What's next?

The concept of software bills of materials (SBOMs) has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea of SBOMs to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

But what is an SBOM?

Software bills of materials (SBOMs) are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The concept of SBOMs has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The concept of SBOMs has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The concept of SBOMs has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The concept of SBOMs has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The concept of SBOMs has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.

What's next?

The concept of SBOMs has risen rapidly following Biden's Executive Order on cybersecurity. The idea is to improve the country's cybersecurity by standardising the way software is managed and monitored. But what is an SBOM, and what does it mean for open source adoption?

SBOMs are essentially a list of all the components used in building software. They include information about the source code, build artefacts, and any binary dependencies. They are designed to help identify vulnerabilities and supply chain risk, and they should include links to embedded dependencies and be shipped as a part of the build.

There are open source projects like OpenSFF and others that are aimed at automatically generating SBOMs. These tools can help formalise and automate the process. However, awareness of SBOMs varies depending on where you are, geographically, culturally, or in terms of your role in the software ecosystem.

For businesses, SBOMs provide a way to accept or reject software based on pre-chosen criteria, such as configuration, licensing, or provenance. They allow organisations to make informed decisions about their software supply chain and to improve their self-protection against potential vulnerabilities.

But in recent months, the concept of SBOMs has risen rapidly, and the US government's edicts have focused minds in a way that has yet to be matched elsewhere. However, for the idea to really take off, it needs to be simple for both creators and consumers of software, with standard formats and playbooks and the right tooling in place.