Hong Kong Computer Emergency Response Team Coordination Centre
HKCERT 香港電腦保安事故協調中心

「網絡世界中的數據安全管理 — 個人資料保安及事故應變實用貼士」網上講座

預先做好準備
有效應對保安事故

吳宇安先生 – 香港電腦保安事故協調中心資訊保安顧問

HKCERT

內容

1. 保安事故應變計劃的重要性
2. 保安事故應變計劃的關鍵步驟是什麼?
3. 保安事故應變指南的應用
4. 真實個案
5. 要點回顧

HKCERT

1 保安事故應變計劃的重要性

網絡攻擊的進化

- 發動網絡攻擊的成本和困難度大減
- 趨向自動化
- 愈趨有組織及針對性
- 針對保護較弱的裝置攻擊
- 缺乏資源來建立更廣泛的網絡防禦

為什麼需要保安事故應變計劃?

目的

- 快速反應，以減低對業務的影響，例如金錢、商譽、重要資料洩漏
- 防止和減少類似的網絡攻擊再次發生
- 符合監管要求

目標

- 了解保安事故應變處理的崗位和責任
- 制定應對網絡攻擊的快速反應措施
- 以有限的資源來維持和增強系統防禦

例子：混亂的保安事故應變措施

Uber admits covering up data breach involving 57 million users

BY IANS PUBLISHED: UPDATED ON - 10:51 AM, TUE - 26 JULY 22

San Francisco: Uber has admitted that it covered up a massive data breach in 2016 that exposed data pertaining to approximately 57 million users and 600,000 drivers' license numbers.

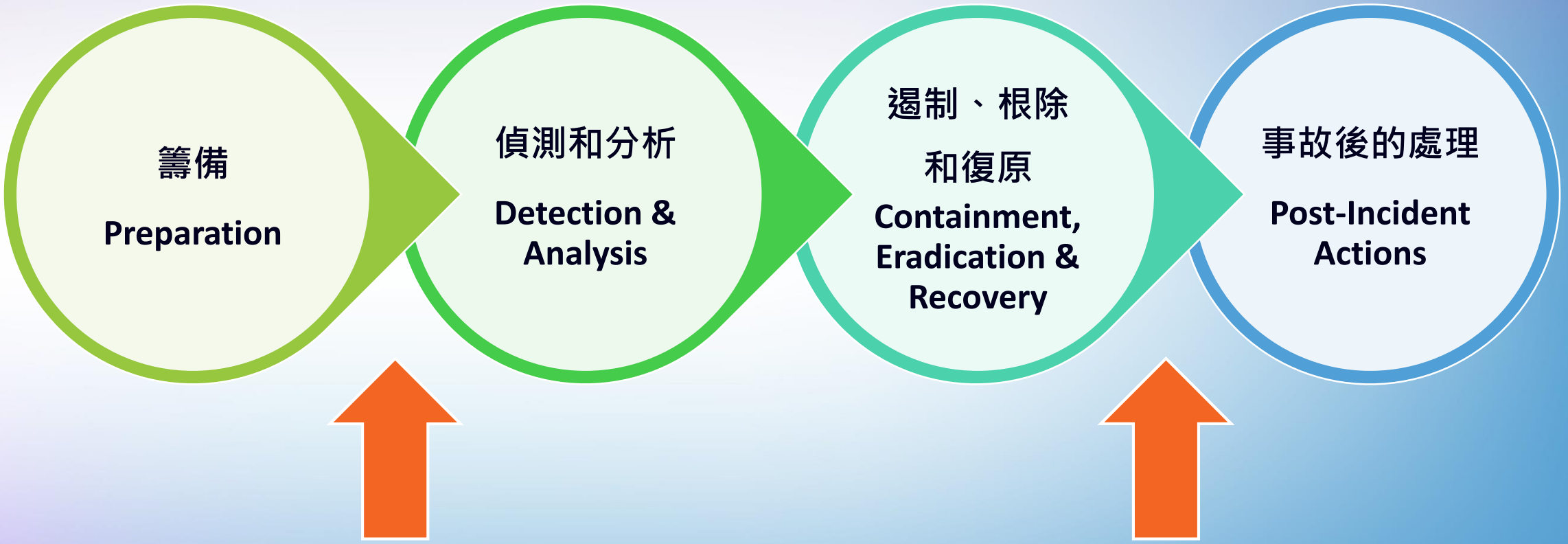
The breach was not reported to the FTC until approximately a year later, when new executive leadership was managing the company, revealed the Justice Department.

Uber settled civil litigation with the attorneys general for all 50 States and the District of Columbia related to the 2016 data breach, paying $148 million and agreeing to implement a corporate integrity programme.

HKCERT

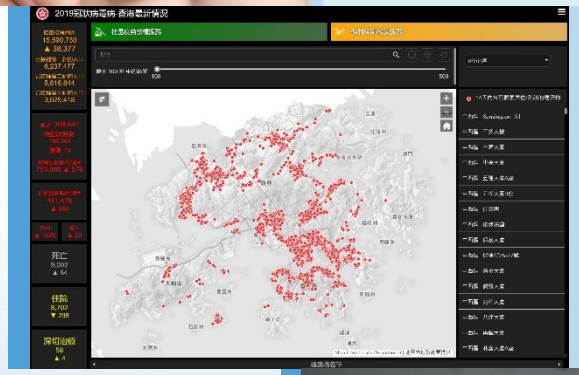
2 保安事故應變計劃的關鍵步驟是什麼?

保安事故應變計劃的處理周期



偵測和分析
Detection & Analysis

- 來源的先導和指標



- 事故分析

- 事故通知

遏制、根除和復原
Containment, Eradication & Recovery

- 選擇遏制策略

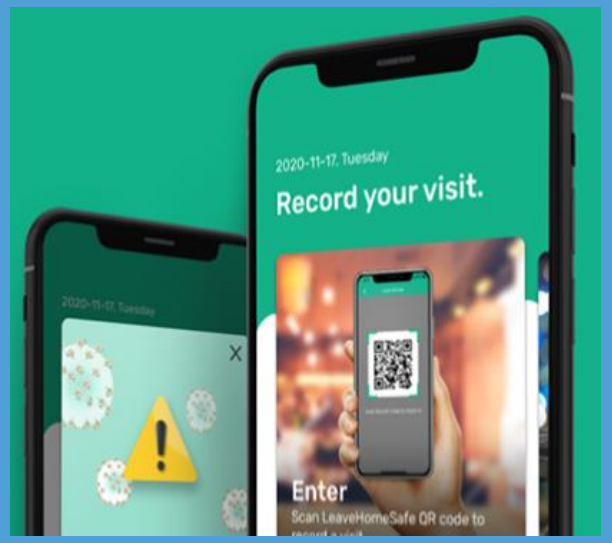
- 根除和復原

- 證據收集和處理

事後行動
Post-Incident Actions

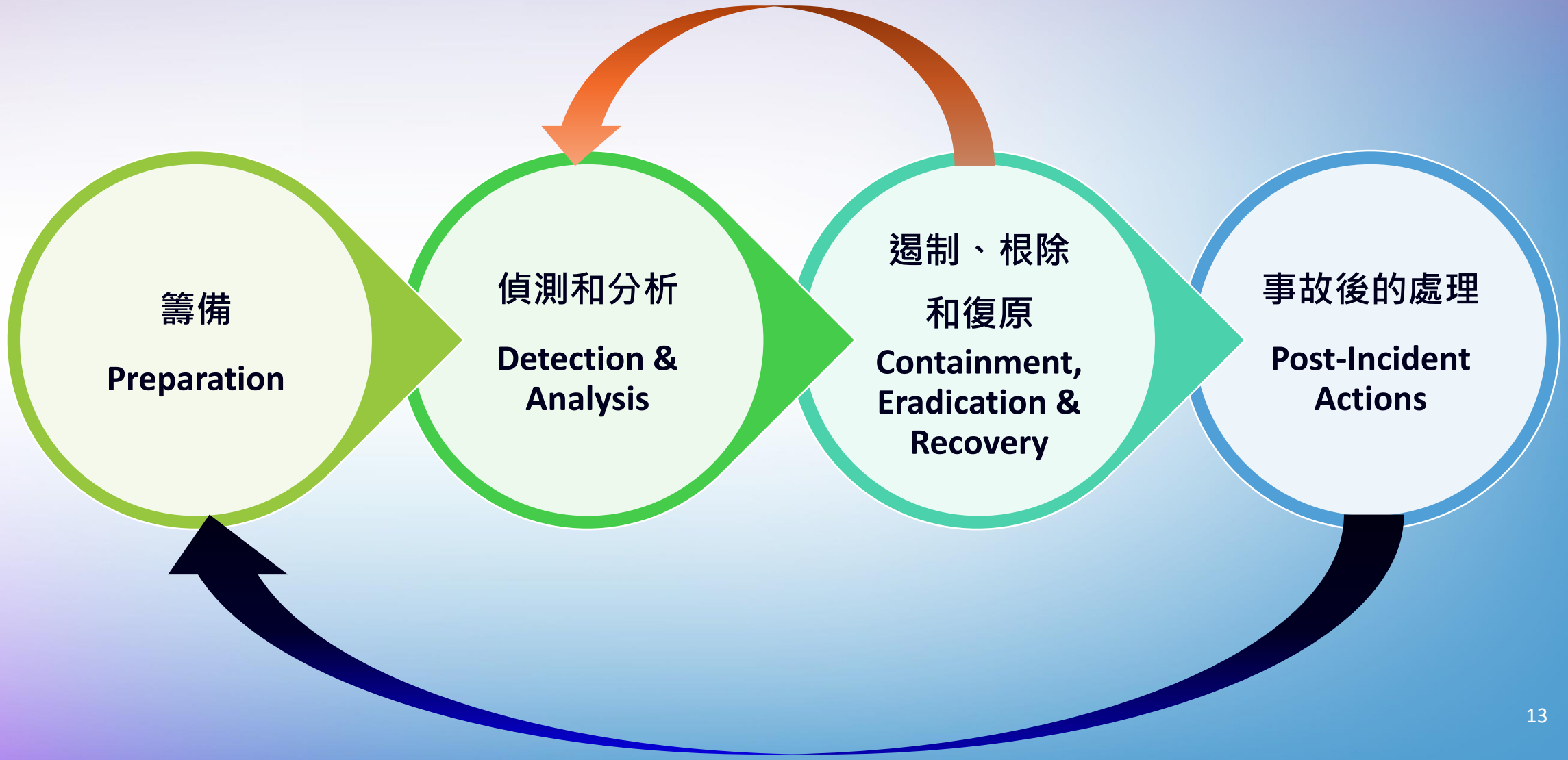
- 證據保留
- 使用收集的事件數據
- 保安改善建議

籌備
Preparation



- 識別重要的系統，適當保存日誌
- 優先考慮和管理風險
- 制定事故應變計劃

保安事故應變計劃的處理周期

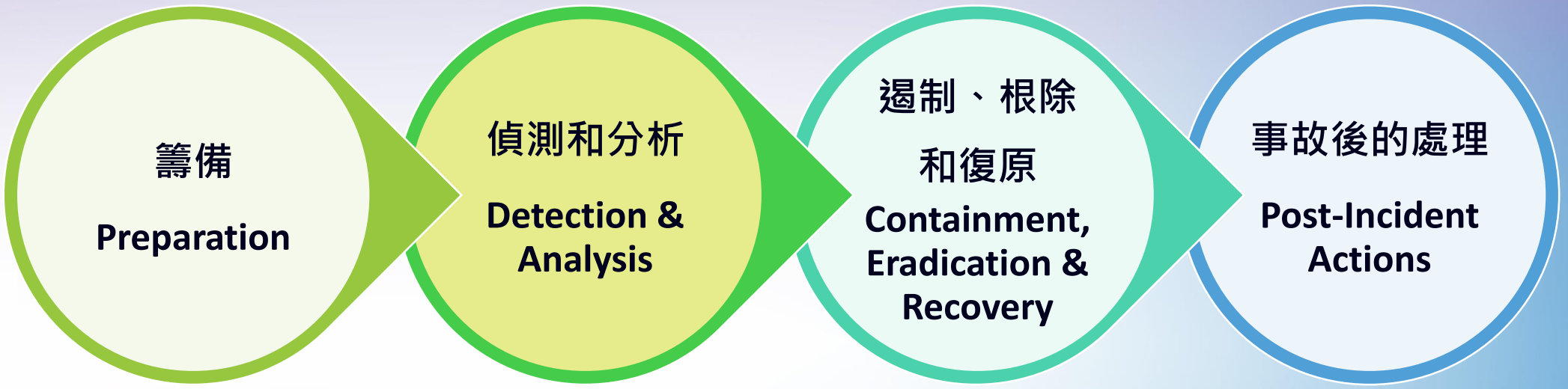


個案研究: HKTVmall 客戶資料未經授權被取覽

- 香港科技探索有限公司於2022年1月26日發現電腦系統出現不正常及可疑活動，未經授權取覽HKTVmall的客戶資料

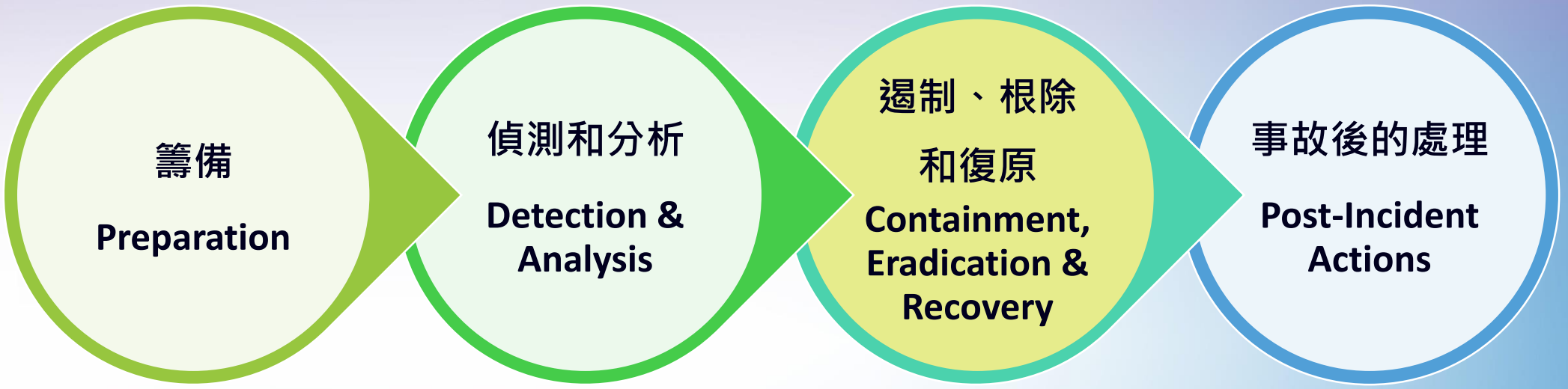
Source 來源：HKTVmall、明報
https://finance.mingpao.com/fin/instantf/20220204/1643967107543/hktvmall-438%E8%90%AC%E7%94%A8%E6%88%B6%E8%B3%87%E6%96%99%E6%9C%89%E5%B0%8F%E9%83%A8%E5%88%86%E8%A2%AB%E6%9C%AA%E7%B6%93%E6%8E%88%E6%AC%8A%E5%8F%96%E8%A6%BD

個案研究: HKTVmall 客戶資料未經授權被取覽



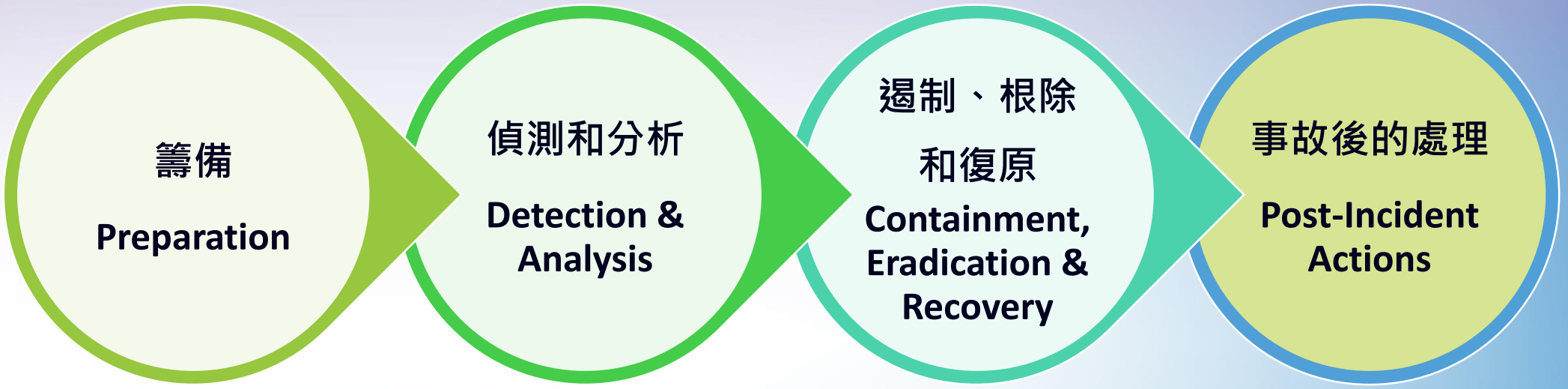
- 未經授權取覽客戶資料的來源/位置
- 被取覽客戶資料的範圍
- 被取覽客戶資料的內容和資料類別

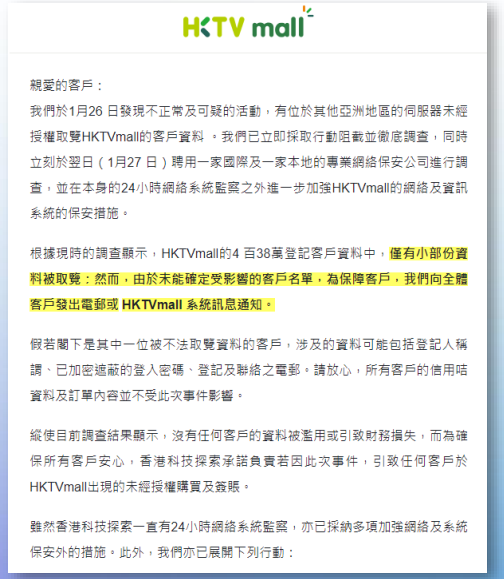
個案研究: HKTVmall 客戶資料未經授權被取覽



- 即時採取阻截事故的行動

個案研究: HKTVmall 客戶資料未經授權被取覽





HKTV mall

親愛的客戶：

我們於1月26 日發現不正常及可疑的活動，有位於其他亞洲地區的伺服器未經授權取覽HKTVmall的客戶資料，我們已立即採取行動阻截並徹底調查，同時立刻於翌日（1月27 日）聘用一家國際及一家本地的專業網絡保安公司進行調查，並在本身的24小時網絡系統監察之外進一步加強HKTVmall的網絡及資訊系統的保安措施。

根據現時的調查顯示，HKTVmall的4 百38萬登記客戶資料中，**僅有小部份資料被取覽；然而，由於未能確定受影響的客戶名單，為保障客戶，我們向全體客戶發出電郵或 HKTVmall 系統訊息通知。**

假若閣下是其中一位被不法取覽資料的客戶，涉及的資料可能包括登記人稱謂、已加密遮蔽的登入密碼、登記及聯絡之電郵。請放心，所有客戶的信用咭資料及訂單內容並不受此次事件影響。

縱使目前調查結果顯示，沒有任何客戶的資料被濫用或引致財務損失，而為確保所有客戶安心，香港科技探索承諾負責若因此次事件，引致任何客戶於HKTVmall出現的未經授權購買及簽賬。

雖然香港科技探索一直有24小時網絡系統監察，亦已採納多項加強網絡及系統保安外的措施。此外，我們亦已展開下列行動：

- 向相關人士/機構通告事故
- 回顧系統使用和資料保存政策

Source 來源：HKTVmall email notification to customer subjected “客戶資料安全事件｜ Information Security Event on Customer Data”

個案研究: HKTVmall 客戶資料未經授權被取覽

- 增加和改善保安措施

參考: http://www.hktvmall.com/infosecurity

個案分析：HKTVmall 客戶資料未經授權被取覽

恰當的處理	
有充分的事故應變能力	• 即時採取行動防止事故惡化
有充分的事故偵測和分析	• 分析事故發生的詳細情況 • 了解受事故影響的範圍
事故後的處理恰當	• 向相關機構報告 • 通知受影響的用戶 • 對系統的設定和防備作出改善 • 改善及增加監控系統

能改善之處	
• 及早更新系統以堵塞漏洞	• 限制系統存取權限
• 在防火牆只容許必要的流量	• 將敏感資料和系統與互聯網分隔
• 訂立數據儲存規例：儲存時限、儲存位置、清除方案 等等	

HKCERT

3 保安事故應變指南的應用

保安事故應變指南架構

- 制定保安事故應變程序
  - 總應變程序 – 事故應變指引及策略
  - 子操作程序 – 遇到某類事故的應對方法
- 保安事故應變的管理
  - 分配保安事故應變中的崗位和責任
  - 訂立保安事故通報渠道

總程序和標準操作程序

- 總保安事故應變程序
  - 提供統一應對準則的指引
  - 通常每年重新審視及更新

- 保安事故應變標準操作程序 (子程序)
  - 不同類別的保安事故方法有所不同
  - 制定專屬一些嚴重和頻繁發生的保安事故
  - 會因應新的攻擊而制定新的標準操作程序

制定總保安事故應變程序的情景問題

籌備：
1. 哪些是機構營運的重要的系統、數據和資產？
2. 機構的保安事故應變團隊裡有什麼崗位和責任？機構是否擁有持份者最新的聯絡名單？
3. 機構會將此問題歸類為保安事故嗎？如會，該行為違反了哪些機構政策？
4. 哪些措施可以防止此類事故的發生或限制其影響？
偵測和分析：
1. 若有事故先兆，機構能偵測到嗎？機構會否在事故發生之前因應這些先兆採取行動？
2. 機構可以偵測到哪些保安事故的跡象？哪些跡象表明事故發生的可能性？
3. 偵測保安事故需要什麼工具？
4. 保安事故應變團隊將如何分析和驗證事故？哪些人士會參與分析和驗證？
5. 應該向機構內的哪些人士和團隊通報事故？
6. 團隊如何優先處理此事故？

引導保安事故應變策劃人員

- 每個周期階段的程序需要哪些元素和資料

一般保安事故情景的標準操作程序

主要階段	要實行的關鍵步驟
籌備	1. 準備惡意軟件事故的溝通渠道 2. 定義事故升級路徑 3. 評估和保護關鍵系統備份，創建可能的恢復點並維護至少一個離線備份 4. 安裝例如防毒軟件等的保護軟件，並將辨識檔保持更新 5. 限制防火牆策略，盡可能採用默認拒絕所有流量的原則 6. 維護重要數據的離線備
偵測和分析	1. 盡快隔離受感染系統，使受感染系統保持通電狀態 2. 確定惡意軟件及其特徵，驗證惡意軟件是否仍在運行中或溝通 3. 分析受影響範圍（即從軟件/系統、文件系統、數據庫等角度來看，受影響的範圍有多大） 4. 檢查網絡和系統日誌以找出惡意活動，找出感染媒介（例如電郵附件、遠程協議、可移除硬碟、點擊的鏈接等） 5. 與被感染單位溝通並保持聯絡
遏制、根除和恢復	1. 隔離惡意軟件並確保在恢復系統正常運作之前將其徹底清除 2. 遇到勒索軟件攻擊時，查看是否有可靠來源的解密工具可用 3. 如果沒有可用的解密工具，確定可行的離線備份並將數據恢復到不受影響的系統/電腦中 4. 阻斷疑似惡意軟件的網絡通訊 5. 如有需要，尋求第三方協助 6. 一旦惡意軟件被遏制，繼續進行數據恢復
事故後的處理	1. 重新考慮系統的安全性：檢查防火牆設置，檢查防毒軟的辨識檔是否最新等。 2. 建立事故報告並提及已採取的措施 3. 討論改進（汲取經驗） 4. 進行用戶意識培訓 5. 如果需要採取進一步行動（例如洩露個人資料等），與執法部門溝通

當處理不同的保安事故情景

- 考慮不同的處理步驟
- 記錄每個階段不同的關鍵步驟

HKCERT

4 真實個案

個案研究: 外國醫院受勒索軟件攻擊

獨立的事後審查

1. **FA1.KF1 The HSE did not have a single responsible owner for cybersecurity, at senior executive or management level at the time of the Incident.**

13. **FA1.KF13 The HSE did not have a documented cyber incident response plan and had not performed typical preparatory activities such as exercising the technical response.**

9. **FA1.KF36 The complexities of recovering applications and systems were not well understood.**

2. **FA1.KF15 The HSE's antivirus identified a tool commonly used by ransomware groups (Cobalt Strike) on six servers on 7 May 2021 (and several more servers in the following days) but these alerts were not appropriately actioned.** The HSE did not identify these alerts

11. **FA1.KF11 The antivirus tool ([redacted] Endpoint Security) was over-relied upon to detect and prevent threats on endpoints.**

HKCERT 保安事故應變指南

籌備

1. 準備惡意軟件事故的溝通渠道
2. 定義事故升級路徑
3. 評估和保護關鍵系統備份，創建可能的復原點並維護至少一個離線備份
4. 安裝例如防毒軟件等的保護軟件，並將辨識檔保持更新
5. 限制防火牆策略，盡可能採用默認拒絕所有流量的原則
6. 維護重要數據的離線備份

1. https://www.meditologyservices.com/case-study-ransomware-locks-up-80-of-54-hospital-health-system/
2. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

個案研究: 外國醫院受勒索軟件攻擊

獨立的事後審查

1. **FA1.KF14 The cyber attack was not actively identified or contained prior to the ransomware execution, despite the Attacker performing noisy and 'unstealthy' actions.**

10. **FA1.KF27 The HSE's Incident Response provider identified evidence of how the Attacker was able to gain unauthorised access to the HSE's IT environment and the Attacker's subsequent activities.**

HKCERT 保安事故應變指南

偵測和分析

1. 盡快隔離受感染系統，使受感染系統保持通電狀態
2. 確定惡意軟件及其特徵，驗證惡意軟件是否仍在運行中或溝通
3. 分析受影響範圍（即從軟件/系統、文件系統、數據庫等角度來看，受影響的範圍有多大）
4. 檢查網絡和系統日誌以找出惡意活動，找出感染媒介（例如電郵附件、遠程協議、可移除硬碟、點擊的鏈接等）
5. 與被感染單位溝通並保持聯絡

1. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

個案研究: 外國醫院受勒索軟件攻擊

獨立的事後審查

3. **FA1.KF30 The HSE took action to contain the ransomware attack by powering down systems and disconnecting the NHN from the internet.**

1. **FA1.KF18 The HSE with the help of third-parties mobilised a response to the ransomware attack and overcame many of the significant challenges the ransomware attack presented, drawing on their experience responding to crises, including COVID-19.**

10. **FA1.KF37 Despite the challenges presented by the ransomware attack and the lack of preparedness, the HSE was able to recover 1,075 applications and over 87,000 systems.**[145]

HKCERT 保安事故應變指南

遏制、根除和復原

1. **隔離惡意軟件**並確保在復原系統正常運作之前將其徹底清除
2. 遇到勒索軟件攻擊時，查看是否有可靠來源的解密工具可用
3. 如果沒有可用的解密工具，確定可行的離線備份並將數據復原到不受影響的系統/電腦中
4. 阻斷疑似惡意軟件的網絡通訊
5. **如有需要，尋求第三方協助**
6. 一旦惡意軟件被遏制，**繼續進行數據復原**

1. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

個案研究: 外國醫院受勒索軟件攻擊

獨立的事後審查

Data Security

Implementing protective and detective measures to secure critical data

FA2.KR20 Review processes, plans and resourcing for response to future potential data breaches

Security Culture

Improving security awareness through tactical activities like training high risk users and strategic initiatives like designing and delivering security awareness and phishing campaigns.

HKCERT 保安事故應變指南

事故後的處理

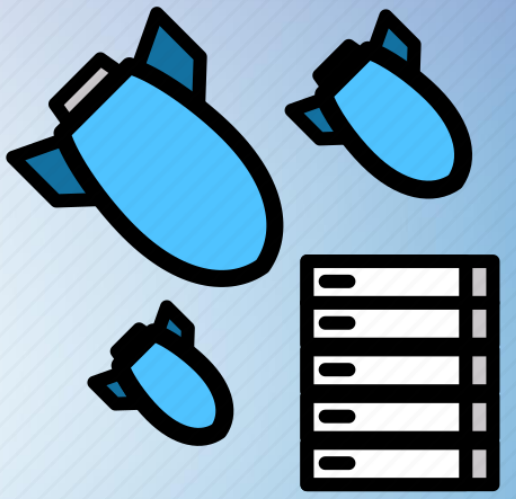
1. **重新考慮系統的安全性**：檢查防火牆設置，檢查防毒軟的辨識檔是否最新等。
2. **建立事故報告並提及已採取的措施**
3. **討論改進（汲取經驗）**
4. **進行用戶意識培訓**
5. 如果需要採取進一步行動（例如洩露個人資料等），與執法部門溝通

1. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

標準操作程序 - 常見網絡攻擊

釣魚 Phishing
（ 詐騙 Scam ）

惡意軟件 Malware
(勒索軟件 Ransomware)



分散式阻斷服務 DDoS

保安事故處理清單

行動		已完成
籌備		
1	確保系統和應用程式的良好行為	○
1.1	了解網絡、系統及應用程式的正常行為（網絡及系統的配置）	○
1.2	由幾種保安軟件構建的警報來識別先兆和跡象	○
1.3	制定日誌保留政策，在所有系統上建立日誌記錄及審計的基線級別，並在所有關鍵系統上建立更高的基線級別	○
1.4	使用及維持系統及應用程式正常運作及事故處理步驟的知識庫	○
1.5	保持所有主機時鐘同步	○
2	加強資料數據保護	○
2.1	識別和驗證敏感資料數據，並加強其保護	○
2.2	保護事故中的資料數據	○
2.3	除檔案系統備份外，還通過完整的取證映像獲取系統快照	○
3	準備事故處理和運作復原計劃	○
3.1	徵集在事故處理過程中或有用處的工具及資源	○
3.2	在機構的事故應變政策中包含有關事故報告的規定	○
3.3	遵循既定的證據收集和處理程序	○
3.4	建立事故通報機制並保持更新聯絡名單	○
3.5	能夠從系統中找出非永久數據作為證據	○
3.6	根據計劃進行事故應變演習	○
3.7	定期檢討和更新計劃	○

保安事故處理中常見的保安最佳實踐

- 用於作自我檢查
- 是否涵蓋了必要的行動步驟
- 確保 IT 系統有足夠準備

保安事故應變中的崗位和責任

崗位	責任
IT 管理部門	• 與營運管理部門分析事故，以評估事故在技術上的影響和嚴重程度（高、低或其他） • 收集和保存有關事故的資訊 • 協調和確保有足夠的資源進行事故應變 • 遏制、補救和解決事故，並以時間標示記錄操作 • 根據營運管理層的意見，確定是否應在事故解決之前將生產服務離線 • 上報嚴重性較高的事故 • 管理事故後的流程並與營運部門草擬評估報告，記錄事故汲取的經驗和跟進 • 定期作出系統監察 • 讓機構做好應對保安事故的準備，例如為第一應變者（系統管理員）提供指導和培訓，以及建立與營運部門的溝通渠道 • 提供事故通報熱線並作出回應
營運管理部門	• 評估事故對營運的影響 • 成為營運數據和系統的擁有者 • 在 IT 管理層的要求下收集事故相關的資訊 • 鑒定事故是否與濫用有關 • 鑒定是否需要啟動應急計劃以應對長期的服務暫停 • 與 IT 管理人員一起草擬事故評估報告和跟進事故 • 按規定實施安全控制並監察系統是否存在攻擊跡象或未經授權/不當接達 • 為資訊資源提供實體和程序上的保障 • 向 IT 管理層報告可能導致事故發生的可疑事件

預先分配員工的崗位和責任

- 確保在發生保安事故時可以適當地應對

保安事故應變程序範本

資料	細節
簡短序述	
保安事故類別	☐ 分散式阻斷服務（DDoS） ☐ 網絡入侵 ☐ 惡意軟件 ☐ 網絡釣魚 ☐ 勒索軟件 ☐ 網頁塗改 ☐ 其他：
受影響的 IT 系統	硬體： 軟體：
嚴重性	低 0 | 1 | 2 | 3 | 4 | 5 高
資訊保安 CIA	機密性 ☐ 完整性 ☐ 可用性 ☐
影響規模	營運影響：
發生的日期 / 時間	
發現的日期 / 時間	
初步調查結果	怎樣發生: 為何發生: 已發現的保安漏洞:
牽涉的個人資料	☐ 是 / ☐ 否 如是，牽涉甚麼個人資料？ 已向香港個人資料私隱專員公署 (PCPD) 匯報？ ☐ 是 / ☐ 否
最長可承受時間	

機構可參考範本以制定應變保安事故的程序

- 充分的保安管理
- 促進對保安事故的整體應變

保安事故通報渠道

名稱： XXX 公司 / XXX 團隊

位置： 辦公室 , x 樓 , 辦公大樓

電話號碼： +852 XXXXXXXX (24 小時 熱線)

電郵地址： [服務台的電郵地址]

服務級別： 8 x 5 x 下一個工作日 / 7 x 24 x 4

相關的保安事故 / 系統： [保安事故 / 系統]

- 內部聯絡和 IT 服務供應商的通報渠道
  - 保安事故應變更有效和一致
  - 「有需要知道」的原則
- 外界機構
  - 執法機構 – 報告潛在的網絡犯罪
  - 監管機構 – 在法例規定的期限內報告保安事故
  - 新聞中心 – 公布公司對保安事故的應對

HKCERT

5 要點回顧

保安事故應變計劃

盡可能找出有機會受網絡保安事故影響的系統及裝置，並評估其嚴重性

應訂立實際可行而有成效的方法

有詳細的計劃來預防和處理保安事故

應定期檢閱並持續更新保安事故應變計劃

向不同機構報告保安事故

香港電腦保安事故協調中心(HKCERT)
惡意程式、網頁塗改、網絡釣魚、網上詐騙、阻斷服務攻擊

香港警務處 網絡安全及科技罪案調查科 (CSTCB)
網絡犯罪行為，例如：網上詐騙和牽涉經濟損失的案件

個人資料私隱專員公署 (PCPD)
涉及個人資料的投訴

香港通訊事務管理局辦公室 (OFCA)
非應邀電子訊息（垃圾郵件）

下載保安事故應變指南

DOWNLOAD

https://www.hkcert.org/tc/security-guideline/incident-response-guideline-for-smes

訂閱HKCERT資訊保安警報服務

要對**資訊保安風險**保持警惕，請訂閱或追蹤：

1. **免費保安公告及月報**
2. **免費電話短訊警報**
3. **HKCERT的社交媒體平台（例如Facebook, LinkedIn及YouTube）**

立即行動！

https://www.hkcert.org/tc/form/subscribe/entry

CTF 2022

香港網絡保安新生代
Hong Kong Cyber Security New Generation
奪旗挑戰賽
Capture the Flag Challenge

- 將於11月11-13日舉行，設有中學組，大專組及公開組 ，設有豐富獎品
- 立即於10月31日前報名，10月中更會有工作坊講解備戰方法
- ☞ https://ctf.hkcert.org

比賽方式

網上比賽以解題模式奪分，成功解題後可以獲得一套特定字串，而該特定字串在CTF世界中叫「旗」，組內頭三隊最高分便為贏家

題目

- 程式漏洞
- 密碼學
- 網絡鑑證
- 逆向工程
- 網站保安

HKCERT

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org