

**Network connections between the SGH Citrix servers & SCM database were allowed**

# Network connections between the SGH Citrix servers & SCM database were allowed

- This **open connection IS not necessary**, more for convenience to administer database (**we shud reduce attack surface area**)
- A basic security review of the network architecture and connectivity between the SGH Citrix servers and the SCM database could have shown that the open network connection created a security vulnerability.
- However, no such review was carried out.
- **MORAL: GET RID OF UNNECESSARY CONNECTIONS!**

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

From 26 June to 4 July 2018, attacker ran queries on the SCM database, including bulk queries. Attacker was able to do so unchallenged because of a lack of monitoring at the SCM database

- there were no existing controls to detect bulk queries being made to the SCM database.
- there were no controls in place at the time of the attack to detect or block any queries to the SCM database made using illegitimate applications.

# 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!*