Incident Response case study SingHealth

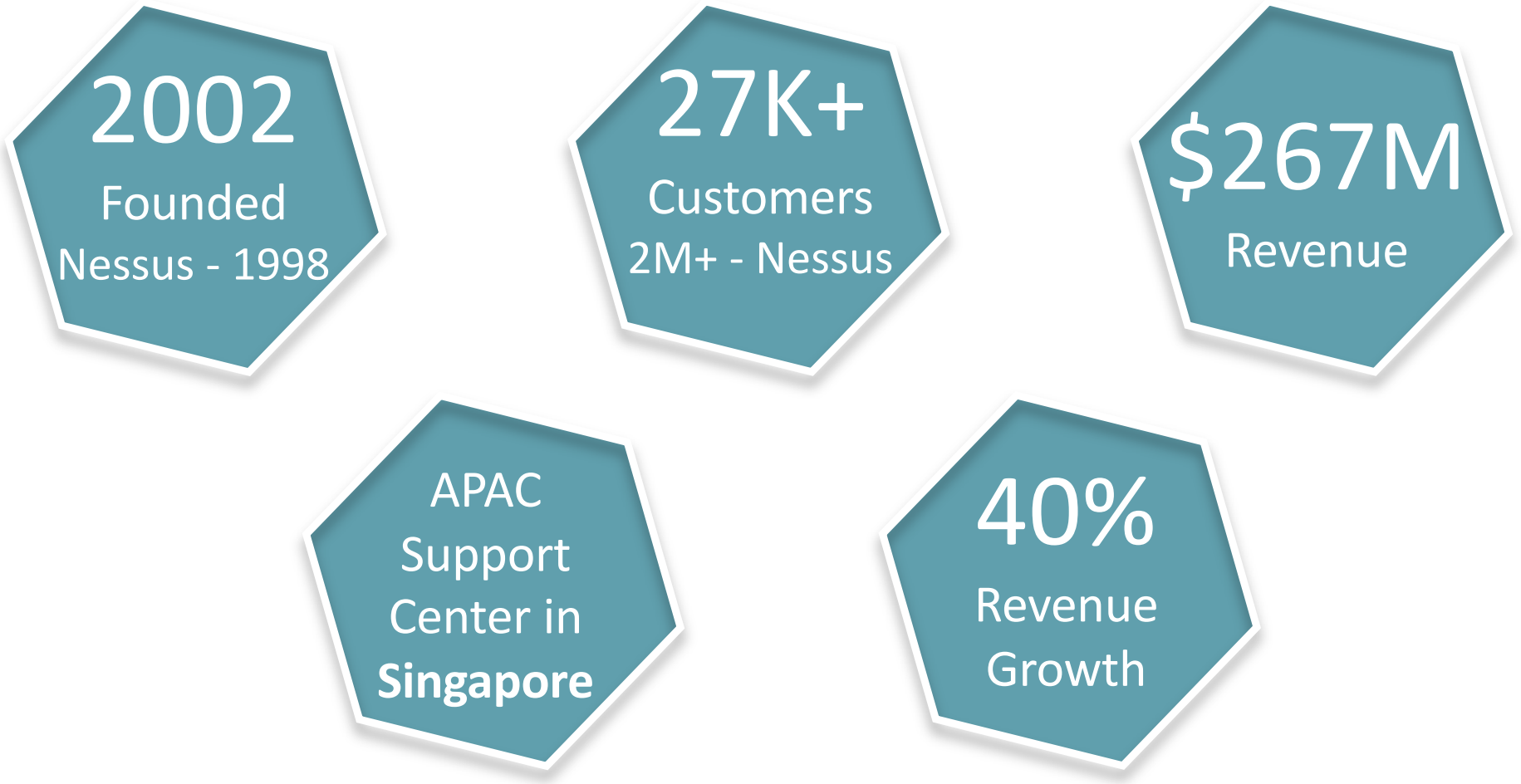
Suwitcha Musijaral,CISSP,CISA| Solution Architect

suwitcha@tenable.com

Agenda

- Background
- Incident Detail
- Incident Response activity
- Recommendation
- Q&A

About Tenable



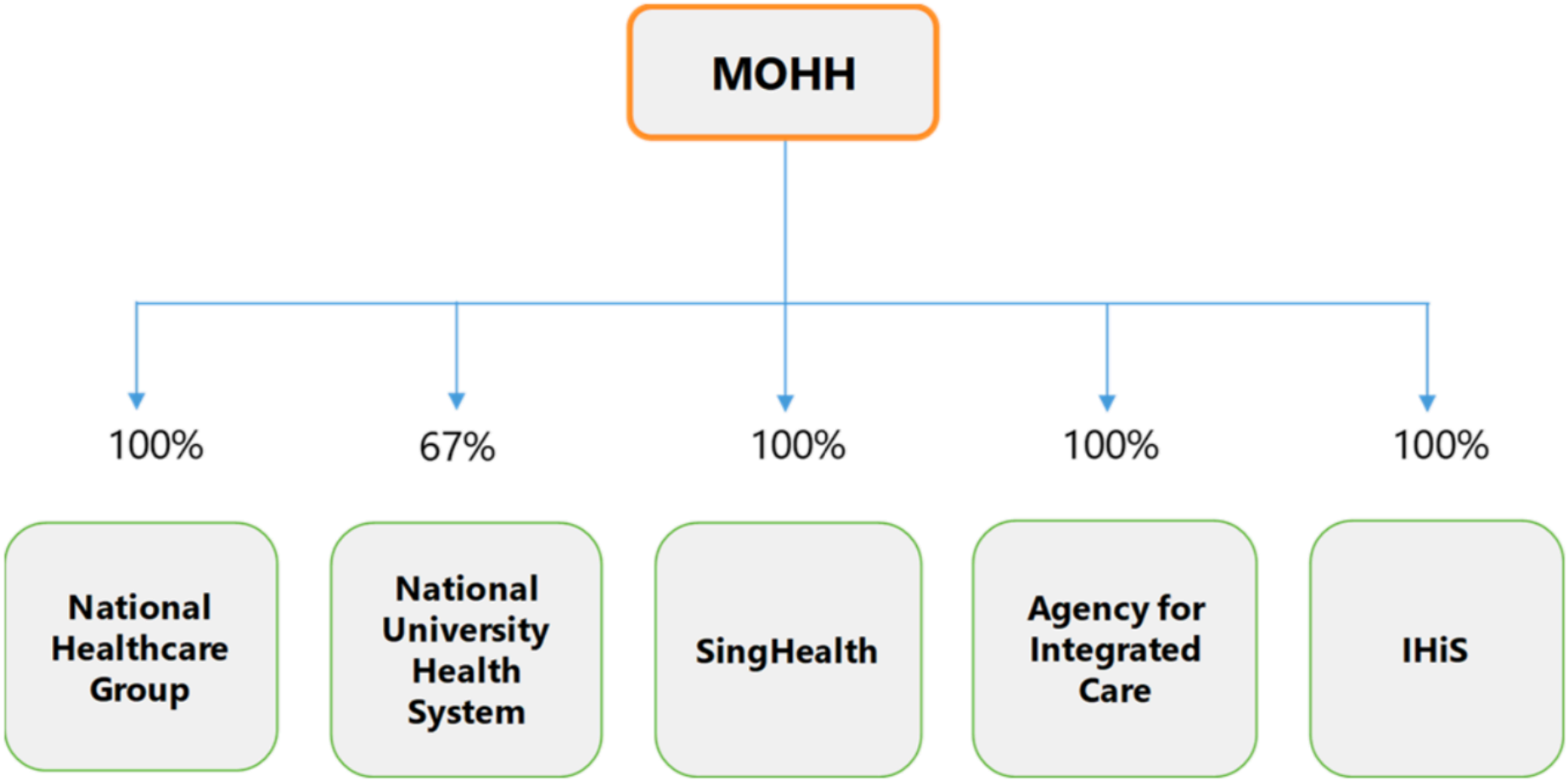
Tenable Pioneers Cyber Exposure

An emerging discipline for:

Managing and measuring your modern attack surface to accurately understand and reduce your cyber risk

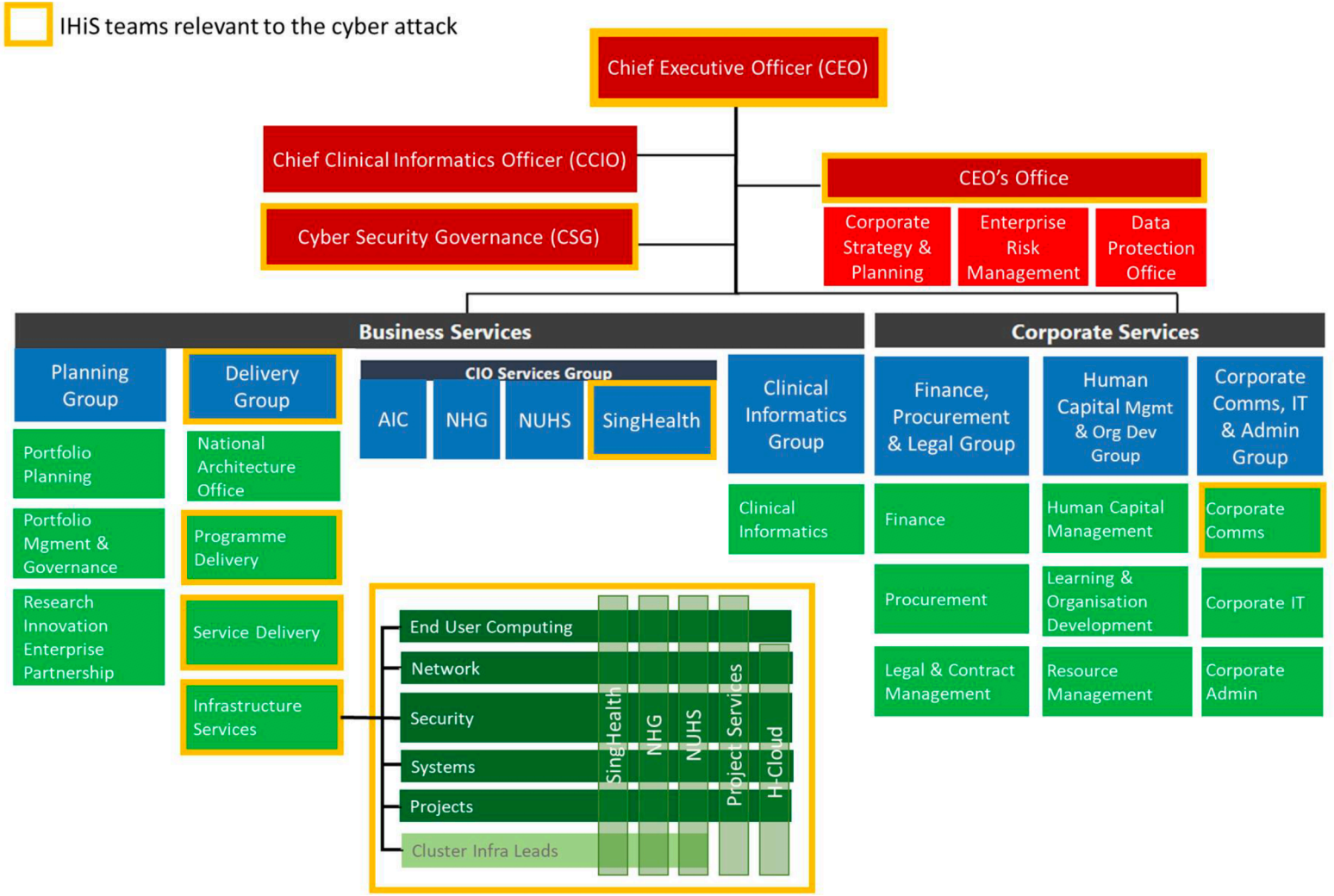
www.cyberexposure.com


CYBERUK
IN PRACTICE
CYBERUK
IN PRACTICE
It is rare for the agency to encounter a “zero-day” exploit. In fact, the NSA has not responded to an intrusion that uses a zero-day vulnerability in over 24 months.
Dave Hogue, Technical Director – National Security Agency


MOHH
100%
67%
100%
100%
100%
National Healthcare Group
National University Health System
SingHealth
Agency for Integrated Care
IHiS

Corporate Profile

Integrated Health Information Systems (IHiS) [*pronounced as i-his*] is the technology agency for the public healthcare sector. A multi-award-winning healthcare IT leader, IHiS digitises, connects, and analyses Singapore's health ecosystem. Its ultimate aim is to improve the Singapore population's health and health administration by integrating intelligent, highly resilient, and cost effective technologies with process and people.


IHiS teams relevant to the cyber attack
Chief Executive Officer (CEO)
Chief Clinical Informatics Officer (CCIO)
Cyber Security Governance (CSG)
CEO's Office
Corporate Strategy & Planning
Enterprise Risk Management
Data Protection Office
Business Services
Corporate Services
Planning Group
Portfolio Planning
Portfolio Mgment & Governance
Research Innovation Enterprise Partnership
Delivery Group
National Architecture Office
Programme Delivery
Service Delivery
Infrastructure Services
CIO Services Group
AIC
NHG
NUHS
SingHealth
Clinical Informatics Group
Clinical Informatics
Finance, Procurement & Legal Group
Finance
Procurement
Legal & Contract Management
Human Capital Mgmt & Org Dev Group
Human Capital Management
Learning & Organisation Development
Resource Management
Corporate Comms, IT & Admin Group
Corporate Comms
Corporate IT
Corporate Admin
End User Computing
Network
Security
Systems
Projects
Cluster Infra Leads
SingHealth
NHG
NUHS
Project Services
H-Cloud

SECURITY BY THE NUMBERS

Scale of Operations & Security Across Public Healthcare

DETECTING SECURITY THREATS ON A DAILY BASIS

500	72 MILLION	4,611
FIREWALL DENIED ATTEMPTS PER SECOND	EMAIL MESSAGES BLOCKED (99%) PER MONTH	MALWARE CLEANED & QUARANTINED PER MONTH

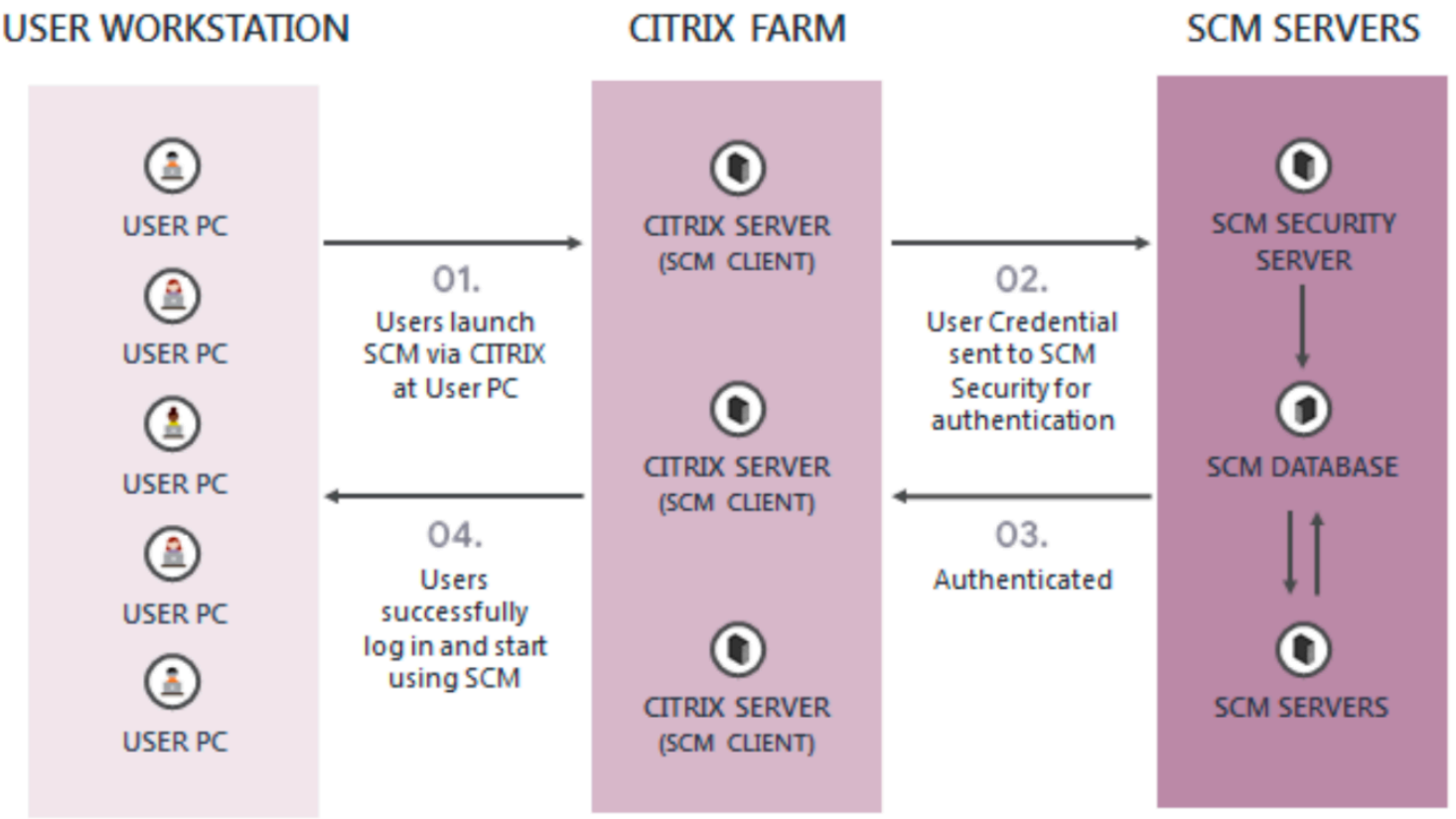
CONTINUOUS MONITORING FOR ATTACKS

3 TB	534 TB
INTERNET TRAFFIC PER DAY	SECURITY LOGS ANALYSED PER MONTH

MANAGING A COMPLEX HEALTHCARE ENVIRONMENT

60,852	6,232	14,635
ENDPOINTS	SERVERS	NETWORK EQUIPMENT

SingHealth Sunrise Clinical Manager



By Kevin Kwang
@KevinKwangCNA

20 Jul 2018 05:29PM
(Updated: 18 Oct 2018 11:17AM)

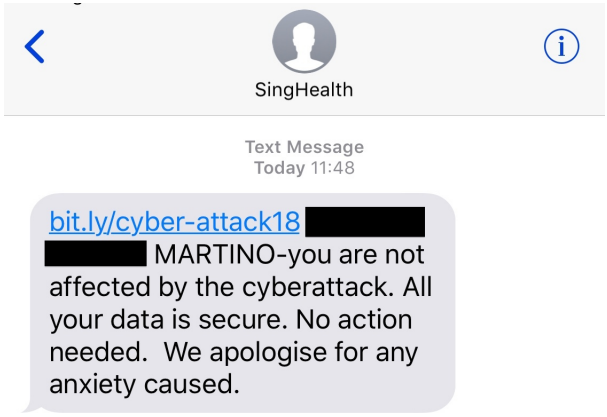
Bookmark

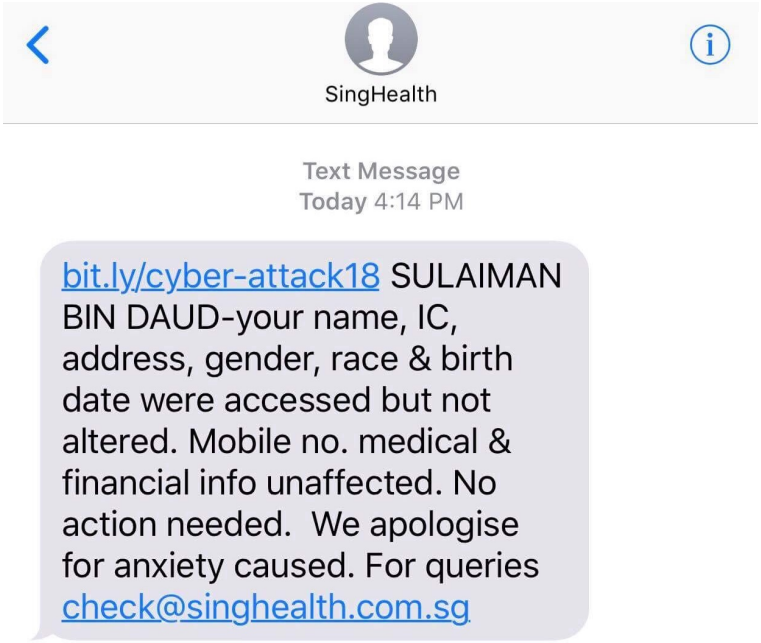
Singapore

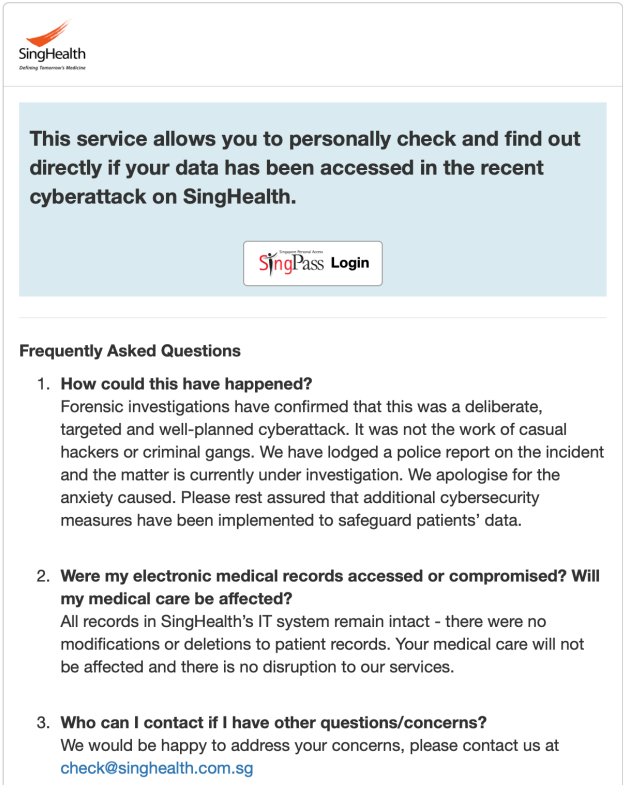
Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.

The "most serious breach of personal data" in Singapore's history took place last month, with 1.5 million SingHealth patients' records accessed and copied while 160,000 of those had their outpatient dispensed medicines' records taken, according to the Ministry of Health and Ministry of Communications and Information. Lee Li Ying has more with the story.

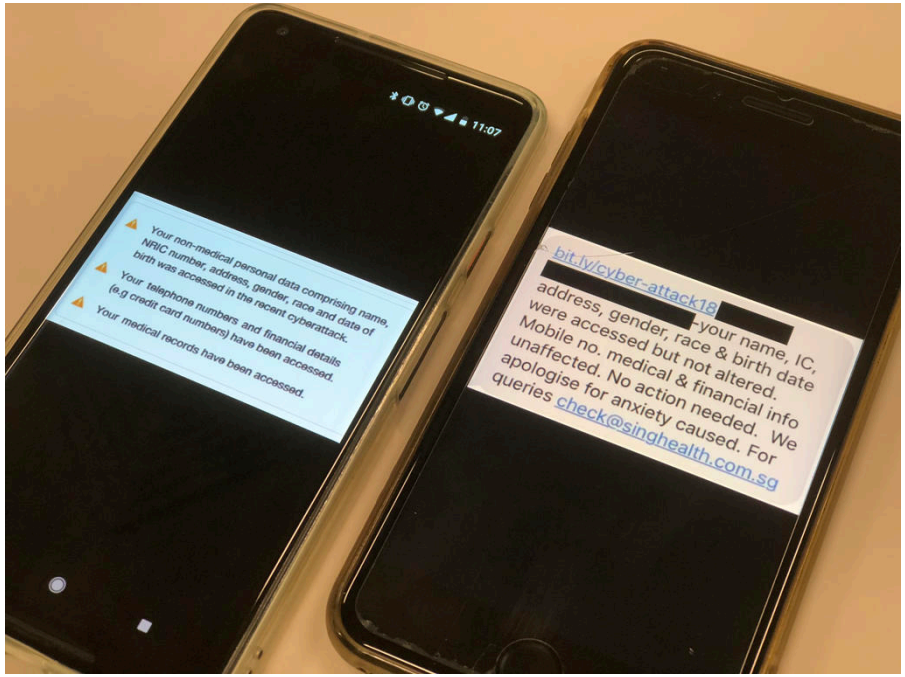






https://mothership.sg/2018/07/goh-chok-tong-singhealth-cyberattack/

Fake SMS



https://www.todayonline.com/singapore/singhealth-warns-fake-smses-capitalising-news-recent-cyberattack

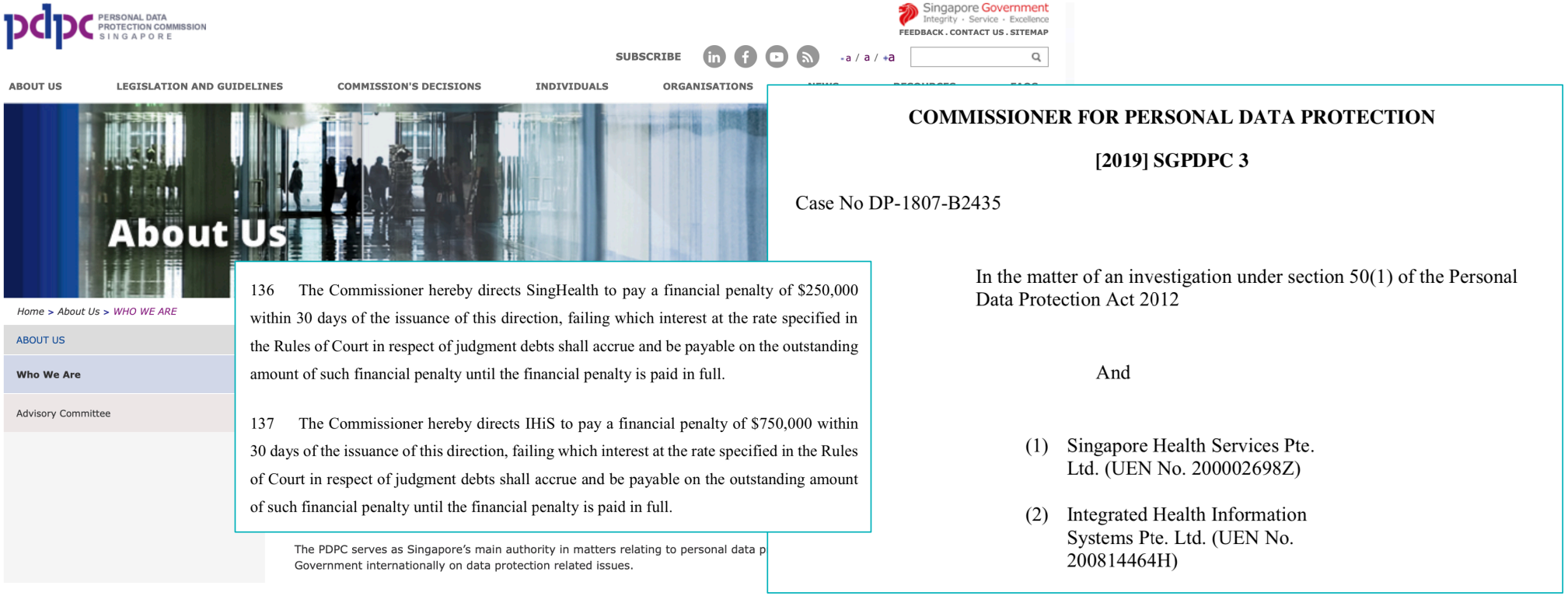
A Singapore Government Agency Website

CSA SINGAPORE

Who We Are | News | Legislation | Programmes | SingCERT | Gosafeonline | Careers

The Cyber Security Agency of Singapore (CSA) is the national agency overseeing cybersecurity strategy, operations, education, outreach, and ecosystem development.

Personal Data Protection Commission



https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf

IHiS fined record S$750,000, SingHealth with S$250,000 for Singapore's worst data breach

TUE, JAN 15, 2019 - 12:40 PM

SINGAPORE'S privacy watchdog has meted out its largest fine of S$750,000 to Integrated Health Information Systems (IHiS) for lapses in securing patient data which resulted in the nation's worst data breach.

The cyber attack on SingHealth in June 2018 compromised the personal information of 1.5 million patients, including Prime Minister Lee Hsien Loong.

Even though IHiS is the technology vendor for Singapore's healthcare sector, SingHealth also has to take responsibility as the owner of the patient database system - a point that the Personal Data Protection Commission (PDPC) stressed in dishing out penalties.

As such, SingHealth was fined S$250,000, the second largest here.

BREAKING

02:07 PM ICE to launch Bitcoin futures contract in Singapore on Dec 9

Incident Detail

tenable

Background

- Committee of Inquiry published extremely detailed report on the SingHealth database breach of August 2017 through July 2018
  - The **424** page report sections include Preliminaries, Events & Contributing factors leading to attack, Incident Response, Key findings and Recommendations (16)
- We'll look at some of the recommendations and how Tenable can help meet them

Download full report

- https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi

✖ CLOSE

10 Jan 19

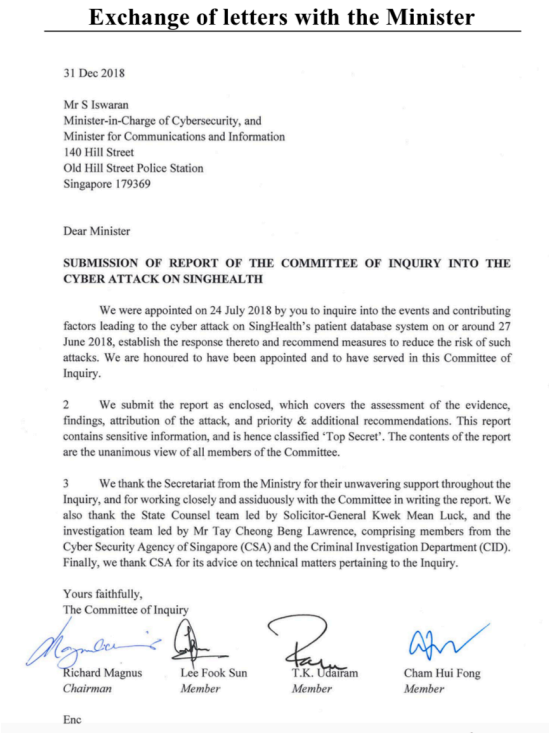
Public Report of the Committee of Inquiry (COI) into the cyber attack on Singapore Health Services Private Limited Patient Database

Category: Cyber Security Type: Press Releases

10 January 2019 - The Committee of Inquiry (COI)[1], convened to inquire into the events and contributing factors leading to the cyber attack on Singapore Health Services Private Limited (SingHealth)'s patient database system, has released its public report.

The report is accessible here.

[1]Convened on 24 July 2018, the chairman of the COI is Retired Senior (subsequently termed Chief) District Judge Mr Richard R Magnus. The other members of the Committee are Mr Lee Fook Sun, Director and Chairman of Ensign InfoSecurity; Mr T K Udairam, Group Chief Operating Officer of Sheares Healthcare Management Pte Ltd; and Ms Cham Hui Fong, Assistant Secretary-General of the National Trades Union Congress.



Exchange of letters with the Minister

31 Dec 2018

Mr S Iswaran
Minister-in-Charge of Cybersecurity, and
Minister for Communications and Information
140 Hill Street
Old Hill Street Police Station
Singapore 179369

Dear Minister

SUBMISSION OF REPORT OF THE COMMITTEE OF INQUIRY INTO THE CYBER ATTACK ON SINGHEALTH

We were appointed on 24 July 2018 by you to inquire into the events and contributing factors leading to the cyber attack on SingHealth's patient database system on or around 27 June 2018, establish the response thereto and recommend measures to reduce the risk of such attacks. We are honoured to have been appointed and to have served in this Committee of Inquiry.

2 We submit the report as enclosed, which covers the assessment of the evidence, findings, attribution of the attack, and priority & additional recommendations. This report contains sensitive information, and is hence classified 'Top Secret'. The contents of the report are the unanimous view of all members of the Committee.

3 We thank the Secretariat from the Ministry for their unwavering support throughout the Inquiry, and for working closely and assiduously with the Committee in writing the report. We also thank the State Counsel team led by Solicitor-General Kwek Mean Luck, and the investigation team led by Mr Tay Cheong Beng Lawrence, comprising members from the Cyber Security Agency of Singapore (CSA) and the Criminal Investigation Department (CID). Finally, we thank CSA for its advice on technical matters pertaining to the Inquiry.

Yours faithfully,
The Committee of Inquiry

Richard Magnus	Lee Fook Sun	T.K. Udairam	Cham Hui Fong
Chairman	*Member*	*Member*	*Member*

Enc

PUBLIC REPORT OF THE COMMITTEE OF INQUIRY INTO THE CYBER ATTACK ON SINGAPORE HEALTH SERVICES PRIVATE LIMITED'S PATIENT DATABASE ON OR AROUND 27 JUNE 2018

10 JANUARY 2019

Executive Summary - Introduction

1. Between 23 August 2017 and 20 July 2018, a cyber attack (the "**Cyber Attack**") of unprecedented scale and sophistication was carried out on the patient database of Singapore Health Services Private Limited ("**SingHealth**"). The database was illegally accessed and the personal particulars of almost 1.5 million patients, including their names, NRIC numbers, addresses, genders, races, and dates of birth, were exfiltrated over the period of 27 June 2018 to 4 July 2018. Around 159,000 of these 1.5 million patients also had their outpatient dispensed medication records exfiltrated. The Prime Minister's personal and outpatient medication data was specifically targeted and repeatedly accessed.

Executive Summary – Introduction

2. The crown jewels of the SingHealth network are the patient electronic medical records contained in the SingHealth Sunrise Clinical Manager ("**SCM**") database. The SCM is an electronic medical records software solution, which allows healthcare staff to access real-time patient data. The SCM system can be seen as comprising front-end workstations, Citrix servers, and the SCM database. Users would access the SCM database *via* Citrix servers, which operate as an intermediary between front-end workstations and the SCM database. The Citrix servers played a critical role in the Cyber Attack.

Executive Summary - Introduction

3. At the time of the Cyber Attack, SingHealth was the owner of 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.

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

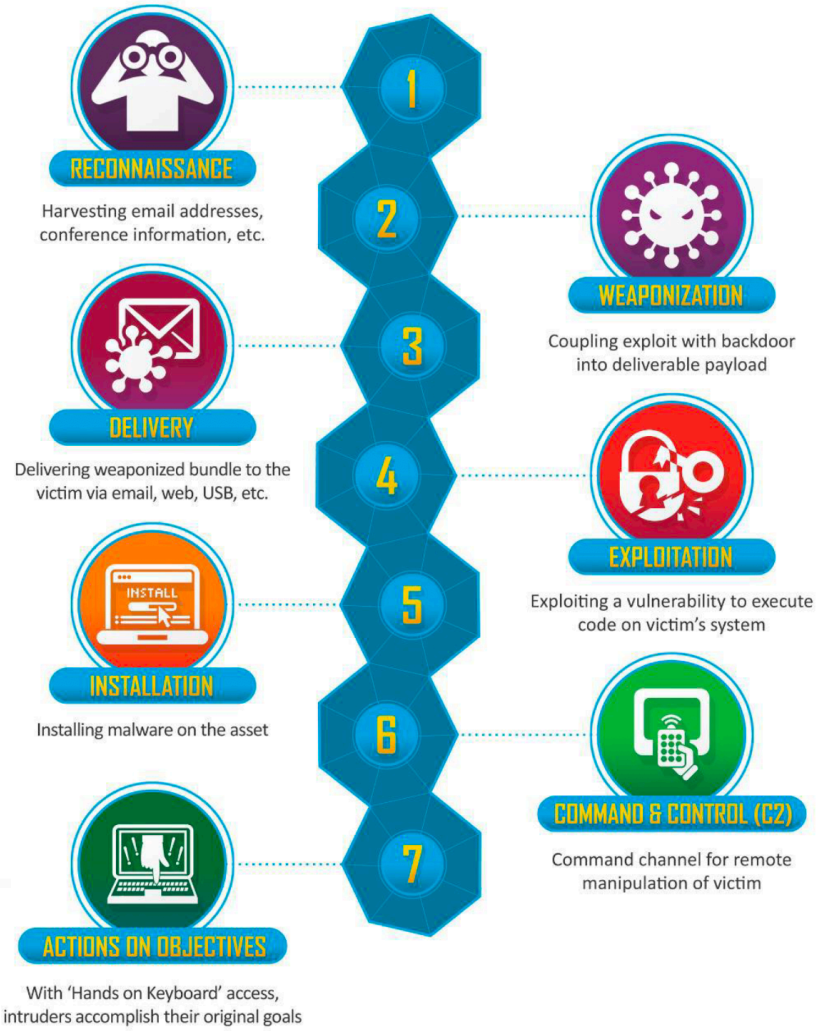
Eric M. Hutchins,* Michael J. Cloppert,† Rohan M. Amin, Ph.D.‡

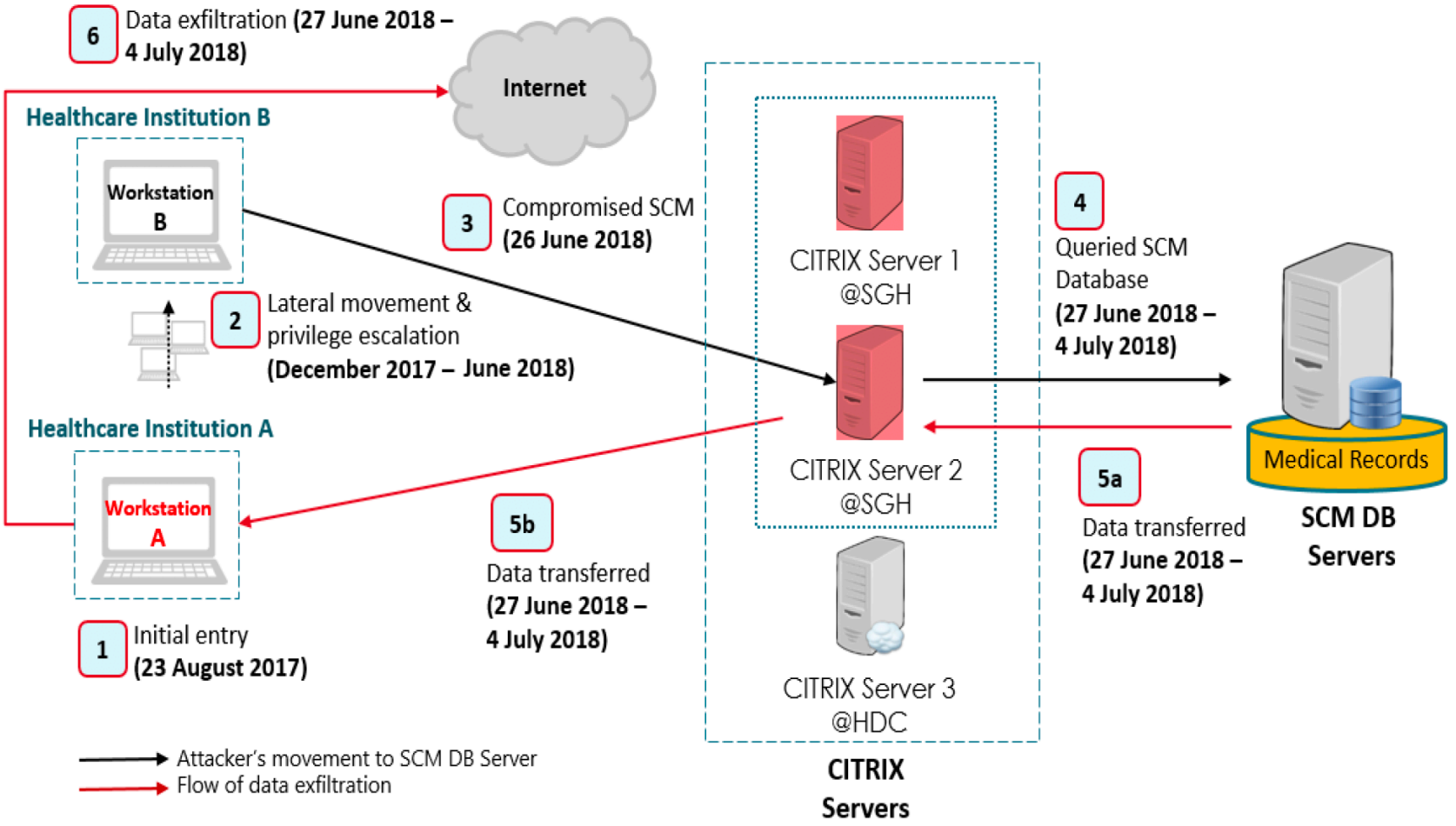
Lockheed Martin Corporation

Abstract

Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component

The Cyber Kill Chain developed by Lockheed Martin



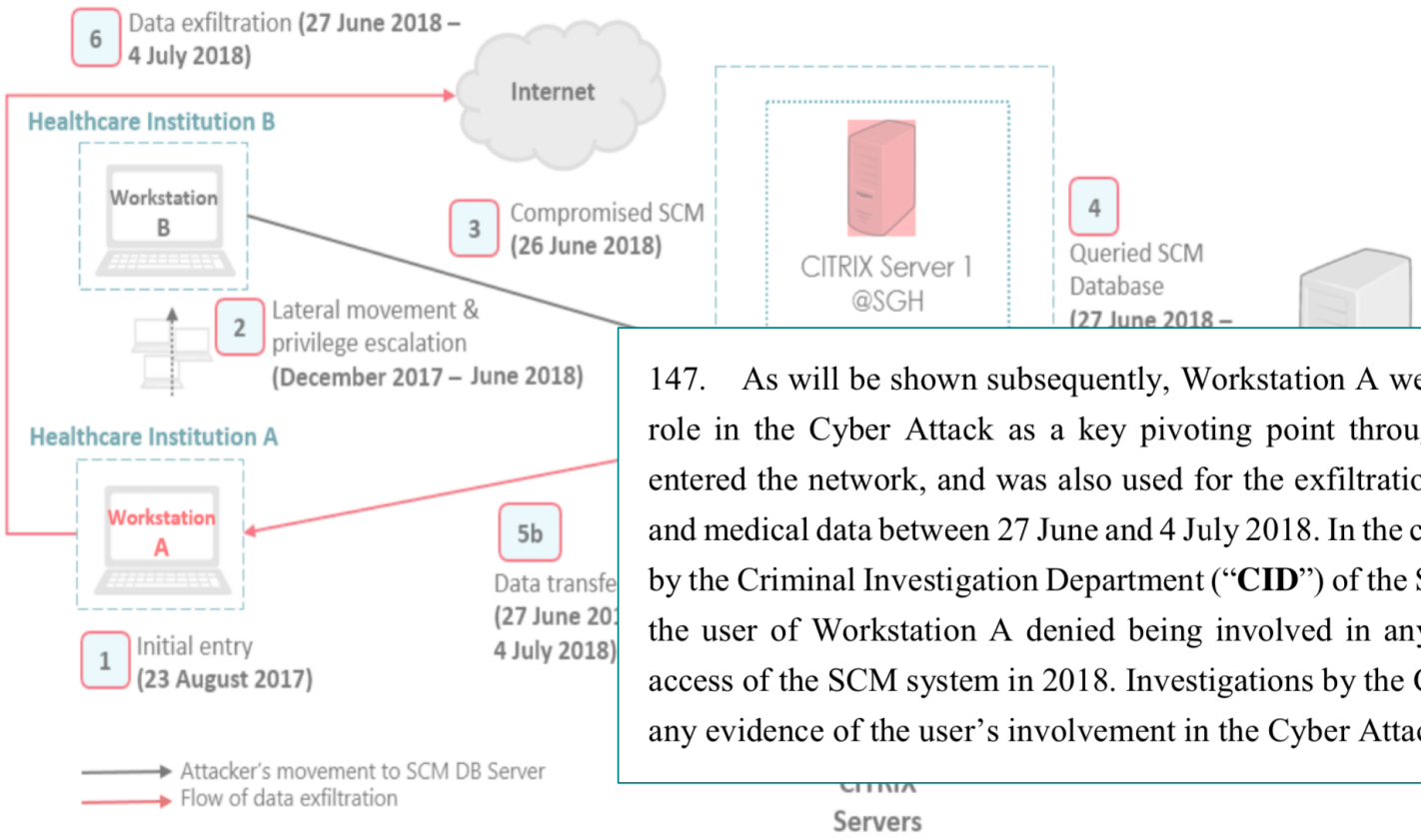


From report of the COI into the Cyber Attack on SingHealth

23 August 2017 – initial infection

- First infection machine (patient zero) is front end machine on healthcare outside SGH premise
- Detect from C&C callback
- Initial infected machine was decommission before incident discover (October 2017)
- 24 August , Second infected machine call to C&C

24 August 2017



147. As will be shown subsequently, Workstation A went on to play a critical role in the Cyber Attack as a key pivoting point through which the attacker entered the network, and was also used for the exfiltration of the stolen patient and medical data between 27 June and 4 July 2018. In the course of investigations by the Criminal Investigation Department ("**CID**") of the Singapore Police Force, the user of Workstation A denied being involved in any way in the unlawful access of the SCM system in 2018. Investigations by the CID also did not reveal any evidence of the user's involvement in the Cyber Attack.

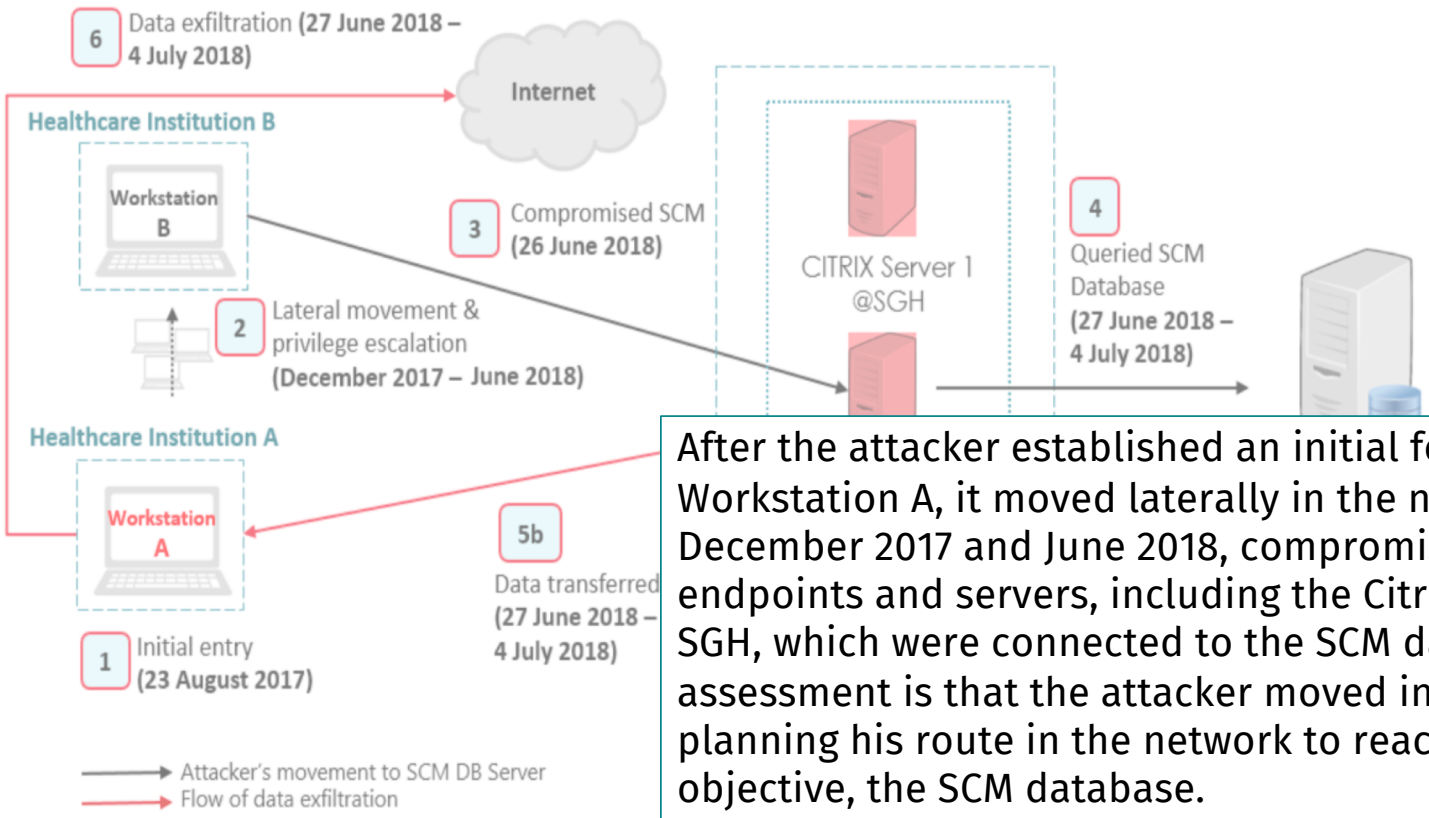
Workstation A forensic result

- Initial vector likely to be phishing e-mail
- Log file of password dump malware (contain username and password of user on workstation A) – 29th August 2017
- Public available hacking tools (implant backdoor on e-mail client) – 1st December 2017
- Remote Access Tools – 1st December 2017
- 23 August – 1st December 2017 to complete cyber kill chain

December 2017 – June 2018

- Lateral movement to compromise more workstation and server include Citrix Server and domain controller
- Use custom malware – stealth, undetected by standard Anti-malware solution
- Powershell command to copy malware via SMB share

December 2017 – June 2018



After the attacker established an initial foothold in Workstation A, it moved laterally in the network between December 2017 and June 2018, compromising a number of endpoints and servers, including the Citrix servers located in SGH, which were connected to the SCM database. CSA's assessment is that the attacker moved in a targeted manner, planning his route in the network to reach his ultimate objective, the SCM database.

Attacker outpost – NCC server

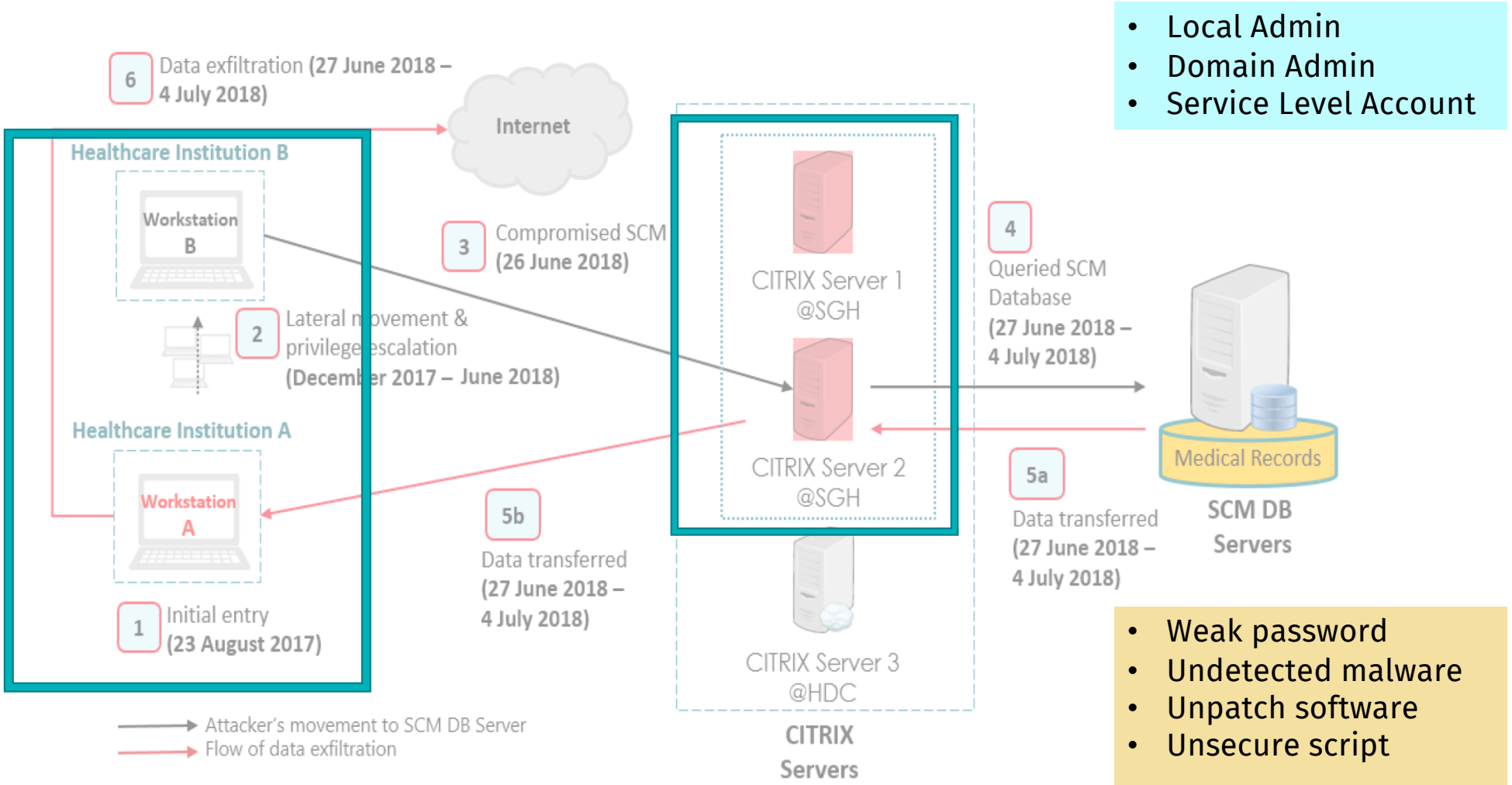
- A server in National Cancer Center , part of SingHealth Network was use to store malware, malicious script and become distribution point during attack
- Oldest malicious file on server was create on 29 September 2017 and January 2018 for malicious Powershell script
- Asset owner is iHIS but operate by NCC staff
  - iHIS best practice was not apply on this server include updated anti-malware solution

Attacker outpost – PHI workstation

- January 2018, Workstation at Public Health Intuition start call back to same C&C server as SGH workstation.
- 19 January 2018, iHIS staff detect malicious call back and block connect from PHI to C&C server
- Connection to C&C server from SGH network still allow until investigation start (10 July 2018)

SGH Server compromised

- Attacker gain access to local admin account on Citrix server and use to attack two Citrix Server in SGH data center.
  - Local admin password is ‘P@ssw0rd’ , attacker may get password hash via domain user account and decrypt for password
  - Or Attacker may obtain local admin password from script on one of Citrix server.
  - Service Level account also got compromise by malware
  - Finally, Domain Admin account also got compromised (detect later after attacker try to use domain account to gain access to others system (SGH and Cloud DC)

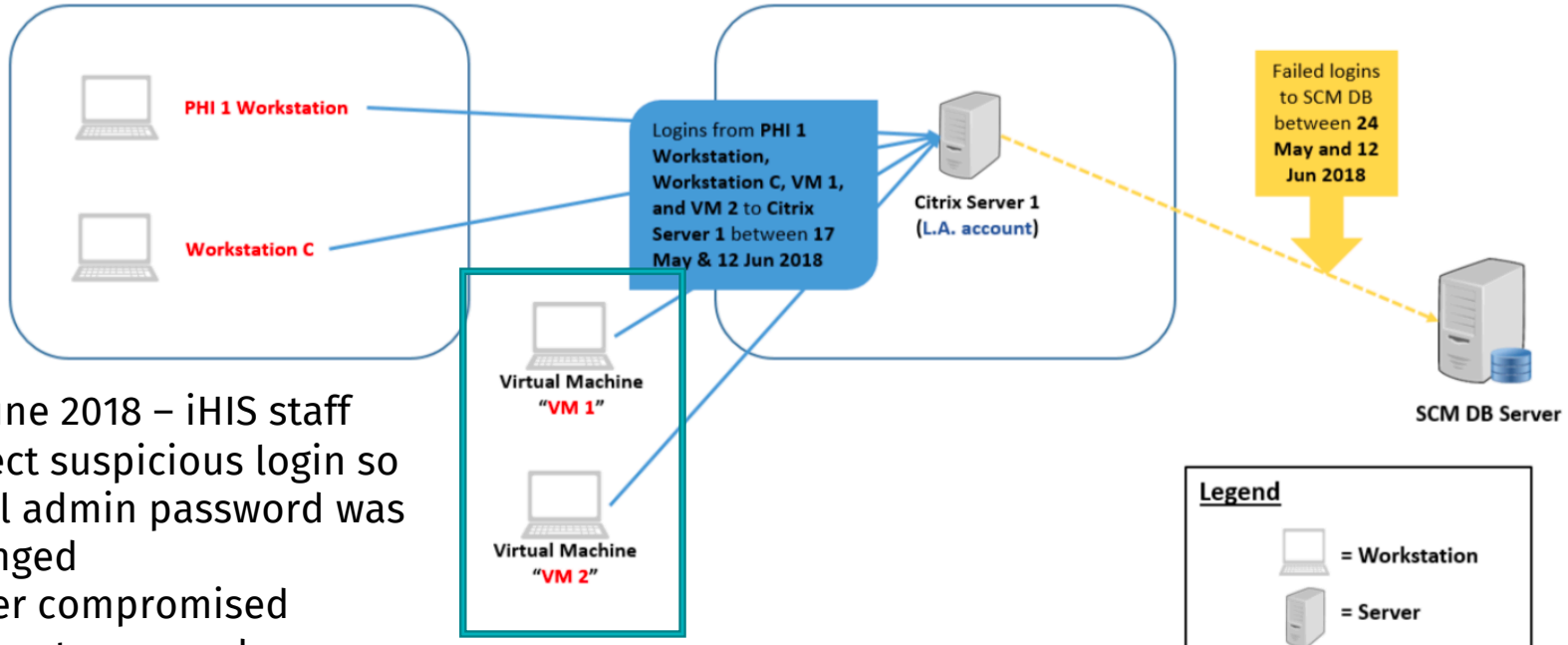


- Local Admin
- Domain Admin
- Service Level Account

- Weak password
- Undetected malware
- Unpatch software
- Unsecure script

24 May – 12 June 2018

- After too many suspicious login
- iHIS system admin shutdown Citrix server 1 on 13 June

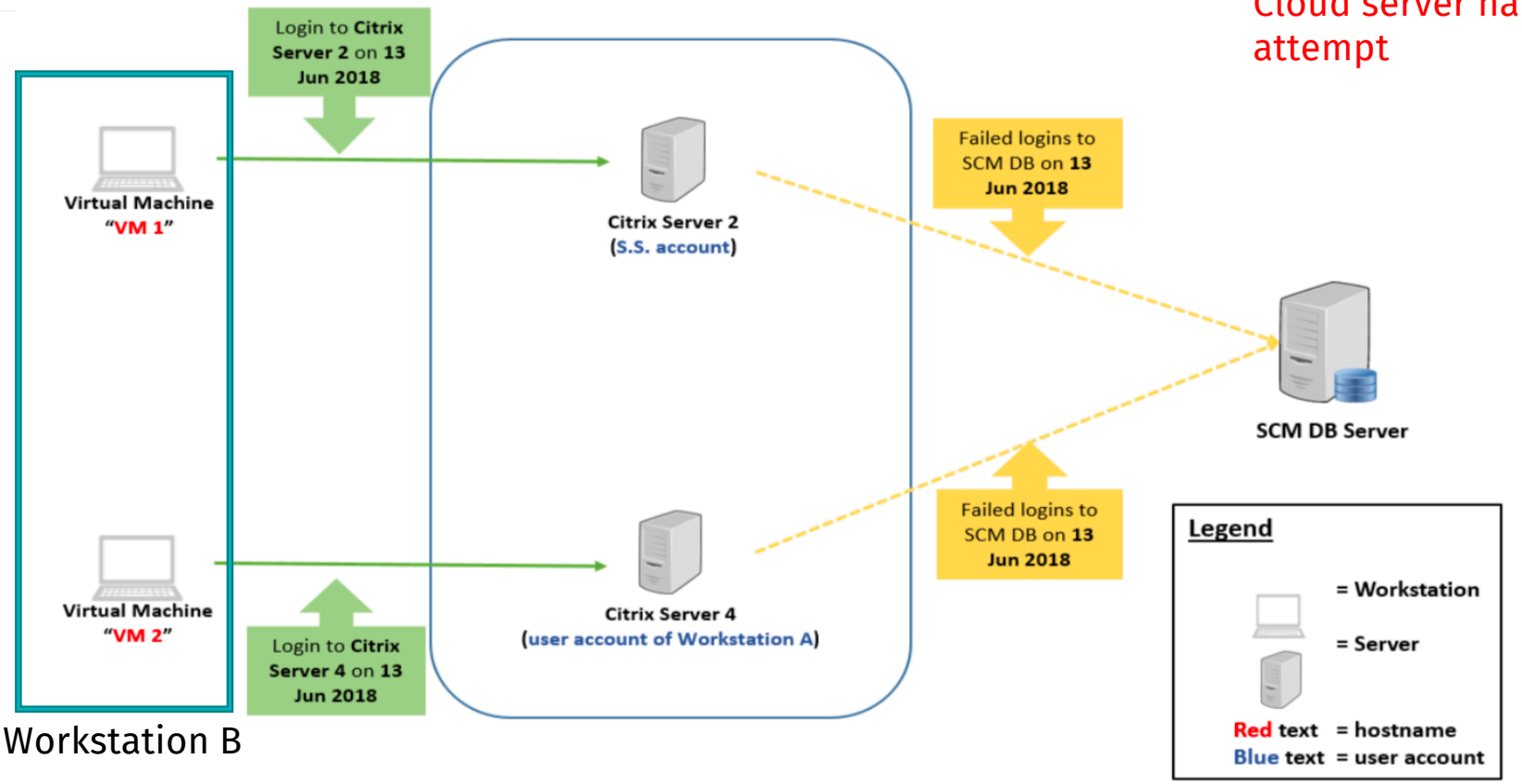


- 11 June 2018 – iHIS staff detect suspicious login so local admin password was changed
- Other compromised account was used
- System Event log was delete by attacker

From report of the COI into the Cyber Attack on SingHealth

13 June 2018

- Attacker use Service admin account to login to SCM
- Log also show attacker use Cloud server name in login attempt

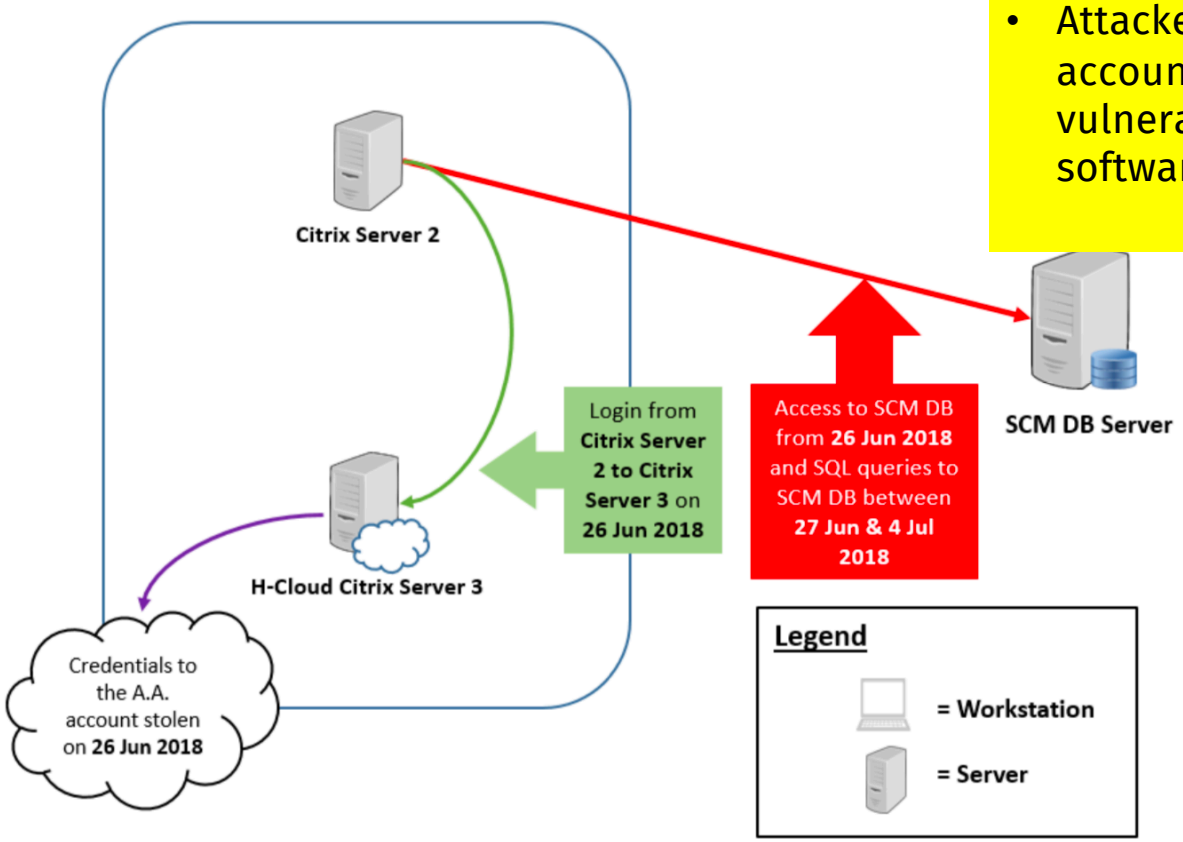


Workstation B

From report of the COI into the Cyber Attack on SingHealth

26 June 2018 – Successfully access to SCM

- From workstation B, attacker login to Citrix Server 2 using Service Account
- From Citrix Server 2, attacker login to Cloud server using Domain Admin
- Attacker get SCM account from cloud server
- SCM system was migrate to cloud on July 2017, no activity from local server to SCM since then.
- Migration plan to complete by August 2018 so local and cloud server still allow



- Attacker may get SCM account from code vulnerability in SCM software

Action on Objective (26 June – 4 July)

- Attacker start query to SCM database from workstation B(VM1,VM2)
- Query was run from standard iHIS program and attacker custom program
- Query on database schema, direct query to individual and bulk query patient information.
- 4 July, iHIS staff detect suspicious query and block all query

Result from attack

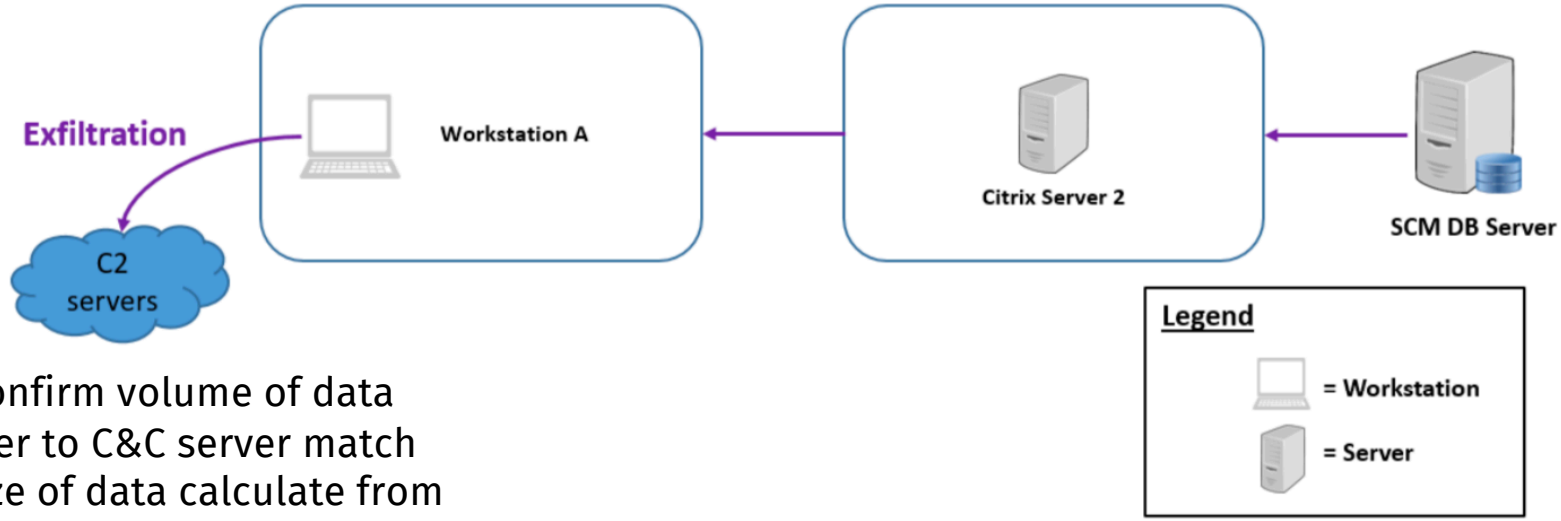
Between 27 June 2018 and 4 July 2018, the attacker was able to retrieve the following information from the SQL queries:

(a) The Prime Minister's personal and outpatient medication data;

(b) The demographic records of 1,495,364 unique patients, including their names, NRIC numbers, addresses, gender, race, and dates of birth; and

(c) The outpatient dispensed medication records of about 159,000 of the 1,495,364 patients mentioned in sub-paragraph (b) above.

Data Exfiltration



CSA confirm volume of data transfer to C&C server match the size of data calculate from query data from database

18-19 July 2018 Re-enter

- Attacker try to re-enter to SGH network
  - 18 July Phishing e-mail sent to SingHealth Institute which target same mail client vulnerability
  - iHIS staff detect and inform CSA on 1 August 2018
  - 19 July, one server in SGH network try to connect to C&C server. Malicious file also create on the same date
  - 20 July 2018, internet separation policy enforce

Episode 0 – software vulnerability

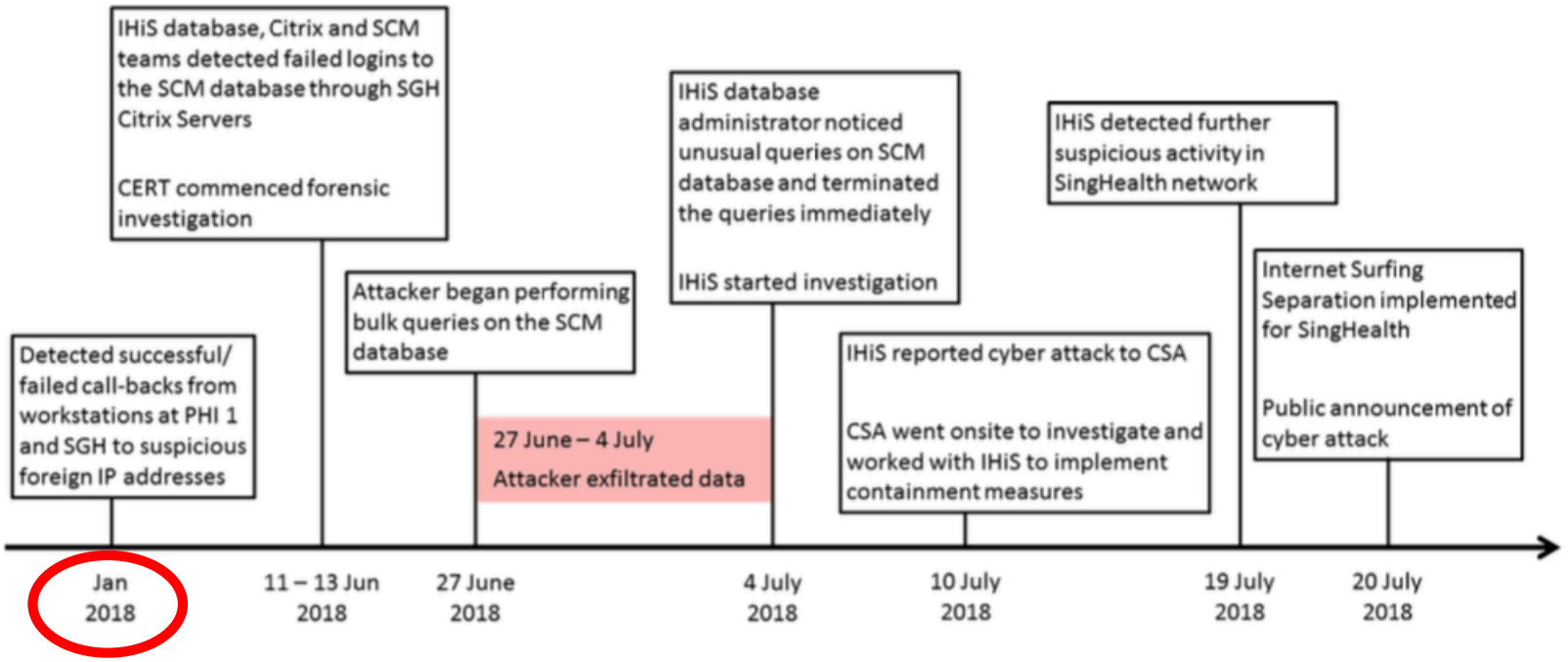
- September 2014, iHIS staff discover vulnerability in SCM software
- He found the way to exploit this vulnerability and inform direct supervisor
- But no record of follow up, case log or technical detail of this vulnerability

Episode 0 – Vulnerability for opportunity

- Ex-iHIS staff also send e-mail to software company which is SCM competitor to inform this critical vulnerability
- 18 September, iHIS executive was inform and terminate those employee.
- In response to SCM software company, no critical vulnerability was found.
- CSA investigate case later but no evidence relate to current cyber attack.

Incident Response Activity

Timeline of Incident Response



Source: COI Report, Page 108

18 January 2018

- iHIS security team got alert on suspicious activity on PHI workstation
  - File name of malicious ,URL and foreign IP address
  - Connection to others two IP in the network
  - Suspect file is legitimate filename but put in suspicious location
- Workstation was remove from network, reimage and C&C communication was block.

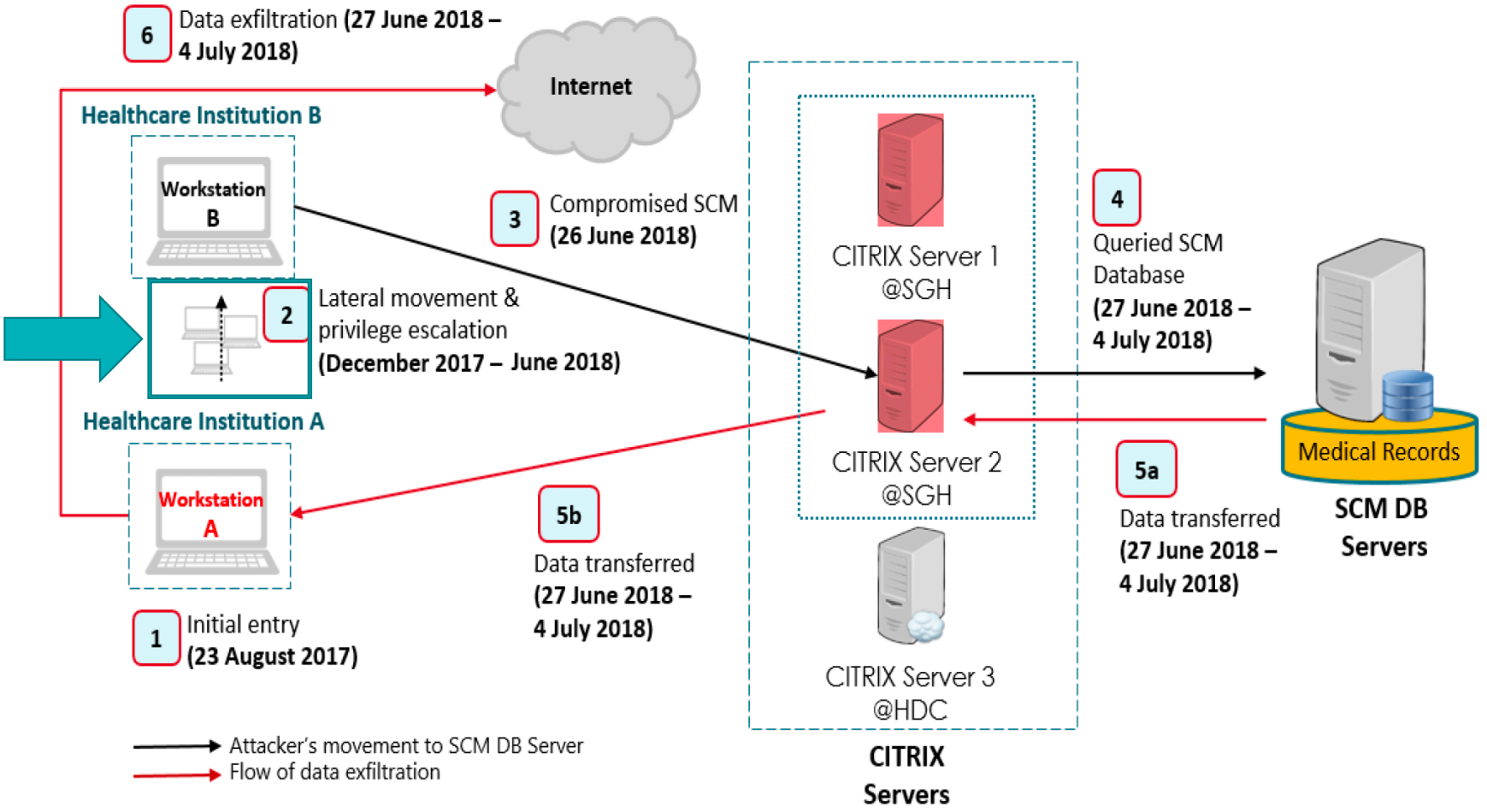
19 January 2018

- iHIS staff continue to investigate all log and found two other workstation connected to same C&C server

- After investigation, connection made from print service on workstation, service was disable during remediation process and it was not suspicious activity.

- 20 January - Malicious file was upload to online free scan and does not report any malicious

- 22 January – report sent to conclude the incident with no formal incident report. (PC always get infected)



From report of the COI into the Cyber Attack on SingHealth

11 June 2018

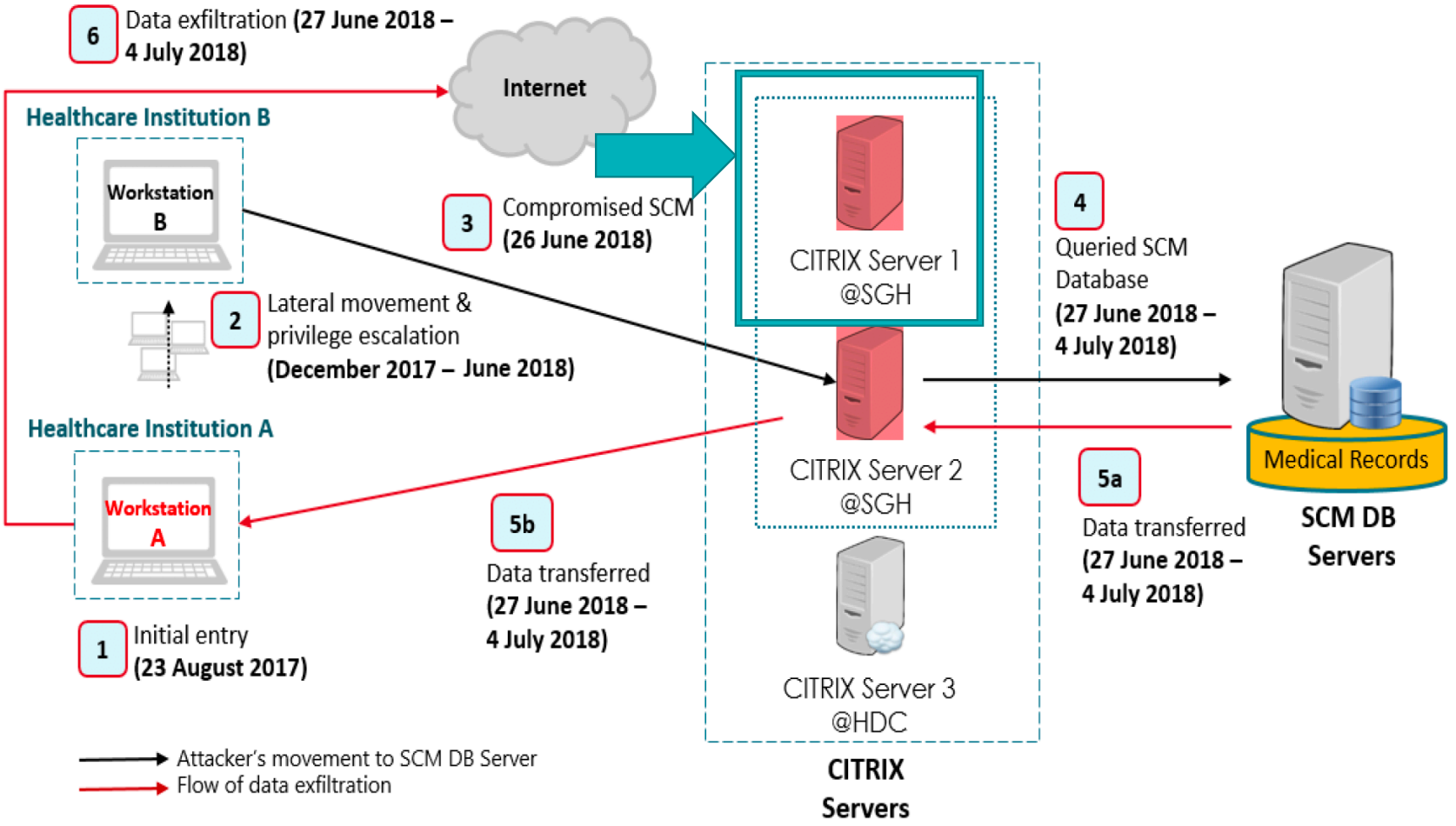
- 3:10PM – e-mail alert on multiple login error on SCM database
- 5:08PM – e-mail was send to service delivery team and Server team as source IP are from Citrix server
- All alert generate from invalid user ID event, include Domain admin so Domain admin password was changed.
- Incident left to Citrix support team to investigate

Unusual login on Citrix Server

- Local Admin + off-shift user ID were use to login to Citrix Server
- Login also come from unknow workstation (Virtual machine) which run on workstation inside SGH network.
- Logs on Citrix server also clear by “System” account but iHIS has separate system log for investigation
- Local Admin password was changed to prevent access (change from P@ssw0rd).
- Anti-malware solution was detect from server on 8 June 2018
- Case was not escalate until next day

12 June 2018

- Found generic SQL tools on user folder on Citrix server 1
- Disable all login to Citrix Server 1
- Case was escalate to CERT team
- 24 hours gap after discovery and incident report
- Seized suspected workstation (PHI and workstation in SGH)
- Shutdown Citrix Server 1



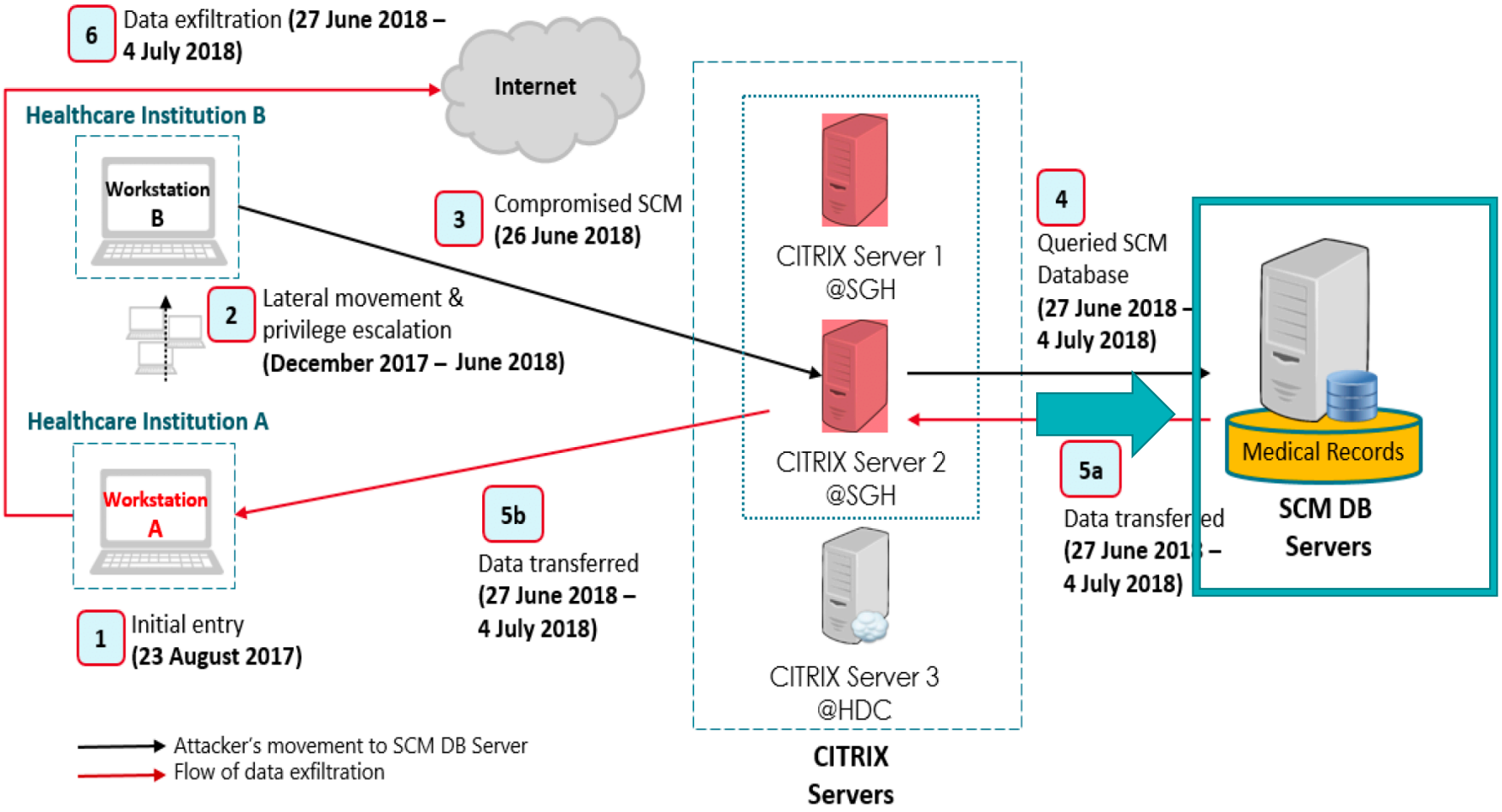
From report of the COI into the Cyber Attack on SingHealth

13 June 2018

- Detect failed login to SCM from another Citrix Server
- All user was notified on password reset
- Computer forensic on suspicious workstation start but only limit to one-by-one due to limit forensic tool

26 June 2018

- Another alert on SCM failed login from another Citrix Server
- During incident, investigator found unknow active RDP session on server (using system account)
- System Account was remove later from admin group
- Due to detection of active RDP session, investigator can detect source IP and seized that workstation.
- First detection of login session to cloud server (than gain access to SCM database)



From report of the COI into the Cyber Attack on SingHealth

Data extraction from SCM

- 27 June – 3 July 2018 Attacker successfully extract data from SCM database using SQL command and undetected by iHIS team
- 4 July 2018 – SCM support team detect alert from SCM database (which later found as bulk query to SCM database)
- Suspicious user ID was used in database query and from suspicious program
- 4 July, similar SQL from incident was terminate and block
- 10 July 2018 , CSA was notified and war room was setup

11 July 2018

- Estimation of extracted data by simulate SQL query and network traffic
- Confirm Prime Minister data also included
- 13 July 2018, after simulation and compare network traffic to C&C, iHIS confirm data was exfiltrated

PUBLISHED NOV 13, 2018, 1:42 PM SGT

Hariz Baharudin

SINGAPORE - To bolster their cyber defences, organisations should put in place a centralised incident management and tracking system that logs all incidents during a breach.

This was the recommendation made to a high-level Committee of Inquiry (COI) looking into June's SingHealth data breach. It found that disorganised communication contributed to a delay in mitigating actions during Singapore's worst cyber attack.

The use of different platforms like WhatsApp, Tigerconnect and e-mail to communicate also meant that valuable details about the attack were lost, a cyber-security expert told the panel.

vendor, Integrated Health Information Systems (IHiS), for such oversight. PHOTO: ST FILE

PUBLISHED JAN 10, 2019, 5:00 AM SGT

COI releases key findings on cyber attack, and makes 16 recommendations with priority for 7

Irene Tham Tech Editor

Staff who fell prey to phishing attacks. Weak administrator passwords. Not applying a patch that could have stopped the hacking. And an IT cyber-security team that could not even recognise a security incident.

These were among the basic failings that opened the door to Singapore's worst data breach, according to the public report by a high-level panel tasked to probe last June's cyber attack on SingHealth.

And such lax cyber-security practices were no match for the sophisticated cyber attackers, believed to be state-linked. In fact, the Singapore authorities contacted foreign law enforcement agencies for information on the users behind servers linked to the attack.

Hacker group behind SingHealth data breach identified, targeted mainly Singapore firms

Hackers that compromised the data of 1.5 million healthcare patients have been identified as a group that launched attacks against several organisations based in Singapore, including multinational firms with operations in the country, and is likely part of a larger operation targeting other countries and regions.

By Eileen Yu for By The Way | March 6, 2019 -- 14:00 GMT (22:00 GMT+08:00) | Topic: Security

Hackers that compromised the data of 1.5 million SingHealth patients have been identified as a group that launched attacks against several businesses based in Singapore, including multinational companies with operations in the city-state. Dubbed Whitefly, the group had attacked organisations in healthcare, media, telecommunications, and engineering, and is likely to be part of a larger operation targeting other nations, according to a report by Symantec.

MORE FROM EILEEN YU

How Upset Should Singaporeans Be About the Penalties for the SingHealth Data Breach?

The Committee of Inquiry (COI) on the SingHealth cyber attack has uncovered a perfect storm of inexperience, ineptitude, and poor decision making in the IT agency responsible for Singapore's healthcare, IHiS. The COI's findings are detailed in this 450-page report, and an overhaul of the IHiS's cyber security and threat reporting system has been prescribed by the Cyber Security Agency (CSA).

The following punitive measures have been taken:

– Two employees have been fired
– One employee was demoted
– Five senior executives, including IHiS CEO Bruce Liang, have been subjected to unknown financial penalties
– The Personal Data Protection Commission (PDPC) has fined IHiS $750,000 and SingHealth $250,000

Data Security Check

SingHealth
Defining Tomorrow's Medicine

CyberAttack on SingHealth IT System - Information for SingHealth Patients

Latest Updates

- 10 Jan 2019 - Media Statement: SingHealth Takes Active Steps to Strengthen Cybersecurity Defence
- 23 Jul 2018 - Cyberattack: SingHealth's 2nd Update on Patient Engagement
- 21 Jul 2018 - Cyberattack: SingHealth Update on Patient Engagement
- 20 Jul 2018 - Joint Press Release by MCI and MOH - SingHealth's IT System Target of Cyberattack

Frequently Asked Questions

A) INCIDENT RELATED

Recommendation

Key finding

- Staff do not have adequate skill level to response to attack
- Person who responsible for incident does not take appropriate action.
- Number of vulnerability existing in IT infrastructure
- Attacker has skill , resource and time.
- This incident can prevent or less damage.

Priority COI Recommendations

- An enhanced security structure and readiness must be adopted by IHiS and Public Health Institutions
- The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats
- Staff awareness on cybersecurity must be improved, to enhance capacity to prevent, detect, and respond to security incidents
- Enhanced security checks must be performed, especially on CII systems
- Privileged administrator accounts must be subject to tighter control and greater monitoring
- Incident response processes must be improved for more effective response to cyber attacks
- Partnerships between industry and government to achieve a higher level of collective security

Additional COI Recommendations

- IT security risk assessments and audit processes must be treated seriously and carried out regularly
- Enhanced safeguards must be put in place to protect electronic medical records
- Domain controllers must be better secured against attack
- A robust patch management process must be implemented to address security vulnerabilities
- A software upgrade policy with focus on security must be implemented to increase cyber resilience
- An internet access strategy that minimises exposure to external threats should be implemented
- Incident response plans must more clearly state when and how a security incident is to be reported
- Competence of computer security incident response personnel must be significantly improved
- A post-breach independent forensic review of the network, all endpoints, and the SCM system should be considered

Enhanced Security Checks

- Vulnerability assessments must be conducted regularly.
- Safety reviews, evaluation, and certification of vendor products must be carried out where feasible.
- Penetration testing must be conducted regularly.
- Red teaming should be carried out periodically.
- Threat hunting must be considered.

Privileged Administrator Accounts

- An inventory of administrative accounts should be created to facilitate rationalisation of such accounts.
- All administrators must use two-factor authentication when performing administrative tasks.
- Use of passphrases instead of passwords
- Password policies enforced across both domain and local accounts.
- Server local administrator accounts must be centrally managed across the IT network.
- Service accounts with high privileges must be managed and controlled.

P@ssw0rd

Domain controllers must be better secured against attack

- The operating system for domain controllers must be more regularly updated to harden these servers against the risk of cyber attack.
- The attack surface for domain controllers should be reduced by limiting login access.
- Administrative access to domain controllers must require two-factor authentication.

Active Directory

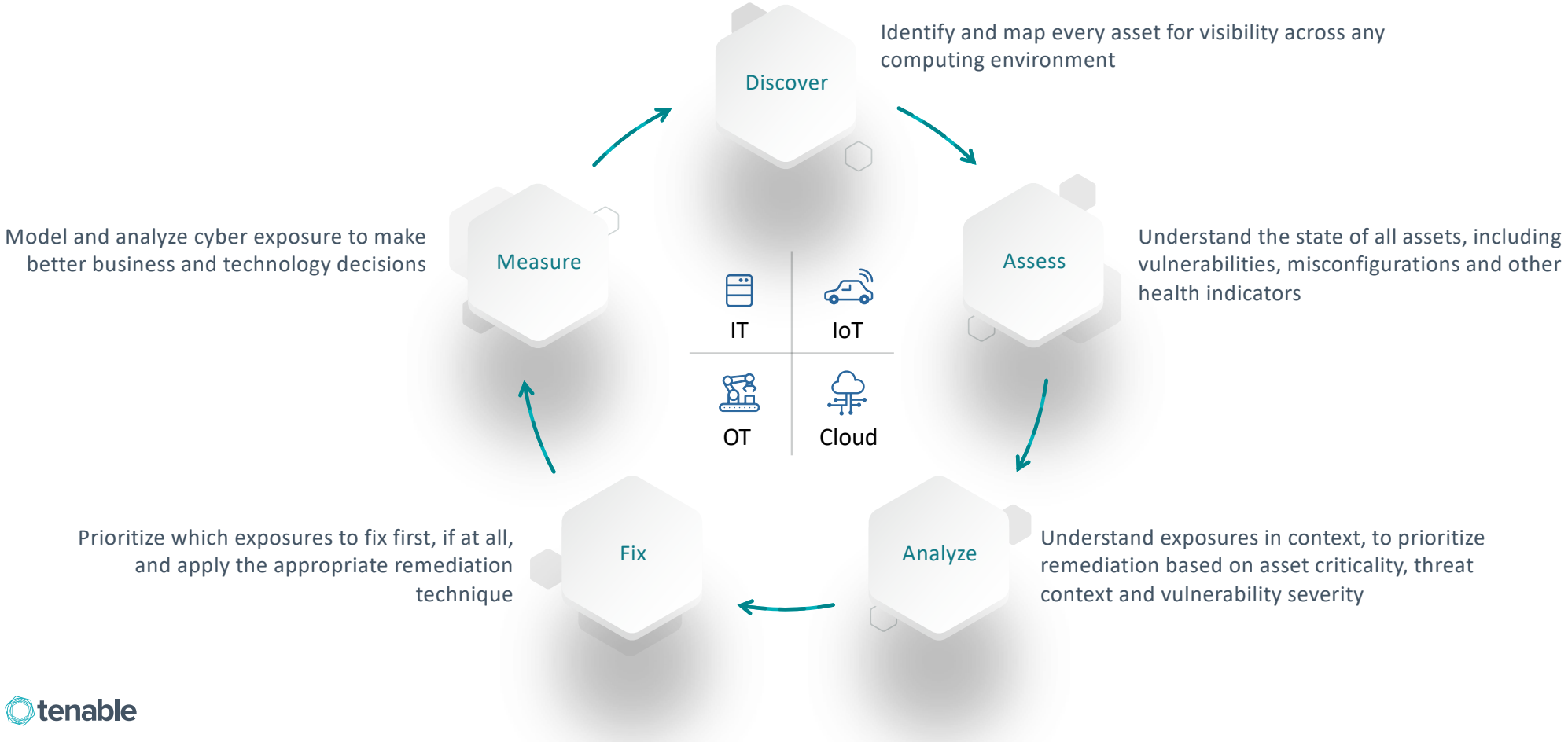
A robust patch management process must be implemented to address security vulnerabilities

- A clear policy on patch management must be formulated and implemented.
- The patch management process must provide for oversight with the reporting of appropriate metrics.

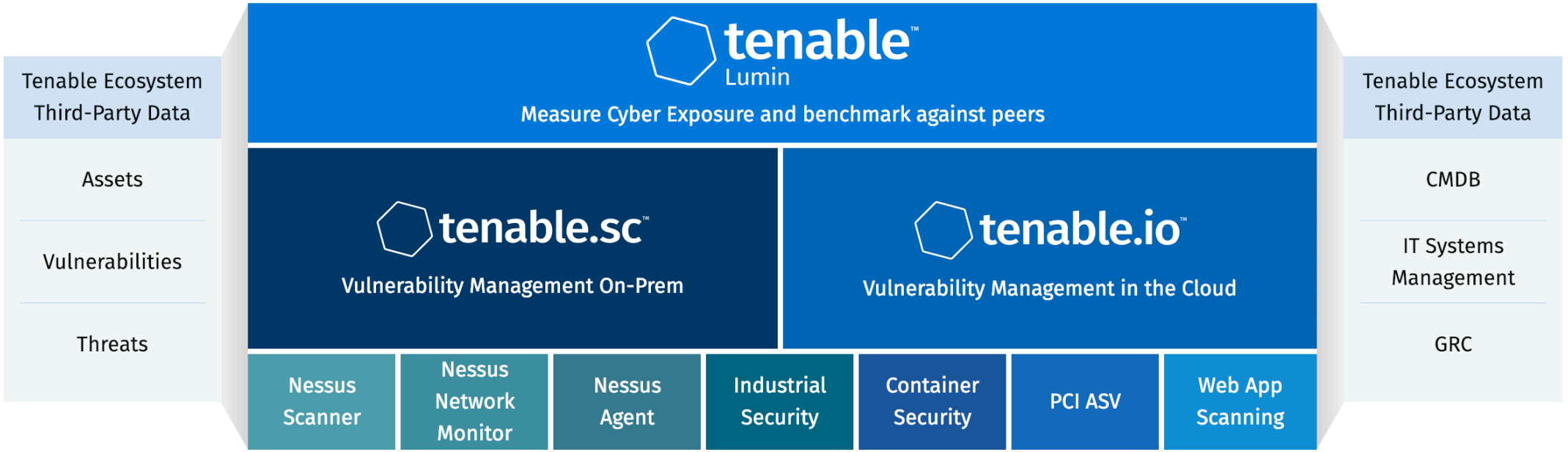
A software upgrade policy with focus on security must be implemented to increase cyber resilience

- A clear policy on patch management must be formulated and implemented.
- The patch management process must provide for oversight with the reporting of appropriate metrics.

Addressing the full Cyber Exposure lifecycle



Tenable Cyber Exposure Platform



Complete Visibility into All Assets

Prioritization & Guidance

Flexibility: Cloud or On-prem

tenable


tenable™