eLearning (detailed below) comes standard with Coverity.

Black Duck® SCA provides enhanced data about open source vulnerabilities—this is data that goes beyond the detail included in the National Vulnerability Database. It includes Black Duck Security Advisories, which provide deep technical details, remediation guidance/workarounds, and other important risk metrics. Data is sourced, curated, and analyzed by the Synopsys Cybersecurity Research Center, focusing on the components and vulnerabilities with the greatest impact on major software components and our customers. Remediation advice helps teams actually perform fixes as needed, allowing them to prevent potential vulnerabilities (addressing challenge 1 above).

Seeker® IAST provides visibility into your web application security posture and helps identify vulnerability trends against compliance standards (e.g., OWASP Top 10, PCI DSS, GDPR, CAPEC, and CWE Top 25). Seeker enables security teams to identify and track sensitive data to ensure that it's handled securely and not stored in log files or databases with weak or no encryption. Seeker's seamless integration into continuous integration / continuous delivery workflows enables fast, interactive application security testing at DevOps speed. Unlike

other IAST solutions, which only identify security vulnerabilities, Seeker can also determine whether a security vulnerability (e.g., cross-site scripting or SQL injection) can be exploited, providing developers with a risk-prioritized list of verified vulnerabilities to fix in their code immediately (addressing challenge 2 above).

Synopsys eLearning helps equip development teams with the skills and behaviors needed to produce more secure software. Challenges with the skill level of testers are easily mitigated through eLearning, regardless of the tester's skill level. Interactive digital courseware is designed to help development teams learn and implement best practices for secure coding. More importantly, as testers use Coverity SAST, Seeker IAST, and Code Sight™, Synopsys' portfolio integrations mean that eLearning can recommend specific lessons based on issues identified by these tools, in real time. Developers don't need to be security experts (addressing challenge 3 above).

IV&V application security best practices checklist

With its extensive DOD support history, the Synopsys team has a clear understanding of software weaknesses and shortcomings. To help guide your IV&V and acceptance testing practices, we developed a detailed checklist of important security considerations to address when improving or implementing application security.

✓	Consideration category	Best practice
	Tools	**Automate testing** to gain efficiencies throughout the software development life cycle in acceptance testing and IV&V/audit.
		Use a variety of AppSec tools to responsively scale to changes in software and release cycles.
		Address the pervasiveness of open source software by providing a tool that defines policies for open source use and automates and enforces them.
		Use tools that offer integrated reporting of exploitable software, including both weaknesses and vulnerabilities, and that prioritize technical risks, which helps better enable informed test and approval processes.
		Use tools that don't require developers, testers, and auditors to be security experts. Tools with security checkers "under the hood" can catch security defects like a spell-checker catches misspellings. This drives savings while rapidly mitigating risks attributable to exploitable software.
	Activities	Focus on prevention and alignment with risk mitigation.
		• Improve coding to prevent bugs that put systems at risk. • Integrate best practices with security guidance. • Provide visibility into risk before it enters the codebase. • Enable developer education to minimize errors.
		• Bring information to the desktop to enable mitigation. • Make guidance available within the developers' tools. • Provide a consistent and validated source for guidance. • Deliver contextual guidance as the code is written.
		• Give development responsibility and tools. • Lower risk and reduce delays by providing better knowledge. • Reinforce security and policy training. • Reduce friction through self-correction prior to security testing.
		Generate software Bills of Material for IT assets.
		Align DevSecOps with risk management.

Synopsys solutions cover the entire application

SEEKER®
Interactive Analysis
Pinpoint exploitable weaknesses (sources of vulnerabilities) and data protection issues in web applications.

COVERITY®
Static Analysis
Find and fix security weaknesses (sources of vulnerabilities) and quality issues in proprietary code as it's being developed.

DEFENSICS®
Protocol Fuzzing
Detect weaknesses and vulnerabilities exposed through protocols in the API/ service interface.

BLACK DUCK®
Software Composition Analysis
Detect and manage open source and third-party component risks in development and production.

Synopsys offers a complete suite of application security solutions that are targeted to cover the entire application. To learn more about how Synopsys can help improve your IV&V and acceptance testing programs, view our recent webinar, or visit our website for more details. Check out our broad portfolio of aerospace and defense solutions.

SYNOPSYS®

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. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

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