

Crisis in a Nutshell

- At time of the Cyber Attack, SingHealth owns the SCM system.
- Integrated Health Information Systems Private Limited (“IHiS”) was responsible for administering and operating the system, including implementing cybersecurity measures.
- IHiS was also responsible for security incident response and reporting.

Figure 3: SingHealth user authentication process to access the SCM Database

USER WORKSTATION



USER PC



USER PC



USER PC



USER PC



USER PC

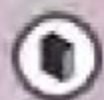
CITRIX FARM



CITRIX SERVER
(SCM CLIENT)



CITRIX SERVER
(SCM CLIENT)



CITRIX SERVER
(SCM CLIENT)

SCM SERVERS



SCM SECURITY
SERVER



SCM DATABASE



SCM SERVERS

01.

Users launch
SCM via CITRIX
at User PC

02.

User Credential
sent to SCM
Security for
authentication

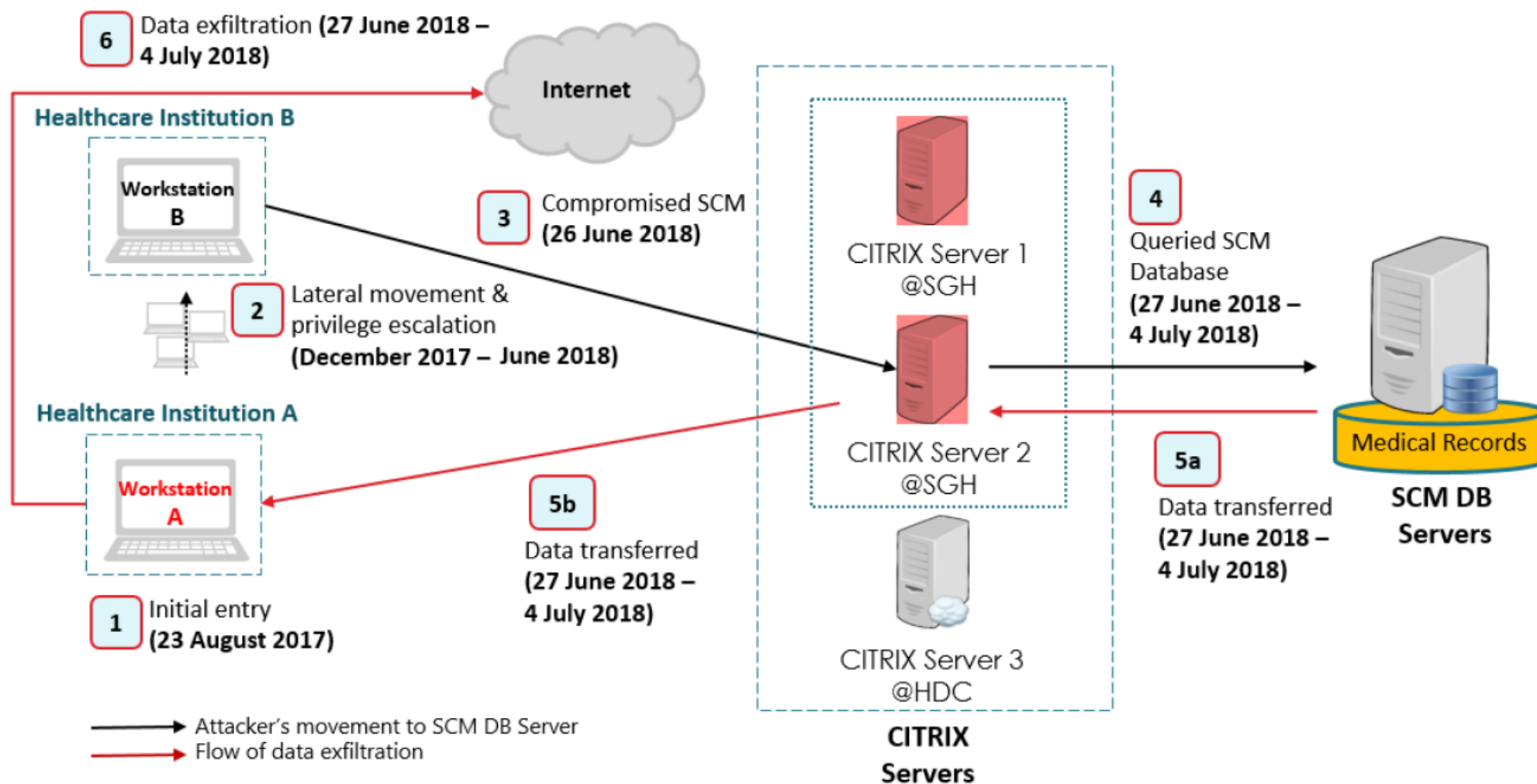
03.

Authenticated

04.

Users
successfully
log in and start
using SCM

Key Events of the Cyberattack -workflow



Summary of Key Events: 1

- The attacker gained initial access to SingHealth's IT network around 23/8/17, **infecting front-end workstations**, most likely through **phishing attacks**.
- Attacker then **lay dormant for 4 months**, before commencing **lateral movement (6 months)** in the **network between Dec2017 and Jun2018**, compromising many endpoints and servers, including the **Citrix servers** located in SGH, which were **connected to the SCM database**.
- Along the way, the attacker **also compromised a large number of user and administrator accounts**.

Summary of Key Events: 2

- Starting from May 2018, the attacker made use of **compromised user workstations** in the SingHealth IT network and suspected virtual machines to **remotely connect to the SGH Citrix servers**.