Black Duck Newsroom

For the Second Consecutive Year, Synopsys Survey Shows Web and Mobile Applications Are Top Security Challenges for IT Professionals in Asia

In Addition, Despite the Rise in Open Source Software (OSS) Adoption, 30 Percent of Organizations Still Lack an Inventory Management Process for OSS

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

SINGAPORE, Oct. 16, 2018 – Synopsys, Inc. (Nasdaq: SNPS) today announced the results of its 2018 survey of 251 IT professionals revealing that customer-facing web applications continue to present the highest security risk to businesses in Asia Pacific (36 percent of the respondents), followed by internal-facing web applications (26 percent) and mobile applications (25 percent). Seventy-one percent of the respondents reported that they have an incident response plan in place in the event of a security incident, an increase over 2017.

Geok Cheng Tan, managing director of Asia Pacific at the Synopsys Software Integrity Group commented, “It is not surprising that web and mobile applications continue to pose such a major challenge to businesses in the Asia Pacific region, as they often process highly sensitive information and cyber-attacks targeting them are growing in sophistication. With an escalating number of cyber security incidents large and small, it is increasingly clear that software development life cycles (SDLC) have to be not about pushing software quickly to market, but building software quickly and securely.”

Main findings of the survey

The survey covered a broad spectrum of important areas, including cyber security and incident response strategies, types of applications at risk, availability of skilled cyber security personnel at the workplace, training and development, and open source adoption approaches. The five main findings from the 2018 survey are as follows:

1. Web and mobile applications present the highest risk

A total of 36 percent of the respondents viewed customer-facing web applications as the area presenting the highest security risk to businesses, followed by internal-facing web applications at 26 percent and mobile applications at 25 percent. Desktop applications and embedded and IoT systems were represented at 24 percent and 16 percent respectively. (Participants were allowed to choose multiple responses to this question.)

2. More organizations have a cyber security incident response strategy

Seventy-one percent of the respondents reported they have a strategy in place in the event of a security incident, a slight improvement over last year’s 66 percent. Thirteen percent said they do not, while 16 percent said that they were unsure.

3. Organizations are not managing open source risk well

Forty-three percent of the respondents have an established process for inventorying and managing open source software, while 30 percent reported that they do not. Twenty-seven percent of the respondents say

they do not use open source.

4. Lack of skilled security personnel is a top challenge
Fifty-six percent of those surveyed highlighted the lack of skilled security personnel or training as one of the biggest challenges to implementing an application security program. Eighteen percent of the respondents said little or no budget is available, while 17 percent identified lack of management buy-in. (Participants were allowed to choose multiple responses to this question.)

5. Organizations recognize the importance of cyber security training
Eighty-three percent of those surveyed have received some form of cyber security training (mandatory or ad hoc), which underlines the importance of training to help organizations protect against threats.

Survey methodology
The survey was conducted at GovernmentWare (GovWare) 2018 from September 18 to 20, 2018, in Singapore, the anchor conference at the Singapore International Cyber Week 2018 – the region's most established cyber security convention. The in-person survey is based on responses from attendees, including C-level IT professionals as well as managers and other executives.

About the Synopsys Software Integrity Platform
Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle. Learn more at www.synopsys.com/software

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
Hui Peng Ter
McGallen & Bolden
+65 6324 6588
synopsys@mcgallen.com

---

https://news.blackduck.com/2018-10-15-For-the-Second-Consecutive-Year-Synopsys-Survey-Shows-Web-and-Mobile-Applications-Are-Top-Security-Challenges-for-IT-Professionals-in-Asia