Black Duck Newsroom

Majority of Organizations Impacted by Software Supply Chain Attacks Over the Past Year, with Many Struggling to Detect and Respond

More than half (54%) of organizations surveyed suffered a software supply chain attack in the past year, according to a new report from Synopsys Software Integrity Group and Ponemon Institute

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

SUNNYVALE, Calif., May 16, 2024 /PRNewswire/ -- The majority of global organizations (54%) suffered a software supply chain attack over the past year, and most are unable to keep up with the growing risk landscape. This is according to "The State of Software Supply Chain Security Risk" report, released today by Synopsys, Inc. (Nasdaq: SNPS) and the Ponemon Institute, which also found that 50% of organizations took more than a month to respond to an attack. One in five say that their organization is not effective in its ability to detect and respond to these attacks.

The data also shows that AI is becoming ubiquitous across the software development life cycle. The majority of security professionals (52%) say their development teams leverage AI tools to generate code, specifically, OpenAI Codex (50%), ChatGPT (45%) and GitHub Copilot (43%). While the use of AI creates efficiencies by automating decision-making, findings indicate that concerningly few protections are put in place. Only a third (32%) of organizations have processes to evaluate AI-generated code for license, security, and quality risks.

Survey respondents also cited a worrisome lack of commitment from decision-makers when mitigating these issues. Only 39% say their organization's leaders are highly committed to reducing the risk of malware in software supply chains. Even though 45% of security professionals say supply chain compromises such as SolarWinds have led to increased investment in software supply chain security, only 38% say resources dedicated to securing the supply chain are sufficient or very sufficient.

"Supply chain attacks are becoming more prevalent across organizations globally, yet this report highlights the sustained weaknesses in existing software development processes and security standards," said Jason Schmitt, general manager, Synopsys Software Integrity Group. "Attackers are getting more sophisticated and thus finding more weaknesses that allow them to explore a supply chain where they can steal sensitive data, plant malware, and control systems. Particularly with the rise of AI-generated code, security teams need to maintain visibility into applications, and continuously evaluate IP, security threats, and code quality to reduce risk."

Additional key findings include:

- **Organizations forgoing SBOM implementation:** Software Bills of Materials (SBOMs) are critical to ensuring a secure software supply chain but only 35% of security professionals say their organizations produce them. Furthermore, only 40% say they immediately stop the use of software if the supplier doesn't provide a requested SBOM. The main reasons organizations generate SBOMs are general dependency and vulnerability management (50%), industry regulations (39%), customer requirements (38%), and government requirements (38%).

- **Open source vulnerabilities remain a huge risk:** Nearly two-thirds (65%) of respondents say they use open source software, although less than half of respondents (47%) say their organizations are very or highly effective in securing it in the supply chain.

To learn more, download a copy of "The State of Software Supply Chain Security Risks" report, read the blog post or register for the May 23 webinar.

Methodology
The survey collected responses from 1,278 IT and IT security practitioners who are in organizations that are committed to achieving a secure software supply chain and have some level of responsibility for their organizations' software supply chain security strategy. The regions and countries in this research are North America (613 respondents), EMEA (362 respondents), and Japan (303 respondents).

About the Synopsys Software Integrity Group
Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software. Learn more atwww.synopsys.com/software.

About Synopsys
Catalyzing the era of pervasive intelligence, Synopsys, Inc. (Nasdaq: SNPS) delivers trusted and comprehensive silicon to systems design solutions, from electronic design automation to silicon IP and system verification and validation. We partner closely with semiconductor and systems customers across a wide range of industries to maximize their R&D capability and productivity, powering innovation today that ignites the ingenuity of tomorrow. Learn more at www.synopsys.com.

Editorial Contact:
Liz Samet
Synopsys, Inc.
336-414-6753
esamet@synopsys.com

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2024-05-16-Majority-of-Organizations-Impacted-by-Software-Supply-Chain-Attacks-Over-the-Past-Year,-with-Many-Struggling-to-Detect-and-Respond