APRIL 2022

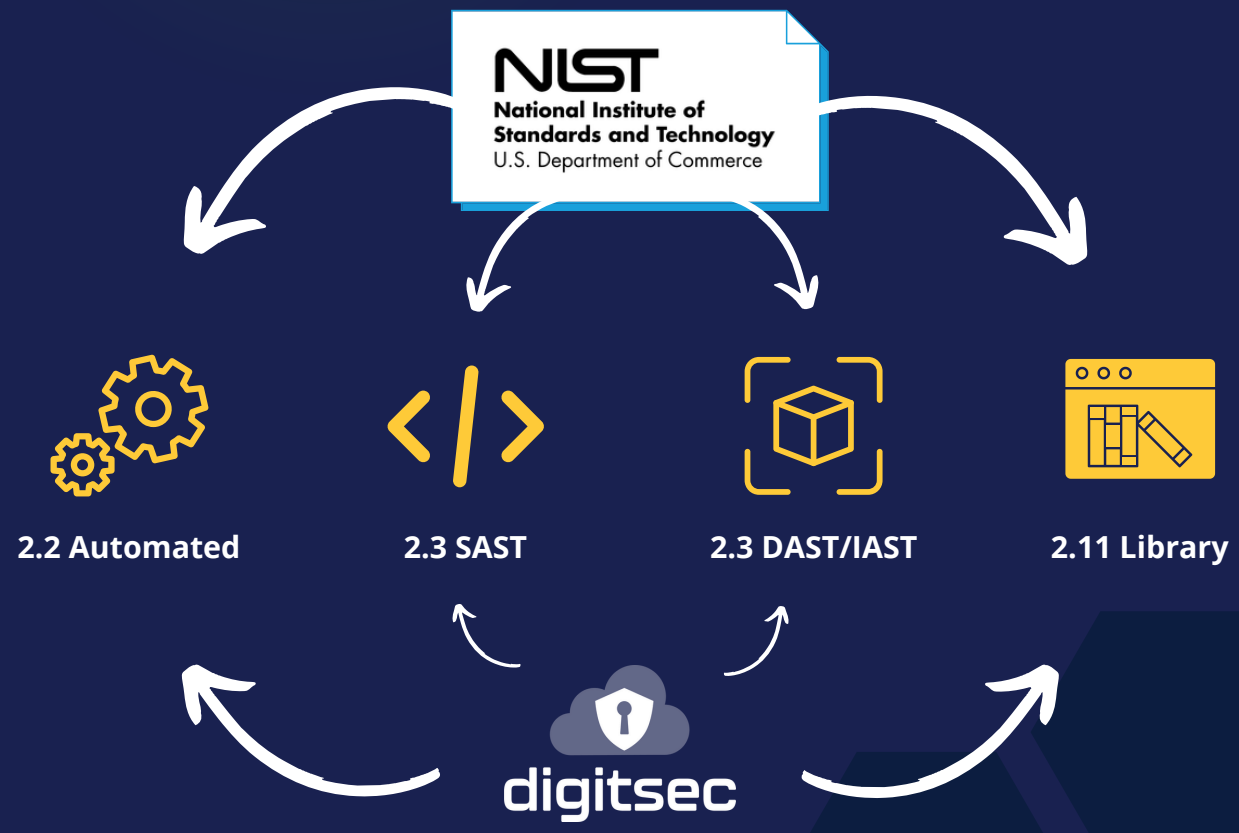
DigitSec Helps Salesforce Users Comply With NIST Standard for Software Testing

DigitSec's powerful security scans help meet requirements for NISTIR 8397 "Guidelines for Minimum Standards for Developer Verification of Software."

In recent weeks, the global political environment could be characterized as fluid and dynamic. While international conflict has been present in our history for a long time, adversarial confrontations in cyberspace have increasingly become a characteristic of both cool and hot conflicts.

On May 12, 2021 the Biden Administration addressed this by issuing Executive Order 14028, directing the National Institute of Standards and Technology to recommend minimum standards for software testing. In October, NIST issued NISTIR 8397, Guidelines for Minimum Standards for Developer Verification of Software.

DigitSec is designed to assist Salesforce Developers address potential security vulnerabilities in their Org Configurations and custom code. **DigitSec can be a tool that teams use to help meet this standard by providing automated, SAST, IAST and external library testing.** We feel that it is important to highlight these components of the guidelines as they are truly best practices to maintaining a strong cybersecurity defense.



DigitSec helps satisfy four testing requirements in NISTIR 8397.

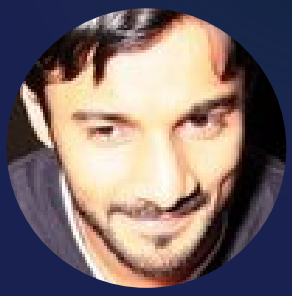
First, the recommendation for automated testing. This is fundamental to best practice. At a very basic level, automated testing means that teams don't have to deploy significant staff resources to review code and config. **By building testing systems that can execute on-demand or on a set schedule, teams are able to focus on meeting functional requirements within specific security standard guardrails.**

Moreover, automated testing also establishes a consistent objective standard that is not subject to the expertise and engagement of a human tester. Teams can rely on tests to identify vulnerabilities during their Software Development Lifecycle and to consistently check deployed code for new vulnerabilities.

Second, the Guidelines are clear in advising that teams link static application security testing (SAST) with dynamic application security testing (DAST/IAST). Static code scanning is an efficient method to look for top bugs and weaknesses in written code very quickly. But, it is critical to test that code in the larger context of an active, deployed environment to see how it interacts with other code objects.

NIST illuminates the fact that this type of testing surfaces true-positive vulnerability findings, providing developers with an execution trace indicating the failure and the input that generated it.

Finally, it's critically important to evaluate included libraries to ensure that these external resources are just as secure as the locally developed code. While your team may have written top-quality, secure code, a new vulnerability in an external library might be reported at any time. By continually monitoring databases of known vulnerabilities and relying on automated checks, organizations can maintain constant vigilance.



"Often organizations customizing SaaS platforms do not realize that these platforms must be evaluated according to the NIST standard. These SaaS platforms can be vulnerable to the same web based attacks that affect common web connected applications. Ultimately, it is the responsibility of the organizations to protect their SaaS apps and data."

-Waqas Nazir, CEO at DigitSec

It doesn't matter whether the threat of an attack or a security breach comes from a ransomware gang or a malicious state actor, organizations must be proactive about protecting their systems and data.

DigitSec urges organizations to review the full scope of these guidelines and to treat them as they have been labeled: as a *minimal* standard. Every organization needs to do their part to keep the internet safe and secure.

digitsec

DigitSec, Inc.

92 Lenora St. #137
Seattle, WA 98121 USA

info@digitsec.com
+1 206-659-9521

To Learn more visit DigitSec.com

Read 2022 eWeek review of DigitSec

Case study: How InCountry accelerated development while saving 1000+ dev hours