



威脅模型與 Metadata 入門

認識你的對手，
以及為什麼匿名工具要開源才可信

最常被問到的問題

「我該用哪個 App？」

沒有一體適用的答案。

挑工具之前，先回答三個問題

1

我要保護什麼？

資料、身分、關係、行蹤

2

**我要防的
對手是誰？**

對方有什麼能力，
決定你要做到什麼程度

3

**我願意付出
多少成本？**

便利、金錢、學習、說服

寫成產品語言：你的服務存了什麼、你的使用者要防誰、你預設替他們擋掉多少。

有人稱之為風險評估。兩者重疊，風險評估多問一層機率與損失。

用一個具體的人走一遍

一位獨立記者

正在做一篇關於某公司勞動條件的報導。

有一位**在職員工**願意提供內部資料。

1 我要保護什麼？

直覺的答案是「保護資料不外洩」。

真正要保護的是**那位員工的身分**，
以及「員工與記者聯繫過」**這個事實**。

記者被知道在查，頂多報導提前曝光。員工被查出來，會失去工作。
而且對手不需要談話內容，只要證明有聯繫，就能從那裡查下去。

2 我要防的對手是誰？

對手	他能做到什麼
廣告商、資料仲介	追蹤你的瀏覽與消費
詐騙集團	社交工程、盜帳號
親密關係加害者 最常被忽略	實體碰得到你的裝置
你自己的機構 最少被列入	IT 看得到你的流量，法務與編輯台看得到你的檔案
公司法務、徵信	調閱內部紀錄、查通聯
國家級監控	電信層攔截、跨境調取

對手決定了結論：那位員工不能用公司的設備與網路。結論從對手推出來，不從工具推出來。

3 我願意付出多少成本？

❖ 便利

每次都要多幾個步驟

❖ 金錢

買裝置、付服務費

❖ 學習

要花多久才會用

❖ 說服

團隊裡每個人都要跟著改

成本太高的方案，
等於**沒有方案**。

給一位記者一套完美但要學兩週的流程，
他在截稿壓力下會回頭使用 LINE。

安全方案的第一個要求，是它**會被使用**。

同一套三問，換一個主角

一個 12 人的 NGO

沒有 IT 人員，同事都不是技術背景

- 1 保護什麼
受訪者名單、案件檔案，以及誰跟誰談過
- 2 防誰
對造律師、被報導的機構，還有離職同事帶走的東西
- 3 成本
11 個人要一起改，說服的成本高過技術

你正在寫的那個服務

你是工程師，不是人權工作者

- 1 保護什麼
使用者的 log、IP、上傳檔案裡沒被清掉的 metadata
- 2 防誰
你的**使用者**的對手，不是你的對手
- 3 成本
預設值改掉多少，而使用者不必知道這件事存在

三個問題不變。換一個主角，**答案就整個不同**。

什麼時候需要做這件事

處境變了

- 換工作、接一條新題目、成為公眾人物
- 有新的人進入信任範圍
新的消息來源、新同事、新的合作組織
- 團隊有人離開
他手上還留著哪些聯絡方式與密碼

環境變了

- 收到律師函、存證信函或告訴
代表對手已經知道你在查
- 出事之後
帳號被盜、被跟蹤、同儕出事
- 每年重看一次
對手會進步，去年的答案會過期

不必每天做，**但也不能只做一次。**

你不會知道你不知道的事

威脅模型只涵蓋**你想得到的威脅**。
想不到的，框架不會替你補上。

威脅模型有它真實的限制。盲點沒辦法歸零，但有兩個方向可以處理。

一、借外部視角把盲點縮小

- 借別人的清單
別人的事故報告就是你的盲點清單，不必從零開始想
- 找一個處境不同的人看你的計畫
盲點多半落在你的專業之外
- 問「如果已經發生了」
從結果回推，會逼出你原本沒想到的路徑

二、假設自己會猜錯

- 不讓單一判斷錯誤造成全盤皆輸
多一層備援，錯了還有第二道
- 每年重看一次
上一頁那條規則的理由就在這裡

把威脅列全做不到。**做得到的是猜錯的時候還有轉圜。**

為什麼匿名工具要開源才可信

對手能檢查你的裝置與通訊時，
「工具本身能不能被檢查」就是安全的一部分。

可重現建置 (reproducible build)：任何人都能從原始碼編出位元完全相同的程式，用來確認你手上這份沒被掉包。Tor Browser 與 Tails 都做了這件事。

但它**不保證原始碼本身乾淨**。髒東西若本來就寫在原始碼或建置腳本裡，一樣會被原封不動編出來。2024 年的 xz-utils 後門就是這樣：有人花了兩年取得專案維護者信任，把後門直接寫進上游原始碼，可重現建置照樣通過。開源讓檢查成為可能，仍然需要有人真的去審。

Metadata 是什麼

內容：你說了什麼

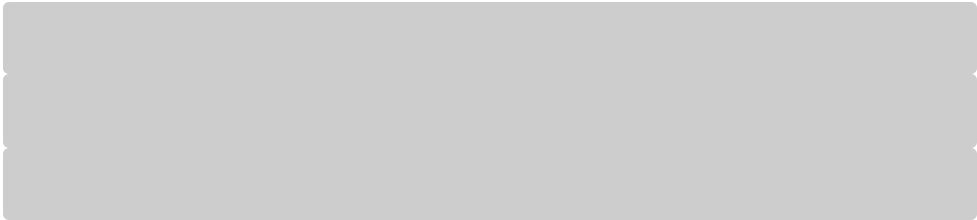
Metadata：你在什麼時候、對誰、說了多久

加密保護的是內容。

Metadata 通常沒有被加密，因為網路要靠這些資訊才能把東西送到正確的地方。

內容加密了，紀錄還在

內容  加密



Google 打不開你的加密壓縮檔。
沒有人在聽你的電話內容。

Metadata  明文

寄件者：you@example.com
收件者：source@example.org
時間：2026-08-08 09:14
大小：4.2 MB

幾點、寄給誰、多大，全都看得到。
換成電話，通聯紀錄依法保存。

沒有人聽你的電話內容，
也知道你幾點打給誰、通話多久。

為什麼這對記者與公民團體是致命的

內容可以否認。 關係不行。

只要能證明「這位員工在報導刊出前兩週，密集聯繫過這位記者」，
對手**不需要知道談了什麼**。

對組織也一樣：一份通聯紀錄可以畫出整個行動網絡，誰是核心、誰與誰協作、
什麼時候行動密集。內容一句都不用看。

還有一種 metadata 更難擺脫：**金流**。一筆捐款的時間、金額、收款對象，
就能說明你支持了誰。今天下午 13:00 教室 TR-511，ETHTaipei 合辦場完整展開。

只能用 LINE 的時候

台灣的預設就是 LINE。來源不會為了你換工具。

不要用「換一個 App」當第一句話，**來源會直接消失**。

不需要來源配合，你單方面就能做的三件事

- ✓ 關掉聊天備份
備份會存到 iCloud 或 Google 雲端，等於在你控制之外多一份
- ✓ 訊息裡絕不出現姓名、職稱、單位
用代稱，紀錄外洩時才不會直接指認
- ✓ 關鍵內容改約實體見面談
見面也有痕跡：基地台紀錄、監視器、消費紀錄。手機留在別的地方
- ✓ 第四件要對方一起做：兩端定期刪除對話
只刪你這端沒有用，得在第一次聯繫時就約定好

但一旦進入法律爭議（收到律師函、存證信函、被通知調查），**停止刪除，改成保存現狀**。刪除紀錄本身可能構成滅證。第三場會展開。

現在就可以開始

先回答第一題：你要保護的是什麼？

多數人第一個念頭是「資料」。多想三十秒，答案通常會變成一個人。

想清楚之後，**挑一件做得到的先做。**

成本太高的方案等於沒有方案，列三十項的下場通常是一項都沒做。

下一場 **10:50** 拿這套框架，看三種人實際在用什麼工具

anoni.net/docs/basics/threat-model/

anoni.net/docs/basics/metadata/

Q&A

我的對手到底有多強，怎麼判斷？

從兩個具體能力去看：對方能不能碰到你的裝置、能不能調閱紀錄。不要用感覺判斷。

開源就一定安全嗎？

不一定。開源是可被檢視的必要條件，還要看是否有人實際審閱、是否有可重現建置、專案是否仍在維護。

那 Signal 到底安不安全？

先回答三個問題。Signal 用 sealed sender（轉送訊息時，連 Signal 自己的伺服器都看不到寄件人是誰）與最小化留存，在 metadata 上做得比多數工具好，但註冊仍需一組手機號碼，也擋不住對手實體接觸你的手機。

我全部都做不到怎麼辦？

成本太高的方案等於沒有方案。挑一件做得到的先做，比列三十項然後放棄好。

後面還有三頁附錄，回答「第一次聯繫怎麼開始」、「報導登出去之後」與「你自己這一端」。時間允許就一起看，來不及的話投影片會放上來。

第一次聯繫，怎麼開始

來源的第一封信，往往就是用公司電腦寄出的。安全管道要在那之前就存在。

- ✓ 把管道事先公開

報導頁尾、個人簡介、社群帳號放上 Signal 帳號或 SecureDrop 位址，讓來源在接觸你之前就看得到

- ✓ 第一次回覆只做一件事

不要在原管道追問細節，只回一句「換到這裡談」。追問會讓對方在不安全的管道上愈說愈多

- ✓ 把那封信算進威脅模型

它已經留下紀錄了。假裝沒發生，等於在錯誤的假設上繼續往下做

- ✓ 引薦來的來源，請引薦人先傳遞管道資訊

由你直接聯繫，等於用你的身分替對方建立了一筆紀錄

報導登出去之後

來源的處境在刊出後才開始。整套準備如果停在截稿，等於只做了一半。

✓ 斷聯本身是訊號

刊出後突然停止聯繫，等於替對方標好了時間點。聯繫的節奏要在刊出前就規劃

✓ 紀錄比報導活得久

通聯紀錄依法保存，對造開始追查的時候它還在。刪掉自己的手機不會讓它消失

✓ 刪除是雙向的

只刪你這端沒有用。要刪什麼、什麼時候刪，事前就要跟來源約好

✓ 把刊出後的作法寫進事前約定

多久聯繫一次、用什麼方式、出事了找誰，全部在刊出前談定，不要等狀況發生才想

你自己這一端

對手表格裡有一列是你自己的機構，最少被列入。設備、帳號、你跟編輯台的往來，全部在別人的管理權限底下。

- ✓ 公司配發的設備不是你的

IT 有管理權限，可以遠端安裝、讀取與回收。敏感作業不要放在上面，離職那天它會被完整稽核

- ✓ 來源的真實身分不要進共用系統

雲端硬碟、共用文件與聯絡人資料庫都會留存並同步。身分與聯絡方式獨立保管，其他人只看得到代稱

- ✓ 事前談定誰需要知道到哪一層

主管、法務、校對各自需要的資訊深度不同。知道的人越多，能被問出來的人也越多

- ✓ 機構自己被盯上的時候

收到律師函或存證信函，停止刪除、保存現狀、先找律師。跟個人的差別在於紀錄不只在你手上，還在機構的系統裡