Cybeats Provides Product Overview for SBOM Studio: Pioneering the Way Forward in SBOM Management

Toronto, Ontario--(Newsfile Corp. - January 5, 2023) - **Cybeats Technologies Corp. (CSE: CYBT) ("Cybeats" or the "Company")** is pleased to provide an overview of its SBOM Studio product, a solution to the pressing issue of cybersecurity vulnerabilities across the global software supply chain. With the increasing frequency of high-profile cyber attacks and new regulations around the world, it is more important than ever for organizations to prioritize the protection of themselves and their customers. SBOM Studio provides a comprehensive solution to this problem, enabling companies to increase efficiency, reduce costs, and improve compliance while improving visibility and security of the software supply chain.

"Our recent industry and customer recognition is a testament to the industry-leading capabilities of our SBOM Studio platform and demonstrates our ability to win over some of the largest enterprises in the world," said **Yoav Raiter, CEO, Cybeats**. *"SBOM adoption is accelerating around the world, in-part by advancing government regulations, and our SBOM Studio is leading the way forward as organizations increasingly look to implement SBOMs to protect their software supply chains."*

"SBOM Studio is defining and pioneering the future of autonomous SBOM management, helping organizations proactively improve visibility and security across the software supply chain," said **Dmitry Raidman, CTO, Cybeats**. *"SBOM Studio was purposefully designed to empower organizations of all sizes and industries to easily and efficiently implement SBOMs, accelerate vulnerability management, and reduce the cost of protecting their software supply chain."*

Background

To remain competitive in today's market, organizations rely on previously developed software or proprietary third party software components known as "open source software" (OSS) to meet the demands of frequent software releases in a cost-effective and timely manner. In fact, 99% all software today contains open source components.[1]

The use of OSS carries inherent risks with studies showing that 75% of open source software contains vulnerabilities that pose cybersecurity threats[2]. With the widespread use of OSS in modern software development, it is crucial for organizations to have a system in place to manage and mitigate these risks.

The threat of cyberattacks that exploit vulnerabilities in open source software (OSS) is increasing rapidly, with a growth rate of 700% per year[3]. Many organizations may not be aware that they are using OSS, making it crucial for them to take steps to protect themselves against these threats. The log4j[4] and SolarWinds[5] events serve as examples of the potential damage caused by attacks that exploit OSS vulnerabilities, affecting 18,000 customers including government agencies and critical infrastructure providers. To mitigate OSS risks, creating and continuously monitoring a Software Bill of Materials (SBOM) is becoming a must.

Introducing SBOMs

Software Bill of Materials (SBOMs) are lists of the ingredients and their versions that make up a particular piece of software, similar to the nutritional facts or ingredient list found on food labels such as for dairy, cookies or juice. SBOMs provide important information about software, including any open source components, which can help companies and governments determine if the software is safe to use. SBOMs are used across a variety of industries and are becoming required by government regulators, such as the FDA's recent mandate requiring SBOMs for medical device submissions. Many companies are already generating SBOMs as part of their software development process, following recent industry standards for SBOM generation. However, implementing SBOM practices can be challenging due to the scale of the change and the manual work involved. As organizations seek to improve the security and reliability of their software in the face of evolving threats and regulatory requirements, the adoption of SBOMs is becoming increasingly important. By using SBOMs, companies can better manage their software supply chain risks and improve the overall quality of their software.

***SBOM Studio* - Managing the Lifecycle of your SBOMs**

To view an enhanced version of this graphic, please visit:
https://images.newsfilecorp.com/files/3927/150445_b89330fe04eff949_001full.jpg

Cybeats' *SBOM Studio* is a comprehensive solution designed to manage and distribute software bill of materials (SBOMs) in a single platform. It provides organizations with a centralized view of cybersecurity vulnerabilities, enabling them to improve the visibility and security of their software supply chain. *SBOM Studio* is useful for organizations of all sizes and industries, as it helps them to improve their vulnerability management processes, reduce the cost of protection, and enhance compliance.

SBOM Studio is also agnostic to SBOM generation tools, meaning it can work with any tool to validate and correct imported SBOMs, improving the accuracy of SBOMs. In addition, it simplifies the implementation process, speeds up the fixing of vulnerabilities, and automates SBOM management, ultimately improving the return on investment of SBOM adoption in an organization.

After generating software bill of materials (SBOMs) using any SBOM generation tool, clients who upload their SBOMs to Cybeats' *SBOM Studio* can gain valuable insights into their software supply chain with the following features:

Automated SBOM Management

- During the import of SBOMs, *SBOM Studio will* validate the SBOM to ensure correct formatting

according to the specification of the SBOM standards
- SBOMs that are not accurately formatted will either be auto-corrected for recoverable errors or rejected with meaningful information describing the root cause of the misalignment
- SBOM Studio enriches SBOMs as part of the import process, populating them with key information and details about the software supply chain intelligence data

Accelerated Vulnerability Management

- Continuous process of monitoring SBOMs, autonomous scanning for new vulnerabilities. SBOMs are living and breathing in *SBOM Studio*
- Categorizes and filters vulnerabilities by level of criticality to inform decision making
- Search for and identify specific SBOMs rapidly, and confidently and securely identify compromised components across the organization

Improved Workflowfor Security Operations

- Prompts cyber teams with the recommended actions to optimally fix vulnerabilities and reduce cyber risk
- Display and categorizes vulnerabilities by level of criticality for prioritization of security workflow
- In leveraging a robust data lake, accurately determine how vulnerabilities affect the organization's security posture
- Native plug-ins and other integrations that allow for seamless workflow
- User-intuitive interface is easy to learn and understand

SBOM Sharing and Exchange Capabilities

- Securely share SBOMs with regulatory agencies, internal and external customers
- Share product SBOMs, while keeping the IP protected
- Ability to redact and hide specific parts of an SBOM before they are shared externally
- SBOM language agnostic with acceptance of all SBOMs, and easy conversion between SBOM languages

Data-Driven Business Decisions

- Report generation and visually appealing dashboard, for use by leadership, to bridge gaps between vulnerability status and the budgeting, forecasting, risk-mitigation, prioritization strategies
- Offers 'Governor View' vantage that allows enhanced visibility into all the layers and subsidiaries of the core business, giving development, cyber teams and leadership more information to better prioritize and evaluate the risks and associated costs across the organization

Regulatory Compliance and Licence Infringement

- Satisfy Governance, Risk and Compliance (GRC) requirements by showing best practices and good cyber hygiene by having an SBOM for all software, and for any 3rd-party products used by the enterprise
- License Infringement Notifications, when software that is used without permissions or licenses that can have associated legal risk and cost

SBOM Studio is* Sector Agnostic, Key Market Verticals Include*:

- Industrial Controls and Critical Infrastructure
- Healthcare and Medical
- Enterprise
- Automotive and Aerospace

SBOM Regulation

With the widespread proliferation and adoption of SBOM following the Whitehouse Executive Order in May of 2021, which announced the new SBOM standard to be implemented in the United States[6], policymakers are recognizing the importance of SBOM standards. Cybeats SBOM management solution provides proactive compliance with anticipated Governance, Risk Management and Compliance (GRC) requirements, demonstrating best practices by having an SBOM for all software, and for any 3rd-party products used by enterprises. From the US Executive Order to the recent EU Cyber Resilience Act[7], the value and imperative to use SBOMs around the world has been further cemented. Cybeats recently applauded the $1.7 Trillion Omnibus Appropriations Bill which would require medical device manufacturers to submit a Software Bill of Materials (SBOM) to the FDA that includes all standard, open source, and critical software components used by the devices.

Upcoming Events

Come meet Cybeats at **CES 2023**[8] at booth 6653! The 'most influential tech event in the world' is in Las Vegas from January 5 - 8, 2023. To register, please visit: https://registration.experientevent.com/ShowCES231

Join us at the **CISO Forum Canada** in Toronto, Ontario from January 30 to 31 as Cybeats leads a panel discussion on Software Supply Chain Security with cybersecurity leaders from CN Rail, Craft Ventures and SAP: https://www.siberx.org/event/ciso-forum-canada-2023/

Join us at the Fira Gran Via, Barcelona from 27 February - 2 March, 2023 at **MWC Barcelona**[9], the world's most influential exhibition for the device connectivity and security industry: https://www.mwcbarcelona.com/

Come meet us at **S4x23** in Miami February 13-16! Discover new ideas and come up with innovative ways to use these new ideas to deploy secure and resilient industrial control systems[10]**:** https://s4xevents.com/

About *SBOM Studio*

Cybeats' SBOM Studio enables organizations to efficiently manage, distribute, and view their software bill of materials (SBOMs) in a single interface. By doing so, they can easily identify and address cybersecurity vulnerabilities, reduce the cost of protection, and improve compliance. SBOM Studio is specifically designed to support software producers and consumers who use open source and 3rd party software components and who are transitioning to more transparent software development practices. The tool is compatible with various SBOM generation tools and can validate and correct imported SBOMs to improve their accuracy.

About Cybeats

Cybeats is a cybersecurity company providing SBOM management and software supply chain intelligence technology, helping organizations to manage risk, meet compliance requirements, and secure their software from procurement to development and operation. Our platform gives customers comprehensive visibility and transparency into their software supply chain, enabling them to improve operational efficiency and increase revenue. Cybeats. Software Made Certain. Website: https://cybeats.com

SUBSCRIBE: For more information, or to subscribe to the Company's mail list, visit: https://www.cybeats.com/investors

Contact:
James Van Staveren
Corporate Development
Phone: 1-888-713-SBOM (7266)

Email: ir@cybeats.com

Forward-looking Information Cautionary Statement

Except for statements of historic fact, this news release contains certain "forward-looking information" within the meaning of applicable securities law. Forward-looking information is frequently characterized by words such as "plan", "expect", "project", "intend", "believe", "anticipate", "estimate" and other similar words, or statements that certain events or conditions "may" or "will" occur. Forward-looking statements are based on the opinions and estimates at the date the statements are made, and are subject to a variety of risks and uncertainties and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements including, but not limited to delays or uncertainties with regulatory approvals, including that of the CSE. There are uncertainties inherent in forward-looking information, including factors beyond the Company's control. There are no assurances that the commercialization plans for the technology described in this news release will come into effect on the terms or time frame described herein. The Company undertakes no obligation to update forward-looking information if circumstances or management's estimates or opinions should change except as required by law. The reader is cautioned not to place undue reliance on forward-looking statements. Company filings are available at sedar.com.

[1] https://en.wikipedia.org/wiki/Open-source_software

[2] https://www.securitymagazine.com/articles/92368-synopsys-study-shows-91-of-commercial-applications-contain-outdated-or-abandoned-open-source-components

[3] https://www.sonatype.com/press-releases/sonatype-finds-700-average-increase-in-open-source-supply-chain-attacks

[4] https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

[5] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[6] https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

[7] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[8] https://www.ces.tech/

[9] https://www.mwcbarcelona.com/

[10] https://s4xevents.com/

CYBEATS

To view the source version of this press release, please visit https://www.newsfilecorp.com/release/150445