

時間鑑識：

運用 CyTix 精準解析多語種資安報告的時序資訊

謝沛錫 | 資料科學家





講者介紹 - 謝沛錫 (Eric)



- > 資料科學家 Data Scientist
- > 清華大學電機所碩士
- > 研究領域
 - > 大型語言模型推理 LLM Reasoning
 - > 大型語言模型偏好最佳化 LLM Preference Optimization



Agenda

- > 開場介紹
- > 資訊安全中的時間資訊
- > 資訊安全中提取時間的挑戰
- > 我們的解決方案
 - > CyCraft Time Extraction (CyTix)
 - > 專注於時間的 RAG 系統
- > 性能評估



資訊安全中的時間資訊



時間在資安報告中的價值

> 時間資訊是還原攻擊過程的關鍵

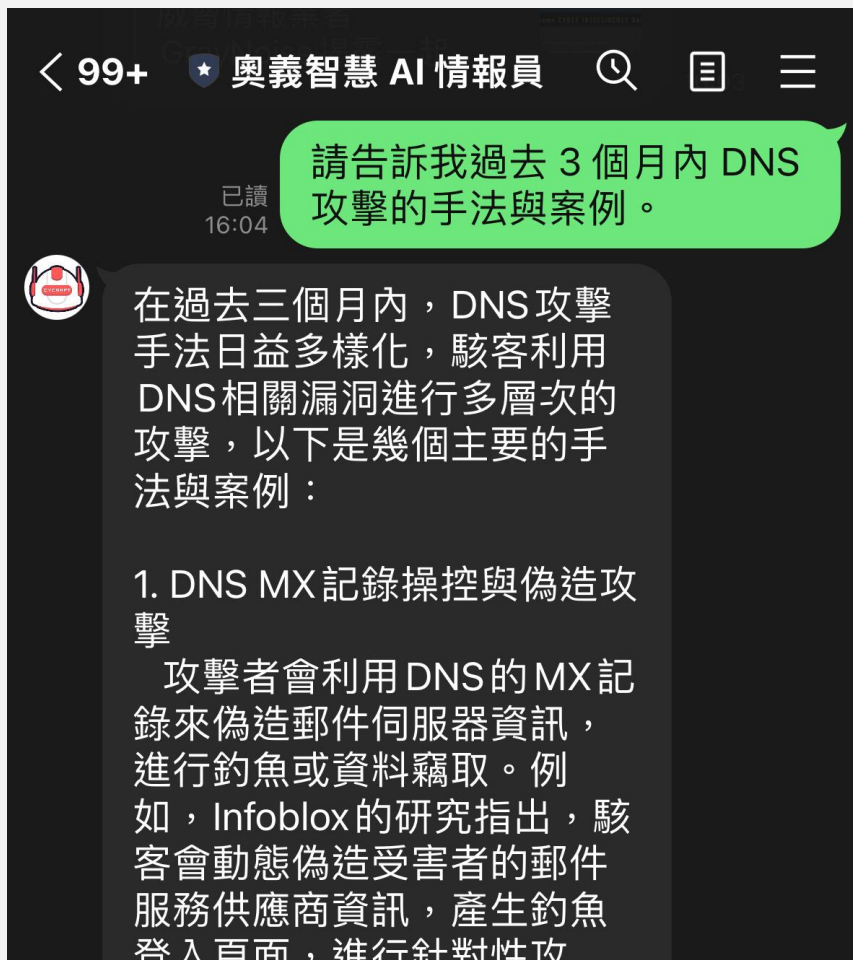
- > 資安報告與新聞中常提到事件發生的「時間點」、「時間長度」或「時間順序」，這些資訊能幫助分析攻擊者的行動節奏與滲透策略。

> 攻擊路徑與時間序列密切相關

- > 攻擊往往是分階段進行的，還原時間序列能幫助揭露攻擊流程與意圖。



🔍 資安調查中的實際應用 in CyCraft



目前時間：2025-07-04

查詢時間範圍：2025-04-04 ~ 2025-07-04 (by CyTix)

Try it yourself —
scan the QR code



<https://go.cycraft.ai/crafty>

XZ / liblzma 後門事件

iThome

新聞 專題 技術 AI Cloud 永續IT 醫療IT 資安 研討會 社群 IT EXPLAINED 搜尋

新聞

震撼整個IT界的XZ程式庫遭植入後門事件，之所以浮上檯面純屬意外！快速了解這項危機的三大關鍵

關於日前XZ Utils程式庫被植入隱密後門的事件，儘管整起事件的調查還沒結束，但已有相當多個重要議題被探討，因此我們也特別聯繫了Linux軟體開發與資安方面的專家來解讀，帮助大家掌握3大重要關鍵，尤其是開發人員是如何幸運發現後門的過程，還有攻擊者竟是長期潛伏以取得信任，且引入後門的手法也非常隱密

文/ 羅正漢 | 2024-04-04 發表

讚 358

分享



Andres FreundTec

@AndresFreundTec@mastodon.social

I accidentally found a security issue while benchmarking postgres changes.

If you run debian testing, unstable or some other more "bleeding edge" distribution, I strongly recommend you to use the

openwall.com/lists/oss-security

www.openwall.com

oss-security - backdoor in upstream xz/liblzma...

Obfuscated/encrypted stages binary backdoor hidden in two test files:

na2.xz
compressed.lzma

XZ/liblzma後門事件

快速了解這項危機的3大關鍵

xz/libzma
v5.6.0 & v5.6.1

iT+ 看影片追技術



全方位供應鏈資安風險
管控

臺灣資安大會 | 25 分



Runtime security
protection for web
applications on K8s

Kubernetes Summit | 35 分



那些年，我們一起踩過
的坑 - EKS 五年企業
級實戰分享

Kubernetes Summit | 30 分



你還記得 XZ / liblzma 後門事件被
攻擊的確切日期嗎？

(A) 2021年10月29日 (B) 2024年2月23日 (C) 2024年3月29日

CVE-2024-3094 - XZ Utils

> **2021-10-29** : Jia Tan 首次在 xz-devel 郵件論壇上發送一個看似無害的修補程式.....

Jia Tan 成為維護者

> **2022-09-27** : Jia Tan 提供了 5.4.0 的版本發布摘要。...

> **2022-10-28** : Jia Tan 被加入 GitHub 上的 Tukaani 組織

攻擊開始

> **2024-02-23** : Jia Tan 合併了藏有後門的二進位程式碼，巧妙地隱藏在幾個二進位測試輸入檔案中.....





Microsoft 數位防禦報告 (MDDR)





Microsoft 數位防禦報告 2020

> COVID-19 疫情

- > 駭客經常會利用像 COVID-19 疫情這類社會高度關注的議題來發動攻擊。從 2020 年上半年的威脅情勢 來看，雖然整體惡意程式的數量變化不大，但可以觀察到攻擊者藉由全球對疫情的關注，展開各種攻擊手法。舉例來說，分析美國的網路釣魚攻擊趨勢後發現，在世界衛生組織 (WHO) 於 3 月 11 日 宣布 COVID-19 為全球大流行疾病之後，與疫情有關的釣魚攻擊數量明顯增加。接著，當美國部分州政府自 5 月 1 日 起逐步恢復運作後.....





你可能想問.....

- > 「自從世界衛生組織（WHO）於 3 月 11 日宣布 COVID-19 為全球大流行疾病以來，全球的資安攻擊趨勢有什麼樣的變化？」
- > 報告發布時間：2020 年 10 月 22 日
- > 我們關心的時間區段：2020-03-11 ~ 2020-10-22



老闆想要你做一個報告

- > 「2020 年下半年，在亞太 / APAC 地區最嚴重的資安威脅是什麼？」
- > 「2020 年第一季有沒有什麼很嚴重的勒索軟體攻擊？」



資訊安全中提取時間的挑戰



以這個問題當作例子：

- > 「自從世界衛生組織（WHO）於3月11日宣布 COVID-19 為全球大流行疾病以來，全球的資安攻擊趨勢有什麼樣的變化？」
- > 報告發布時間：2020年10月22日
- > 我們關心的時間區段：2020-03-11 ~ 2020-10-22

網頁 / 檔案搜尋 ?



Microsoft 數位防禦報告 2020

- > COVID-19 疫情
- > 駭客經常會利用像 COVID-19 疫情這類社會高度關注的議題來發動攻擊。從 2020 年上半年的威脅情勢來看，雖然整體惡意程式的數量變化不大，但可以觀察到攻擊者藉由全球對疫情的關注，展開各種攻擊手法。舉例來說，分析美國的網路釣魚攻擊趨勢後發現，在世界衛生組織 (WHO) 於 3 月 11 日宣布 COVID-19 為全球大流行疾病之後，與疫情有關的釣魚攻擊數量明顯增加。接著，當美國部分州政府自 5 月 1 日起逐步恢復運作後.....

CRAFT CON
TAIWAN





網頁 / 檔案搜尋 ?

The image shows a document search interface with a search bar containing '3月11日'. The search results are displayed on a page titled 'Microsoft 數位防禦報告 2020'. The text discusses COVID-19 and mentions that the WHO announced COVID-19 as a global pandemic on March 11, 2020. The date '3月11日' is highlighted with a red box in the original image.

在文件中尋找

在文件中尋找

Q 3月11日 0/0 X

Q 3月11日 0/0 X

Microsoft 數位防禦報告 2020

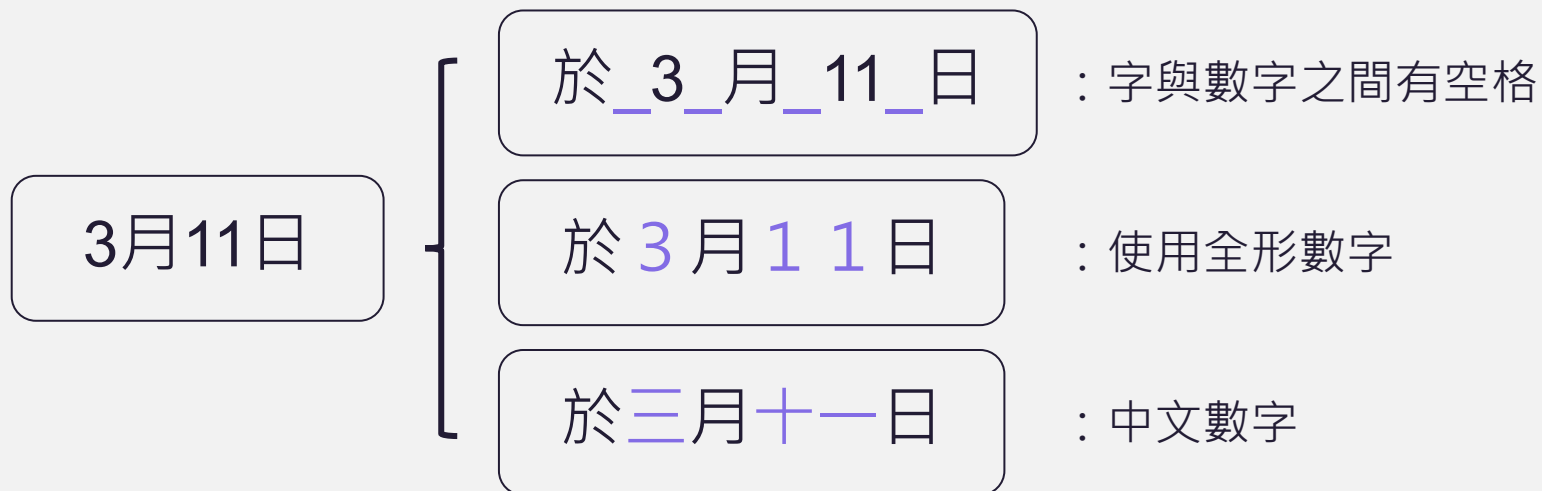
- > COVID-19 疫情
- > 駭客經常會利用像 COVID-19 疫情這類社會高度關注的議題來發動攻擊。從 2020 年上半年的威脅情勢 來看，雖然整體惡意程式的數量變化不大，但可以觀察到攻擊者藉由全球對疫情的關注，展開各種攻擊手法。舉例來說，分析美國的網路釣魚攻擊趨勢後發現，在世界衛生組織（WHO）於 3月11日 宣布 COVID-19 為全球大流行疾病之後，與疫情有關的釣魚攻擊數量明顯增加。接著，當美國部分州政府自 5月1日 起逐步恢復運作後.....

CRAFT CON TAIWAN

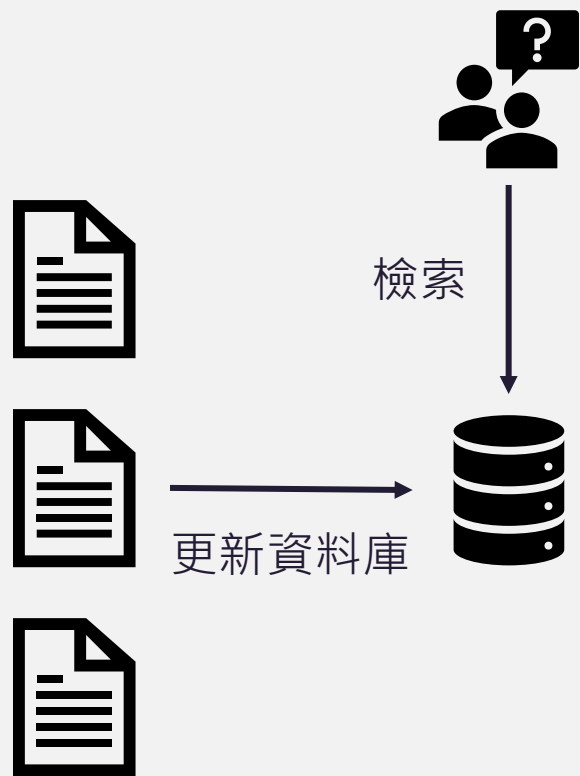
A photograph of a woman walking on a city street. She is wearing a black winter coat with a fur-lined hood, black pants, and a blue face mask. The street is lined with tall buildings and cars.



網頁 / 檔案搜尋 ?



RAG 應用的挑戰



「2020 年下半年，在亞太 / APAC 地區最嚴重的資安威脅是什麼？」

"What were the top cyber threats in the APAC region during the second half of 2020?"

根據對 2020 年上半年威脅情勢的分析，.....



在微軟企業用戶事件偵測與應變團隊 (DART) 支援的資安事件中，自 2019 年 10 月至 2020 年 7 月期間，.....





RAG 應用的挑戰



「2020 年下半年，在亞太 / APAC 地區最嚴重的資安威脅是什麼？」
"What were the top cyber threats in the APAC region during the second half of 2020?"

根據對 2020 年 **上半年**.....

自 2019 年 10 月至 2020 年 7 月期間，.....



GPT-4o

很抱歉，您提供的內容中，並未包含 **2020 年下半年** 在亞太地區的主要網路威脅資訊。.....



到目前為止的重點整理

時間資訊至關重要

> 資安報告與技術部落格高度依賴時間框架

 例如：XZ Utils 攻擊事件——透過時間點連結關鍵事件

時間抽取與檢索的挑戰

> 傳統的規則式 (rule-based) 方法在多語言環境中難以適用

 例如：「3月11日」這類表達難以被正確辨識

> 基於 RAG 的檢索模型，對時間相關的查詢表現不佳

 **SOON** 接下來：我們如何使用 AI 克服這些挑戰！



我們的解決方案： CyTix & Time-Focused RAG



CyTix 與 RAG 系統的結合





CyTix 與 RAG 系統的結合



「2020 年下半年，在亞太 / APAC 地區最嚴重的資安威脅是什麼？」

2020-07-01 ~ 2020-12-31

根據
語意 + 時間檢索

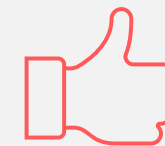


2020 年 9 月，微軟發佈了全新的年度報告書《Microsoft Digital Defense Report》，全面整理回顧了前一年度的資安趨勢，其中亞洲.....



2020-09-01 ~ 2020-09-30

2020 年 10 月 28 日 (星期三) 與 29 日 (星期四)，由日本微軟主辦的.....



2020-10-28 ~ 2020-10-29



CyTix 與 RAG 系統的結合



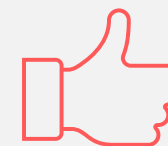
「2020 年下半年，在亞太 / APAC 地區最嚴重的資安威脅是什麼？」
"What were the top cyber threats in the APAC region during the second half of 2020?"

2020 年 9 月，微軟發佈.....

2020 年 10 月 28 日 (星期三)
與 29 日 (星期四)




微軟報告指出，2020 年下半年網路犯罪分子正透過以下手法持續進化其網路釣魚攻擊：.....



實作方法

實作方法


Base model
(Llama 3 8B)

Supervised Fine-Tuning



CyTix

單一時間資料集

合併

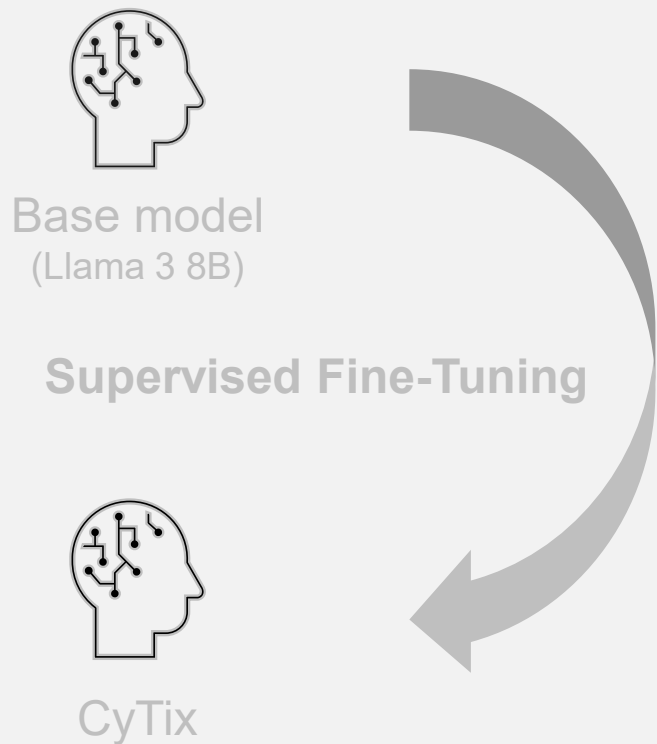
多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT

建構單一時間資料集

雙向延伸式擴展法



單一時間資料集

合併

多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT



建構單一時間資料集

雙向延伸式擴展法

目前時間：2025-07-04

> 使用 Regular expression 雙向提取時間描述

去年8月至今
←
1

1. 8月: 08-01 ~ 08-31

```
r'(\d{1,2}\s*月)'
```



建構單一時間資料集

雙向延伸式擴展法

目前時間：2025-07-04

> 使用 Regular expression 雙向提取時間描述



1. 8月: 08-01 ~ 08-31
2. 去年8月: 2024-08

```
relateYear = {  
  '大前年': ('<', 3), ...  
  '去年': ('<', 1),  
  '来年': ('>', 1), ...}
```



建構單一時間資料集

雙向延伸式擴展法

目前時間：2025-07-04

> 使用 Regular expression 雙向提取時間描述



3. ...至今: ~2025-07-04

['以來', '至今', '迄今', ...,
'から現在まで']



建構單一時間資料集

雙向延伸式擴展法

目前時間：2025-07-04

> 使用 Regular expression 雙向提取時間描述

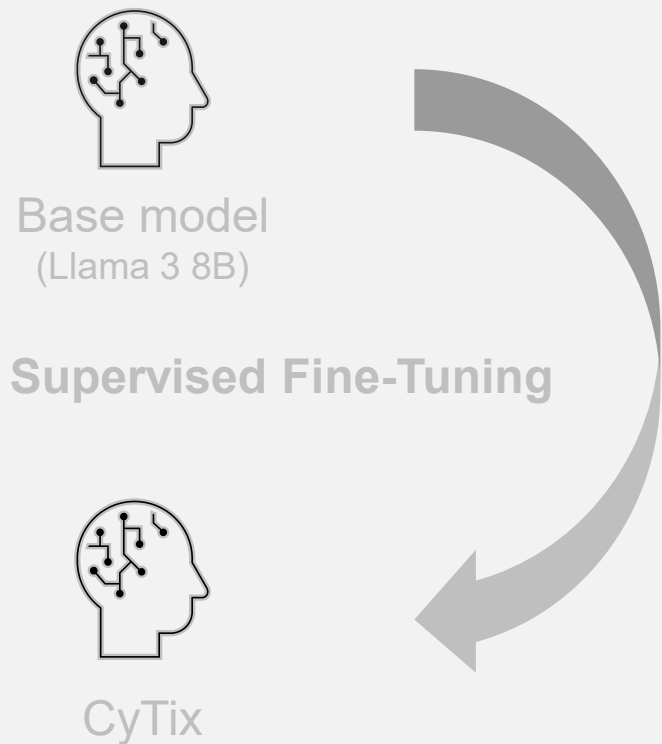


1. 8月: 08-01 ~ 08-31
2. 去年8月: 2024-08
3. ...至今: ~2025-07-04

→ 2024-08-01 ~ 2025-07-04

建構單一時間資料集

資料增強 Data Augmentation



單一時間資料集

合併

多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT

資料增強 Data Augmentation

> 可省略的副詞/連接詞

- > 最: 近三個月 / 最近三個月 (Last three months)
- > の: 先週土曜日 / 先週の土曜日 (Last Saturday)

> 從過去到現在的用法

- > ...迄今 / ...到目前為止 / 從...到現在
- > ...から現在まで

建構單一時間資料集

資料增強 Data Augmentation

> 最近...的用法

- > 最近這兩個禮拜
- > 這三天

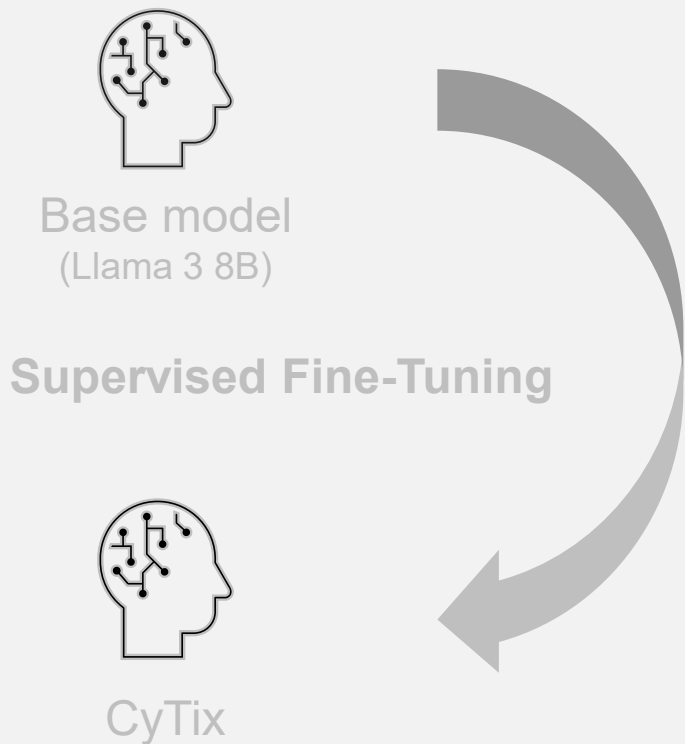
> 季度與半年

- > 上半年 / 下半年, 年初 / 年末
- > 第一季, 第三季度
- > 日本年號：令和 7 年



建構單一時間資料集

固定格式思維鏈 (CoT)



單一時間資料集

合併

多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT



建構單一時間資料集

單一時間資料集的樣本

美國紐約州參議院在**上周四**通過了 AI 安全法案《RAISE Act》

(Responsible AI Safety and Education Act)，目的在於預防 OpenAI、Google 或 Anthropic 等大型開發者.....。

> 發布時間:

2025-06-16

> 對應答案:

Get_Time_Specific

Start: datetime.date(2025, 6, 12)

End: datetime.date(2025, 6, 12)

TimeString: '上周四'



建構單一時間資料集

固定格式思維鏈 (CoT)

> 列出關鍵時間描述

The core timeString is: 上周四.

I will find the time relationship between current time and core timeString.

Relationship: Core timeString 上周四 is a date description.



建構單一時間資料集

固定格式思維鏈 (CoT)

> 拆解時間描述

- Year description: , Half year description:
- Quarter description: , Season description:
- Month description: , Month Section description:
- Week description: 上周, Weekday description: 周四
- Day description:



建構單一時間資料集

固定格式思維鏈 (CoT)

> 逐步推理計算目標時間

The current time is 2025-06-16, Monday. Time operations:

1. The 上周 is 1 weeks before the current time. The date of the target week is $06-16 - 1 * 7 \text{ days} = 06-16 - 7 \text{ days} = 06-09, \text{Monday}$.
2. The 周四 means 3 days after Monday. The last Monday is $06-09 - 0 = 06-09, \text{Monday}$. The start and end timestamp is $06-09 + 3 = 06-12, \text{Thursday}$.



建構單一時間資料集

固定格式思維鏈 (CoT)

> 總結並輸出

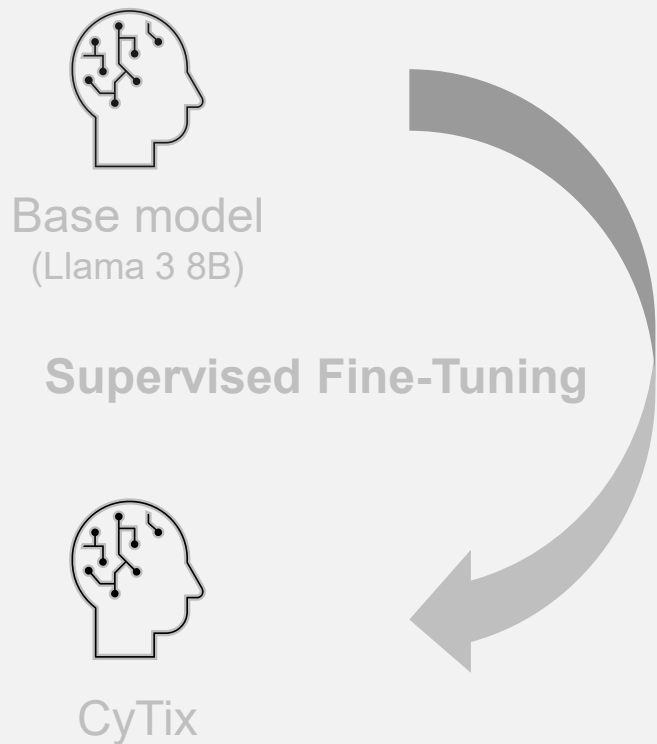
get_time_specific

<|reserved_special_token_249|>

{"start": 2025-06-12, "end": 2025-06-12}

建構單一時間資料集

不固定的時間描述



單一時間資料集

合併

多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT



建構單一時間資料集

不固定的時間描述

- > 在處理使用者輸入的問題時特別有用
 - > 可以根據需求自定義數量

- > 最近幾個月

- > `get_time_not_specific {"scale": "months"}`
→ 最近 3 個月

- > 前幾年

- > `get_time_not_specific {"scale": "years"}`
→ 前 2 年

在進入下一部分之前...腦筋急轉彎

 你能算出正確的出發日期嗎？

 你朋友說他「四個禮拜前的週二」去日本大阪玩

 今天是 7 月 4 日（五）

請問他出發是哪一天？

(A) 2025 年 6 月 3 日 (B) 2025 年 6 月 5 日 (C) 2025 年 6 月 7 日



當一句話中出現多個時間描述時 ...



建構多時間資料集

多個時間描述

> COVID-19 疫情

駭客經常會利用像 COVID-19 疫情這類社會高度關注的議題來發動攻擊。從 2020 年上半年的威脅情勢來看，雖然整體惡意程式的數量變化不大，但可以觀察到攻擊者藉由全球對疫情的關注，展開各種攻擊手法。舉例來說，分析美國的網路釣魚攻擊趨勢後發現，在世界衛生組織（WHO）於 3 月 11 日宣布 COVID-19 為全球大流行疾病之後，與疫情有關的釣魚攻擊數量明顯增加。接著，當美國部分州政府自 5 月 1 日起逐步恢復運作後.....

建構多時間資料集

多個時間描述



Base model
(Llama 3 8B)

Supervised Fine-Tuning



CyTix

單一時間資料集

合併

多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT



單一時間 → 多時間資料集

單一時間資料集

合成的 50,000+ 樣本句
(固定格式 CoT)

樣本句 1

樣本句 1

樣本句 2

⋮

樣本句 1

樣本句 2

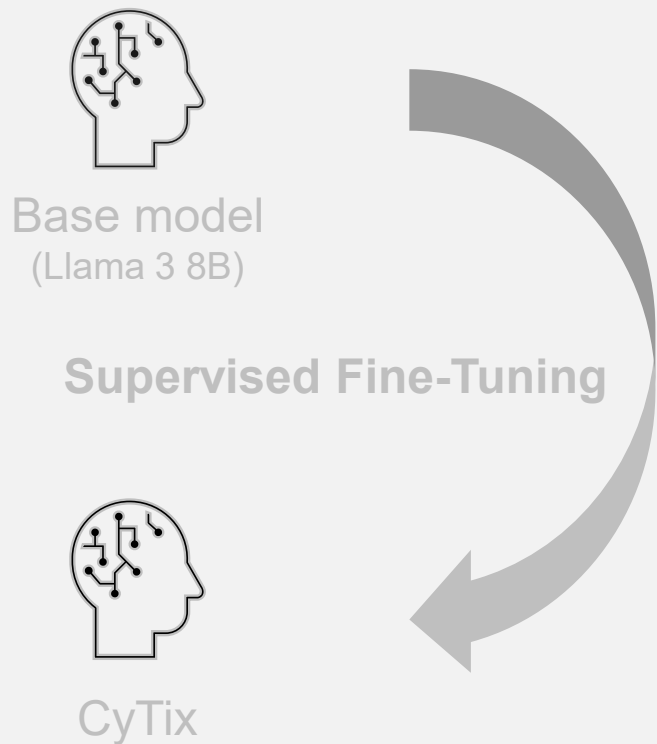
樣本句 3

多時間資料集

22,000+ 多時間樣本句
從單一時間樣本句合併而成

建構多時間資料集

以波浪號 / 連字號表示的時間區段



單一時間資料集

合併

多時間資料集

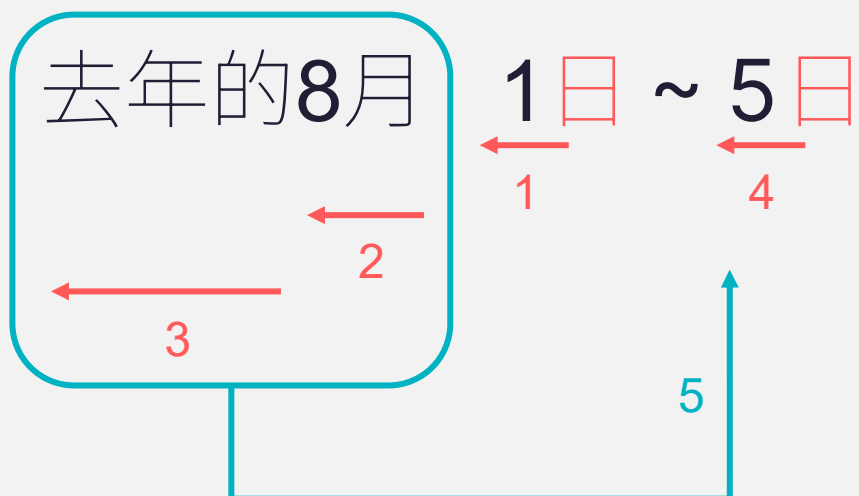
1. 雙向延伸式擴展法
2. 資料增強 Data Augmentation
3. 思維鏈 Chain-of-Thought (CoT)
4. 不固定的時間描述

1. 波浪號與連字號
2. 縮寫與省略
3. 更簡潔的 CoT

以波浪號 / 連字號表示的時間區段

> 包含省略的用法

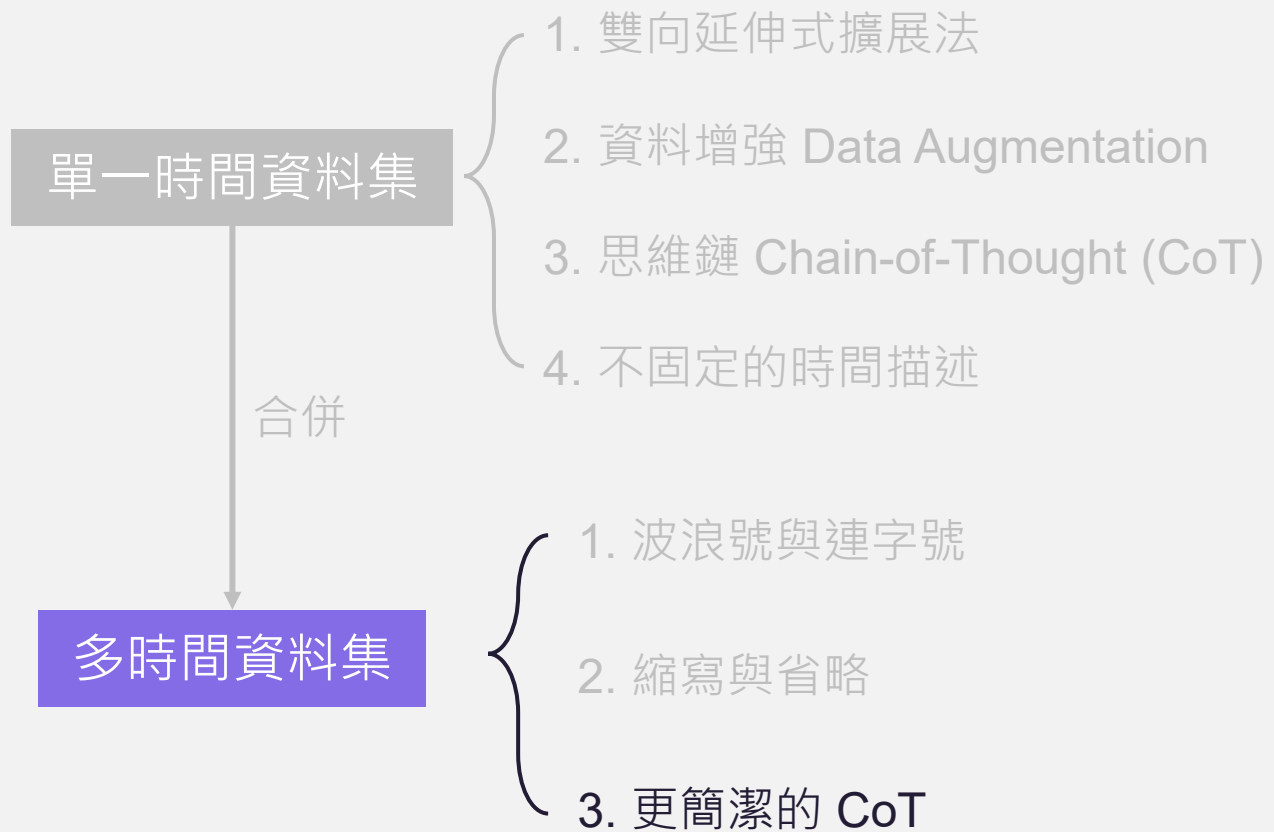
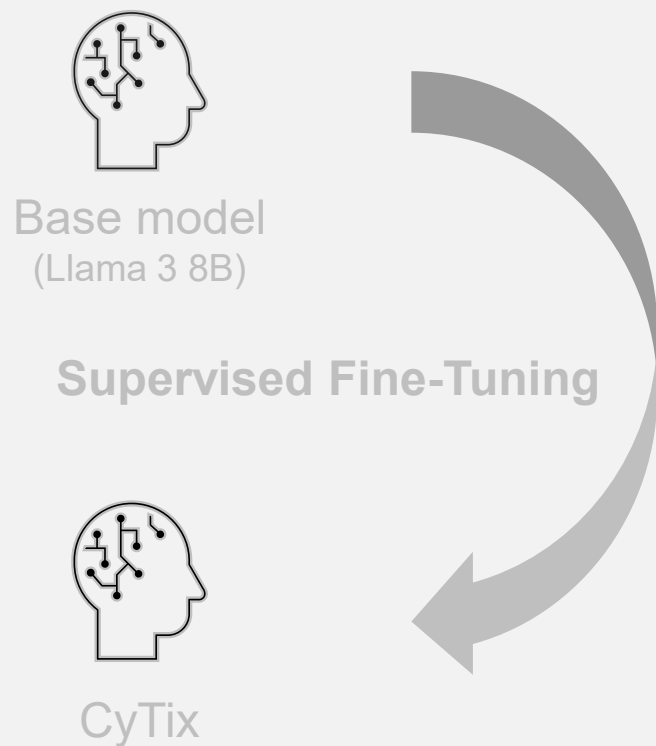
目前時間：2025-07-04



1. 1日: 01
2. 8月: 08-01
3. 去年的8月1日: 2024-08-01
4. 5日: 05
5. 去年的8月5日: 2024-08-05

→ 2024-08-01 ~ 2024-08-05

實作方法



建構多時間資料集

更簡潔的 CoT

> 減少 system prompt 長度

> 390 → 220

-44%



```
// Supported function definitions that should be called when necessary.\nnamespace functions {\n\n// Extract the start timestamp and end timestamp from a Chinese text time description with explicit timestamp. You will get the current time and day of the week at the end of the text in the format %Y-%m-%d <weekday> for year-month-day <weekday>, e.g. 2024-04-02 Tuesday for April 2, 2024 Tuesday. There are a few word conversions to note, "大前年" means "three years ago" while "大後年" means "three years from now", "大前天" means "three days ago" and "大後天" means "three days from now".\ntype get_time_specific = (_: {\n// Start timestamp in the format %Y-%m-%d, where the start timestamp must be the same as or earlier than the end timestamp.\nstart: string,\n// End timestamp in the format %Y-%m-%d, where the end timestamp must be the same as or later than the start timestamp.\nend: string,\n}) => any;\n\n// Extract the scale of time described in Chinese text without explicit timestamp.\nYou will get the current time and day of the week at the end of the text in the format %Y-%m-%d <weekday> for year-month-day <weekday>, e.g. 2024-04-02 Tuesday for April 2, 2024 Tuesday.\nIf there is no time description, then scale is set to "noTimeString".\ntype get_time_not_specific = (_: {\n// Specifies the time scale for the most recent interval or recent. Options include "days", "weeks", "months", "years", "recent", or "noTimeString".\nscale: "days" | "weeks" | "months" | "years" | "recent" | "noTimeString",\n}) => any;\n\n} // namespace functions
```

```
// Supported function definitions that should be called when necessary.\nnamespace functions {\n\n// There are a few word conversions to note, "大前年" means "three years ago" while "大後年" means "three years from now", "大前天" means "three days ago" and "大後天" means "three days from now".\ntype get_time_specific = (_: {\n// The start timestamp must be the same as or earlier than the end timestamp.\nstart: string,\n// The end timestamp must be the same as or later than the start timestamp.\nend: string,\n}) => any;\n\n// If there is no time description, then scale is set to "noTimeString".\ntype get_time_not_specific = (_: {\n// Specifies the time scale for the most recent interval or recent. Options include "days", "weeks", "months", "years", "recent", or "noTimeString".\nscale: "days" | "weeks" | "months" | "years" | "recent" | "noTimeString",\n}) => any;\n\n} // namespace functions
```

建構多時間資料集

更簡潔的 CoT

> 合併重複的推理步驟

Query:

駭客經常會利用像 COVID-19 疫情這類社會高度關注的議題來發動攻擊。從 2020 年上半年的威脅情勢來看，雖然整體惡意程式的數量變化不大，但可以觀察到攻擊者藉由全球對疫情的關注，展開各種攻擊手法。舉例來說，分析美國的網路釣魚攻擊趨勢後發現，在世界衛生組織 (WHO) 於 3 月 11 日宣布 COVID-19 為全球大流行疾病之後，與疫情有關的釣魚攻擊數量明顯增加。接著，當美國部分州政府自 5 月 1 日起逐步恢復運作後.....

。 Current time: 2020-10-22 Thursday

Raw Output:

The core timeString: 2020 年上半年, 3 月 11 日, 5 月 1 日.

<reasoning process here>.....

建構多時間資料集

更簡潔的 CoT

The core timeString is: 2020 年上半年. I will find the time relationship between current time and core timeString.
 Relationship: The core time string 2020 年上半年 is the date description. Relationship: Core timeString 2020 年上半年 is a date description.
 Extract the time description in core timeString:
 - Year: 2020 年. Half year:上半年. Quarter: . Season: .
 - Month: . Month Section: .
 - Week: . Weekday: .
 - Day: .
 The current time is 2020-10-22, so the year of the start timestamp is 2020. The year of end timestamp is 2020. The year, month and day of the start timestamp are 2020-01-01. The year, month and date of the end timestamp are 2020-06-30. I will select the most suitable tool to extract the time information based on relationship.
 <|reserved_special_token_249|>get_time_specific{"start": "2020-01-01", "end": "2020-06-30"}<|stop|>
 The core timeString is: 3 月 11 日. I will find the time relationship between current time and core timeString.
 Relationship: The core time string 3 月 11 日 is the date description. Extract the time description in core timeString:
 - Year: . Half year: . Quarter: . Season: .
 - Month: 3 月 11 日. Month Section: .
 - Week: . Weekday: .
 - Day: 3 月 11 日.
 The current time is 2020-10-22, so the year of the start timestamp is 2020. The year of end timestamp is 2020. The year, month and day of the start timestamp are 2020-03-11. The year, month and date of the end timestamp are 2020-03-11. I will select the most suitable tool to extract the time information based on relationship.
 <|reserved_special_token_249|>get_time_specific{"start": "2020-03-11", "end": "2020-03-11"}<|stop|>
 The core timeString is: 5 月 1 日. I will find the time relationship between current time and core timeString.
 Relationship: The core time string 5 月 1 日 is the date description. Extract the time description in core timeString:
 - Year: . Half year: . Quarter: . Season: .
 - Month: 5 月 1 日. Month Section: .
 - Week: . Weekday: .
 - Day: 5 月 1 日.
 The current time is 2020-10-22, so the year of the start timestamp is 2020. The year of end timestamp is 2020. The year, month and day of the start timestamp are 2020-05-01. The year, month and date of the end timestamp are 2020-05-01. I will select the most suitable tool to extract the time information based on relationship.
 <|reserved_special_token_249|>get_time_specific{"start": "2020-05-01", "end": "2020-05-01"}<|stop|>

→ -38%

The core timeString: 2020 年上半年, 3 月 11 日, 5 月 1 日.

Relationship: Core timeString 2020 年前半 is a date description.

Extract the time description in core timeString:

- Year: 2020 年. Half year:上半年. Quarter: . Season: .
- Month: . Month Section: .
- Week: . Weekday: .
- Day: .

The current time is 2020-10-22, Thursday. Time operations:

1. The 2020 年 is 2020.
2. The 上半年 means the first half of the year, from month 1 to month 6.

<|reserved_special_token_249|>get_time_specific {"start": "2020-01-01", "end": "2020-06-30"}<|stop|>

Relationship: Core timeString 3 月 11 日 is a date description.

Extract the time description in core timeString:

- Year: . Half year: . Quarter: . Season: .
- Month: 3 月 11 日. Month Section: .
- Week: . Weekday: .
- Day: 3 月 11 日.

The current time is 2020-10-22, Thursday. Time operations:

1. The 3 月 11 日 is month 3.
2. The 3 月 11 日 is day 11.

<|reserved_special_token_249|>get_time_specific {"start": "2020-03-11", "end": "2020-03-11"}<|stop|>

Relationship: Core timeString 5 月 1 日 is a date description.

Extract the time description in core timeString:

- Year: . Half year: . Quarter: . Season: .
- Month: 5 月 1 日. Month Section: .
- Week: . Weekday: .
- Day: 5 月 1 日.

The current time is 2020-10-22, Thursday. Time operations:

1. The 5 月 1 日 is month 5.
2. The 5 月 1 日 is day 1.

<|reserved_special_token_249|>get_time_specific {"start": "2020-05-01", "end": "2020-05-01"}<|stop|>



建構多時間資料集

更簡潔的 CoT

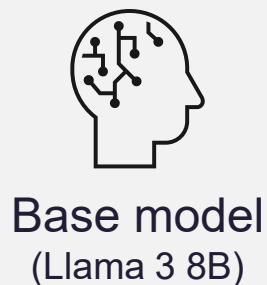
> 合併重複的推理步驟

Output:

```
get_time_specific<|reserved_special_token_249|>
{"start": "2020-01-01", "end": "2020-06-30"}
get_time_specific<|reserved_special_token_249|>
{"start": "2020-03-11", "end": "2020-03-11"}
get_time_specific<|reserved_special_token_249|>
{"start": "2020-05-01", "end": "2020-05-01"}
```

訓練 CyTix

Supervised Fine-Tuning



Supervised Fine-Tuning



單一時間資料集

合併

多時間資料集

- 1. 雙向延伸式擴展法
- 2. 資料增強 Data Augmentation
- 3. 思維鏈 Chain-of-Thought (CoT)
- 4. 不固定的時間描述

- 1. 波浪號與連字號
- 2. 縮寫與省略
- 3. 更簡潔的 CoT

訓練 CyTix

泛化性 Generalizability

我們的模型「CyTix」

- > 雖然是以啟發式資料訓練，但具備超越訓練情境的泛化能力

沒有在訓練資料集中出現！

Query:

SECCON 是在三月的頭兩天舉行。

Current time: 2025-07-04 Friday

Raw Output:

The core timeString: 三月的頭兩天.

Relationship: Core timeString 三月的頭兩天 is a date description.

Extract the time description in core timeString:

- Year: . Half year: . Quarter: . Season: .
- Month: 3月. Month Section: .
- Week: . Weekday: .
- Day: 的頭兩天.

訓練 CyTix

泛化性 Generalizability

我們的模型「CyTix」

- > 雖然是以啟發式資料訓練，但具備超越訓練情境的泛化能力

沒有在訓練資料集中出現！

Query:

SECCON 是在三月的頭兩天舉行。

Current time: 2025-07-04 Friday

The current time is 2025-07-04, Friday.

Time operations:

1. The 3月 is month 3.
2. The 的頭兩天 means day 1 to day 2 of the month.

get_time_specific

`{"start": "2025-03-01", "end": "2025-03-02"}`

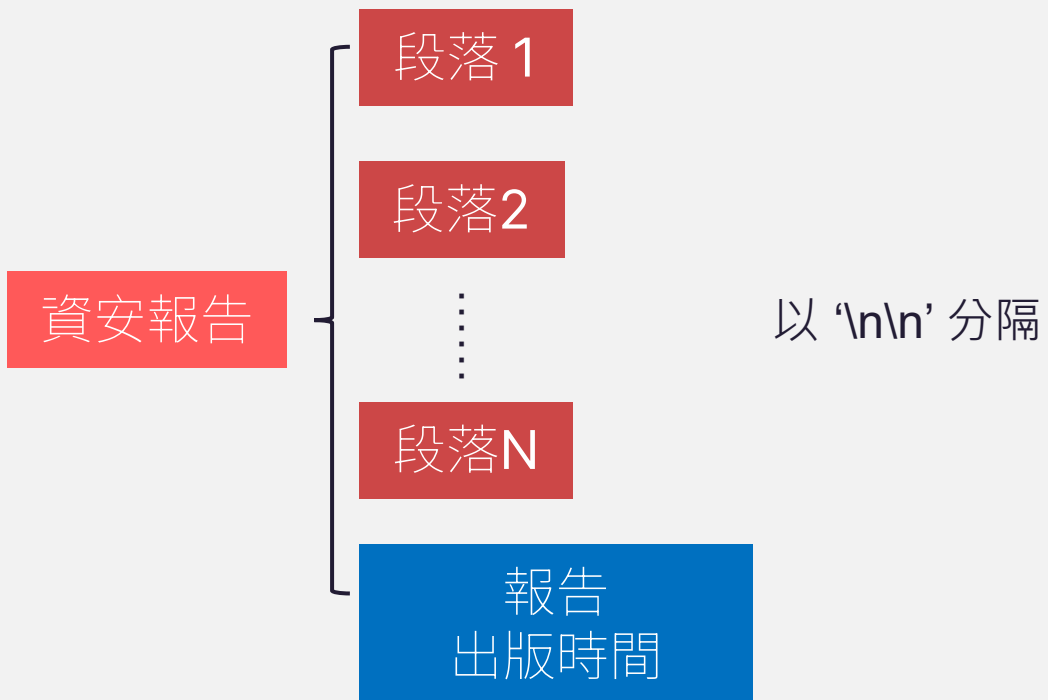


實際應用與案例研究



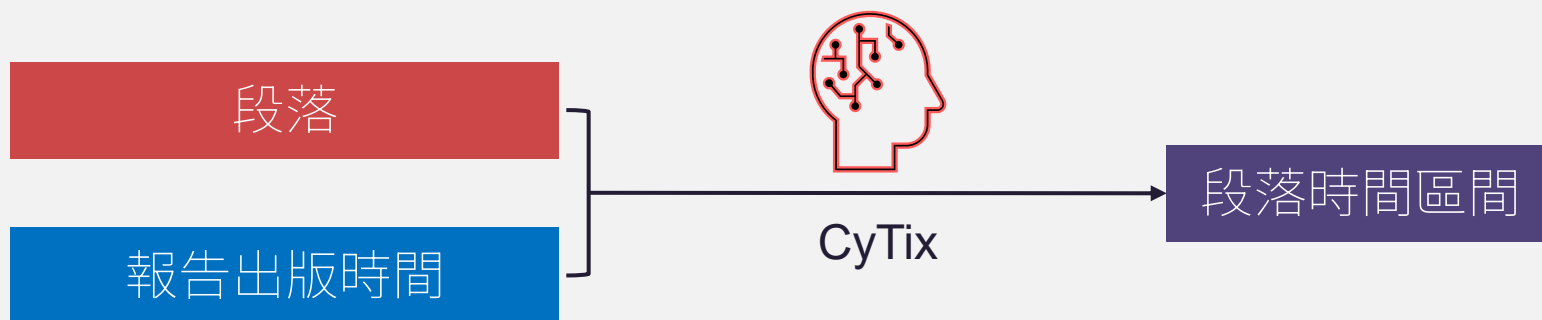
實際應用

> 報告 → 段落



實際應用

> 段落 → 段落所包含的時間區間





實際應用

> 透過向量嵌入 (embedding) 相似度選取相關段落





無關 這則新聞中，哪裡出現了與主題無關的背景資訊？

> 西雅圖機場疑遭網攻，IT斷線數天

iThome 2024年08月27日

美國西雅圖主要的 Seattle Tacoma 國際機場上周六疑似遭到網路攻擊，包括網站、郵件系統連線中斷，影響通訊及旅客服務，截至周一仍未恢復。

Seattle Tacoma (SEA-TAC) 國際機場是西雅圖最大國際機場，也是美國西北太平洋航線最繁忙的機場，2013年服務旅客超過5,100萬人次。

上周六 (8/24) 太平洋時間周六一早，西雅圖機場發生疑似網路攻擊，引發部份系統斷線。機場飛航主任 Lance Lyttle 記者會說明，這起事件造成數個系統網路中斷，包括網站及電子郵件系統。.....

無關緊要的背景資訊

> 西雅圖機場疑遭網攻，IT斷線數天

iThome 2024年08月27日

美國西雅圖主要的 Seattle Tacoma 國際機場上周六疑似遭到網路攻擊，包括網站、郵件系統連線中斷，影響通訊及旅客服務，截至周一仍未恢復。

Seattle Tacoma (SEA-TAC) 國際機場是西雅圖最大國際機場，也是美國西北太平洋航線最繁忙的機場，2013年服務旅客超過5,100萬人次。

上周六 (8/24) 太平洋時間周六一早，西雅圖機場發生疑似網路攻擊，引發部份系統斷線。機場飛航主任 Lance Lyttle 記者會說明，這起事件造成數個系統網路中斷，包括網站及電子郵件系統。



案例研究

> 西雅圖機場疑遭網攻，IT斷線數天

iThome 2024年08月27日

美國西雅圖主要的 Seattle Tacoma 國際機場上週六疑似遭到網路攻擊，包括網站、郵件系統連線中斷，影響通訊及旅客服務，截至周一仍未恢復。

Seattle Tacoma (SEA-TAC) 國際機場是西雅圖最大國際機場，也是美國西北太平洋航線最繁忙的機場，2013年服務旅客超過5,100萬人次。

上週六 (8/24) 太平洋時間週六一早，西雅圖機場發生疑似網路攻擊，引發部份系統斷線。機場飛航主任 Lance Lyttle 記者會說明，這起事件造成數個系統網路中斷，包括網站及電子郵件系統。



案例研究

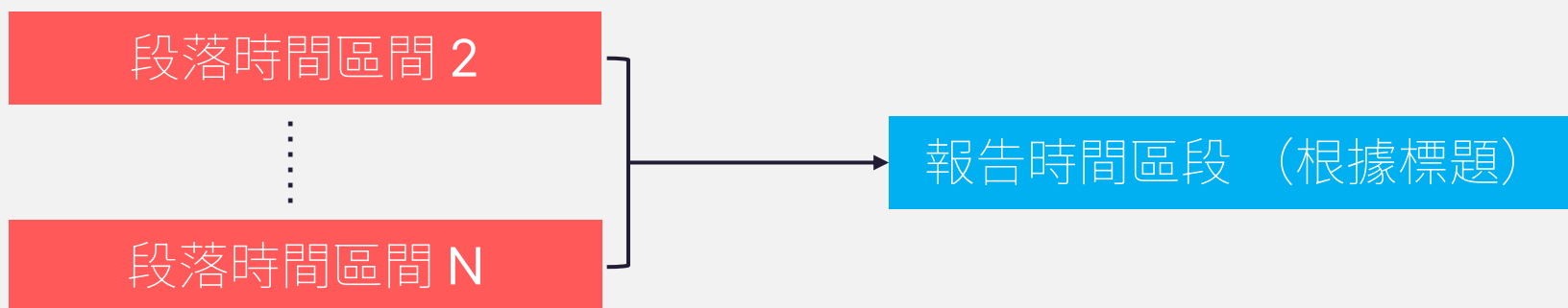
> 西雅圖機場疑遭網攻，IT斷線數天

iThome 2024年08月27日

1. 美國西雅圖主要的 Seattle Tacoma 國際機場上**周六**疑似遭到網路攻擊，包括網站、郵件系統連線中斷，影響通訊及旅客服務，**截至周一**仍未恢復。 **0.611**
2. Seattle Tacoma (SEA-TAC) 國際機場是西雅圖最大國際機場，也是美國西北太平洋航線最繁忙的機場，2013年服務旅客超過5,100萬人次。 0.403
3. **上周六 (8/24)** 太平洋時間**周六**一早，西雅圖機場發生疑似網路攻擊，引發部份系統斷線。機場飛航主任 Lance Lytle 記者會說明，這起事件造成數個系統網路中斷，包括網站及電子郵件系統。 **0.608**
4. 此事不到二個月前，許多機場才因為Crowdstrike軟體更新引發作業大亂。CrowdStrike的軟體臭蟲觸發Windows電腦當機... 0.469

實際應用

> 合併各段落時間區間



以天為最小單位



案例研究

> 西雅圖機場疑遭網攻，IT斷線數天

iThome 2024年08月27日

1. 美國西雅圖主要的 Seattle Tacoma 國際機場 **上週六** 疑似遭到網路攻擊，包括網站、郵件系統連線中斷，影響通訊及旅客服務，**截至周一** 仍未恢復。
→ 2024-08-24 (六) ~ 2024-08-26 (一)
3. **上週六 (8/24)** 太平洋時間週六一早，西雅圖機場發生疑似網路攻擊，引發部份系統斷線。機場飛航主任 Lance Lyttle 記者會說明，這起事件造成數個系統網路中斷，包括網站及電子郵件系統。.....
→ 2024-08-24 (六)

報告時間區段 (根據標題)

2024-08-24 ~ 2024-08-26



性能評估



性能評估

- > 真實世界資料 (CyCraft 聊天機器人使用者問題)
- > 合成測試資料
- > 預測速度及 **GPU** 記憶體使用量



性能評估

> 真實世界資料 (CyCraft 聊天機器人使用者問題)

~ 2024/09 約 2900 筆

GPT-4o	Mode ACC	Time ACC	Time Overlap
	0.965	0.642	0.731
CyTix (Ours)	Mode ACC	Time ACC	Time Overlap
	0.995	0.984	0.985

性能評估

> 合成測試資料

gpt-4o-2024-08-06
3-shots, 903 samples

	GPT-4o	CyTix
Precision	0.566	0.935
Recall	0.443	0.956
F1	0.497	0.945
Accuracy	0.443	0.956
Avg Overlap	0.570	0.971
Scale precision	0.383	0.920
Scale Recall	0.668	0.951
Scale F1	0.486	0.935
Scale Accuracy	0.668	0.951

 44.8%

 40.1%

⚠️ GPT-4o 無法正確推論省略的資訊

Query:

到了 23 日，資安廠商 Fox-IT 已確認了這項推測，並補充說明他們當時沒有事先掌握相關情報，因此不得不對外公佈這個問題。

Current time: **2024-04-03** Saturday

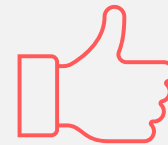


```
get_time_specific  
{"start": "2024-04-23",  
 "end": "2024-04-23"}
```



CyTix

```
get_time_specific  
{"start": "2024-03-23",  
 "end": "2024-03-23"}
```





性能評估

Number of Sentences

1	2	3	Total
526	266	111	903

> 預測速度及 GPU 記憶體使用量

CyTix
Llama3 - 8B

CyTix-Light
Qwen2.5 - 1.5B

Quantize	Second per sample	Memory Usage
bf16	0.967	14.926 GB (15284 MB)
5-bit	0.589 x0.56	9.523 GB (9752 MB) x0.59
4-bit	0.548 x0.19	8.840 GB (9052 MB) x0.325
bf16	0.419	5.66 GB (5796 MB)
AWQ 4-bit	0.187	4.85 GB (4966 MB)

llama-server async threads=10
On single RTX4090

Conclusion and Takeaway

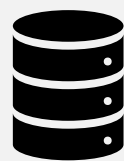
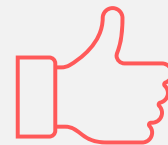
> 在 RAG 系統中，時間檢索機制至關重要



「2020 年下半年，在亞太 / APAC 地區最嚴重的資安威脅是什麼？」

2020-07-01 ~ 2020-12-31

根據
語意 + 時間檢索



2020 年 9 月，微軟發佈了...，其中亞洲.....

2020-09-01 ~ 2020-09-30



2020 年 10 月 28 日 (星期三) 與 29 日 (星期四)，由日本微軟主辦的.....

2020-10-28 ~ 2020-10-29



Conclusion and Takeaway

> 專為任務設計的模型「CyTix」效能超越第三方 LLM

	GPT-4o	CyTix	
F1	0.497	0.945	 44.8%
Accuracy	0.443	0.956	
Avg Overlap	0.570	0.971	 40.1%
Scale F1	0.486	0.935	



Conclusion and Takeaway

> 高效且具擴展性的解決方案

	Quantize	Second per sample	Memory Usage
CyTix	4-bit	0.548	8.840 GB (9052 MB)

	Quantize	Second per sample	Memory Usage
CyTix-Light	AWQ 4-bit	0.187	4.85 GB (4966 MB)

 可在單張 RTX 3060 / 3080 / 3090 / 4060... 上運行
真實場景中具可行性與實用性

Thanks!

Q&A



CRAFT CON
TAIWAN



CYCRAFT

AGENTIC AI
BLUE TEAM X RED TEAM