What are SBOMs?

Terence Wong
September 26, 2022 • 4 mins

If you're a developer or you manage an enterprise software application, you may have been asked about the components in your application. Why do people want to know? Customers want to trust your application, they want your application to be secure. Enterprise vendors and government bodies want to know because they're concerned with security issues for their customers using your software.

Software applications are made up of several sources, open-source, in-house, or a mixture of both. As the list of dependencies grows, how can an application be secure if the individual components used to build the application aren't known?

A bill of materials lists the required inventory to produce a given output reliably. Bills of materials have been used for years to provide transparency and repeatability in manufacturing processes. Software bills of materials (SBOMs) apply a similar concept. SBOMs itemize the components in a software application in a list that developers can share across teams.

Executive Order on Improving the Nation's Cybersecurity

On May 12, 2021, The United States government released an Executive Order on Improving the Nation's Cybersecurity.

> The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

The Executive Order is trying to minimize the cybersecurity risk in the supply chain when people acquire software. Risk increases as the number of unknown components in the software applications increases.

The Executive Order requires all software bought by the US government to produce an SBOM. This has several implications for business inside and outside the US. Any US government project now has to produce SBOMs for security purposes. Any vendor that can't produce SBOMs for their products won't be approved to work on government projects.

The Order is likely the beginning of many similar orders to require SBOMs worldwide. As awareness of SBOMs increase, it's probable businesses will begin to demand SBOMs. If you work in software, SBOMs are likely in your future.

What goes into SBOMs?

The National Telecommunications and Information Administration (NTIA) provides guidelines on constructing an SBOM. NTIA conducted a proof of concept of SBOMs in healthcare, which informed the baseline elements required for an SBOM.

The baseline elements include:

- Author Name - The author of the SBOM document describing the Primary Component. The author may not be the same as the supplier of the Primary Component.
- Supplier Name - the supplier of a component.
- Component Name - the name of the component.
- Version String - the version of the component.
- Component Hash - a cryptographic hash used to identify the binary instance of a component.
- Unique Identifier - a unique identifier for a component. Multiple identifiers may exist for an element because different systems may use anoter identifier.
- Relationship - is used to establish that a component includes another component. In addition, Relationship is used to document knowledge about the completeness of the list of components included in another component.
- Component Relationships
- Primary Component – the component described by the SBOM.
- Included Component – the components included in another component.

Why are SBOMs important?

The requirement for SBOMs significantly impacts software. Software is built collaboratively and often contains several third-party libraries that use other third-party libraries. Without the ability to generate SBOMs, software won't be compliant with the Executive Order.

Government bodies and organizations acting under the Executive Order need to choose software that can produce an SBOM on demand and can prove that each component is not a cybersecurity risk. The widespread use of SBOMs will increase the trust between vendors and government bodies.

Software vendors need a reliable way to detect any known vulnerabilities in their deployed application. SBOMs let you be proactive in addressing risks, reducing the likelihood your tools can be hacked. Vulnerability scanning also helps you avoid awkward conversations with customers who scan your applications themselves and report vulnerabilities.

The requirement for SBOMs can be seen as just an additional step in the build process to generate the artifact, but it does raise some questions, such as:

- How do you pair an SBOM to a deployable artifact so one can be matched to the other?
- How do you know what version of your application is in production so you can scan the associated SBOM in the weeks or months after the application was deployed?
- How do you orchestrate the deployment of your application and publish the associated SBOM?
- How do you schedule SBOM scanning to proactively detect newly discovered vulnerabilities?

- How do you scan old SBOM versions to identify previous releases of your software that include vulnerable components?

At Octopus, we built a free tool that answers all of those questions for you and meets your SBOM requirements.

How the Octopus Workflow Builder helps with SBOM requirements

The Octopus Workflow Builder helps you generate SBOMs and build them into your deployment process. The tool demonstrates how SBOM files are constructed as part of the build, and then demonstrates how Octopus Deploy can scan the SBOM as part of the deployment.

With the Builder, you're provided with a sample project demonstrating how deployable artifacts and their associated SBOMs are tightly coupled in a release, allowing you to orchestrate and publish the SBOM with any application deployment, schedule SBOM scanning, or access old SBOM versions.

Conclusion

In 2021, the US government issued an Executive Order to improve the nation's cybersecurity. The Order mandated that software components be known to the government to minimize security risks. If you work in software, this requires you to expose the components of your applications or risk being excluded from government IT-related projects.

You can make your software components known through SBOMs. SBOMs are a list of components in a software application that is sharable and generated automatically on each application release.

To help you with this requirement, the Octopus Workflow Builder produces SBOMs as part of the build and scans them as part of the deployment.

Happy deployments!

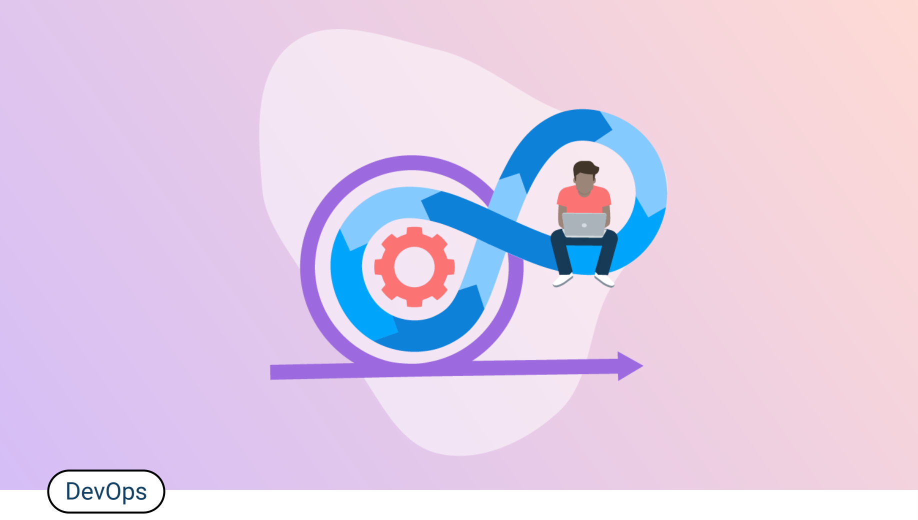
Tagged with: DevOps Cloud Orchestration Testing

Related posts

DevOps

Common mistakes in DevOps metrics

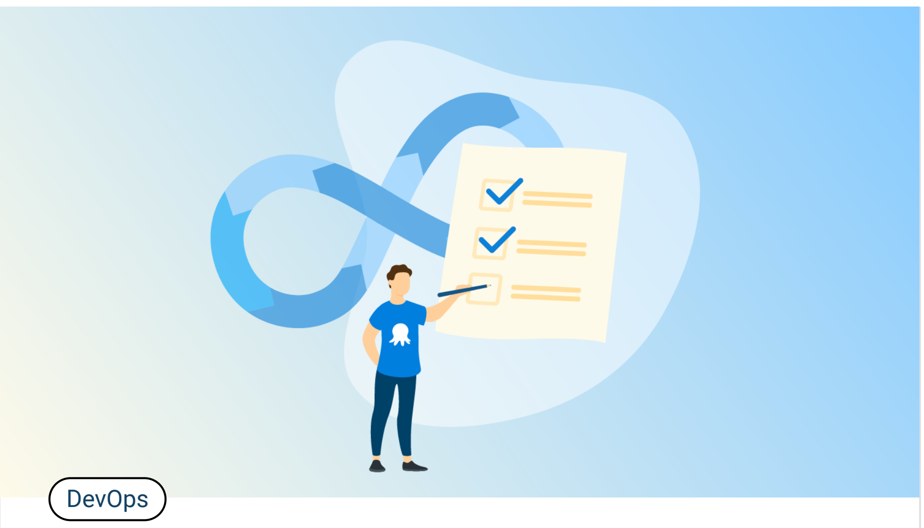
Steve Fenton
December 7, 2022 • 6 mins



DevOps

Comparing Lean, Agile, and Continuous Delivery

Steve Fenton
December 5, 2022 • 6 mins



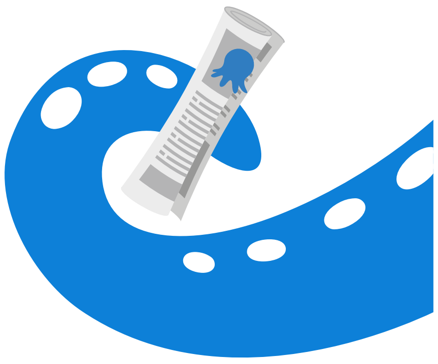
DevOps

Best practices for CI/CD

Terence Wong

November 30, 2022 • 5 mins

Newsletter



Logged in as Terence Wong (terence.wong@octopus.com)

Join ~48,000 DevOps professionals and sign up for the latest Octopus news, events, and opinions. No spam. Unsubscribe at any time.

Subscribe

Your privacy is important to us. Read more in our Privacy Policy.