OASIS Launches Global Initiative to Standardize Supply Chain Information Models

Checkmarx, Cisco, Cyware, Google, IBM, Legit Security, Microsoft, Root, SAP, US NSA, CISA, and Others to Build Framework to Complement SBOM Data Formats

BOSTON, MA, USA, June 20, 2024 /EINPresswire.com/ -- With escalating cybersecurity threats exploiting software supply chain vulnerabilities, there's an urgent need for better understanding and proactive measures to identify and prevent future risks. Members of OASIS Open, the global open source and standards organization, have formed the [Open Supply Chain Information Modeling (OSIM) Technical Committee (TC)](#) to standardize and promote information models crucial to supply chain security.

The aim of OSIM is to build a unifying framework that sits on top of existing SBOM data models-- such as CSAF, CycloneDX, OpenVEX, and SPDX. OSIM is not intended to replace or endorse any one of these models. Instead, as an information model, OSIM will bring clarity to software supply chain partners, mitigate vulnerabilities and disruptions, reduce security risks, and make it easier for companies to plan for upgrades and contingencies.

"CISA is excited to be a part of this technical effort to bring greater visibility to the software supply chain," said Allan Friedman, Senior Technical Advisor at CISA. "We have many of the basic building blocks for software transparency and security, including SBOM, VEX, and CSAF. This work by OASIS will facilitate automation for easier and cheaper implementation and tooling, and help provide a unifying supply chain framework and raise the level of collaboration across industries."

"OSIM represents an important effort to address the need for greater structure and comprehensibility of software supply chains," said Isaac Hepworth, Google, and OSIM co-chair. "By establishing standardized information models we can enhance transparency, interoperability, and resilience in end-to-end operations — ultimately aiding cyber risk management and protecting critical infrastructure."

Recognizing the crucial role of Software Bill of Materials (SBOMs) in fortifying software supply chain security, the OSIM TC aims to create, for example, a standardized SBOM information model that would enhance understanding and interoperability across diverse SBOM data formats (i.e. SPDX and CycloneDX). Competing data models, like SPDX, CycloneDX, CSAF, and OpenVex, show the need for creating information models that would bring coherence across diverse specifications.

"OSIM's approach not only drives a universal taxonomy of thought, it also brings clarity and ease to how we implement standards and frameworks to support multiple industry software supply chain security needs. OSIM facilitates the identification of similarities and differences across specifications, enhancing interoperability and simplifying processes. The current cybersecurity landscape can no longer be defended in a silo," said Jay White, Microsoft, and OSIM co-chair.

The OSIM TC welcomes a diverse range of contributors, including software and hardware vendors, open-source maintainers, technology consultants, business stakeholders, government organizations, and regulatory bodies. Participation is open to all through [membership in OASIS](#), with interested parties encouraged to join and contribute to shaping the future of supply chain information modeling.

Support for OSIM
Checkmarx
"Checkmarx is proud to be working with OASIS and be part of the OSIM Technical Committee. A major part of Checkmarx' mission to secure the applications driving our world involves sharing our time, experience, and threat intelligence to help make the software supply chain ecosystem safer. As one of the biggest challenges remains education and closing the knowledge gap, we believe standardization is a crucial step and are committed to assisting in laying the foundations."
– Erez Yalon, VP of Security Research, Checkmarx

Root
"The OASIS OSIM is a vital project for enhancing security and trust in the software supply chain. As a part of the OSIM Technical Committee, Root is committed to advancing supply chain security and transparency, aligning perfectly with this initiative's goals. By collaborating on data schemas, data modeling, and security standards, we aim to improve vulnerability management and software security, ensuring threats are identified and mitigated promptly. This enhances software integrity, benefiting our customers and strengthening trust in the broader digital ecosystem."
- Ian Riopel, CEO Root.io

SAP SE
"Having a unified information model for representation of objects in the supply chain domain would enable efficient integration models and interoperability. Especially with the wave for

generative AI, such aligned models can bring benefits in development efficiency , reduced maintenance and operations for upcoming innovations in the domain."
- Gururaj Raman, Chief Development Expert, SAP SE

Additional Information
OSIM Project Charter

About OASIS Open
One of the most respected, nonprofit open source and open standards bodies in the world, OASIS advances the fair, transparent development of open source software and standards through the power of global collaboration and community. OASIS is the home for worldwide standards in identity, IoT, cybersecurity, blockchain, privacy, cryptography, cloud computing, urban mobility, emergency management, and other content technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement. Visit www.oasis-open.org for more information.

Media Inquiries: communications@oasis-open.org

Disclaimer: CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked or referenced within this press release. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

Carol Geyer
OASIS
carol.geyer@oasis-open.org
Visit us on social media:
LinkedIn
Facebook
X
YouTube