Black Duck SSDF Readiness Assessment

Overview

Legislation requiring stringent software security practices by software producers is being passed around the globe. This requires organizations to rethink their approach to software security, which industry standards they follow, and the best practices for their software development teams. While largely focused on the software procured by governmental departments, agencies, and contractors, such legislation also has a direct impact on enterprise software, cloud services, and consumer-level products. This turns governmental procurement from a simple transaction into something that has a much broader impact across critical infrastructure sectors and related technology suppliers.

The National Institutes of Standards and Technology (NIST) has produced guidance known as the Secure Software Development Framework (SSDF). The SSDF presents a series of practices and associated tasks that serve as a baseline for teams seeking to securely develop software in a standardized way. Attestation to conformance with a subset of the SSDF has been signaled by the U.S. government as a requirement for all software procured directly or indirectly by the U.S. government and produced after September 2022, and software suppliers will need to self-attest to their adherence to the SSDF.

The Black Duck® SSDF Readiness Assessment identifies whether your organization's software development practices align with the practices and tasks of the SSDF. It also provides an assessment of which controls are lacking in conformance. This assessment, and the associated corrective recommendations, can be used when completing U.S. government attestations.

Build on the Proven BSIMM

A Black Duck Building Security in Maturity Model (BSIMM) assessment empowers you to analyze and benchmark your software security program against 100+ organizations across several industry verticals. It's an objective, data-driven analysis from which to base decisions of resources, time, budget, and priorities as you seek to improve your security posture.

The Black Duck SSDF Readiness Assessment quantifies the security of development environments in addition to the governance, culture, and process measurements of a BSIMM assessment. Equivalency between the BSIMM and SSDF can be found within the SSDF (SP 800-218 Version 1.1) as references on each SSDF activity.

Improve software security while maintaining conformance to SSDF for procurement activities. Anyone selling software made after September 14, 2022, directly or indirectly to the U.S. government needs to attest to their conformance to specific NIST SSDF tasks. If searching for solutions to any of these items, an SSDF Readiness Assessment may be beneficial.

- EO 14028
- NIST SP 800-218 Version 1.1
- OMB Memo M-22-18
- DHS CISA self-attestation
- IEC 62443

For Both Organizations and Products

The core assessment is designed for security teams that need to demonstrate their conformance to the activities in the SSDF. This might be required by an external customer for regulatory or contractual reasons. Or it could be to assess the state of software development following an acquisition, to create an integration effort aligned with the needs of the security and product teams.

Some companies want to look at their development practices at the product level, and the Black Duck SSDF Readiness Assessment is perfect for that. Examples of when to perform this assessment include when products are deemed critical infrastructure; when there are different contractual requirements, development methodologies, or security targets; or during different stages in the overall product life cycle.

Align with OMB/CISA Self-Attestation Requirements

The U.S. Office of Management and Budget (OMB) has issued memos requiring software providers within the procurement chains in the U.S. government to attest to their conformance with SSDF. This attestation is a key component of any compliance program related to President Biden's executive order on cybersecurity. Software is considered "in-scope" if it was produced after September 14, 2022, or if it is deployed via a continuous update or continuous delivery model. Importantly, this brings any cloud-based or SaaS software solution into scope.

OMB directly cites SSDF as a baseline for attestation requirements, and the Cybersecurity and Infrastructure Security Agency (CISA) was tasked by OMB to create those requirements. The Black Duck SSDF Readiness Assessment is uniquely positioned to demonstrate that required SSDF activities are occurring consistently within the business or product line. By default, Black Duck uses an average of the confidence level score for each activity or task when calculating the confidence level for each attestation question. For more risk-adverse businesses, we change that model and use a floor, which results in the lowest-performing activity or task becoming the confidence level for the attestation question.

Regardless of whether an average or floor-based confidence level is used, the Black Duck SSDF Readiness Assessment shows which tasks are contributing to lower scores.

Identify Areas for Remediation or POAM

The Black Duck SSDF Readiness Assessment provides a confidence level for the 42 activities within the SSDF. If an activity results in a low confidence level, it's an indication that the activity is not being consistently performed, and represents an area for improvement. Based on the nature of the requirements defined by a procurement team, any deficiencies may be subject to a plan of action and milestone (POAM).

Crucial Component of a Mature Software Supply Chain Strategy

Properly managing software supply chains involves multiple disciplines. It all starts with software composition analysis like that from Black Duck, but also includes business requirements like a Software Bill of Materials and a secure software development life cycle. From a governance perspective, the Black Duck SSDF Readiness Assessment is uniquely positioned to ensure that any SSDF activities are consistently performed throughout the business, within a business unit or product line, or at the individual product level.

SSDF CONFIDENCE SCORE

Prepare the Organization (PO)

SSDF Task	Enterprise	Product 1	Product 2	Product 3	Product 4	Product 5
PO.1.1	Very High	Very High	Very High	Very High	Very High	Very High
PO.1.2	Very High	Very High	Very High	Very High	Very High	Very High
PO.1.3	High	Medium	HIgh	High	Very High	Very High
PO.2.1	Very High	High	Very High	Very High	Very High	Very High
PO.2.2	Very High	High	Low	Very High	Very High	Very High
PO.2.3	Very High	Low	Very High	Very High	Very High	Very High
PO.3.1	Very High	Medium	Very High	Very High	Very High	Very High
PO.3.2	Very High	Very High	Very High	Very High	Very High	Very High
PO.3.3	Very High	Very High	Very High	Very High	Very High	Very High
PO.4.1	Medium	Very High	Very High	Very High	Very High	Very High
PO.4.2	Very High	Very High	Very High	Very High	Very High	Very High
PO.5.1	Very High	Very High	Very High	Very High	Very High	Very High
PO.5.2	Very High	Very Low	Very High	Very High	Very High	Very High

Produce Well-Secured Software (PW)

SSDF Task	Enterprise	Product 1	Product 2	Product 3	Product 4	Product 5
PW.1.1	Low	Medium	High	High	Low	High
PW.1.2	Very Low	High	High	High	High	Very High
PW.1.3	Very Low	Very High	Very High	Very High	Medium	Very High
PW.2.1	Low	Very High	Very High	Very High	Medium	Very High
PW.4.1	High	High	High	High	High	High
PW.4.2	Very Low	Very High	Very High	Very High	Medium	Very High
PW.4.4	Medium	Medium	Medium	Medium	Medium	Medium
PW.5.1	Low	Low	Low	Low	High	Low
PW.6.1	Low	Very Low	Very Low	Low	Low	Low
PW.6.2	Low	Very Low	Very Low	Low	Low	Low
PW.7.1	Medium	Very High	High	Very High	Very High	Very High
PW.7.2	Medium	Very High	Very High	Very High	Very High	Very High
PW.8.1	Low	Very High	High	Very High	Medium	Very High
PW.8.2	High	High	Very High	High	High	Very High
PW.9.1	Very High	Very Low	Very High	Very High	Very High	Very High
PW.9.2	Very High	Very Low	Very High	Very High	Very High	Very High

Protect the Software (PS)

SSDF Task	Enterprise	Product 1	Product 2	Product 3	Product 4	Product 5
PS.1.1	High	Medium	High	Very High	Very High	Very High
PS.2.1	Low	High	Very Low	Very High	Very High	Very High
PS.3.1	Very Low	Very High	Very High	Very High	Very High	Very High
PS.3.2	Very High	Very Low	Very High	Very High	Very High	Very High

Respond to Vulnerabilities (RV)

SSDF Task	Enterprise	Product 1	Product 2	Product 3	Product 4	Product 5
RV.1.1	Very High	Medium	Very High	Very High	Very High	Very High
RV.1.2	Very Low	Very Low	High	High	High	High
RV.1.3	Very High	High	High	Very High	Very High	Very High
RV.2.1	Medium	Medium	Very High	Very High	Very High	Very High
RV.2.2	Medium	Medium	Medium	Very High	Very High	Very High
RV.3.1	Very Low	Low	Low	Low	Low	Low
RV.3.2	Medium	High	High	High	High	High
RV.3.3	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
RV.3.4	Medium	High	High	High	High	High

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.