aws | Deloitte.

Software Supply Chain Security

Contents

Software supply chain security 3

Executive order 104028 overview 3

Secure software development framework 3

Attestation of conformity 4

Risk-based approach to attestation 4

Enhanced validation methods 4

Artifacts of conformance 5

High-level artifacts 5

Low-level artifacts 5

Critical software 5

Timeline and next steps 6

Next steps for software providers 6

Significant timelines 6

Deloitte difference 7

Software supply chain security

Rapid economic and technical advances require organizations to operate in a digitally interconnected world. While interconnectivity offers several benefits, like reduced costs, scalability, and productivity, interconnectivity also introduces new risks to supply chains. Recent cyberattacks and zero-day exploits, including Log4J and SolarWinds, have highlighted the lack of transparency organizations have across their software supply chains.

The inherent threats within software supply chains have motivated the US government, in partnership with many in the software industry, to develop a secure software development baseline to provide guidance and establish accountability across the federal software supply chain.

Executive order 104028 overview

Executive Order (EO) 14028 "Improving the Nation's Cybersecurity" was released on May 12, 2021, as a reaction to the critical impacts of recent software supply chain attacks. The EO directed the National Institute of Standards and Technology (NIST) to identify or develop standards, tools, leading practices, and other guidelines to enhance software supply chain security.

Secure software development framework

NIST, in response to the EO, developed the Secure Software Development Framework (SSDF), National Institute of Standards and Technology Special Publication (NIST SP 800-218), updated the Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1), and has provided a multitude of additional guidance for federal procurers of software.

EO 14028 places the responsibility on Federal agencies to ensure software vendors have implemented the SSDF's secure software development practices before using the software on government networks. The SSDF serves as a common reference framework for organizations to communicate to federal agencies how they have implemented secure software development practices throughout the software development life cycle. However, the SSDF does not prescribe specific implementation requirements.

Organizations with specific implementation questions should refer to the SSDF's informative references, such as NIST SP 800-53 Rev. 5 and NIST SP 800-161 Rev. 1, which provide guidance for implementing SSDF practices and tasks.

Attestation of conformity

Office of Management and Budget (OMB) released Memo M-22-18, dated September 14, 2022, which directs federal agencies to begin collecting attestations from software vendors of their conformance to the SSDF beginning in September 2022. For critical or higher-risk software acquisition, however, OMB encourages agencies to consider additional enhanced software validation mechanisms beyond the mandatory self-attestation.

Self-attestations of conformance to the SSDF practices will be required from all commercial-off-the-shelf, government-off-the-shelf, and other custom software for all new software acquisitions, software renewals, and major software version changes (e.g., from version 2.5 to 3.0).

Risk-based approach to attestation

NIST encourages Federal Agencies to conduct a risk assessment of software acquisitions and require an attestation from vendors' commensurate with the level of risk of the software. The following are examples of risk that might lead Federal Agencies to request enhanced validation methods:

- Suppliers under Foreign Ownership, Control, or Influence
- Critical software vendors
- Software and/or vendors that require access to controlled unclassified information or classified information
- Suppliers who represent a single source of supply with limited availability
- Suppliers who are frequently associated with foreign adversary tactics, techniques, and procedures; security alerts; or threat intelligence reports

Enhanced validation methods

Federal Agencies have a wide selection of methods available for enhanced validation, and the EO does not prescribe or suggest any one specific method. NIST guidance points to the Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161) for suggested enhanced validation methods, such as:

- Supplier certifications, site visits, and/or third-party assessment and attestation
- Higher frequency and/or continuous monitoring of supplier adherence to attestation commitments
- Collection and review of lower-level artifacts, including functional and technical security controls
- Higher fidelity Software Bill of Material (SBOM), including vendor vulnerability disclosure reports, at the component level

Additionally, EO 14028 encourages software vendors to go beyond the SSDF baseline and employ the minimum standards for vendor testing and validation found in the National Institute of Standards and Technology Internal Reports (NISTIR) 8397; however, these guidelines are, and will remain, voluntary.

Artifacts of conformance

High-level artifacts

To aid in validating conformance, Federal Agencies are encouraged to request high-level artifacts from software vendors, such as process and procedure documentation. These high-level artifacts should provide a summary of, and relate directly to, the granular secure software development practices implemented by the software provider.

A SBOM may be required as an artifact of conformance. SBOMs are a nested inventory of software components, like a list of ingredients, that make up a piece of software. The EO encourages a standardization of SBOMs across industries by requiring that they contain, at a minimum, the following elements :

- Data Fields: Documenting baseline information about each component that should be tracked
- Automation Support: Allowing for scaling across the software ecosystem through automatic generation and machine readability
- Practices and Processes: Defining the operations of SBOM requests, generation, and use

Low-level artifacts

Agencies may additionally request low-level artifacts from software vendors, such as audit logs, to validate the high-level artifacts. While NIST strongly discourages agencies from requesting low-level artifacts, agencies have broad discretion when determining validation methods and artifacts.

Critical software

NIST defines EO-critical software as software that has, or its direct software dependencies have, one or more components with one (or more) of these attributes.

- Designed to run with elevated privileges or manages privileges
- Has direct or privileged access to networking or computing devices
- Designed to manage access control
- Performs critical trust security functions, such as network control, endpoint security, and network protection
- Operates outside of normal trust boundaries with privileged access

Software providers should be additionally aware of the added security controls employed by Federal Agencies when using critical software. Software developers should ensure their critical software is designed to implement the necessary controls, such as specific encryption and multifactor.

Timeline and next steps

Next steps for software providers

To comply with the SSDF baseline and additional EO requirements, software vendors are expected to meet these minimum requirements.

- Align secure software development processes and practices to the SSDF to enable attestation of conformance to Federal Agencies
- Prepare attestations of conformance to the SSDF practices for all unclassified software provided to the Federal government
- Document a plan of action and milestones for implementing any practices not currently implemented
- Prepare and gather SBOMs and other articles of conformance related to each software product intended for use by the Federal government
- Determine which software products could be subject to enhanced validation methods and/or designated as EO-critical software
- Ensure EO-critical software can accommodate the additional Federal security controls
- Enroll in an Agency Vulnerability Disclosure Program (VDP)

Significant timelines

The EO and OMB memo provide aggressive deadlines for Federal Agencies to enact these changes:

- September 14, 2022: SSDF and attestation requirements apply to software developed on, or after, this date
- December 14, 2022: Agencies must have identified all software impacted by the EO requirements and identified EO-critical software
- January 13, 2023: Federal Chief Information Officers must have developed the procedures for communicating EO requirements to vendors and established an agency-wide attestation repository
- June 11, 2023: Agencies must have collected all attestations from software vendors with software designated as EO-critical
- September 14, 2023: Federal Agencies must have collected attestations for all software covered by the EO

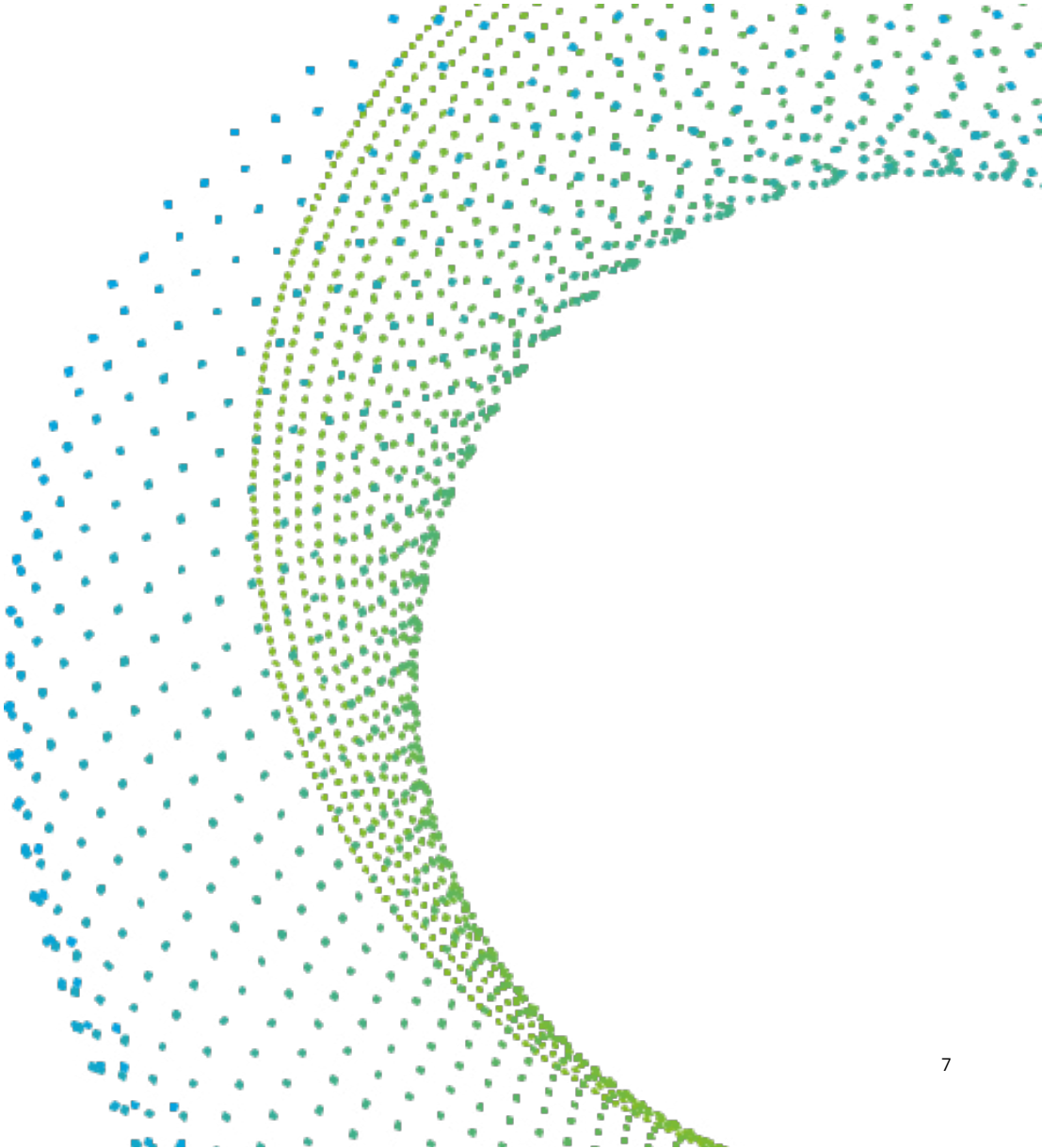
Deloitte difference

Deloitte & Touche LLP, is here to guide and support software providers in developing and implementing a secure software supply chain. Deloitte has developed innovative approaches for clients of all sizes who are working to comply with various supply chain government directives and regulations, as well as developed and implemented strategies to strengthen our clients' end-to-end supply chains.

Deloitte's approach to software supply chain security is anchored in SBOM operationalization. Our solutions extend beyond the generation of an SBOM and includes optimizing security risk management by utilizing information from ingested SBOMs to provide transparency in the software supply chain.

Some of Deloitte's leading software supply chain solutions and services are outlined below.

- Developing custom solutions that leverage existing tools in the Software Composition Analysis market to manage artifact generation, maintenance, and reporting requirements
- Optimizing SBOM utilization by creating custom platforms that enable visibility and transparency across the end-to-end software supply chain
- Ingesting SBOMs from software vendors to perform vulnerability scanning and risk assessments
- Utilizing SBOM data to validate and update n-tier supplier illumination and map relationships to primary vendors
- Managing vulnerability triage and investigation to assess validity and applicability, and activate playbooks to manage remediation processes



Deloitte.

Designed by CoRe Creative Services. RITM1396170