

# Lack of monitoring at the SCM database for unusual queries and access

- database activity monitoring (“**DAM**”) solutions available on the market which could address some or all of the three gaps highlighted above.
  - DAM was not implemented by IHiS at the time of the attack


# SGH Citrix servers were not adequately secured against unauthorised access

The **compromise of the SGH Citrix servers was critical** in giving the attacker access to the SCM database.

- *Privileged Access Management was not the exclusive means for accessing the SGH Citrix servers, and **logins to the servers** by other **means without 2-factor authentication were possible!***
- *IHiS Citrix administrators not only were aware of this alternative route, but made use of it for convenience!*

SGH Citrix servers were not adequately secured against unauthorised access

*Lack of firewalls to prevent unauthorised remote access using RDP to the SGH Citrix servers*

- RDP in cybersecurity stands for **Remote Desktop Protocol**. 
- It is a proprietary network communication protocol developed by **Microsoft** that enables a user to connect to and control another computer remotely over a network connection

# *Observations on the overall management of SGH Citrix servers*

They were treated as not mission critical, unlike SCM database

- The SGH Citrix servers were not monitored for real-time analysis and alerts of vulnerabilities and issues arising from these servers.
- Vulnerability scanning, which was carried out for mission-critical systems, was not carried out for the SGH Citrix servers.
  - Vulnerability scanning is an inspection of the potential points of exploit on a computer to identify gaps in security.

# Internet connectivity in the SingHealth IT network increased the attack surface

- The SingHealth network's connection to the Internet, while serving their operational needs, created an avenue of entry and exit for the attacker.
- This allowed the attacker to make use of an internet-connected workstation (Workstation A) to gain entry to the network, before making his way to the SCM database to steal the medical data.