

Singapore kicks off licencing cybersecurity vendors

- A Monitor Desk Report

Date: 17 April, 2022



Vendors offering two categories of cybersecurity services in Singapore now must apply for a licence to continue providing such services. They have up to six months to do so or will have to cease the provision of such services, if they do not wish to face the possibility of a jail term or fine.

Specifically, companies that provide penetration testing as well as managed security operations centre (SOC) monitoring services will need a licence to offer these services in Singapore. These include companies and individuals directly engaged in such services, third-party vendors that support these companies, and resellers of the licensable cybersecurity services, according to Cyber Security Authority (CSA) Singapore.

The industry regulator said the licensing framework, effective from April 11, was parked under the country's Cybersecurity Act and aimed to better protect consumers' interests. It also served to improve service providers' standards and standing over time.

CSA added that the two service categories were prioritised to kickstart the licensing regime because providers of these services had significant access into their customers' ICT systems and sensitive data.

Should such access be abused, the client's operations could be disrupted, the regulator noted. It added that because these services were widely available and adopted, they also had the potential to cause significant impact on the wider cybersecurity landscape.

Existing vendors currently engaged in the provision of either or both service categories had up to October 11, 2022, to apply for a licence. Those that failed to do so on time would have to stop providing the service until a licence was obtained.

A CSA spokesperson said white hat or ethical hackers involved in such initiatives aimed to uncover vulnerabilities in systems, which then were reported to the

organisation in the bug bounty programme for remediation.

Businesses that organised bug bounty programmes and the individual white hat hackers involved in such initiatives were excluded from the licensing framework, unless they also were in the business of providing penetration testing or managed SOC services, the spokesperson said.

“Bug bounty programmes complement the conventional methods of vulnerability assessment and penetration testing, enabling the participant undergoing the programme to benchmark its defences against the global and local community of researchers and white hats,” CSA told .

Services providers required to have licences under the new framework should submit their application for one within six months. They would be permitted to continue delivering the licensable service until a decision on the application was made.

Any person who provided the licensable services without a licence after October 11, 2022, would face a fine not exceeding SG\$50,000 (\$36,673) or a jail term of up to two years, or both.

Individuals would have to pay SG\$500 for their licence, while businesses would have to fork out SG\$1,000. Each licence would be valid for two years.

CSA said there would be a one-time 50% fee waiver for applications submitted within the first year, before April 11, 2023.

-B