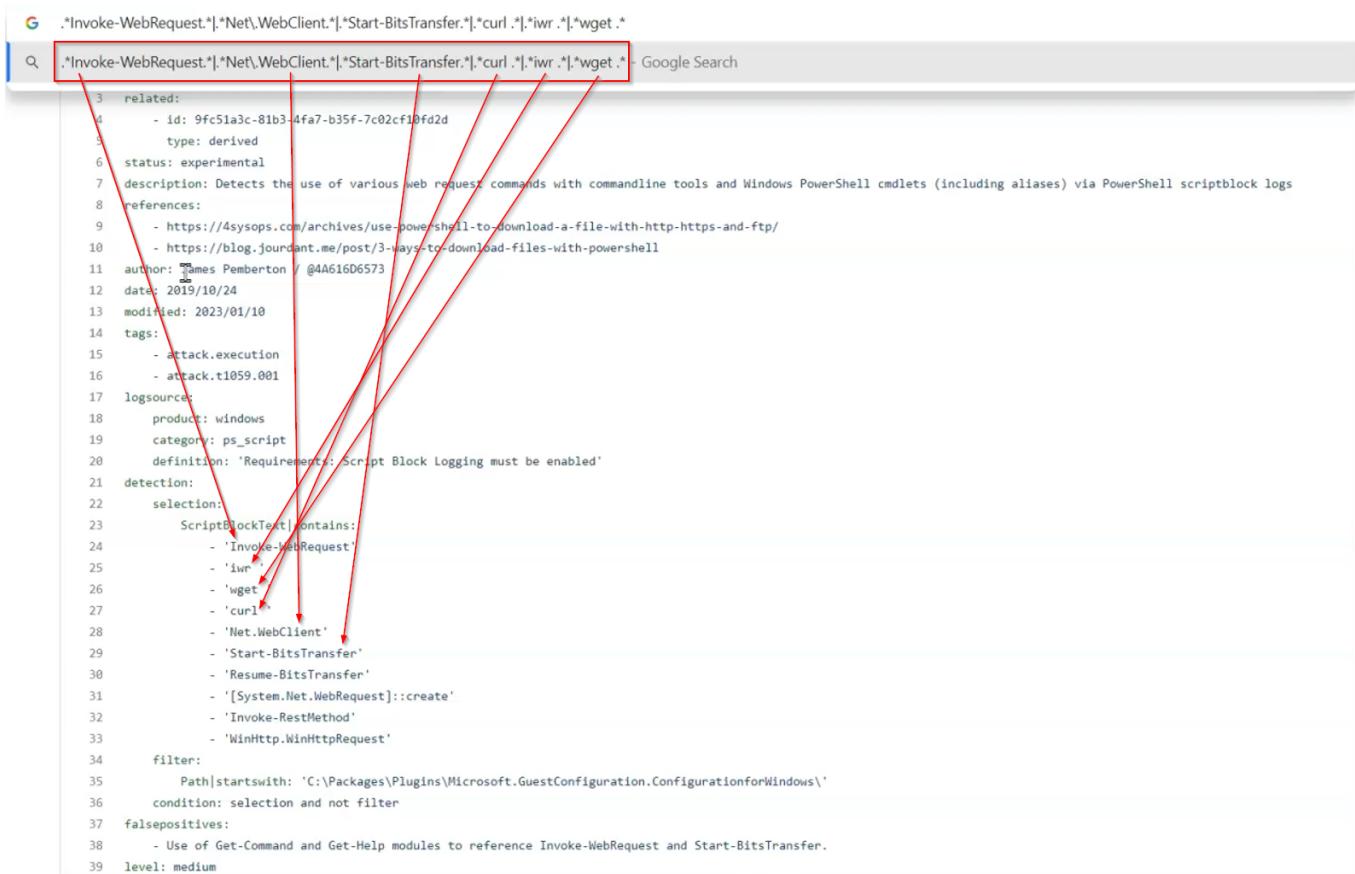


- ◆ Sigma rules adopted in FortiSIEM 
- ◆ Sigma rules on Github 
- ◆ How you can convert **sigma** rules into **FortiSIEM** rule?
- ◆ Many rules are adopted from sigma rules in FortiSIEM. for example,
  - ◆ Windows: Windows Powershell Web Request  this can be found in **FortiSIEM** > **RESOURCES** > **Rules** and search for it in search bar.
  - ◆ to get the name refer this [link](#) 
  - ◆ you can edit the rule with **Edit** option

## Comparison between Sigma and FortiSIEM rule



```

G .Invoke-WebRequest.*|.Net\WebClient.*|.Start-BitsTransfer.*|.curl.*|.iwr.*|.wget.*
Q .Invoke-WebRequest.*|.Net\WebClient.*|.Start-BitsTransfer.*|.curl.*|.iwr.*|.wget.* Google Search

3 related:
4   - id: 9fc51a3c-81b3-4fa7-b35f-7c02cf10fd2d
5   type: derived
6   status: experimental
7   description: Detects the use of various web request commands with commandline tools and Windows PowerShell cmdlets (including aliases) via PowerShell scriptblock logs
8   references:
9     - https://4sysops.com/archives/use-powershell-to-download-a-file-with-http-https-and-ftp/
10    - https://blog.jourant.me/post/3-ways-to-download-files-with-powershell
11   author: James Pemberton / @AA616D6573
12   date: 2019/10/24
13   modified: 2023/01/10
14   tags:
15     - attack.execution
16     - attack.t1059.001
17   logsource:
18     product: windows
19     category: ps_script
20     definition: 'Requirement: Script Block Logging must be enabled'
21   detection:
22     selection:
23       ScriptBlockText|contains:
24         - 'Invoke-WebRequest'
25         - 'iwr'
26         - 'wget'
27         - 'curl'
28         - 'Net.WebClient'
29         - 'Start-BitsTransfer'
30         - 'Resume-BitsTransfer'
31         - '[System.Net.WebRequest]::create'
32         - 'Invoke-RestMethod'
33         - 'WinHttp.WinHttpRequest'
34     filter:
35       Path|startswith: 'C:\Packages\Plugins\Microsoft.GuestConfiguration.ConfigurationforWindows\' 
36     condition: selection and not filter
37   falsepositives:
38     - Use of Get-Command and Get-Help modules to reference Invoke-WebRequest and Start-BitsTransfer.
39   level: medium

```

- ◆ we can see here, some of them are adopted by Fortinet in FortiSIEM rules
- ◆ it's not exact one to one mapping, they just use it for partial case, the sigma rule they referred is general, here they are using it for specific use case

The screenshot shows the FortiSIEM interface with the 'Rules' section selected. A specific rule titled 'Windows: 7Zip Compressing Dump Files' is being edited. The 'Step 3: Define Action' tab is active. The configuration includes:

- Severity:** 7 - MEDIUM
- Category:** Security
- Subcategory:** Collection
- Technique:** [T1560.001] Archive Collected Data: Archive via Utility
- Tactics:** Collection
- Action:** Defined
- Exception:** Undefined
- Watch List:** Undefined
- Clear:** Undefined
- Tag:** (empty)

Below the configuration is a 'Blame' panel displaying the JSON code for the rule:

```

1 title: 7Zip Compressing Dump Files
2 id: ec570e53-4c76-45e9-804d-cc3f355ff7ea
3 related:
4   - id: 1ac14d38-3a0fc-4635-92c7-e3fd1c5f5bfc
5     type: derived
6     status: experimental
7     description: Detects execution of 7z in order to compress a file with a ".dmp"/".dump" exten
8     references:
9       - https://theofficerreport.com/2022/09/20/bumblebee-round-two/
10      author: Nasreddine Bencherchali (Nextron Systems)
11      date: 2022/09/27
12      modified: 2023/09/12
13      tags:
14        - attack.collection
15        - attack.t1560.001
16      logsource:
17        category: process_creation
18        product: windows
19      detection:
20        selection_img:
21          - Descr|contains: '7-Zip'
22          - Image|endswith:
23            - '7z.exe'
24            - 'V7z.exe'
25            - '7za.exe'
26            - OriginalFilename:
27              - '7z.exe'
28              - '7za.exe'
29        selection_extension:
30          CommandLine|contains:
31            - '.dmp'
32            - '.dump'
33            - '.hmp'
34        condition: all of selection_
35        falsepositives:
36          - legitimate use of 7z with a command line in which ".dmp" or ".dump" appears accidentally
37          - legitimate use of 7z to compress WER ".dmp" files for troubleshooting
38      level: medium

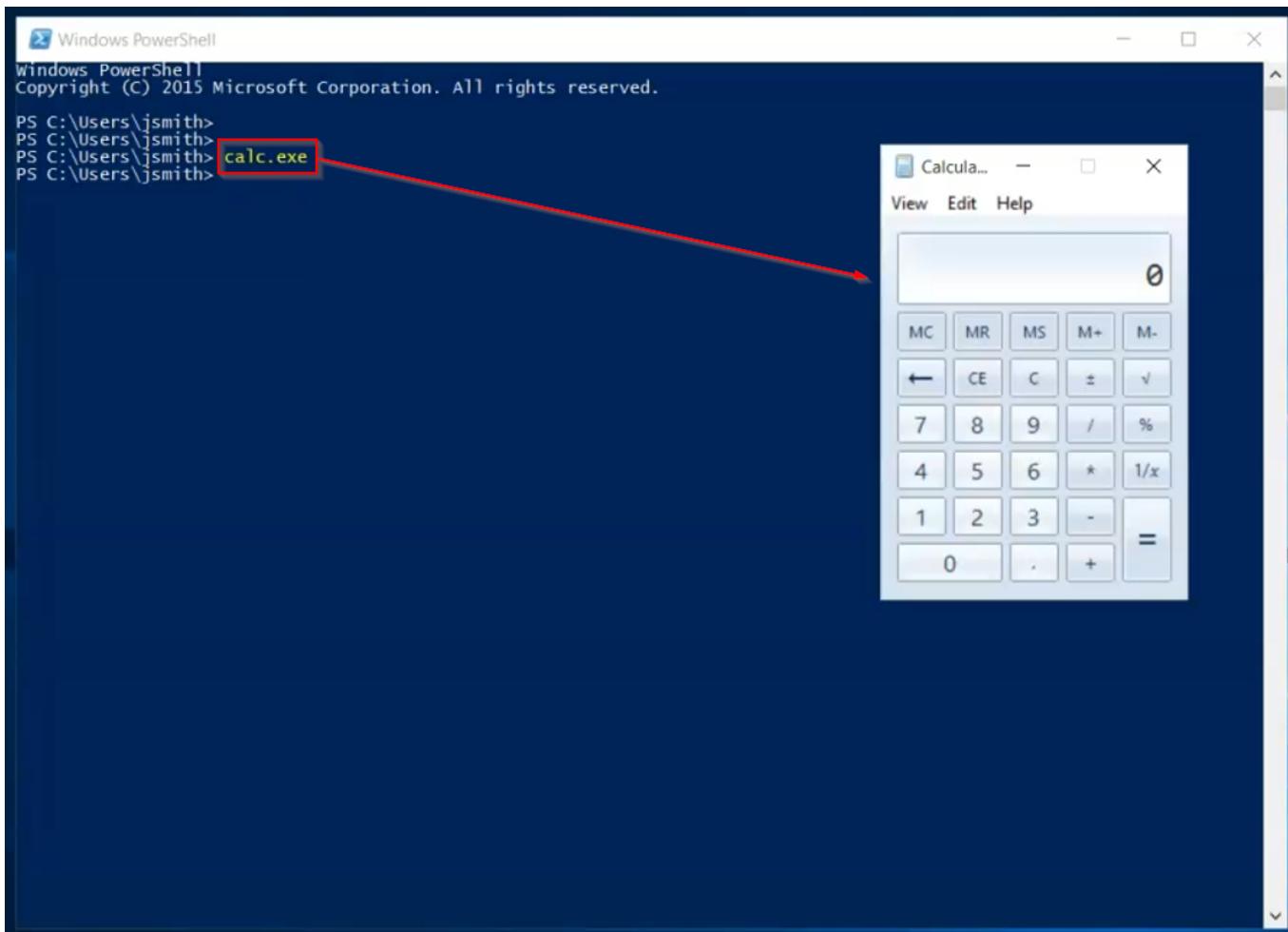
```

## Developing our own rule

- ◆ let's create the one that will actually utilize the parent command line and the parent process and also the fields for the file name or the software that is being triggered by this parent process to check for malicious behavior.
- ◆ first let's start with simple rule, as powershell command or powershell as the parent process and the commands issued by interpreter of powershell (which is odd case, because powershell shouldn't be used to issue executable like notepad or to open the winword something like it)
- ◆ here we will try to how to utilize sysmon logs and utilize the different fields inside it to build your own use cases.

## Goal:

- ◆ To simulate our use case to trigger any executable from the powershell and check the logs in sysmon logs and try to write a rule to give us an incident based on that
- ◆ just execute any executable (e.g., calc.exe) in the powershell.



◆ now check the **ANALYTICS** tab to check the log

A screenshot of the FortiSIEM interface, specifically the "ANALYTICS" tab. The search bar shows the query "Event Type != PH\_DEV\_MON\_PING\_STAT". The main area displays a histogram titled "Raw Messages - Last 10 Minutes" with a single bar at 10:54. Below the histogram is a table of raw event logs. One event is highlighted, showing details about a Windows logon success with a process named "calc.exe".

DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES TASKS ADMIN

Actions [1] Raw Messages +

Event Type != PH\_DEV\_MON\_PING\_STAT Run

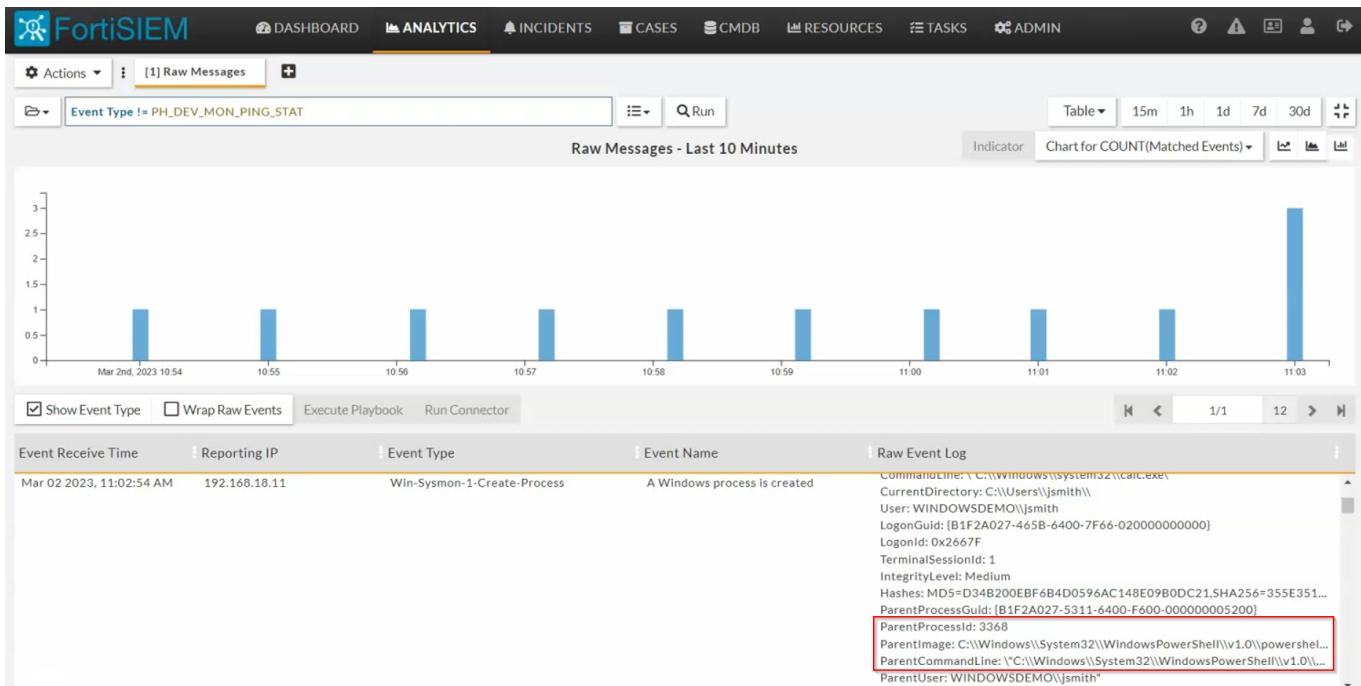
Raw Messages - Last 10 Minutes

Indicator Chart for COUNT(Matched Events)

Show Event Type Wrap Raw Events Execute Playbook Run Connector

Event Receive Time	Reporting IP	Event Type	Event Name	Raw Event Log
Mar 02 2023, 11:02:54 AM	192.168.18.11	Win-Security-4624	Windows logon success	2023-03-02T08:02:53Z WindowsDemo 192.168.18.11 Acce!Ops-WUA-WinLo... 2023-03-02T08:02:53Z WindowsDemo 92.168.18.11 Acce!Ops-WUA-WinLo... RuleName:- UtcTime: 2023-03-02 08:02:51.997 ProcessGuid: [B1F2A027-582B-6400-1C01-000000005200] ProcessId: 2116 Image: C:\Windows\System32\calc.exe FileVersion: 10.0.10240.16397 (th1.150721-1806) Description: Windows Calculator Product: Microsoft® Windows® Operating System Company: Microsoft Corporation OriginalFileName: CALC.EXE

◆ and the parent process is powershell



- ◆ first make sure that logs are logging then click on raw event log

The screenshot shows a "Raw Event Log" window with the following details:

Company: MICROSOFT CORPORATION

OriginalFileName: CALC.EXE

CommandLine: "\C:\Windows\System32\calc.exe"

CurrentDirectory: C:\Users\jsmith\

User: WINDOWSDEMO\jsmith

LogonGuid: {B1F2A027-465B-6400-7F66-020000000000}

LogonId: 0x2667F

TerminalSessionId: 1

IntegrityLevel: Medium

Hashes: MD5=D34B200EBF6B4D0596AC148E09B0DC21,SHA256=355E351...

ParentProcessGuid: {B1F2A027-5311-6400-F600-000000005200}

ParentProcessId: 3368

ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

ParentCommandLine: '\C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoProfile -NonInteractive -Command & exit'

ParentUser: WINDOWSDEMO\jsmith

- ◆ then look for some interesting field

2023-03-02T08:02:53Z WindowsDemo 192.168.18.11 AcclOps-WUA-WinLog-  
Microsoft-Windows-Sysmon/Operational [phCustomerId]=“1” [customer]=“super”  
[monitorStatus]=“Success” [Locale]=“fr-CH” [MachineGuid]=“b1f2a027-cbe1-4798-  
8749-70d9865bfcb1” [timeZone]=“+0300” [eventName]=“Microsoft-Windows-  
Sysmon/Operational” [eventSource]=“Microsoft-Windows-Sysmon” [eventId]=“1”  
[eventType]=“Information” [domain]=“NT AUTHORITY” [computer]=“WindowsDemo”  
[user]=“SYSTEM” [userSID]=“S-1-5-18” [userSIDAcctType]=“User” [eventTime]=“Mar 02  
2023 08:02:52” [deviceTime]=“Mar 02 2023 08:02:52” [msg]=“Process Create:  
RuleName: -  
UtcTime: 2023-03-02 08:02:51.997  
ProcessGuid: {B1F2A027-582B-6400-1C01-000000005200}  
ProcessId: 2116  
Image: C:\Windows\System32\calc.exe  
FileVersion: 10.0.10240.16397 (th1.150721-1806)  
Description: Windows Calculator  
Product: Microsoft® Windows® Operating System  
Company: Microsoft Corporation

Search... Lines: 63

Display	Filter	Item	Value
<input type="checkbox"/>	<input type="checkbox"/>	Collector ID	10001
<input type="checkbox"/>	<input type="checkbox"/>	Command	C:\Windows\system32\calc.e...
<input type="checkbox"/>	<input type="checkbox"/>	Company	Microsoft Corporation
<input type="checkbox"/>	<input type="checkbox"/>	Computer	WindowsDemo
<input type="checkbox"/>	<input type="checkbox"/>	Count	1
<input type="checkbox"/>	<input type="checkbox"/>	Description	Windows Calculator
<input type="checkbox"/>	<input type="checkbox"/>	Destination Host Name	WindowsDemo

OK Close

ADMIN

Table 15m 1h 1d 7d 30d

Indicator Chart for COUNT(Matched Events)

11.01 11.02 11.03

1/1 12 >

C:\Windows\system32\calc.exe

Name: CALC.EXE  
Path: "C:\Windows\system32\calc.exe"  
Category: C:\Users\jsmith\WindowsDemo\jsmith  
ProcessId: 467F  
Priority: 1  
SecurityLevel: Medium  
SHA256=355E351...  
Guid: {B1F2A027-5311-6400-F600-000000005200}  
SId: 3368

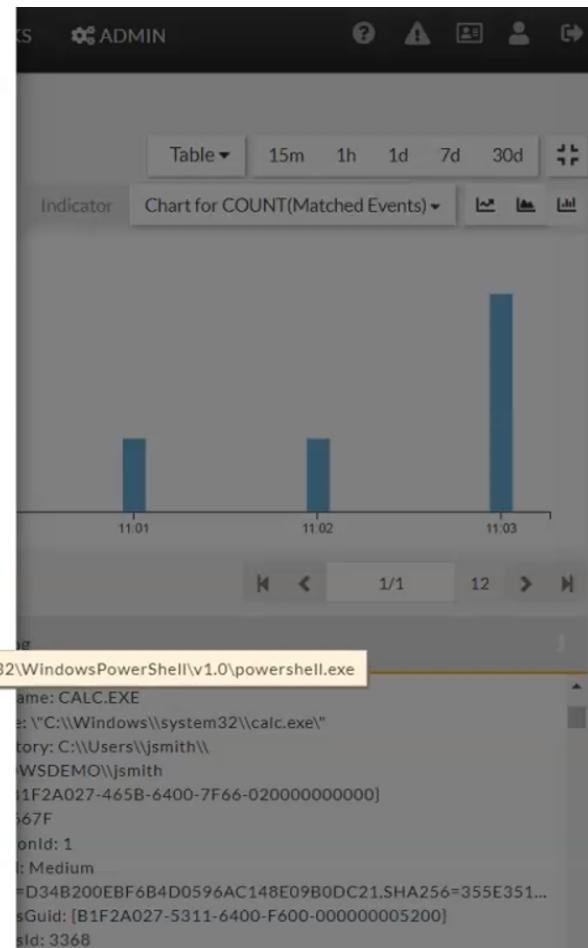
```

2023-03-02T08:02:53Z WindowsDemo 192.168.18.11 AcclOps-WUA-WinLog-
Microsoft-Windows-Sysmon/Operational [phCustId]="1" [customer]="super"
[monitorStatus]="Success" [Locale]="fr-CH" [MachineGuid]="b1f2a027-cbe1-4798-
8749-70d9865bfcbb1" [timeZone]="+0300" [eventName]="Microsoft-Windows-
Sysmon/Operational" [eventSource]="Microsoft-Windows-Sysmon" [eventId]="1"
[eventType]:"Information" [domain]:"NT AUTHORITY" [computer]:"WindowsDemo"
[user]:"SYSTEM" [userSID]:"S-1-5-18" [userSIDAcctType]:"User" [eventTime]:"Mar 02
2023 08:02:52" [deviceTime]:"Mar 02 2023 08:02:52" [msg]:"Process Create:
RuleName: -
UtcTime: 2023-03-02 08:02:51.997
ProcessGuid: {B1F2A027-582B-6400-1C01-000000005200}
ProcessId: 2116
Image: C:\Windows\System32\calc.exe
FileVersion: 10.0.10240.16397 (th1.150721-1806)
Description: Windows Calculator
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation

```

		Display	Filter	Item	Value
<input type="checkbox"/>	<input type="checkbox"/>	Parent Process Id		3368	
<input type="checkbox"/>	<input type="checkbox"/>	Parent Process Name		C:\Windows\System32\Wind...	
<input type="checkbox"/>	<input type="checkbox"/>	Process GUID		{B1F2A027-5...	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
<input type="checkbox"/>	<input type="checkbox"/>	Process Id		2116	
<input type="checkbox"/>	<input type="checkbox"/>	Process Name		C:\Windows\System32\calc.e...	
<input type="checkbox"/>	<input type="checkbox"/>	Product		Microsoft® Windows® Oper...	
<input type="checkbox"/>	<input type="checkbox"/>	Relaying Device		WindowsDemo	

OK      Close



- ◆ these are the two interesting fields that we can check

## To create the rule

- ◆ click on **RESOURCES** > **New**
- ◆ Step1: General
  - ◆ Group - Most of the time **security**
  - ◆ Rule Name - to distinguish from the default rule, add some prefix
  - ◆ Description
  - ◆ Event Type - it will be **Rule Name** with underscore
- ◆ Step2: Define Condition
  - ◆ here you need to add time window
  - ◆ and you can add filters (in Subpattern section)

The screenshot shows the FortiSIEM interface for creating a new rule. The top navigation bar includes links for Dashboard, Analytics, Incidents, Cases, CMDB, Resources, Tasks, and Admin. On the left, a sidebar lists categories such as Reports, Rules (which is selected), Machine Learning Jobs, Watch Lists, Lookup Tables, Osquery, Connectors, Playbooks, Remediations, Malware Domains, and Malware IPs. The main content area is titled 'Add New Rule' and is divided into three steps: Step 1: General, Step 2: Define Condition (which is active and highlighted in blue), and Step 3: Define Action. Under Step 2, a condition is defined as 'If this Pattern occurs within any 300 second time window'. Below this, there is a toolbar with buttons for Paren, Subpattern, Row, and Next, along with a central edit icon (pencil) which is highlighted with a red box. At the bottom right are 'Save' and 'Cancel' buttons.

- ◆ from the sysmon log we can find the the value of the Attribute

```
2023-03-02T08:02:53Z WindowsDemo 192.168.18.11 AccelOps-WUA-WinLog-  
Microsoft-Windows-Sysmon/Operational [phCustomerId]=“1” [customer]=“super”  
[monitorStatus]=“Success” [Locale]=“fr-CH” [MachineGuid]=“b1f2a027-cbe1-4798-  
8749-70d9865bfcb1” [timeZone]=“+0300” [eventName]=“Microsoft-Windows-  
Sysmon/Operational” [eventSource]=“Microsoft-Windows-Sysmon” [eventId]=“1”  
[eventType]=“Information” [domain]=“NT AUTHORITY” [computer]=“WindowsDemo”  
[user]=“SYSTEM” [userSID]=“S-1-5-18” [userSIDAcctType]=“User” [eventTime]=“Mar 02  
2023 08:02:52” [deviceTime]=“Mar 02 2023 08:02:52” [msg]=“Process Create:  
RuleName: -  
UtcTime: 2023-03-02 08:02:51.997  
ProcessGuid: {B1F2A027-582B-6400-1C01-000000005200}  
ProcessId: 2116  
Image: C:\Windows\System32\calc.exe  
FileVersion: 10.0.10240.16397 (th1.150721-1806)  
Description: Windows Calculator  
Product: Microsoft® Windows® Operating System  
Company: Microsoft Corporation
```

event ty

Lines: 1 / 63

Display Filter Item



Event Type

Value

Win-Sysmon-1-Create-Process

Win-Sysmon-1-Create-Process

OK

Close

Event Type: Win-Sysmon-1-Create-Process

Name: filter\_0

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
-	attribute...	=	value...	-	+ AND OR	+ -

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
-	attribute...	=	value...	-	+ AND OR	+ -

Group By: Attribute

Type in attribute...

Run as Query Save as Report Save Cancel

- ◆ You can check and validate value in **Express on Builder** option. and note that sometimes the **spaces** matters
- ◆ now we can add for parent process

```
2023-03-02T08:02:53Z WindowsDemo 192.168.18.11 AccelOps-WUA-WinLog-  
Microsoft-Windows-Sysmon/Operational [phCustomerId]="1" [customer]="super"  
[monitorStatus]="Success" [Locale]="fr-CH" [MachineGuid]="b1f2a027-cbe1-4798-  
8749-70d9865bfcb1" [timeZone]="+0300" [eventName]="Microsoft-Windows-  
Sysmon/Operational" [eventSource]="Microsoft-Windows-Sysmon" [eventId]="1"  
[eventType]="Information" [domain]="NT AUTHORITY" [computer]="WindowsDemo"  
[user]="SYSTEM" [userSID]="S-1-5-18" [userSIDAcctType]="User" [eventTime]="Mar 02  
2023 08:02:52" [deviceTime]="Mar 02 2023 08:02:52" [msg]="Process Create:  
RuleName: -  
UtcTime: 2023-03-02 08:02:51.997  
ProcessGuid: {B1F2A027-582B-6400-1C01-000000005200}  
ProcessId: 2116  
Image: C:\Windows\System32\calc.exe  
FileVersion: 10.0.10240.16397 (th1.150721-1806)  
Description: Windows Calculator  
Product: Microsoft® Windows® Operating System  
Company: Microsoft Corporation
```

parent pro

Lines: 3 / 63

Display Filter Item

Value

		Parent Process GUID	{B1F2A027-5311-6400-F600...}
--	--	---------------------	------------------------------

		Parent Process Id	3368
--	--	-------------------	------

		Parent Process Name	C:\Windows\System32\Wind...
--	--	---------------------	-----------------------------

Parent Process Name

OK Close

◆ and the value should be **powershell.exe**

parent pro

Display Filter Item Value

<input type="checkbox"/>	<input type="checkbox"/>	Parent Process GUID	[B1F2A027-5311-6400-F600...]
<input type="checkbox"/>	<input type="checkbox"/>	Parent Process Id	3368
<input type="checkbox"/>	<input type="checkbox"/>	Parent Process Name	C:\Windows\System32\Wind... C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Lines: 3 / 63

11.22 11.27 11.3

0.10240.16397 [th1.150/21-1806] soft® Windows® Operating System

- ◆ we can also use the **regular expressions (REGEXP)** for complex filters

Edit SubPattern

Name:	filter_0																					
Filters:	<table border="1"> <tr> <td>Paren</td> <td>Attribute</td> <td>Operator</td> <td>Value</td> <td>Paren</td> <td>Next</td> <td>Row</td> </tr> <tr> <td>+ -</td> <td>Event Type</td> <td>=</td> <td>Win-Sysmon-1-Create-Process</td> <td>+ -</td> <td>AND</td> <td>- + -</td> </tr> <tr> <td>+ -</td> <td>Parent Process Name</td> <td>CONTAIN</td> <td>powershell.exe</td> <td>+ -</td> <td>AND</td> <td>- + -</td> </tr> </table>	Paren	Attribute	Operator	Value	Paren	Next	Row	+ -	Event Type	=	Win-Sysmon-1-Create-Process	+ -	AND	- + -	+ -	Parent Process Name	CONTAIN	powershell.exe	+ -	AND	- + -
Paren	Attribute	Operator	Value	Paren	Next	Row																
+ -	Event Type	=	Win-Sysmon-1-Create-Process	+ -	AND	- + -																
+ -	Parent Process Name	CONTAIN	powershell.exe	+ -	AND	- + -																
Aggregate:	<table border="1"> <tr> <td>Paren</td> <td>Attribute</td> <td>Value</td> <td>Paren</td> <td>Next</td> <td>Row</td> </tr> <tr> <td>+ -</td> <td>attribute...</td> <td>value...</td> <td>+ -</td> <td>AND</td> <td>- + -</td> </tr> </table>	Paren	Attribute	Value	Paren	Next	Row	+ -	attribute...	value...	+ -	AND	- + -									
Paren	Attribute	Value	Paren	Next	Row																	
+ -	attribute...	value...	+ -	AND	- + -																	
Group By:	<table border="1"> <tr> <td>Attribute</td> <td>Move</td> </tr> <tr> <td>Type in attribute...</td> <td>↓</td> </tr> </table>	Attribute	Move	Type in attribute...	↓																	
Attribute	Move																					
Type in attribute...	↓																					

Save | Save as Report | Run as Query | Cancel

A dropdown menu is open over the 'CONTAIN' operator in the first filter row, showing options: =, !=, <, >, <=, >=, BETWEEN, NOT BETWEEN, IN, NOT IN, CONTAIN, NOT CONTAIN, IS, IS NOT, REGEXP, and NOT REGEXP. The 'REGEXP' option is highlighted with a red box.

### Note:

- ◆ **REGEXP** will allow you to account for all the path syntax (like \\ for account for the backward slash (\))

Parent Process Name C:\Windows\System32\Wind... 0.10240.16397 [th1.150/21-1806]

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

soft® Windows® Operating System

- ◆ Also we need to look for any executable in the **Command** (here **calc.exe**)

command

Lines: 3 / 63

Display Filter Item

Value

<input type="checkbox"/>	<input type="checkbox"/>	Command	C:\Windows\system32\calc.e...
<input type="checkbox"/>	<input type="checkbox"/>	Message	Process Create: RuleName: - ...
<input type="checkbox"/>	<input type="checkbox"/>	Parent Command	C:\Windows\System32\Wind...

- ◆ And also software being called

software

Lines: 1 / 63

Display Filter Item

Value

<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> Software Name	C:\Windows\System32\calc.e...
Software Name			

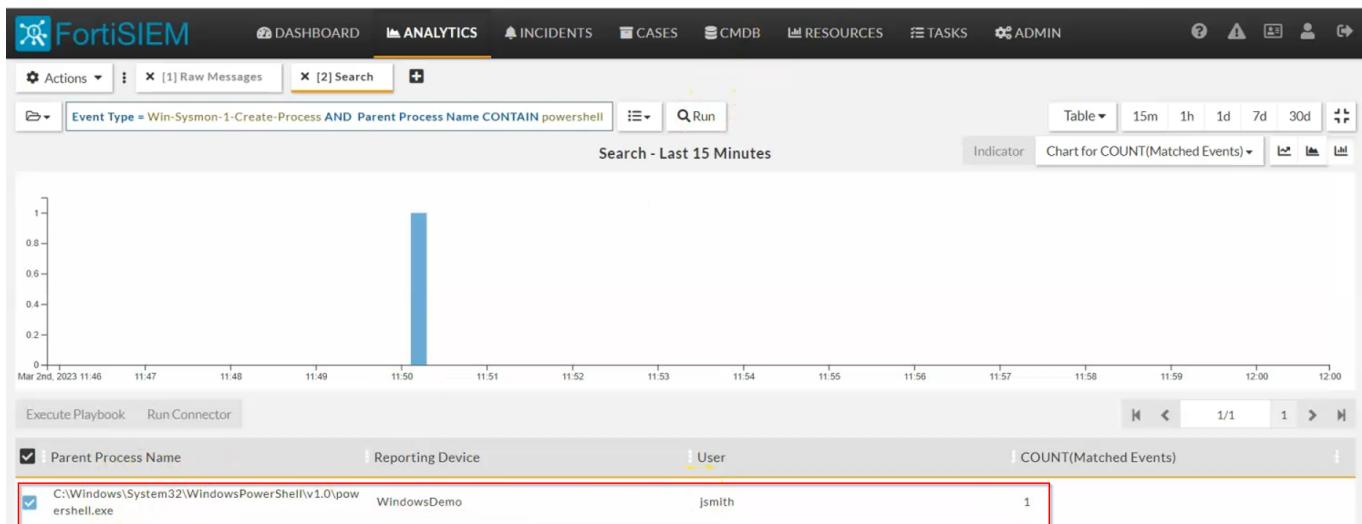
- ◆ we can **Run as Query** against historical data

Edit SubPattern

Name:	filter_0						
Filters:	Paren	Attribute	Operator	Value	Paren	Next	Row
	<input type="button"/> <input type="button"/>	Event Type	=	<input type="button"/>	Win-Sysmon-1-Create-Process	<input type="button"/> <input type="button"/>	AND <input type="button"/> <input type="button"/>
	<input type="button"/> <input type="button"/>	Parent Process Name	CONTAIN	<input type="button"/>	powershell.exe	<input type="button"/> <input type="button"/>	AND <input type="button"/> <input type="button"/>
	<input type="button"/> <input type="button"/>	Software Name	CONTAIN	<input type="button"/>	exe	<input type="button"/> <input type="button"/>	AND <input type="button"/> <input type="button"/>
Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	<input type="button"/> <input type="button"/>	COUNT(Matched Events)	>=	<input type="button"/>	1	<input type="button"/> <input type="button"/>	AND <input type="button"/> <input type="button"/>
Group By:	Attribute	Row	Move				
	User	<input type="button"/> <input type="button"/>	<input type="button"/> <input type="button"/>				
	Reporting Device	<input type="button"/> <input type="button"/>	<input type="button"/> <input type="button"/>				
	Parent Process Name	<input type="button"/> <input type="button"/>	<input type="button"/> <input type="button"/>				

Save Save as Report Run as Query Cancel

- ◆ output



- ◆ Step3: Define Action
  - ◆ at least one event attribute in **Action** section

Generate Incident for: HMT: Detect PS Call to some EXE

Event Attribute	Subpattern	Filter Attribute	Row
Reporting Device	= filter_0	Reporting Device	<input type="button" value="+"/> <input type="button" value="-"/>
Software Name	= filter_0	Software Name	<input type="button" value="+"/> <input type="button" value="-"/>
User	= filter_0	User	<input type="button" value="+"/> <input type="button" value="-"/>
Parent Process Name	= filter_0	Parent Process Name	<input type="button" value="+"/> <input type="button" value="-"/>
Triggered Event Count	= filter_0	COUNT(Matched Events)	<input type="button" value="+"/> <input type="button" value="-"/>

Insert Attribute:

Incident Title:

Triggered Attributes: Available:  1/31   Selected:

Balloon Target Memory KB	<input type="button" value="&gt;"/>	Reporting IP
Output Ix K-Factor	<input type="button" value="&gt;"/>	Reporting Device
DDNS Succesful Updates	<input type="button" value="&lt;"/>	User
Free Inodes NonRoot	<input type="button" value="^"/>	Event Receive Time
Power Chord Status	<input type="button" value="v"/>	Event Type

- ◆ finally save and review
- ◆ activate the rule and try to simulate the attack, and test the rule

- ◆ to test the rule:
  - ◆ go to **ANALYTICS** tab, and look for the exe file you have runned
  - ◆ in **INCIDENT** section, we should receive one **Medium** severity incident
  - ◆ if it's not showing check in **Rules** tab in **RESOURCES** section if there is any **Sync Error**
    - ◆ if there is check the original system which is running **FortiSIEM** for our rule
    - ◆ tail for **phoenix.log**

```
tail -f /opt/phoenix/log/phoenix.log | egrep -i
'PHL_ERROR|OUR_RULE_PREFIX'
```

- also you can `Run as Query` against historical events

- ◆ now you can see the rule triggering in **INCIDENT** section

The screenshot shows the FortiSIEM web interface. At the top, there is a navigation bar with tabs: DASHBOARD, ANALYTICS, INCIDENTS (which is highlighted), CASES, CMDB, and RESOURCES. Below the navigation bar, there is a toolbar with various filters and search functions. The main area displays a list of security incidents. A specific incident is selected, showing details: Severity is MEDIUM, Occurred on Mar 02 2023, 12:33:30 PM, and the event is HMT: Detect PS Call to some EXE. To the right of the incident details, there is a context menu with two options: "Rule Summary" and "Triggering Events". The "Triggering Events" option is highlighted with a red box.

- ◆ here is the rule summary

## Rule Summary

Name:

HMT: Detect PS Call to some EXE

Description:

Pattern: filter\_0

IF                   Event Type = Win-Sysmon-1-Create-Process  
                  AND Parent Process Name CONTAINS powershell.exe  
                  AND Software Name CONTAINS exe

WHERE              COUNT(Matched Events) >= 1

GROUP BY          Software Name, Parent Process Name, Reporting Device, User