2024

LSCM

LOGISTICS SUMMIT 物流高峰會

From Smart City to Digital Economy

從智慧城市邁向數字經濟

Strengthening IT infrastructure resilience via diversification - Introduction to ISSRAC

通過多元化加強資訊科技基礎設施韌性

- 簡介信息系統安全可靠評測中心

目錄

多元化加強資訊科技基礎設施韌性的好處

持續營運

控制成本

降低風險

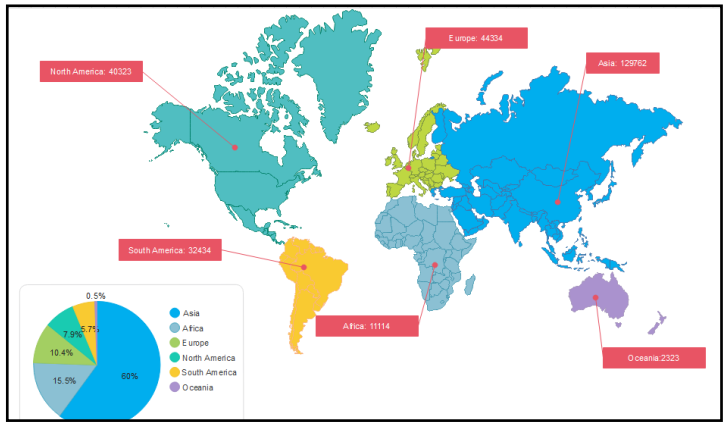
增強安全性

提升靈活性

系統性風險：後門

事件概況

2017年5月12日，駭客組織利用美國國家安全局的 “永恆之藍” (EternalBlue) 工具以攻擊執行 Microsoft Windows 作業系統的電腦,並以自動傳播到網路中電腦的蠕蟲病毒 “WannaCry” 進行攻擊、勒索，中毒電腦檔案將被加密、鎖定，需支付贖金一比特幣才能解鎖



影響範圍

- 勒索軟體已攻擊150個國家/地區的 30 多萬台電腦， 各地企業及公共組織受到不同程度的影響
- 根據 Verizon 的《2023 年數據洩露調查報告》，勒索軟體攻擊在過去一年中佔據了 24% 的數據洩露事件
- 內地感染範圍覆蓋了幾乎所有地區，遍佈高校、加油站、醫院、政府辦事終端等各大領域，超過 30萬臺機器受有關病毒感染 ， 至少有28388個機構受到影響

穩定性風險：漏洞

事件概況

2024年7月19日美國網路安全企業“群集打擊”（CrowdStrike）軟體出現問題引發的操作系統藍屏、全球宕機事件。

影響範圍

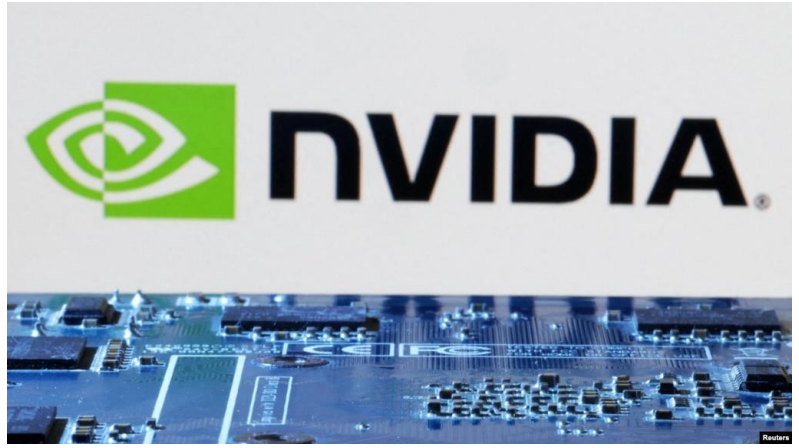
本次故障主要系美國網路安全公司CrowdStrike的更新導致，影響了約850萬臺Windows設備，導致多國航空公司、銀行、電信公司和媒體、健康醫療等各個行業陷入混亂。

產業鏈風險：斷供

ChatGPT的母公司OpenAI早前宣佈，由7月9日起禁止不支援地區使用應用程式界面（API），包括中國、香港和澳門。

彭博：美國擬進一步限制中國發展先進晶片技術

外國政府正考慮採取措施，進一步限制中國取得用於人工智能（AI）晶片的技術，當中包括限制中國獲取閘極全環電晶體（GAA）晶片技術。目標是令中國更加難以取得建立和運作AI模型所需的先進電腦系統。



原文網址：www.881903.com@12 June 2024

加强資訊科技基礎設施韌性

關後門

防斷供

堵漏洞

信息系統安全可靠評測中心

ISSRAC

- 成立於2024 年6月13 日

- 與中國軟件與技術服務股份有限公司簽署戰略合作協議

引入安全及可持續性產品來港

- 為國家科研機構和企業來港提供諮詢服務
- 構建安全性和可持續性產品測試平台和演示環境
- 支援信息系統的產品及技術兼容性測試，並建立適配產品名單

支援香港各行業信息系統安全提升

- 為安全性和可持續性的產品提供兼容性適配環境及認證
- 針對香港本地應用系統的獨特需求進行拓展研發
- 支援應用系統的安全提升項目的驗收
- 合辦相關產品的技術培訓，提升人才與技能儲備

安全可靠評測的核心產品範疇

關後門	計算產業鏈	CPU芯片、操作系統、伺服器、存儲單元等	測試中心	諮詢 測評
關後門	網路產業鏈	交換機、防火墙、雲計算平台、大數據平台、災備儲存等		
堵漏洞	安全產業鏈	基礎架構安全、重要設施安全、數據安全、工控安全等		
防斷供	關鍵製造環節	芯片生產綫、芯片設計軟件、最新GPU芯片等		
強應用	資訊化產業鏈	現代化數字城市、行業數字化辦公等		

如何做好安全可靠的評測?

安全可靠評測的整體思路

“先評估、再實施、系統思維、應用主導”

研究分析

系統評估
對現有系統進行安全可靠性的评估

改造策略

產品選型
應用遷移或重構產品範圍及選型

製定計劃

詳細計劃
立項，確定改造週期及要求，實施方案製定

改造實施

實施階段
遷移/開發
資料庫適配、中間件適配等

優化驗證

優化測試
針對性能、穩定性、可靠性開展優化測試

仿真運行

模擬運行
在試驗環境及生產環境分別開展模擬運行

運行監測

長期運行
系統上綫監測運行狀態

過往評估案例分享

一、評估流程

Part A

系統資料調研
（IT系統部門）

主要工作：

- IT 系統部門填寫系統資料調查表。
- 向評估小組提供其他相關文件。

時間周期：5-10天

Part B

研究與分析
（ISSRAC評估小組）

主要工作：

- 根據系統調查表，分析各組件可能存在的安全可靠風險。
- 根據安全可靠評估分析結果評估安全提升的可行性，並提出替換建議。
- 評估過程中可能需要針對部分問題與 IT 系統部門進行溝通 。

時間周期：15 - 30天

Part C

生成建議報告
（ISSRAC評估小組）

主要工作：

- 根據研究與分析結論，編寫IT系統安全可靠評估的建議報告。
- 審核並提交給 IT 系統部門，跟進並講解建議報告相關內容。

時間周期：5 - 10天

一、評估案例的具體進程


第 1 日
系統資料調研
ISSRAC 發出調查表
第 3 日
系統資料輸入
ISSRAC 收到IT部門的
資料反饋
第 14 日
過程交流
IT 部門同ISSRAC進
行綫上溝通
第 18 日
報告初稿
ISSRAC提交報告的初稿
給IT部門咨詢意見
第 24 日
第一次反饋
IT 部門跟ISSRAC的
第一輪意見反饋
第 32 日
第二次反饋
IT 部門跟ISSRAC的
第二輪意見反饋
第 45 日
第三次反饋
IT 部門跟ISSRAC的
第三輪意見反饋
第 46 日
報告終稿
ISSRAC提交正式報告
給IT部門

二、系統資料調研

調查表

需要填寫 IT 系統/子系統每個組件的詳細信息，包括組件類別、組件的產品名稱、組件功能、供應商名稱、廠商來源等信息。

編號	調查表內容分類
1	IT系統/子系統中每個組件的類別 （硬件，軟件，操作系統，雲平臺等）
2	每個組件的產品名稱
3	每個組件功能及當前運行狀態
4	供應商名稱
5	廠商來源

二、系統資料調研

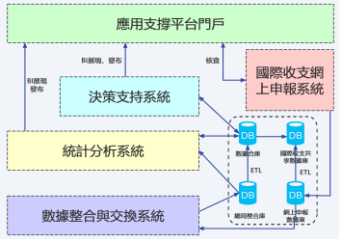
其它輸入資料（以附件文件提供）

01 IT系統簡介

提供 IT 系統的概要說明文件

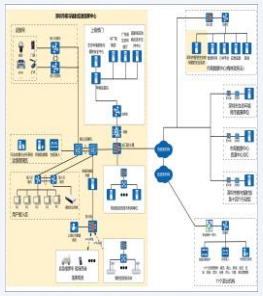
02 IT系統架構圖

提供IT系統架構圖，說明IT系統的各組件/子系統的組成及協作關係。



03 IT系統網絡拓撲圖

提供IT系統的網絡拓撲結構。包括網絡設計、安全防護等。



04 IT系統對瀏覽器的要求

如果涉及瀏覽器，說明IT系統對 瀏覽器的要求及應用情況

05 IT系統涉及的外設

IT 系統終端如果涉及外設，說明當前外設類型及型號

二、系統資料調研

其它輸入資料（以附件文件提供）

06 IT系統技術棧

- IT系統的開發語言（Java、Python、C/C++等）
- 開發框架（SpringBoot、Gtk等）
- 代碼量（不包含框架）、
- 系統架構（單體架構、微服務、SOA等）。

07 IT系統規模

- IT系統當前的用戶規模、平均用戶訪問量以及設計的最大並發量。

08 IT系統資源使用情況

為核心應用程序、存儲和數據庫提供物理服務器或雲平台資源的使用情況

存儲：

- 存儲系統中數據量(TB)

數據庫：

- 表規模（約 XX 張表）
- 數據量（約 XX TB）
- 存儲位置
- 資源佔用情況等

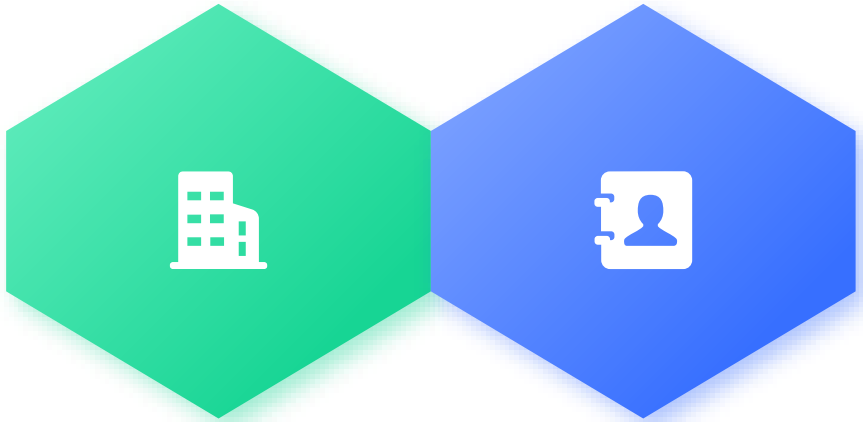
雲平台：

- Host的CPU數目。
- 可配置內存。

三、研究與分析

評估目標

分析產品潛在的安全可靠性風險，包括供應鏈中斷風險以及後門和漏洞問題的評估。

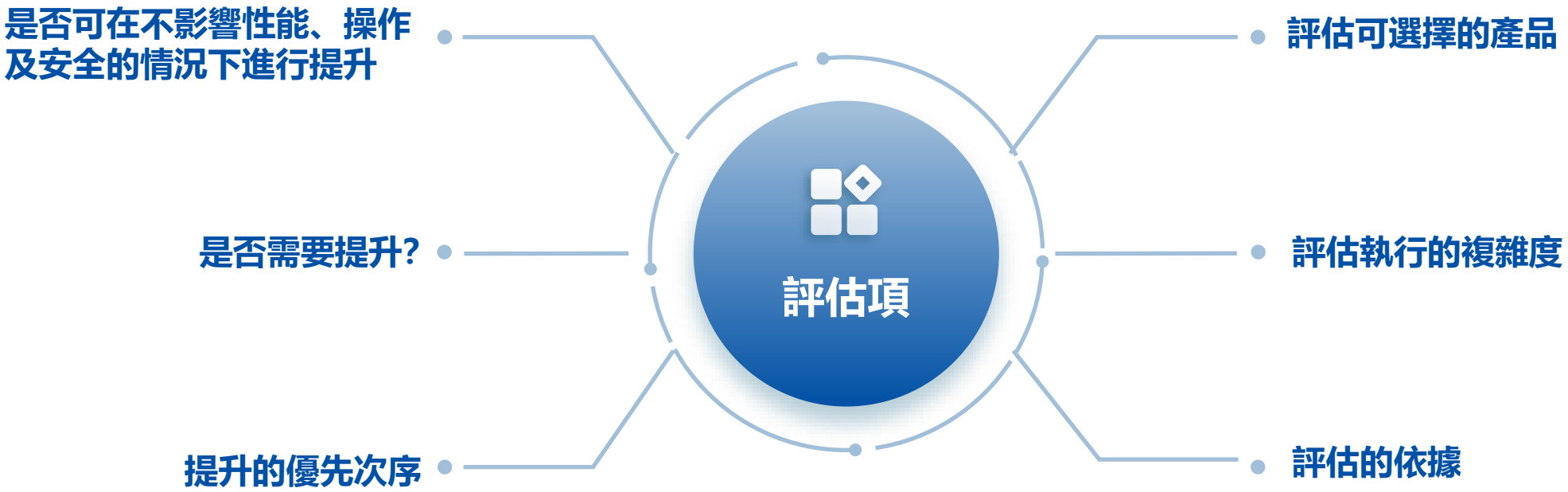


評估範圍

系統基礎設施、終端設備、軟件產品、用於開發定製程序的軟件組件以及系統的其他組件。

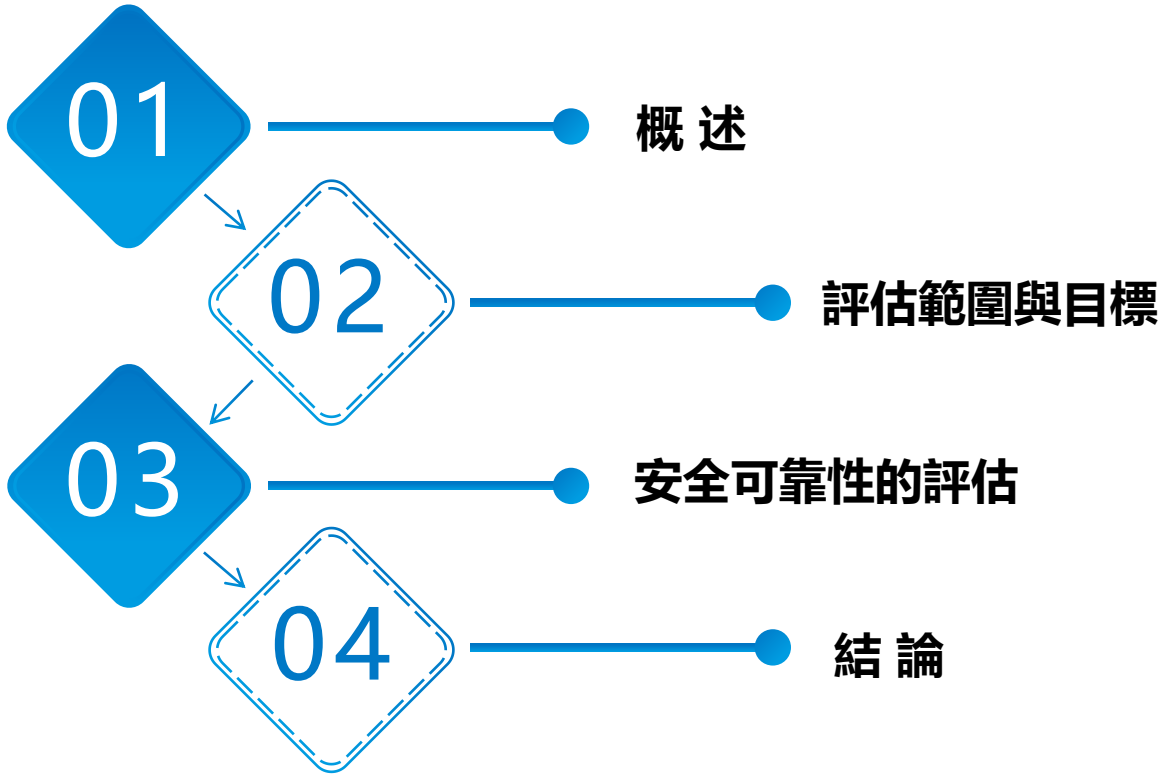
三、研究與分析

根據填寫的調查表，將對目標 IT 系統的每個組件進行安全風險分析和評估，評估項目包括以下六個方面。



四、評估報告- 建議報告

評估報告將以電子版形式編寫。報告將按照目標 IT 系統的子系統和組件編排。每個組件的分析結果和提升建議將以表格形式呈現。報告末尾將概述整個系統安全提升的挑戰和建議。



Thank You!

Email: hotline.issrac@lscm.hk

LSCM Website

LSCM Facebook