Software Supply Chain Security

- Why is SSCS important?
- How Docker Hardened Images contribute to SSCS

SSCS encompasses practices and strategies designed to safeguard the entire lifecycle of software development from initial code creation to deployment and maintenance. It focuses on securing all components. This includes code, dependencies, build processes, and distribution channels in order to prevent malicious actors from compromising the software supply chain. Given the increasing reliance on open-source libraries and third-party components, ensuring the integrity and security of these elements is paramount

Why is SSCS important?

The significance of SSCS has escalated due to sophisticated cyberattacks targeting software supply chains. High-profile supply chain attacks and the exploitation of vulnerabilities in open-source components underscore the critical need for robust supply chain security measures. Compromises at any stage of the software lifecycle can lead to widespread vulnerabilities, data breaches, and significant financial losses.

How Docker Hardened Images contribute to SSCS

Docker Hardened Images (DHI) are purpose-built container images designed with security at their core, addressing the challenges of modern software supply chain security. By integrating DHI into your development and deployment pipelines, you can enhance your organization's SSCS posture through the following features:

- Minimal attack surface: DHIs are engineered to be ultra-minimal, stripping away unnecessary components and reducing the attack surface by up to 95%. This distroless

approach minimizes potential entry points for malicious actors.

- Cryptographic signing and provenance: Each DHI is cryptographically signed, ensuring authenticity and integrity. Build provenance is maintained, providing verifiable evidence of the image's origin and build process, aligning with standards like SLSA (Supply-chain Levels for Software Artifacts).
- Software Bill of Materials (SBOM): DHIs include a comprehensive SBOM, detailing all components and dependencies within the image. This transparency aids in vulnerability management and compliance tracking, enabling teams to assess and mitigate risks effectively.
- Continuous maintenance and rapid CVE remediation: Docker maintains DHIs with regular updates and security patches, backed by an SLA for addressing critical and high-severity vulnerabilities. This proactive approach helps ensure that images remain secure and compliant with enterprise standards.

□□□ #2
□ □□□ □□□ 2026-10-31 19:16:01 UTC
□ □□□ □□□ 2026-10-31 19:16:03 UTC