Synopsys and Ponemon Study Highlights Critical Security Deficiencies in Medical Devices

Survey of Medical Device Manufacturers and Healthcare Delivery Organizations Reveals Industry's Lack of Confidence and Alignment in Securing Medical Devices

MOUNTAIN VIEW, Calif., May 25, 2017 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the results of the study "Medical Device Security: An Industry Under Attack and Unprepared to Defend," which found that **67 percent** of medical device manufacturers and **56 percent** of healthcare delivery organizations (HDOs) believe an attack on a medical device built or in use by their organizations is likely to occur over the next 12 months. The survey also found that roughly **one third** of device makers and HDOs are aware of potential adverse effects to patients due to an insecure medical device, but despite the risk only **17 percent** of device makers and **15 percent** of HDOs are taking significant steps to prevent such attacks.

The Synopsys study conducted by the Ponemon Institute, a leading IT security research organization, aimed at identifying whether device makers and HDOs are in alignment about the need to address cybersecurity risks. Focused on the North America market, the study surveyed approximately 550 individuals from manufacturers and HDOs, whose roles involve the security of medical devices, including implantable devices, radiation equipment, diagnostic and monitoring equipment, robots, as well as networking equipment designed specifically for medical devices and mobile medical apps.

"The security of medical devices is truly a life or death issue for both device manufacturers and healthcare delivery organizations," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "According to the findings of the research, attacks on devices are likely and can put patients at risk. Consequently, it is urgent that the medical device industry makes the security of its devices a high priority."

Other key findings from the study highlight:

- **Building secure devices is challenging.** 80 percent of device makers and HDOs report that medical devices are very difficult to secure. The top reasons cited for why devices remain vulnerable include accidental coding errors, lack of knowledge/training on secure coding practices and pressure on development teams to meet product deadlines.
- **Lack of security testing.** Only 9 percent of manufacturers and 5 percent of HDOs say they test medical devices at least once a year, while 53 percent of HDOs and 43 percent of manufacturers do not test devices at all.
- **Lack of accountability.** While 41 percent of HDOs believe they are primarily responsible for the security of medical devices, almost one-third of both device makers and HDOs say no one person or function in their organizations is primarily responsible.
- **FDA guidance is not enough.** Only 51 percent of device makers and 44 percent of HDOs follow current FDA guidance to mitigate or reduce inherent security risks in medical devices.

"These findings underscore the cybersecurity gaps that the healthcare industry desperately needs to address to safeguard the well-being of patients in an increasingly connected and software-driven world," said Mike Ahmadi, global director of critical systems security for Synopsys' Software Integrity Group. "As we saw with the past two studies on the Building Security in Maturity Model (BSIMM), the healthcare industry continues to struggle when it comes to software security. The industry needs to undergo a fundamental shift, building security into the software development lifecycle and across the software supply chain to ensure medical devices are not only safe, but also secure."

A complete copy of the "Medical Device Security: An Industry Under Attack and Unprepared to Defend" report can be found here. In addition, Synopsys and the Ponemon Institute are hosting a webinar on June 21 at 9 a.m. PT to discuss the key findings of the study.

More information about software security for the healthcare industry can be viewed here.

About the Survey

The report – Medical Device Security: An Industry Under Attack and Unprepared to Defend – consists of two sets of survey responses. The first group of participants is a sampling frame of 5,996 individuals who are involved in or have a role as a device maker, returning a total of 277 responses. Reliability checks required the removal of 35 surveys. The final sample consists of 242 surveys, or a 4 percent response rate. The second group of participants is a sampling frame of 7,991 individuals who are involved in or have a role as an HDO, returning a total of 287 responses. Reliability checks required the removal of 25 surveys. The final sample consists of 262 surveys, or a 3.3 percent response rate. Survey respondents included decision makers in manufacturing, quality assurance, IT, security and compliance among others.

About the Synopsys Software Integrity Platform

Through its Software Integrity Platform, Synopsys provides advanced solutions and services for improving software security and quality. This comprehensive platform of automated analysis and testing technologies integrates seamlessly into the software development process and enables organizations to detect and remediate quality defects, security vulnerabilities and compliance issues early in the software development lifecycle, as well as to gain security assurance and visibility into their software supply chain.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contacts:
Simone Souza
Synopsys, Inc.
650-584-6454
simone@synopsys.com

SOURCE Synopsys, Inc.