CISCO TALOS

獵捕到偵測的最後一哩路

Joey Chen

Leader, Security Research

Cisco Talos

APT/cybercrime investigation, malware analysis and cryptography analysis

Botconf, CodeBlue, HITB, AAVAR, Virus Bulletin, DeepSec, HITCON etc.

CISCO TALOS

Agenda

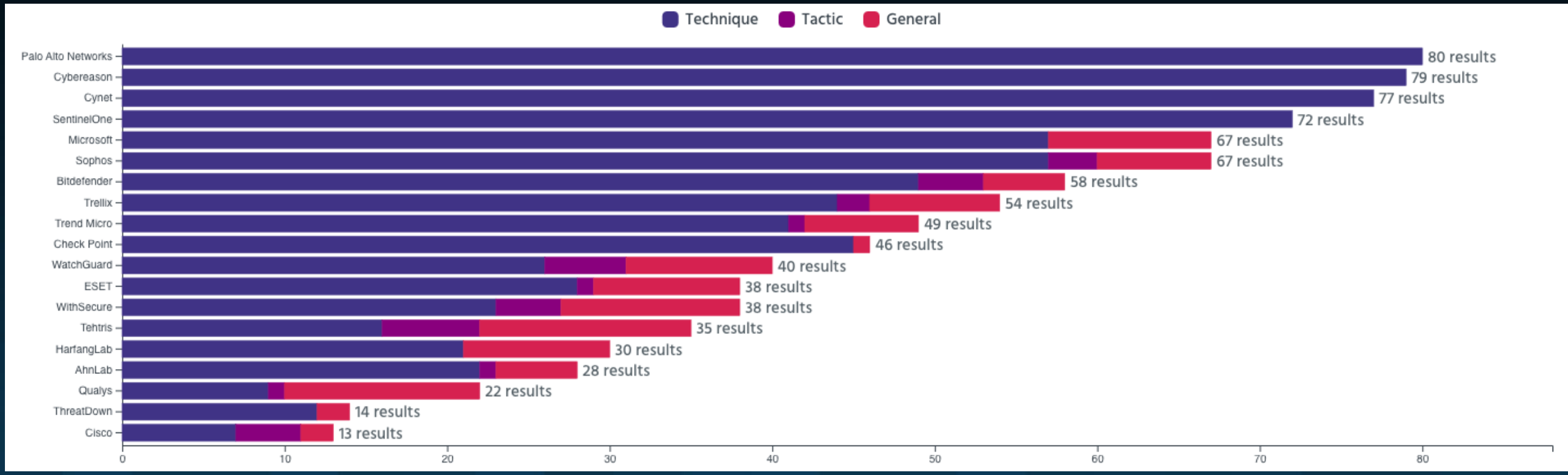
1. 威脅獵捕 vs. 威脅偵測
2. EDR的產品 = 模組化防禦
3. EDR log + 工人智慧找出奇耙的東西
4. EDR + AI 幫助偵測的能力
5. 看到駭客攻擊擋不擋?

CISCO TALOS

威脅獵捕 vs. 威脅偵測

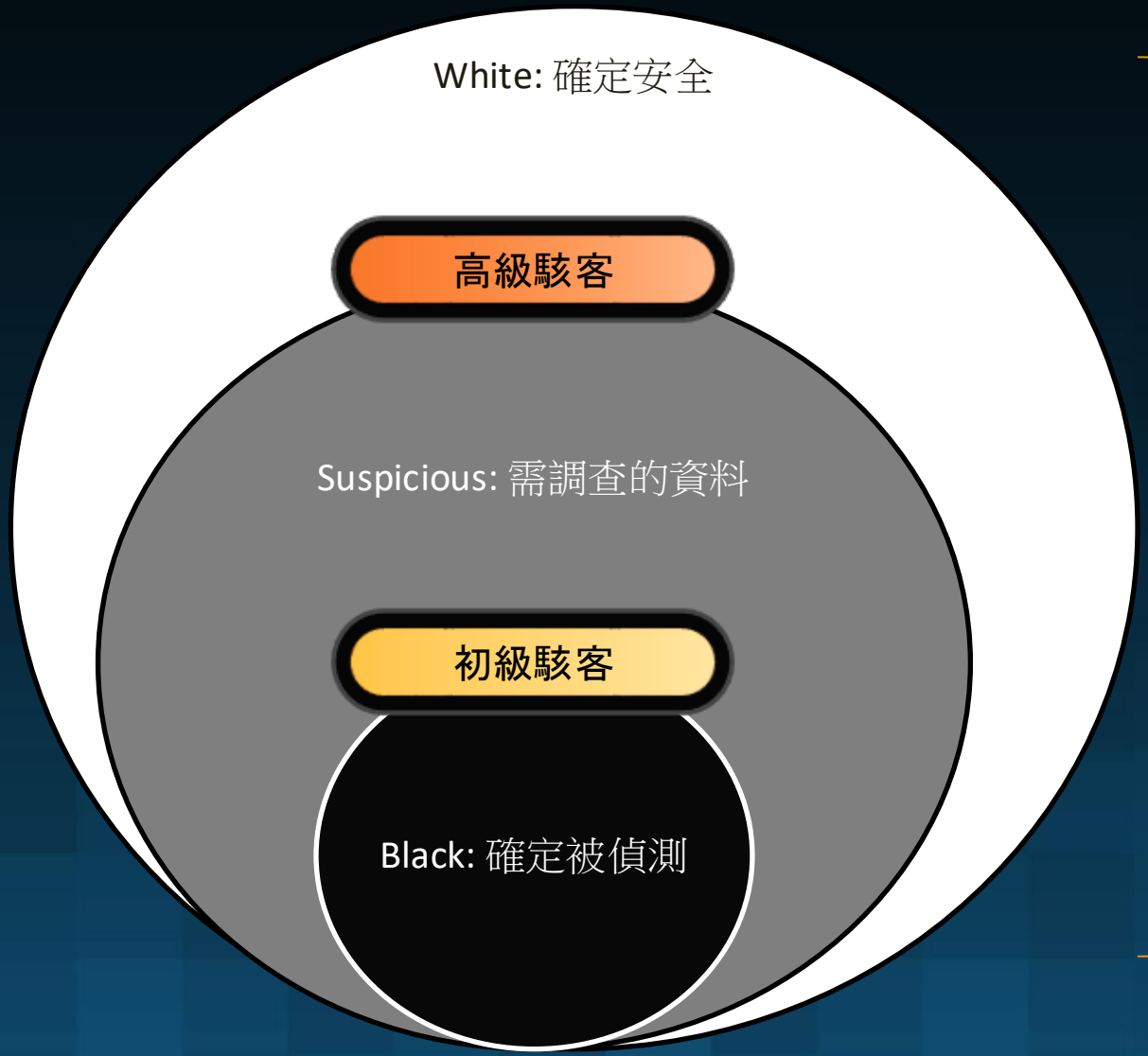
什麼時候會偵測？紅隊需要注意誰？

MITRE | ATT&CK® Evaluations



CISCO TALOS

大量的資料只有少部分會偵測



資料用於調查
- 識別因素和根本原因
- 威脅搜尋/溯源
- 感染案例
- 等等

請求偵測

送白名單

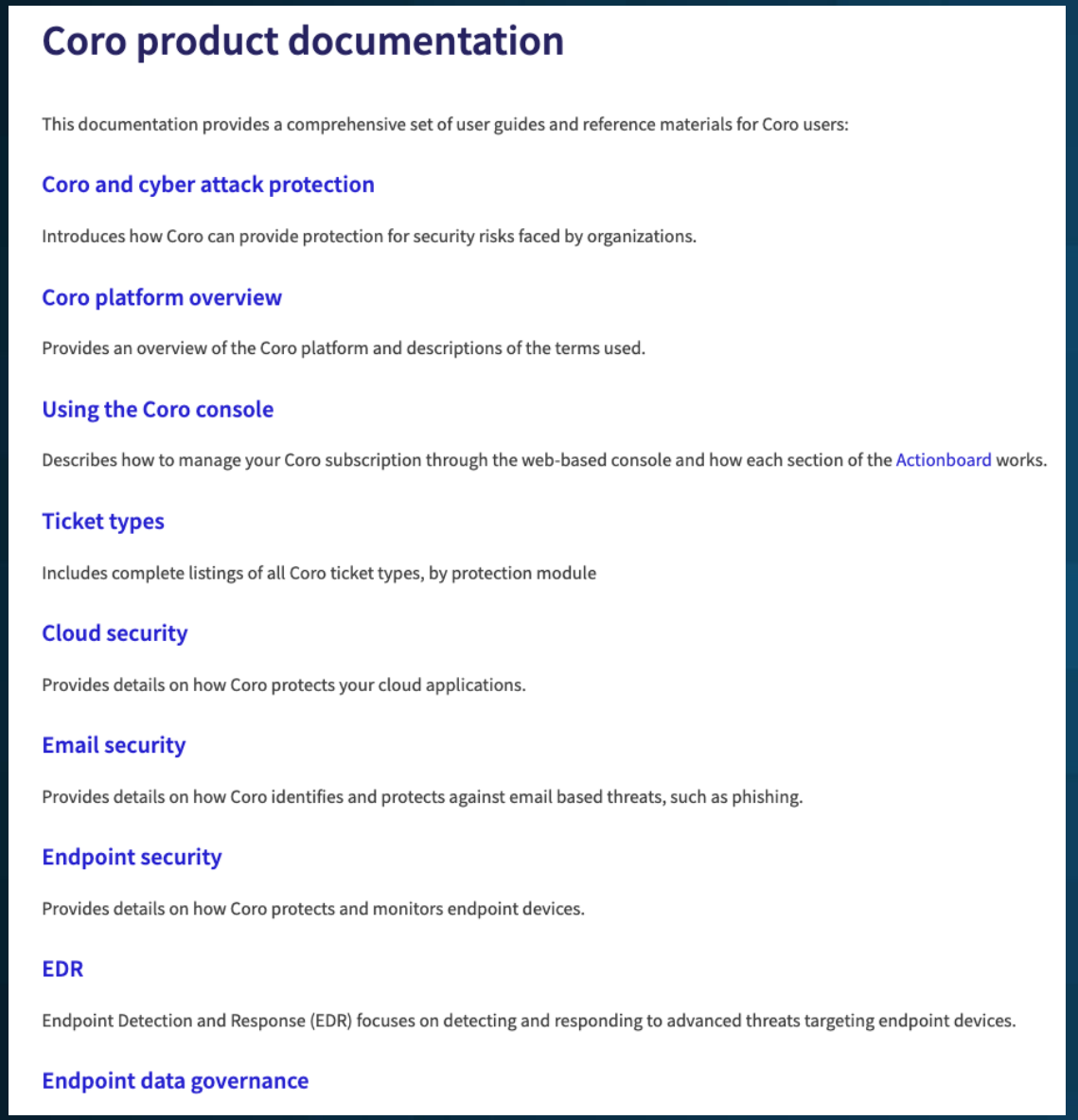
EDR 的產品 = 模組化防禦

傳統大廠常見的方式

CISCO TALOS

模組功能通常有公開介紹

- 一套產品會包含一個或多個模組
- 每個模組會有各自的分享方式或有整合的方式去存於雲端資料庫中
  - 回傳格式不一
- 模組間會有自己的計算威脅方式與偵測方式
  - 效能吃緊



Coro product documentation

This documentation provides a comprehensive set of user guides and reference materials for Coro users:

Coro and cyber attack protection

Introduces how Coro can provide protection for security risks faced by organizations.

Coro platform overview

Provides an overview of the Coro platform and descriptions of the terms used.

Using the Coro console

Describes how to manage your Coro subscription through the web-based console and how each section of the Actionboard works.

Ticket types

Includes complete listings of all Coro ticket types, by protection module

Cloud security

Provides details on how Coro protects your cloud applications.

Email security

Provides details on how Coro identifies and protects against email based threats, such as phishing.

Endpoint security

Provides details on how Coro protects and monitors endpoint devices.

EDR

Endpoint Detection and Response (EDR) focuses on detecting and responding to advanced threats targeting endpoint devices.

Endpoint data governance

https://docs.coro.net/about-the-docs/

CISCO TALOS

模有

- 一個
- 每方於
  -
- 模
  - 效能吃緊

Coro product documentation

he Actionboard works.

endpoint devices.

https://docs.coro.net/about-the-docs/

CISCO TALOS

記憶體掃描模組 pro

為了偵測紅隊送 exploit 跑在記憶體中

- Assembly locality sensitive hashing(ALSH)
- 針對組合語言的邏輯去做 Hash 並進行比對
- 切分方式會針對 function 邏輯指令或跳轉指令等進行區塊 Hash

Sample 1

```
74B13069    8B0D 00F0B274    mov ecx,dword ptr ds:[74B2F000]
74B1306F    56               push esi
74B13070    57               push edi
74B13071    BF 4EE640BB      mov edi,BB40E64E
74B13076    BE 0000FFFF      mov esi,FFFF0000
74B1307B    3BCF             cmp ecx,edi
74B1307D    74 04            je ab03a7caed279fc6411ec19386faff3b65be
74B1307F    85CE             test esi,ecx
74B13081    75 26            jne ab03a7caed279fc6411ec19386faff3b65b
```

Sample 2

```
70682C29    8B0D 00D06970    mov ecx,dword ptr ds:[7069D000]
70682C2F    56               push esi
70682C30    57               push edi
70682C31    BF 4EE640BB      mov edi,BB40E64E
70682C36    BE 0000FFFF      mov esi,FFFF0000
70682C3B    3BCF             cmp ecx,edi
70682C3D    74 04            je 6be5c8882bc02cf4e86d2ab9d20aa3446b71
70682C3F    85CE             test esi,ecx
70682C41    75 26            jne 6be5c8882bc02cf4e86d2ab9d20aa3446b7
```

CISCO TALOS

記憶體掃描模組 pro 續

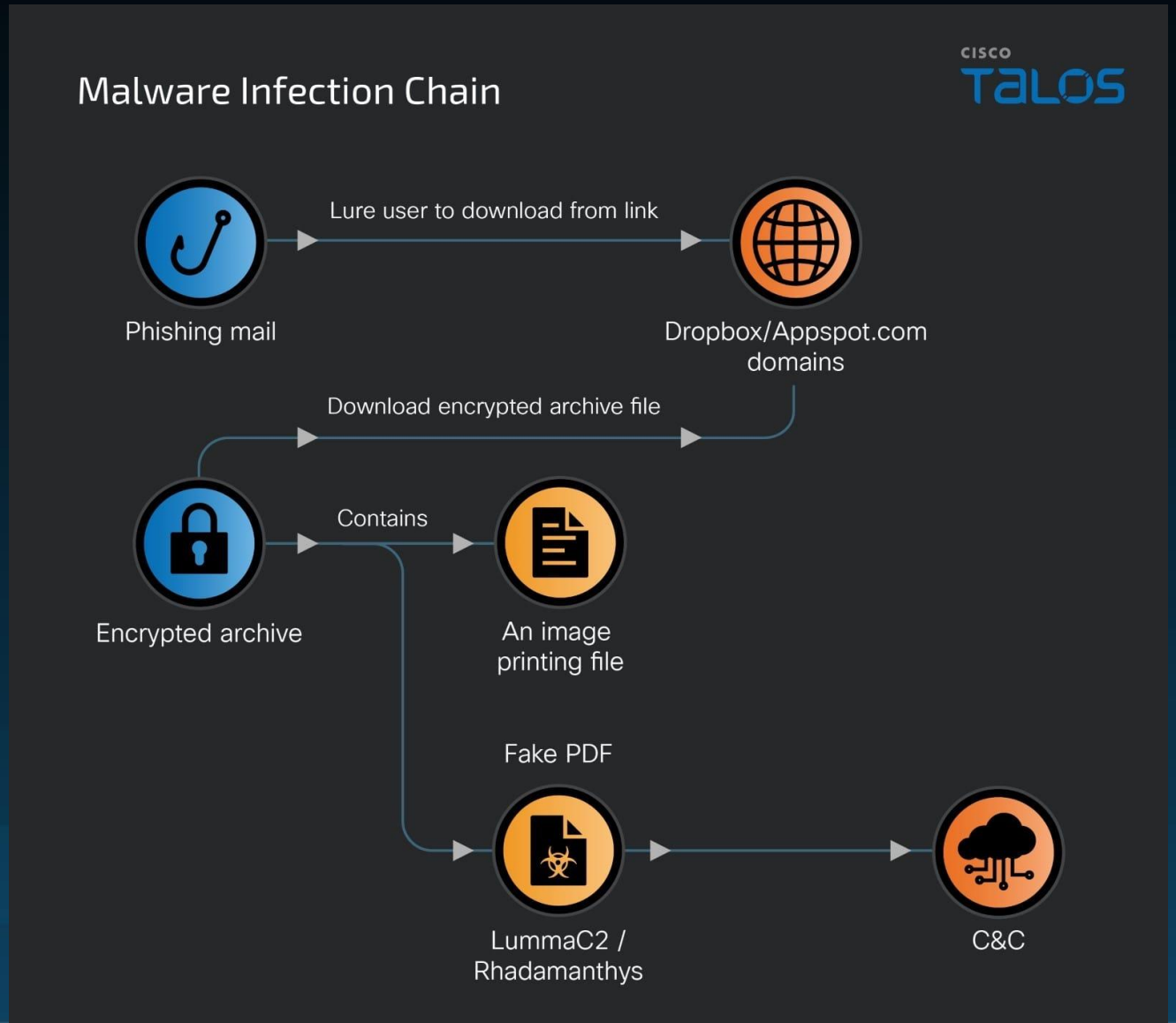
EDR log + 工人智慧找出奇耙的東西

Mitre 模擬測試的情況 & 現實的案例

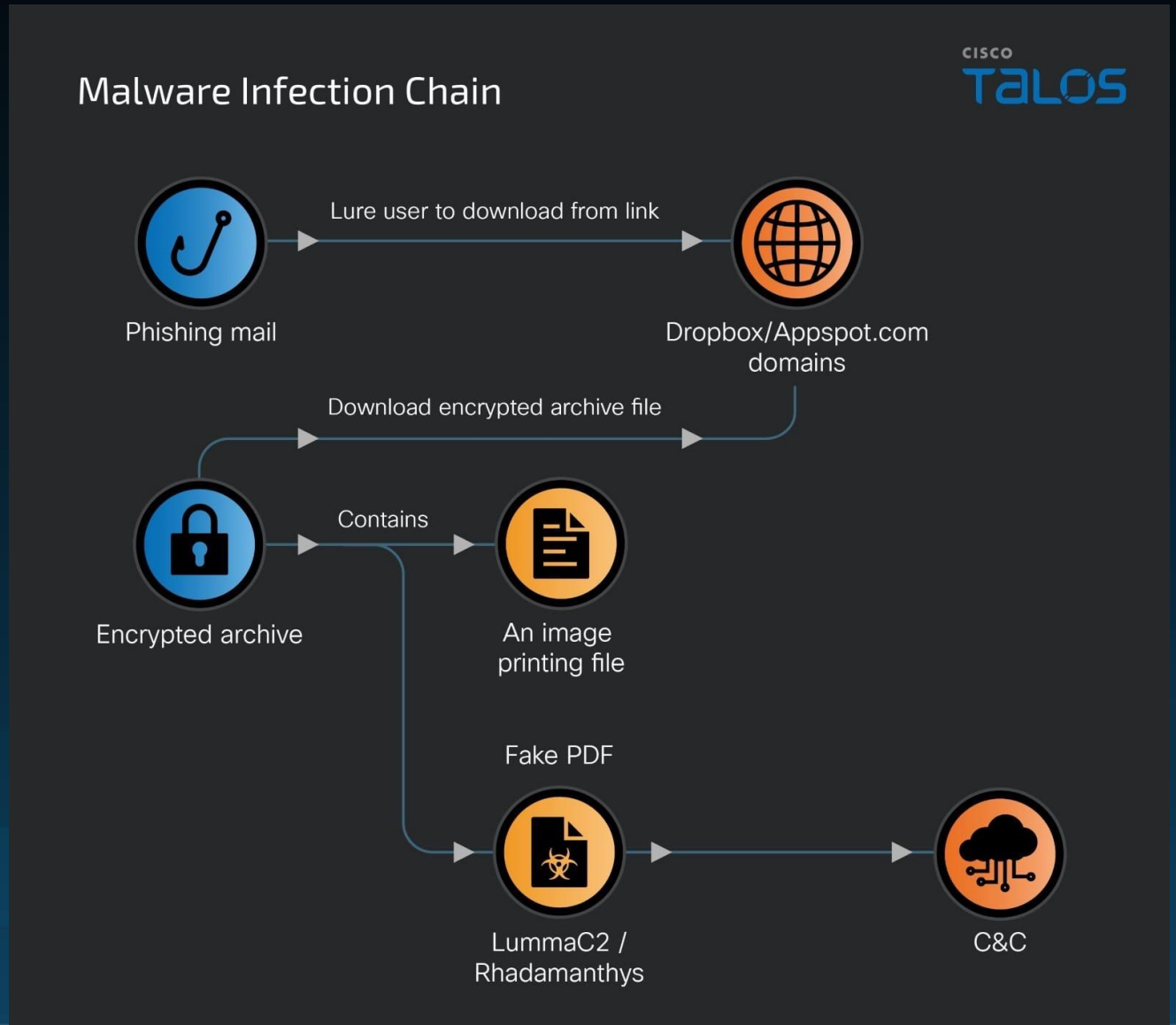
CISCO TALOS

尋找相似項目的群組

LummaC2 在前端的樣子



LummaC2 在後端的樣子

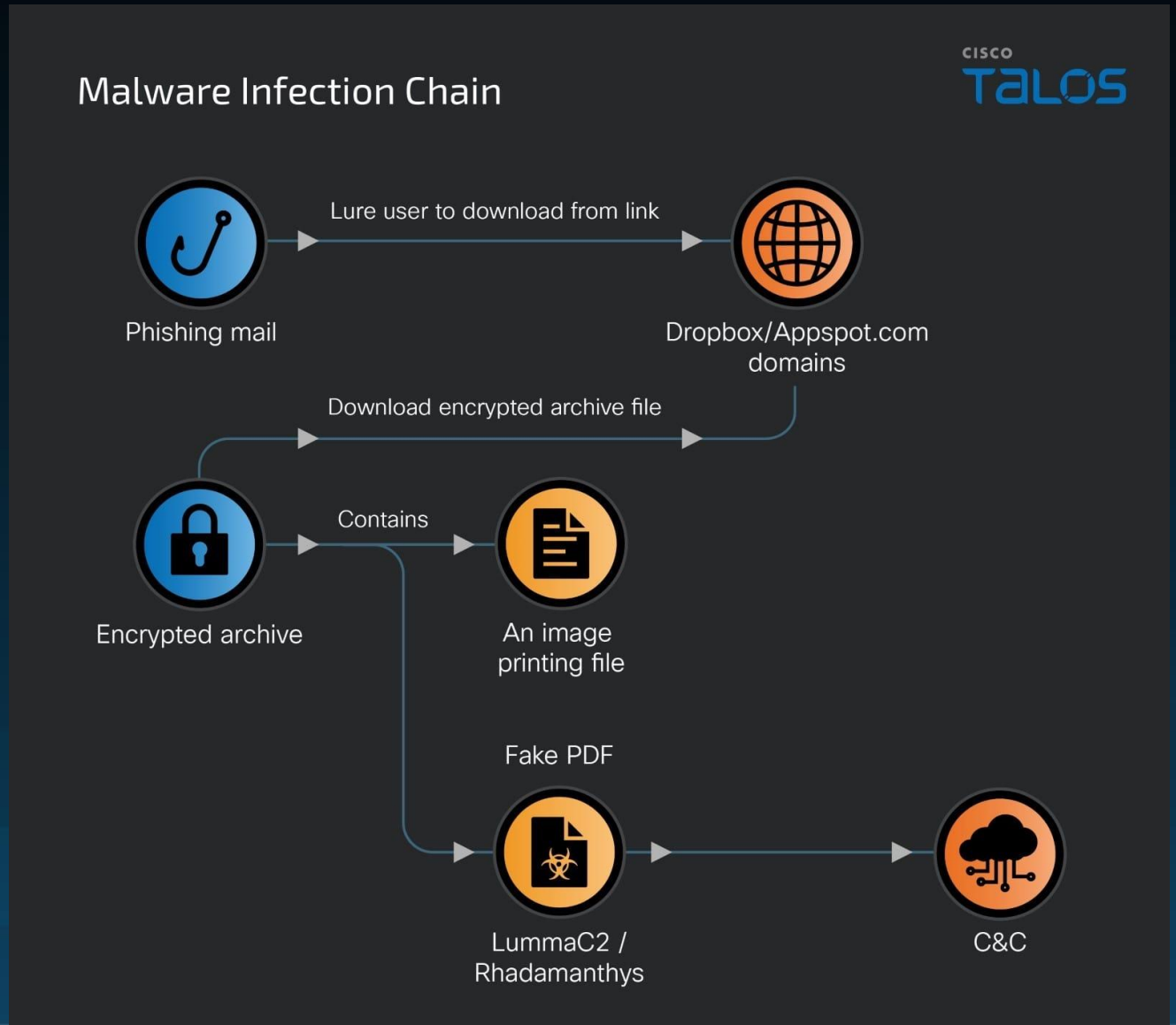


Step 1

- 收集巨量資料，聚合分類並萃取出唯一
- 檢視已有偵測之行為
- 過濾非惡意行為
- 請求偵測惡意行為與檔案

CISCO TALOS

LummaC2 在後端的樣子



Step 2

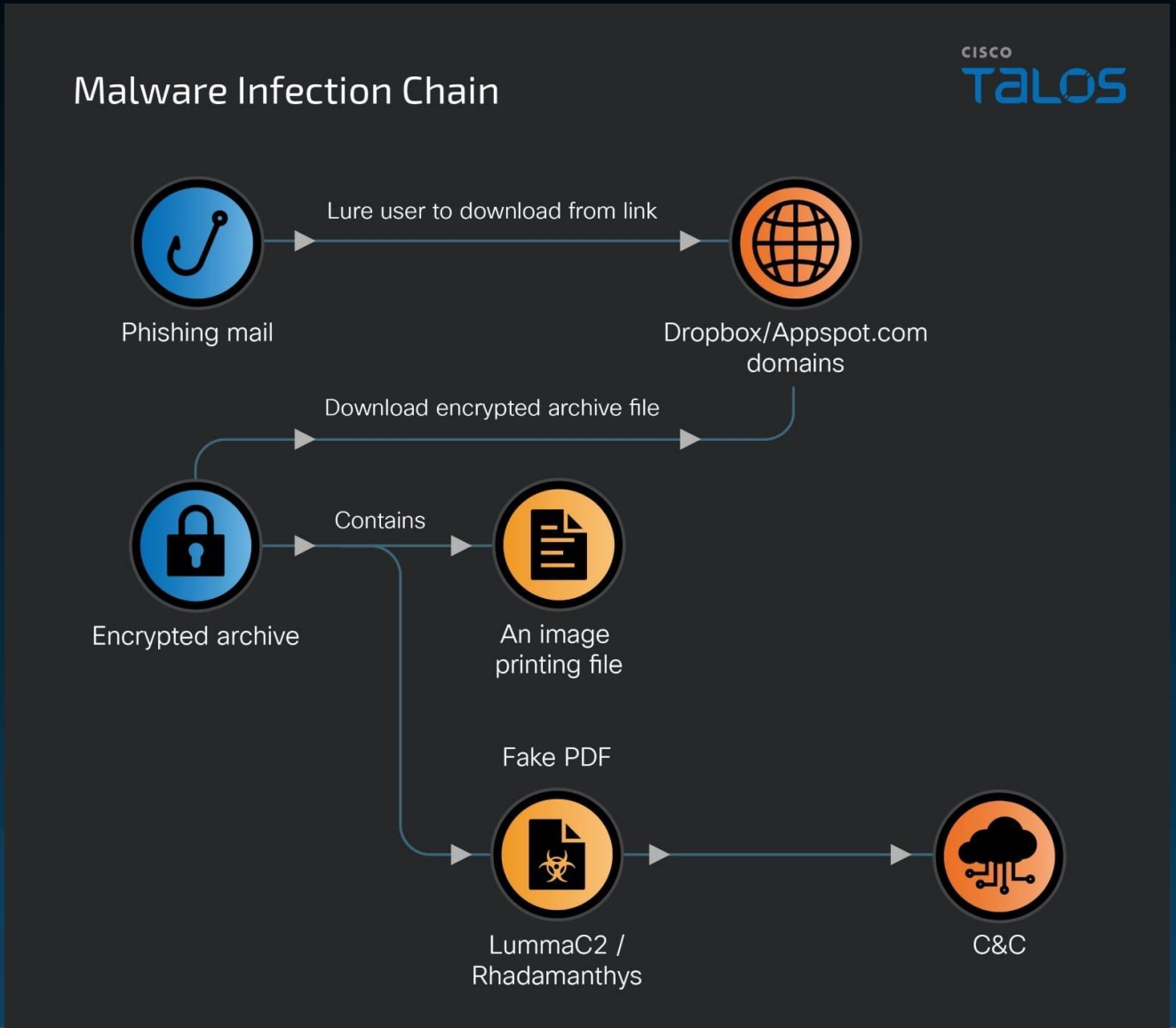
- 收集檔案名稱和 metadata
- 調查該主機的行為
- 檢查檔案的動/靜態偵測

CISCO TALOS

LummaC2 在後端的樣子

Step 3

- 使用檔案名稱和其他 metadata 調查來源電子郵件
- 使用電子郵件標題進行分析



找到偵測的極限也是一種方法

善加利用低威脅的偵測 ->
使用低威脅與白名單的攻擊手法，讓自己隱藏大數據中的大群組

資源耗損作戰 ->
讓目標把偵測模組越關越少，減少自己被偵測的機率

增加冗余代碼 ->
增加邏輯與跳轉的指令，有時比減少還好用

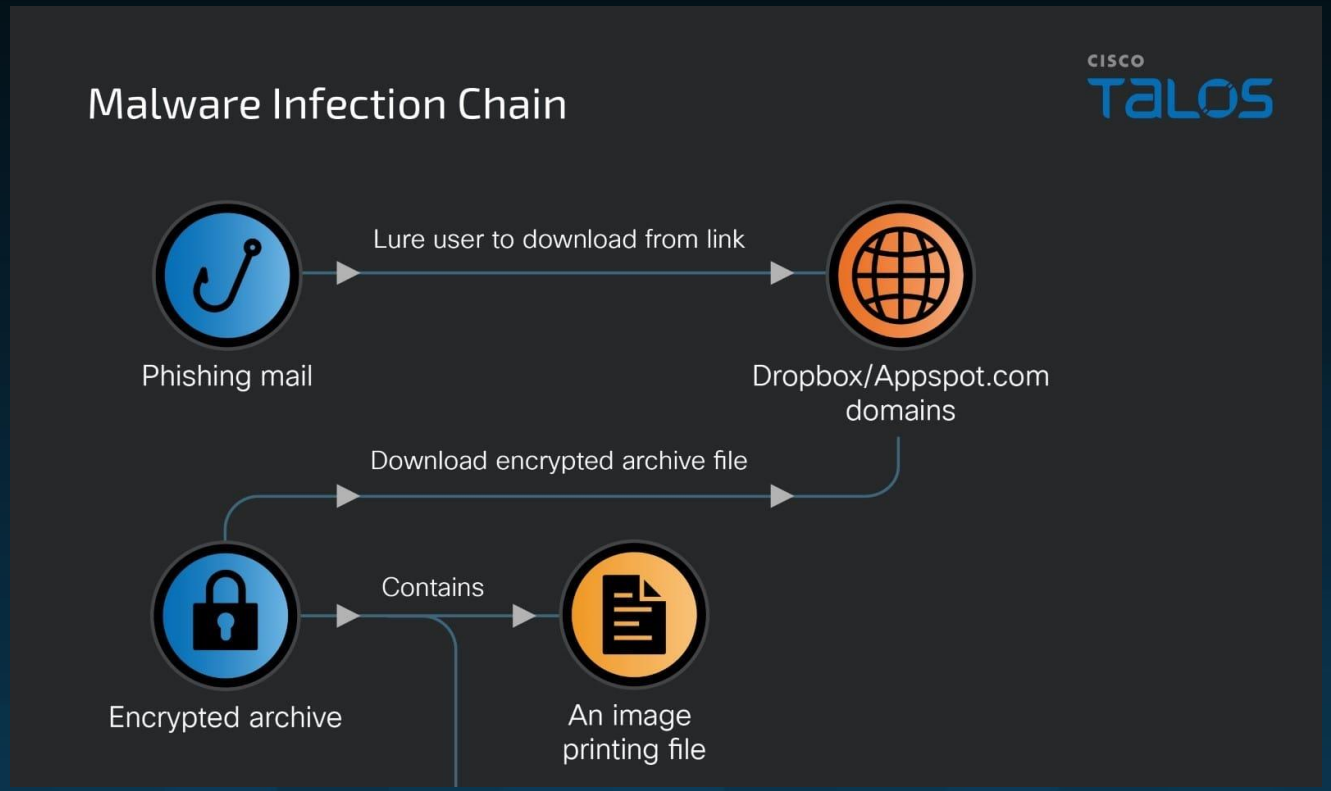
來些例子，偵測與否？

CISCO TALOS

駭客忘記放樣本進釣魚信，偵測否？

一樣的信箱

類似的加密檔案



一樣的Domain

一樣的圖片檔案

CISCO TALOS

駭

可疑指令->丟惡意程式->拿密碼，偵測否？

cmd.exe /Q /c cd
cmd.exe /Q /c query user
cmd.exe /Q /c tasklist /SVC
cmd.exe /Q /c dir
cmd.exe /Q /c cd Program Files

cmd.exe /Q /c bin4u.exe load
cmd.exe /Q /c bin4u.exe dump lsass.exe C:\temp\s
cmd.exe /Q /c bin4u.exe unload
cmd.exe /Q /c del bin4u.exe

背景設定：

- 郵件伺服器
- 拿 CVE-2023-41444 Windows Driver Exploit 去提權拿密碼
- 還記得砍掉惡意檔案

EDR logs，偵測否？

cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c query user 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c tasklist /SVC 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c cd Program Files 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c bin4u.exe load 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c bin4u.exe dump lsass.exe C:\temp\s 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c bin4u.exe unload 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1
cmd.exe /Q /c del bin4u.exe 1> \\127.0.0.1\ADMIN$__1708631776.8172357 2>&1

背景設定：

- 郵件伺服器
- 拿 CVE-2023-41444 Windows Driver Exploit 去提權拿密碼
- 還記得砍掉惡意檔案

CISCO TALOS

可疑指令->丟惡意程式->拿密碼，偵測否？

背景設定：

- 郵件伺服器
- 拿 CVE-2023-41444 Windows Driver Exploit 去提權拿密碼
- 還記得砍掉惡意檔案

結論：

- IT 忘記 Admin 密碼
- 把惡意程式設定白名單
- 自己上傳 webshell 到伺服器 dump 密碼

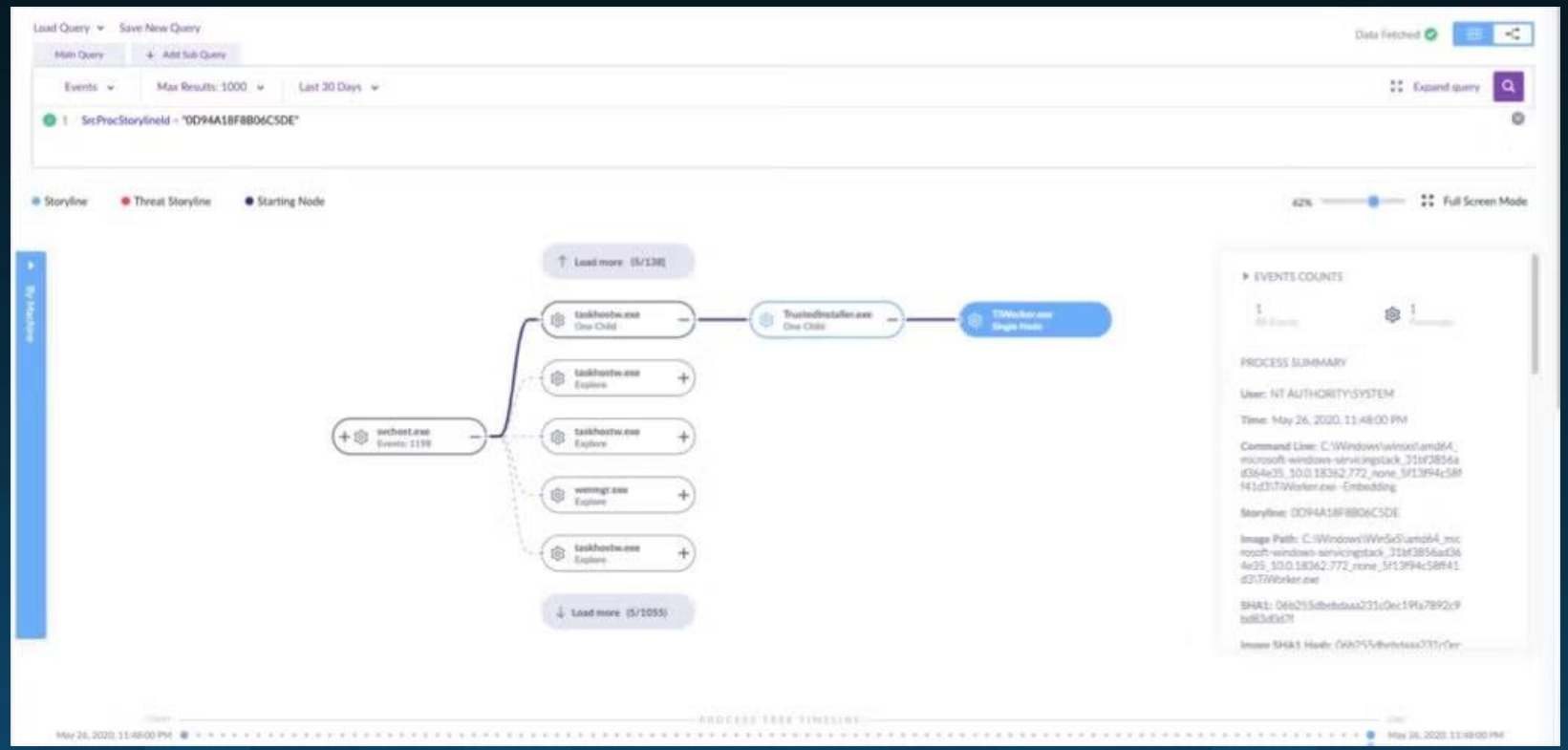
EDR + AI 幫助偵測的能力

非傳統大廠公司

CISCO TALOS

從流程上做偵測 - Storyline

- Storyline 是基於資料模型中的群組實體。
- Group是一組 Process 的集合，這些 Process 作為一個整體進行追蹤、判斷和偵測。
- 威脅實際上是一個群組(而不是一個 Process /File)。
- 簡而言之，它是「增強型」的 Process 樹，將其作為模型中的錨點，可以讓最準確的上下文解釋作業系統中的任何操作



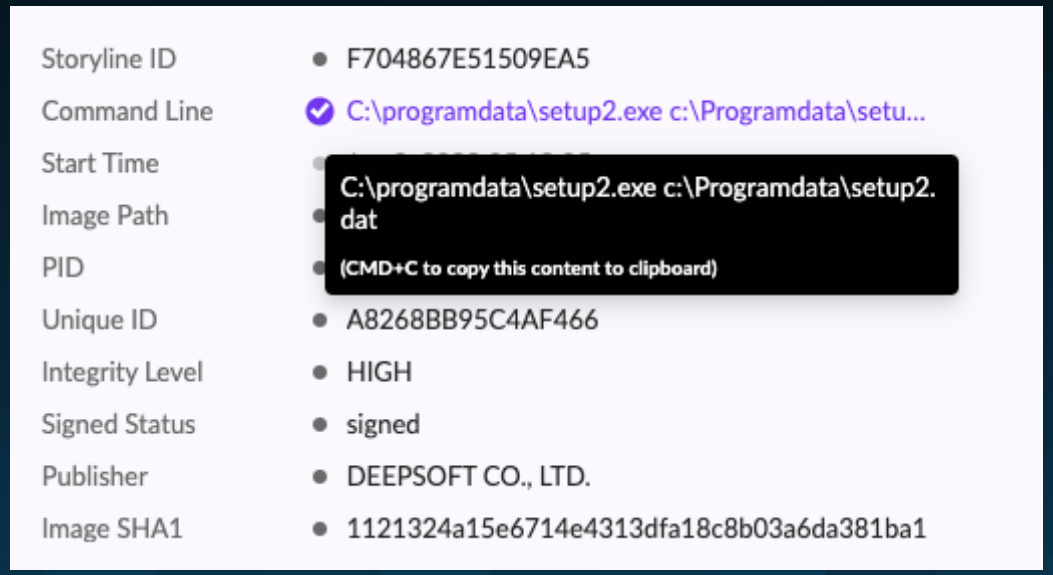
從流程上做偵測

用於收集系統層級的事件日誌。

從流程上做偵測的範例

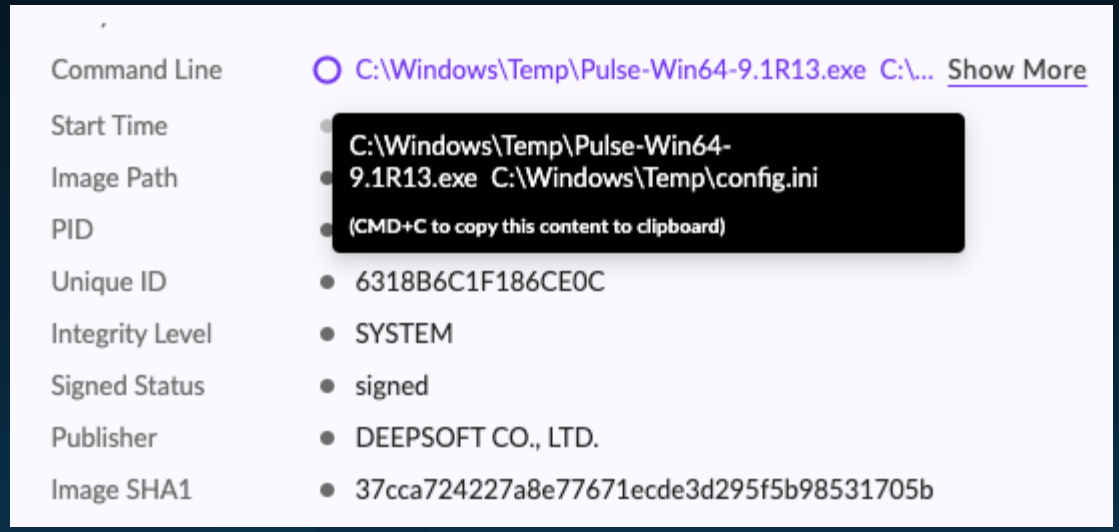
沒看過、沒看到，AI 想偵測

安裝檔



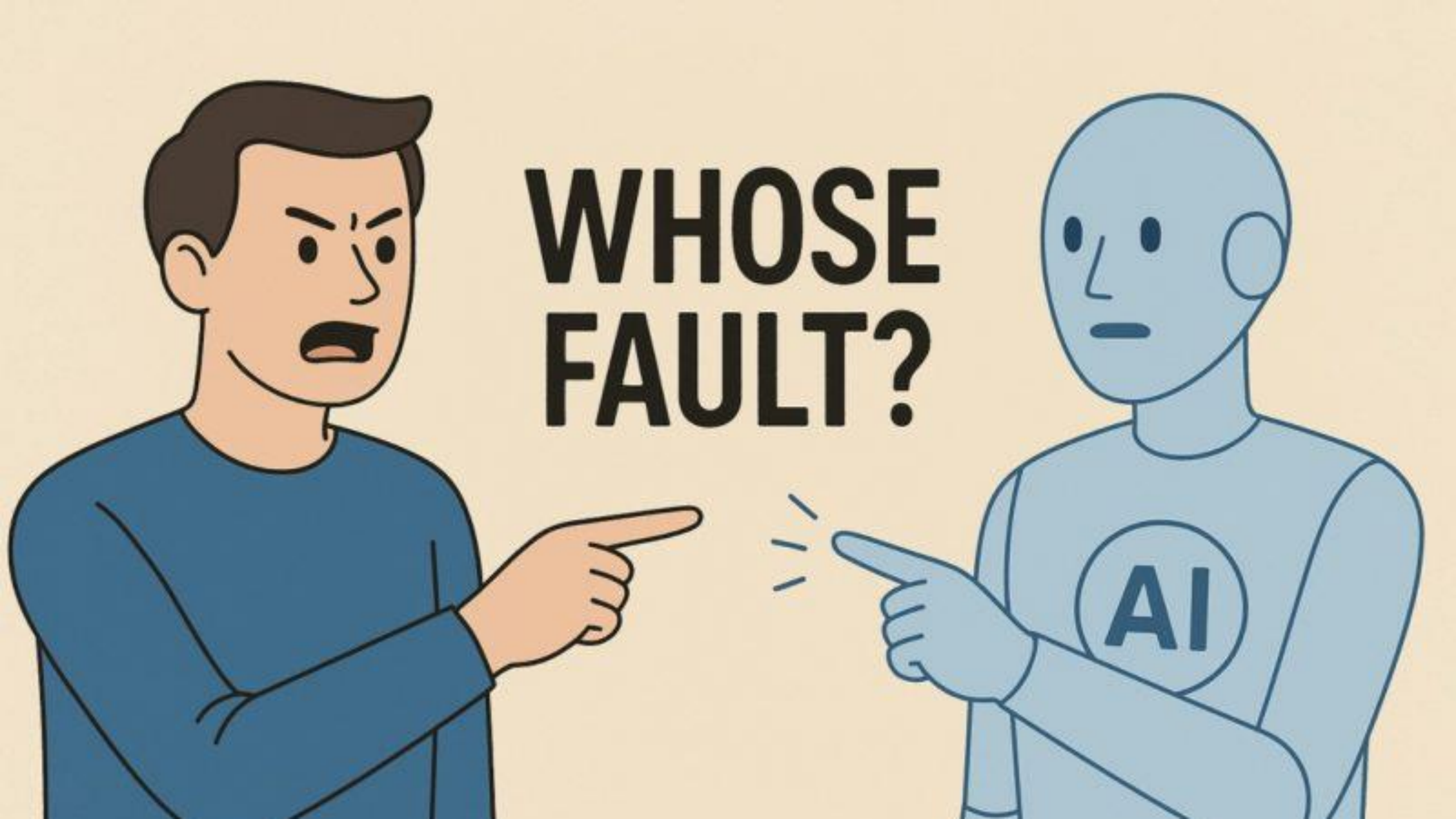
有簽章

丟Config

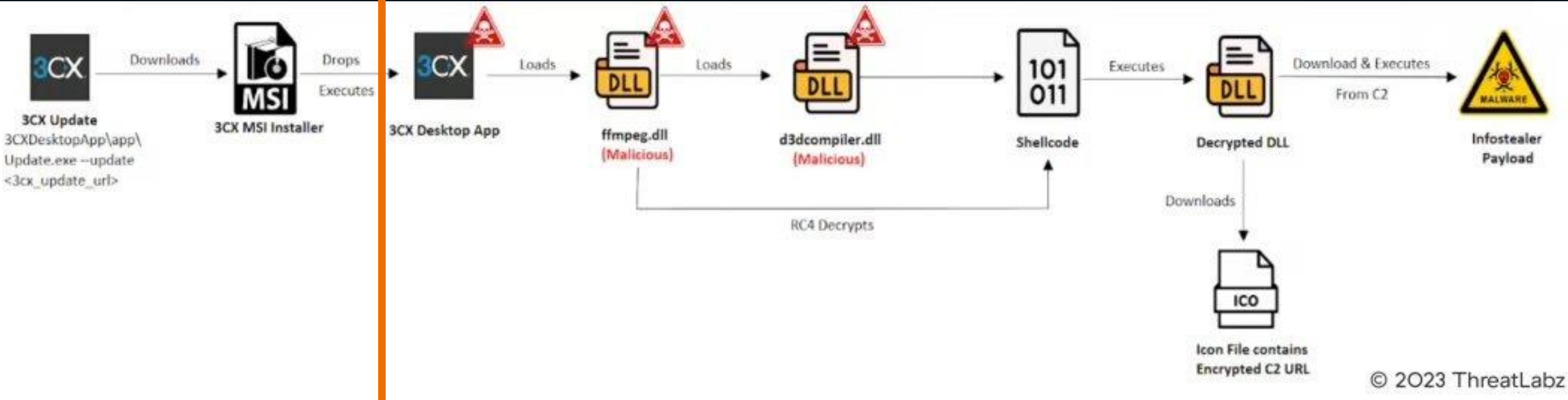


CISCO TALOS

研究員遇上 AI Hunting


WHOSE
FAULT?
AI

2023最大的供應鏈攻擊 - 3/29後狂發blogs



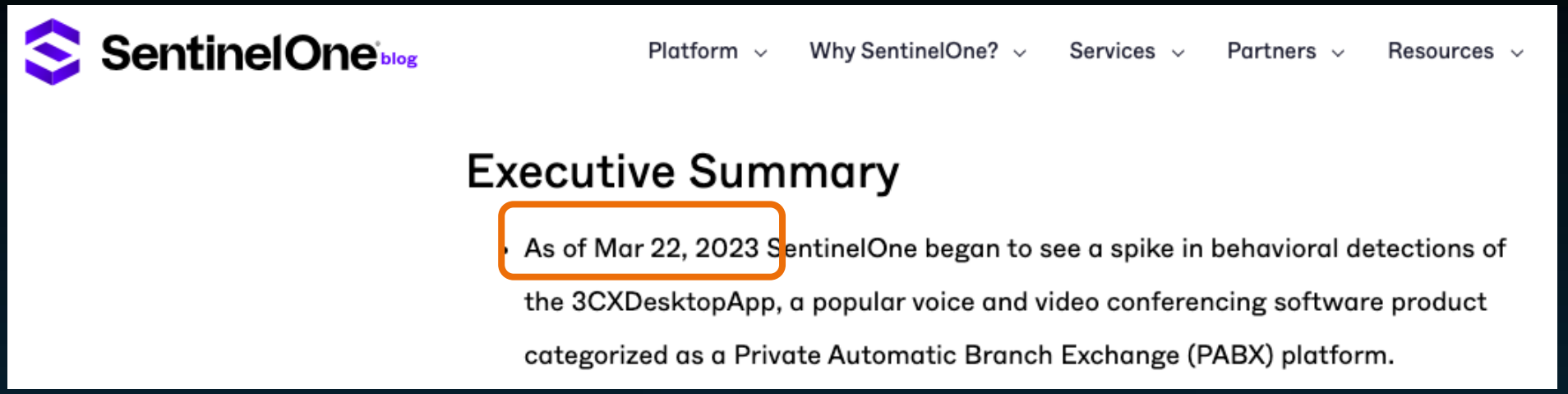
合法軟體

惡意程式

https://www.zscaler.com/blogs/security-research/3cx-supply-chain-attack-campaign

CISCO TALOS

完美案例 - 偵測否？




```
<code example>
    if file_operation == 'File Modification' or file_operation == 'File Creation':
            counter_file_operations = counter_file_operations + 1
                try:
                    file_path = threat[3], file_size = int(threat[5])
                except:
                    continue
            classifier_result = self.__classifier_controller(file_operation, file_path, file_size)
                if classifier_result:
                    result = classifier_result
     self.__detect_shellcode_executions(file_operation, file_path, file_size)
            alert_msg()
```

完美案例 - 偵測否？

SentinelOne blog

Platform Why SentinelOne? Services Partners Resources

tions of

oduct

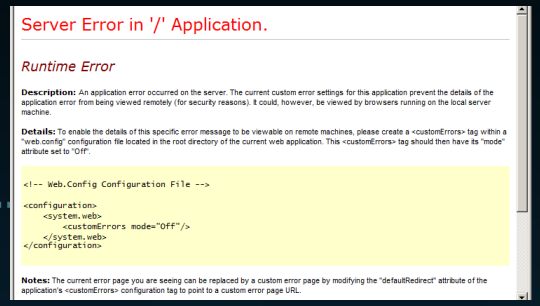
```
<code exampl
    if file_
            c
                                                    th, file_size)
        self.__detect_shellcode_executions(file_operation, file_path, file_size)
            alert_msg()
```

TALOS

到底什麼會被偵測？

Exploit Web application

Web Server



Time	Detection
2025-02-06 6:10:12	Trojan.IFrame.TC
2025-02-06 7:20:24	Trojan.IFrame.TC
2025-02-06 9:04:05	Auto.3B7BAAEA93.252049.in07.Talos
2025-02-06 9:04:08	Auto.D4C975.252155.in02
2025-02-06 9:04:12	Generic.ASP.BackFrm.A.5C2F6371
2025-02-06 9:04:16	Generic.ASP.WebShell.AO.D63F6E87
2025-02-06 9:17:10	Gen:Variant.Zusy.533783
2025-02-06 9:19:00	Gen:Variant.Ulise.471205
2025-02-06 10:21:02	Gen:Variant.Ulise.471205
2025-02-06 10:25:11	Gen:Variant.Ulise.471205
2025-02-06 11:50:18	Generic.WebShell.Z.AF618D1A
2025-02-06 12:00:41	Generic.ASP.WebShell.AO.F63C6737

Discovery

- net user Guest [REDACTED]
- whoami
- tasklist /svc
- find /i term
- netstat -ano
- find /i 3556

Defense Evasion

- powershell.exe Set-MpPreference -ExclusionPath ”c:\windows\ime”
- netsh advfirewall set allprofiles state off

Privilege Escalation

- uc3.log guest administrator /clone
- net user administrator admin@123

Execution & Persistence

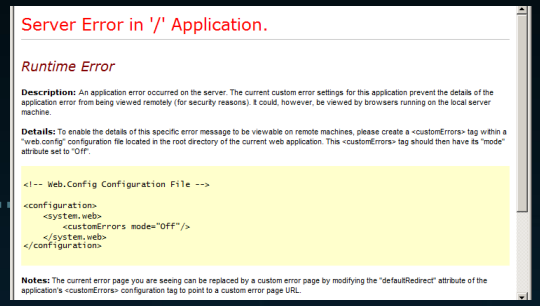
- cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win -silent
- Install PlugX
- Deploy BadIIS

cisco TALOS

到底什麼會被偵測？

Exploit Web application

Web Server



Time	Detection
2025-02-06 6:10:12	Trojan.IFrame.TC
2025-02-06 7:20:24	Trojan.IFrame.TC
2025-02-06 9:04:05	Auto.3B7BAAEA93.252049.in07.Talos
2025-02-06 9:04:08	Auto.D4C975.252155.in02
2025-02-06 9:04:12	Generic.ASP.BackFrm.A.5C2F6371
2025-02-06 9:0[illegible]:16	Generic.ASP.WebShell.AO.D63F6E87
2025-02-06 9:1[illegible]:10	Gen:Variant.Zusy.533783
2025-02-06 9:[illegible]9:00	Gen:Variant.Ulise.471205
2025-02-06 10:21:02	Gen:Variant.Ulise.471205
2025-02-06 10:25:11	Gen:Variant.Ulise.471205
2025-02-06 11:50:18	Generic.WebShell.Z.AF618D1A
2025-02-06 12:00:41	Generic.ASP.WebShell.AO.F63C6737

Discovery

- net user Guest [REDACTED]
- whoami
- tasklist /svc
- find /i term
- netstat -ano
- find /i 3556

Defense Evasion

- powershell.exe Set-MpPreference -ExclusionPath ”c:\windows\ime”
- netsh advfirewall set allprofiles state off

Privilege Escalation

- uc3.log guest administrator /clone
- net user administrator admin@123

Execution & Persistence

- cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win -silent
- Install PlugX
- Deploy BadIIS

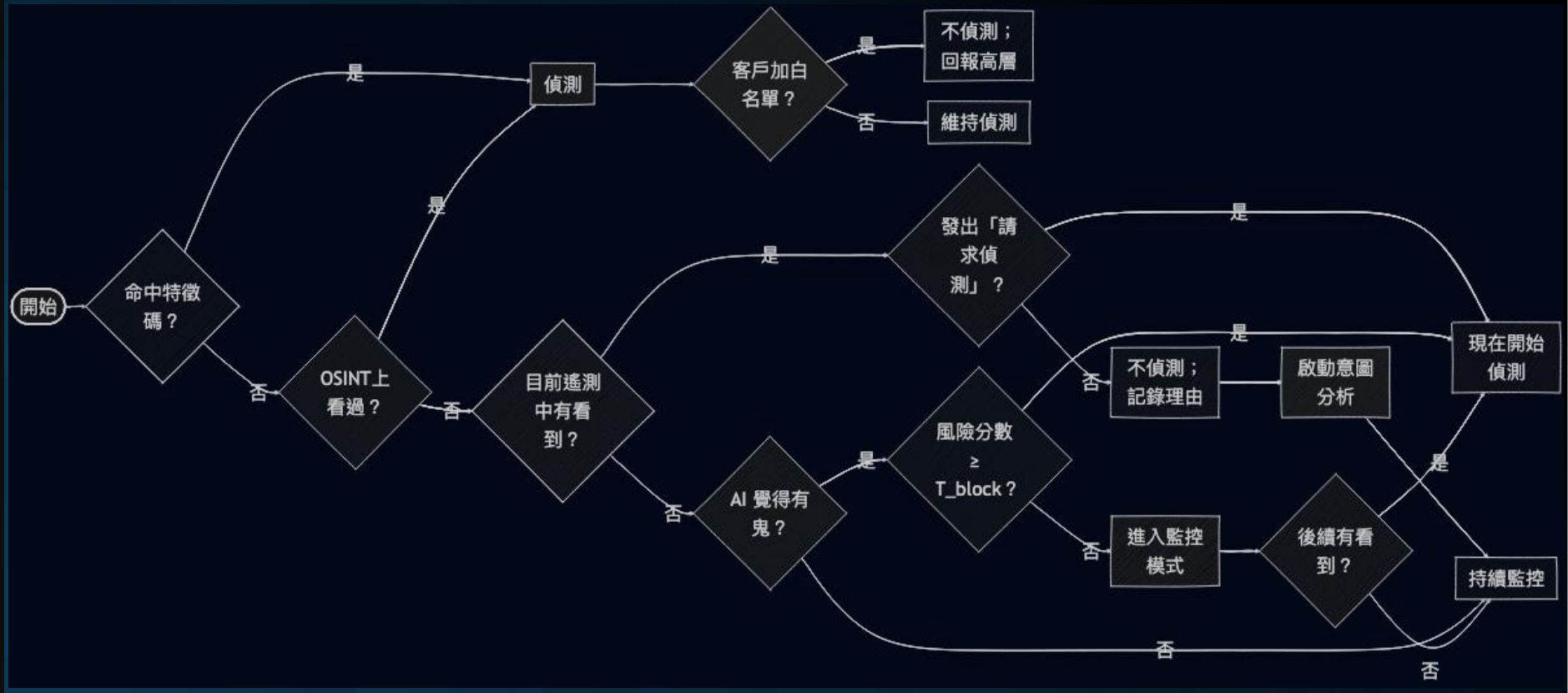
CISCO TALOS

總結

心得

- 沒偵測≠沒看到
- 從單點到故事
- AI 提示、人來定奪
- 新舊 EDR 都有極限

3CX 再一次
一定賭 AI



TALOSINTELLIGENCE.COM