KEY FINDING 3

There were a number of vulnerabilities, weaknesses, and misconfigurations in the SingHealth network and SCM system that contributed to the attacker's success in obtaining and exfiltrating the data, many of which could have been remedied before the attack

KEY FINDING 4

The attacker was a skilled and sophisticated actor bearing the characteristics of an Advanced Persistent Threat group

Key Finding #4-1

1. The attacker had a clear goal in mind, namely the personal and outpatient medication data of PM in the main, and other patients.

2. The attacker employed advanced TTPs (tools/tactics, techniques, procedures), as seen from the suite of advanced, customised, and stealthy malware used, generally stealthy movements, and its ability to find and exploit various vulnerabilities in SingHealth's IT network and the SCM application.

Key Finding #4-2

3. The attacker was persistent, having established multiple footholds and backdoors, carried out its attack over a period of over 10 months, and made multiple attempts at accessing the SCM database using various methods.

4. The attacker was a well-resourced group, having an extensive command and control network, the capability to develop numerous customised tools, and a wide range of technical expertise.

KEY FINDING 5

While our cyber defences will never be impregnable, and it may be difficult to prevent an Advanced Persistent Threat from breaching the perimeter of the network, the success of the attacker in obtaining and exfiltrating the data was not inevitable