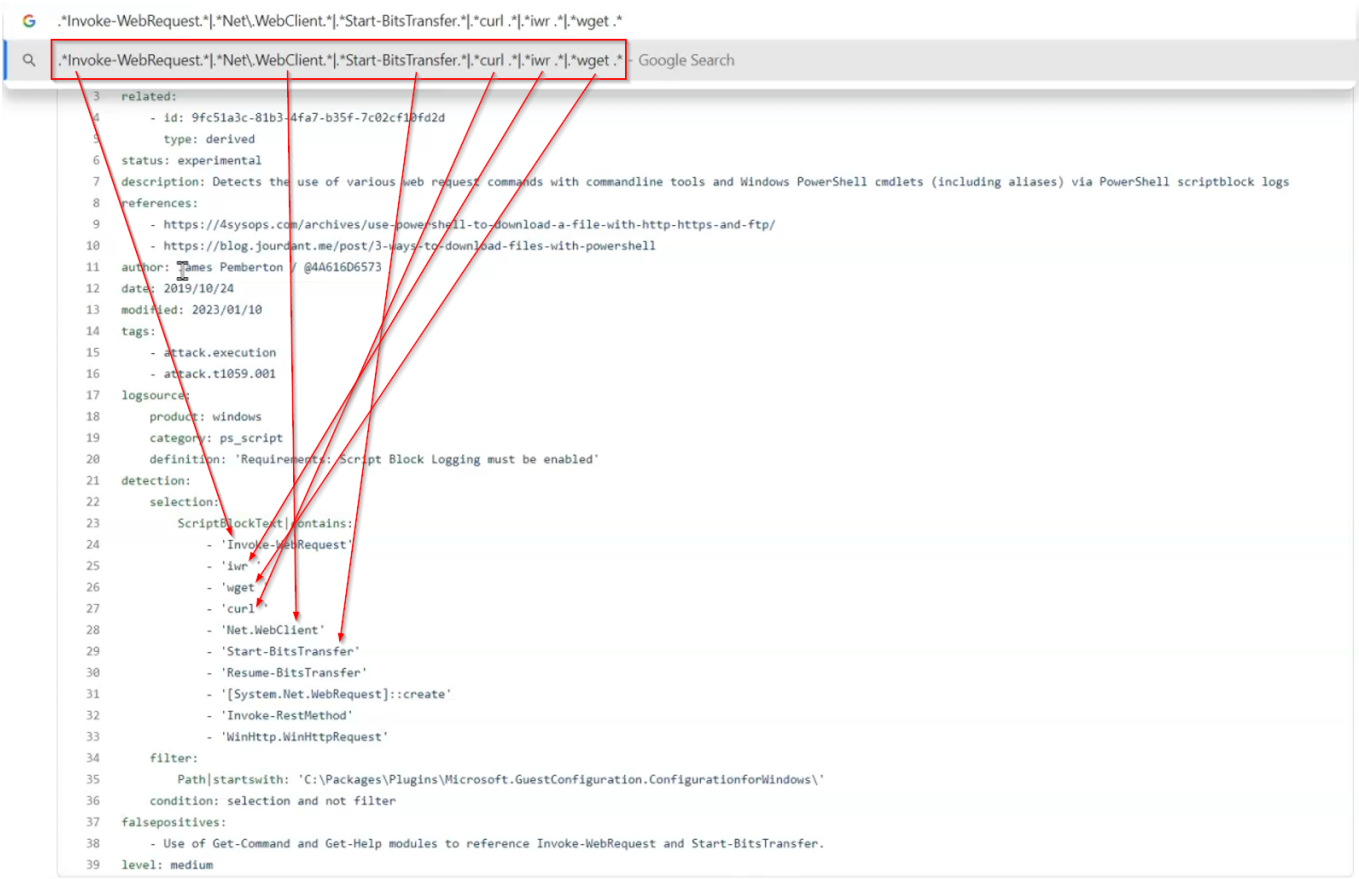
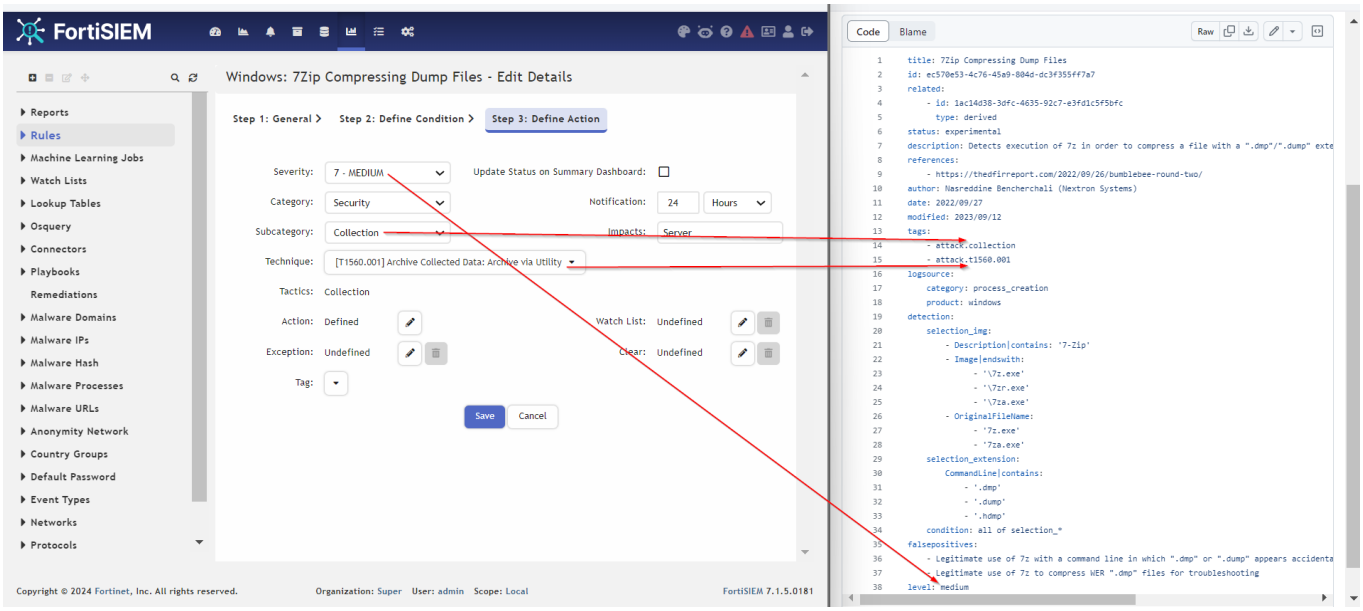
- Sigma rules adopted in FortiSIEM
- Sigma rules on Github
- How you can convert `sigma` rules into `FortiSIEM` rule?
- Many rules are adopted from sigma rules in FortiSIEM. for example,
  - Windows: Windows Powershell Web Request this can be found in `FortiSIEM` > `RESOURCES` > `Rules` and search for 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



- 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

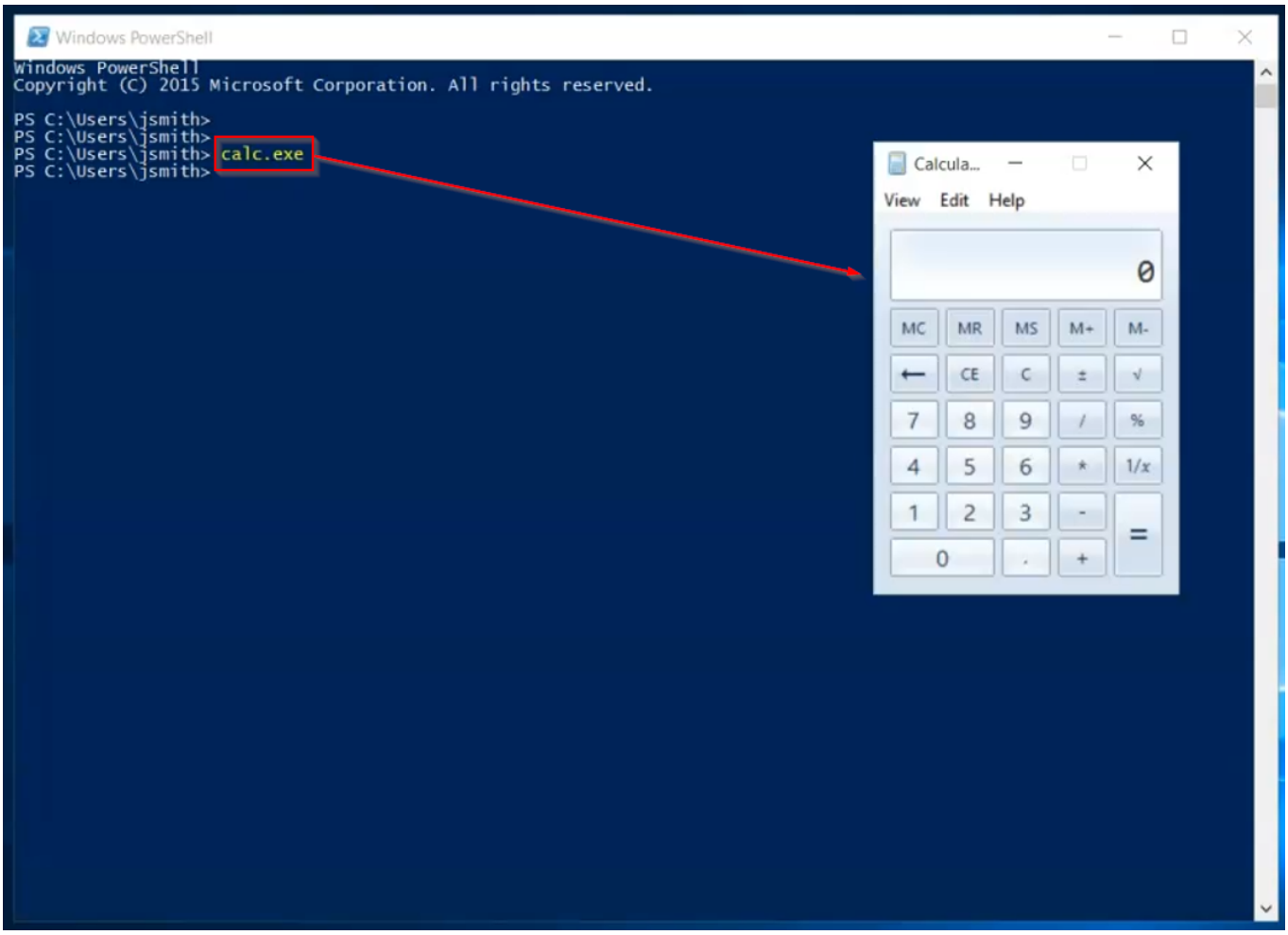


Developing our own rule

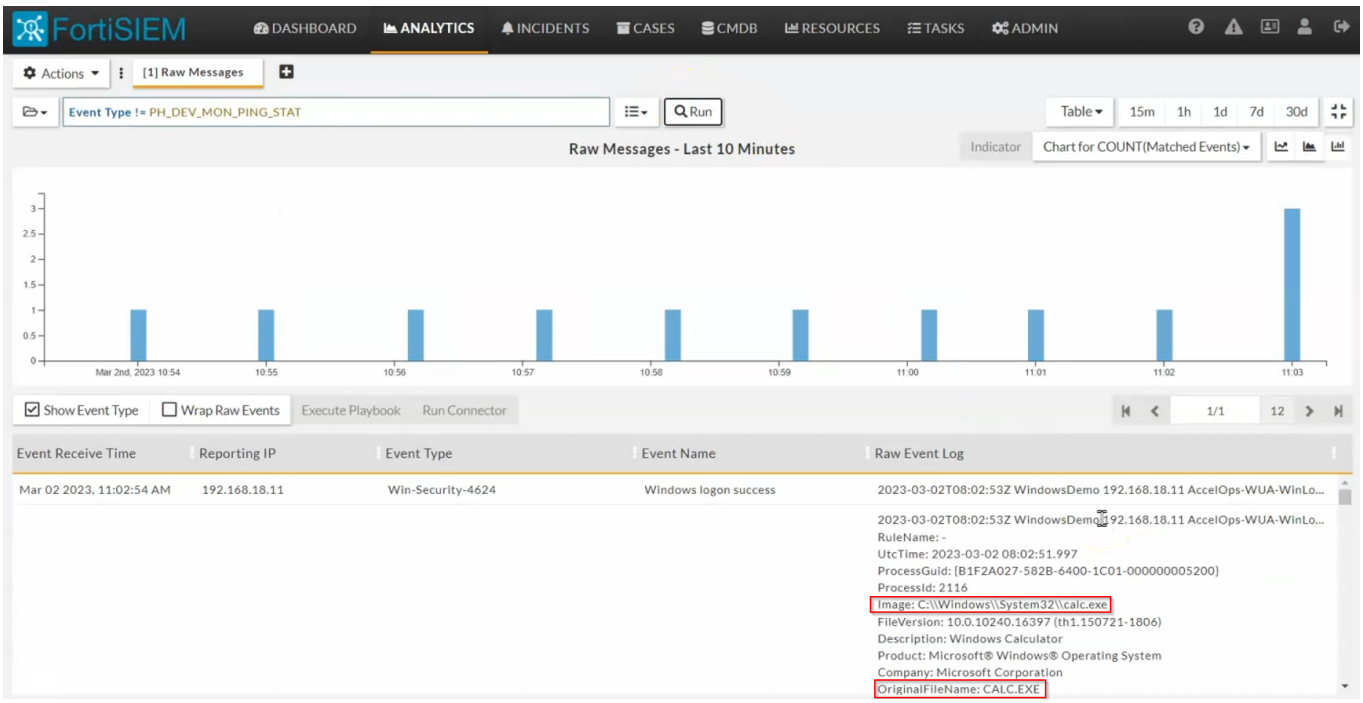
- let's create the one that will actually utilize the parent command line and the parent process and also the fields for the file name or the software that is being triggered by this parent process to check for malicious behavior.
- first let's start with simple rule, as powershell command or powershell 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:

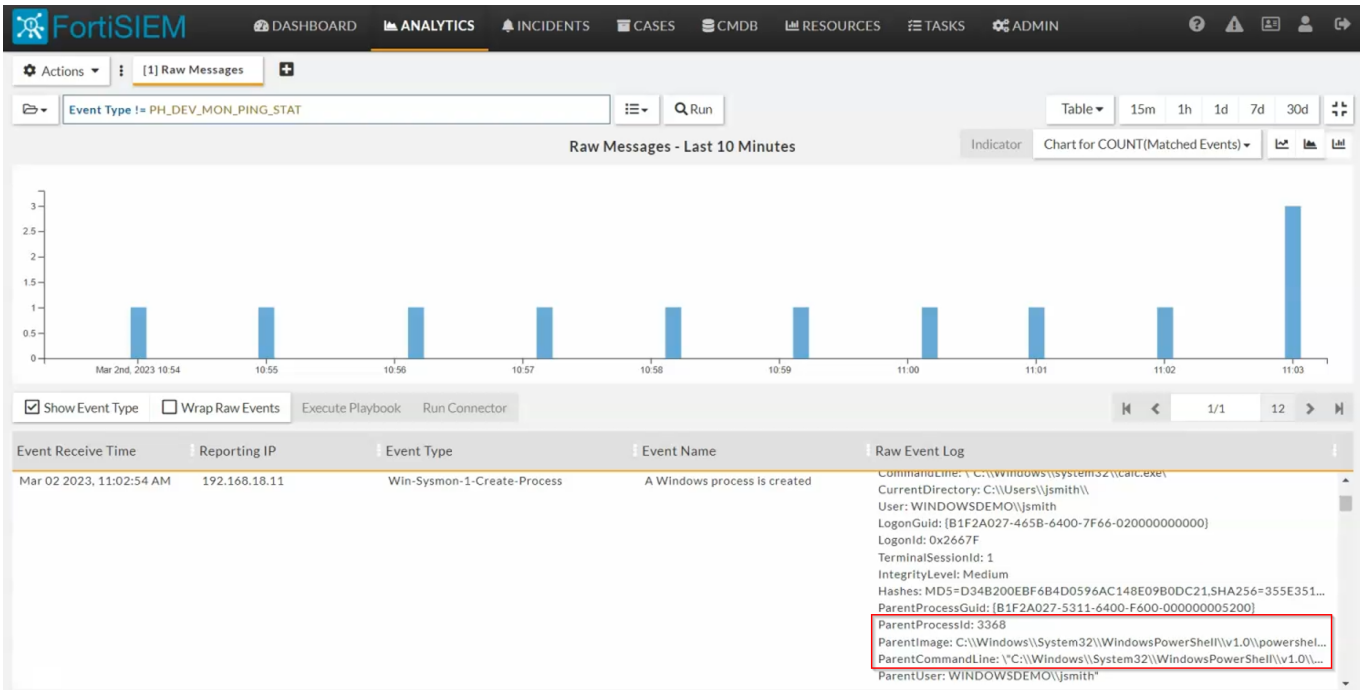
- To simulate our use case to trigger any executable from the powershell and check the logs in sysmon logs and try to write a rule to give us an incident based on that
- just execute any executable (e.g., calc.exe) in the powershell.



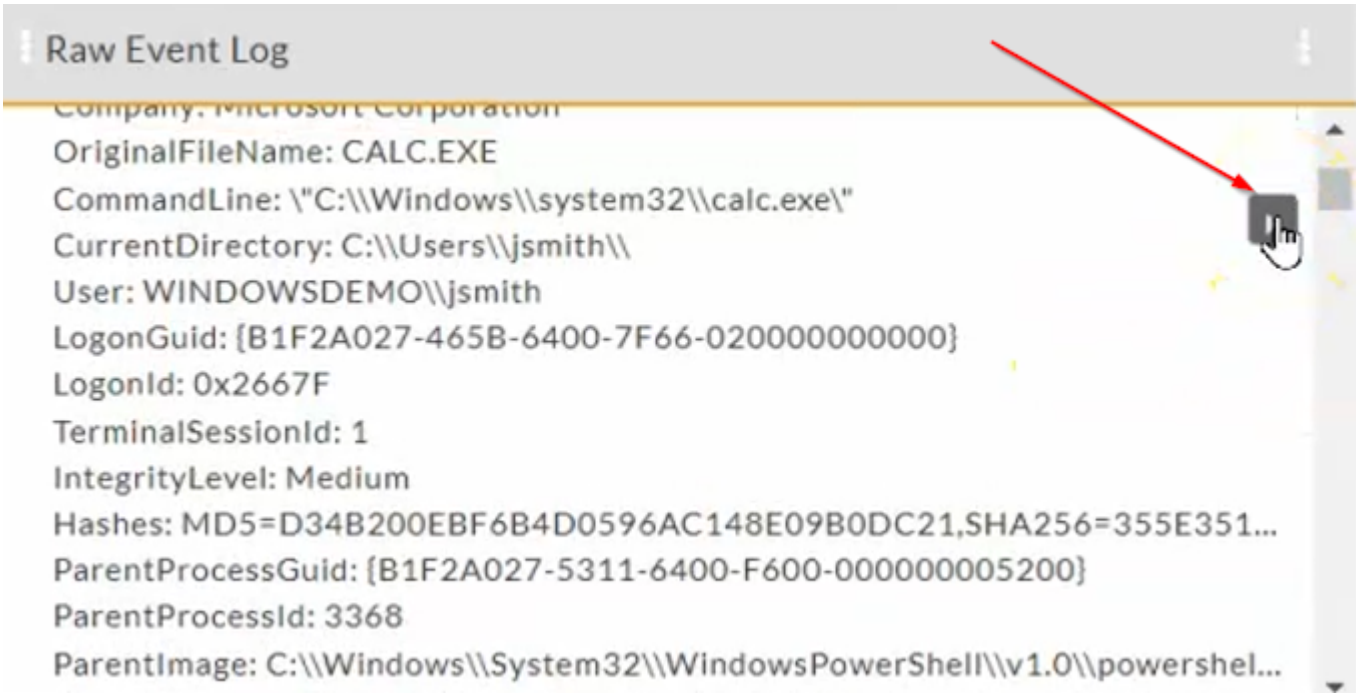
- now check the `ANALYTICS` tab to check the log



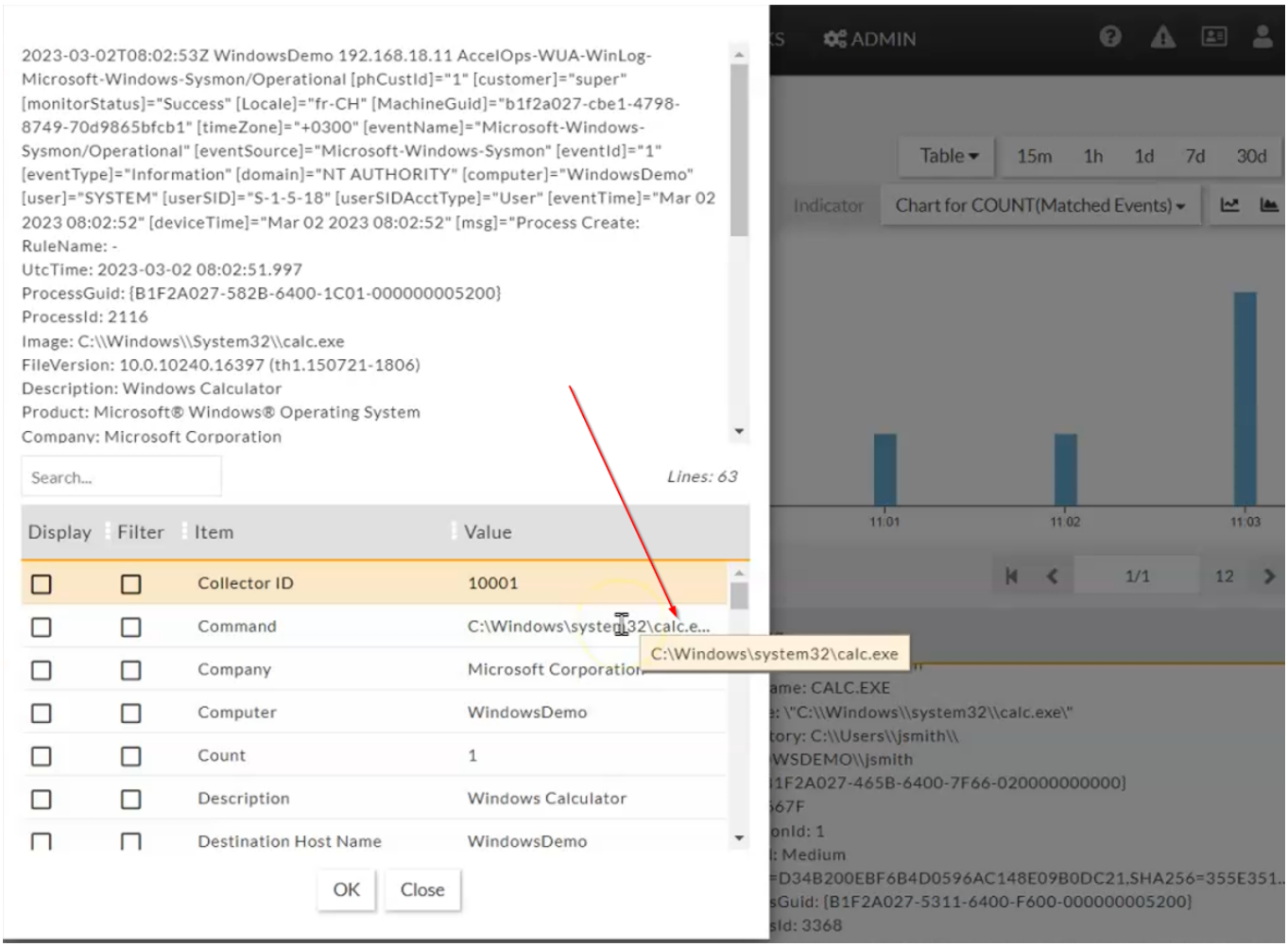
- and the parent process is powershell

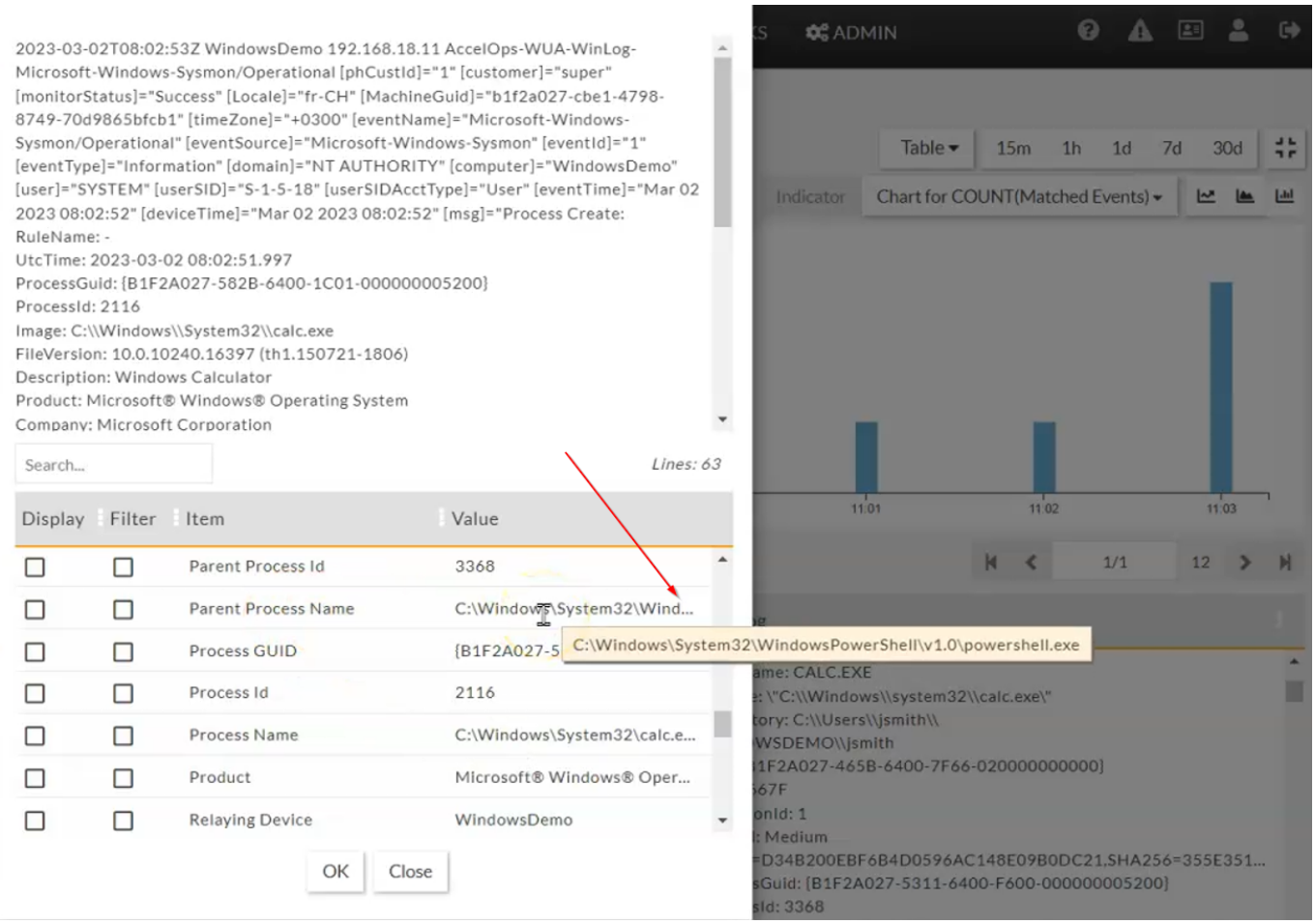


- first make sure that logs are logging then click on raw event log



- then look for some interesting field

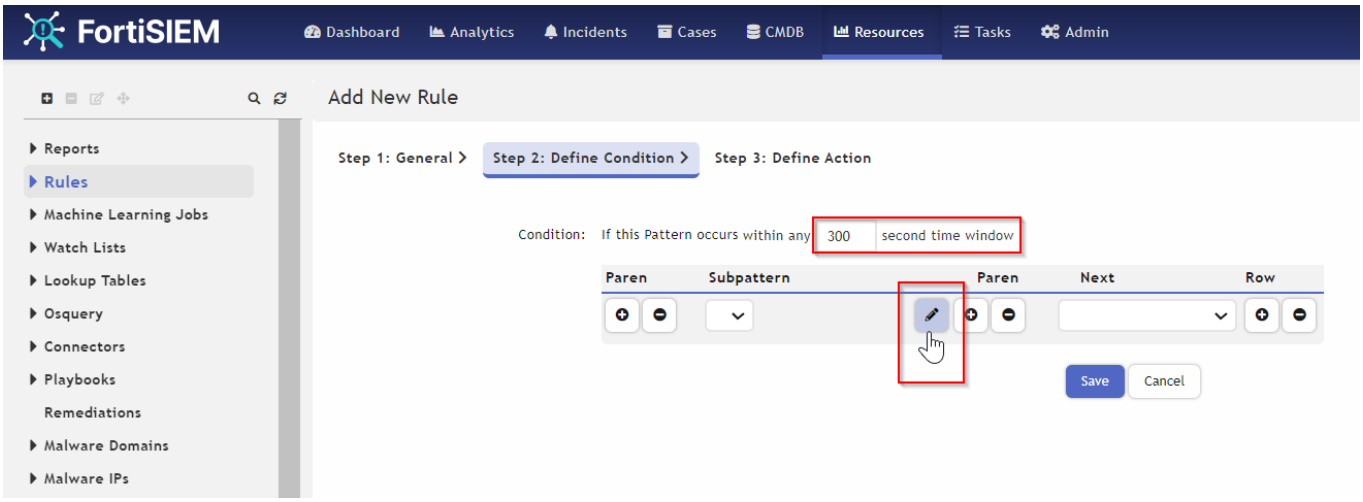

2023-03-02T08:02:53Z WindowsDemo 192.168.18.11 AccelOps-WUA-WinLog-Microsoft-Windows-Sysmon/Operational [phCustId]="1" [customer]="super" [monitorStatus]="Success" [Locale]="fr-CH" [MachineGuid]="b1f2a027-cbe1-4798-8749-70d9865bfcb1" [timeZone]="+0300" [eventName]="Microsoft-Windows-Sysmon/Operational" [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
Collector ID
10001
Command
C:\Windows\system32\calc.e...
Company
Microsoft Corporation
Computer
WindowsDemo
Count
1
Description
Windows Calculator
Destination Host Name
WindowsDemo
OK
Close
C:\Windows\system32\calc.exe
ADMIN
Table
15m
1h
1d
7d
30d
Indicator
Chart for COUNT(Matched Events)
11:01
11:02
11:03
1/1
12



- 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)



- 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 [phCustId]="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

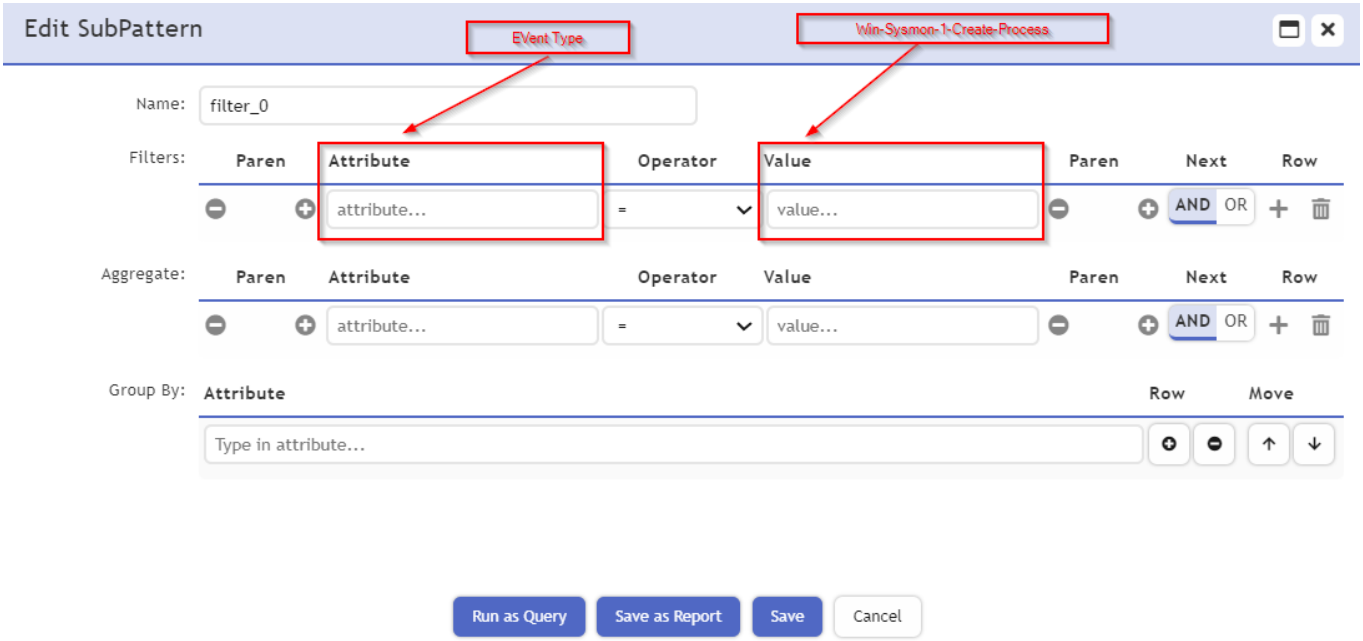
event ty

Lines: 1 / 63

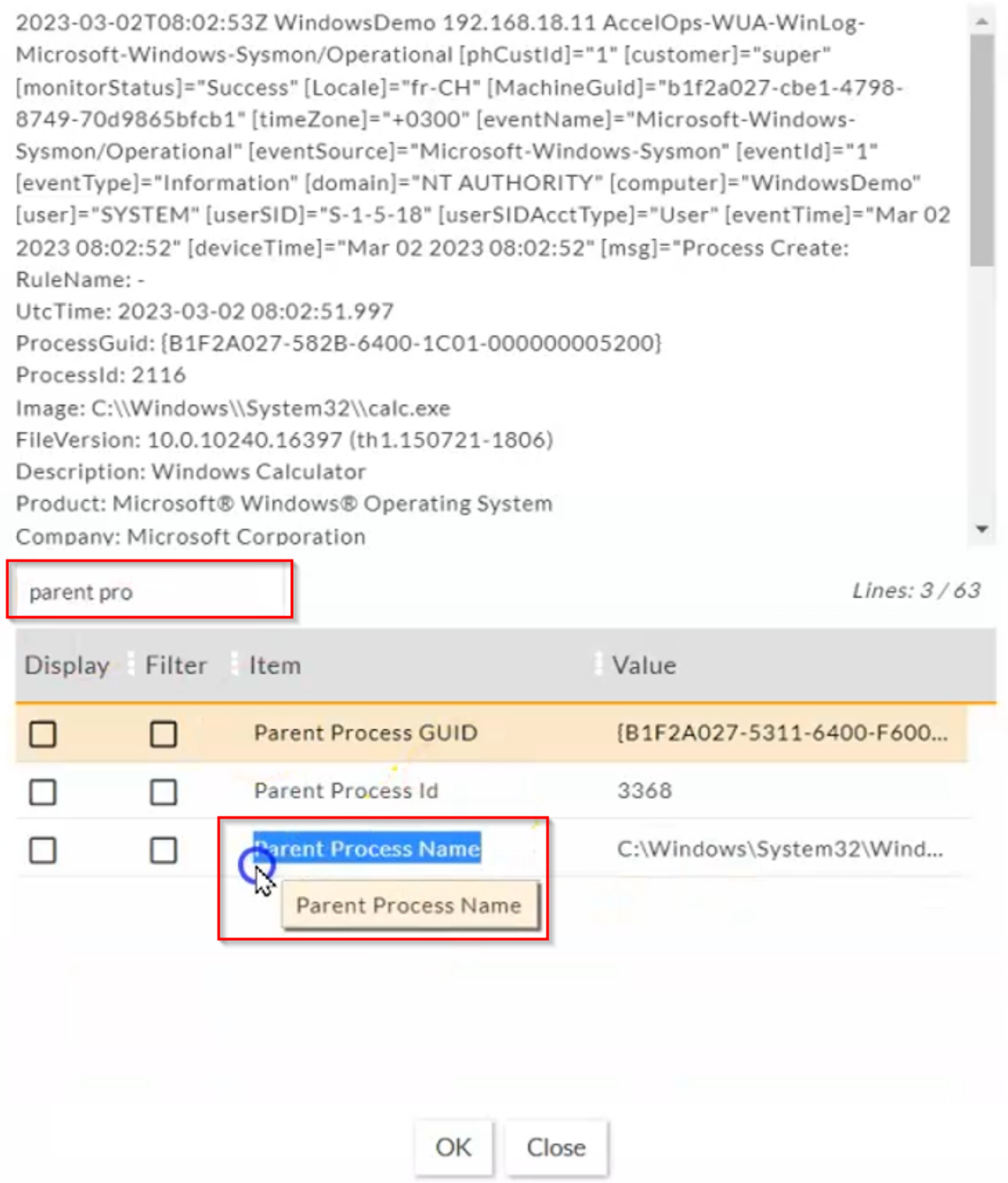
Display	Filter	Item	Value
☑	☑	Event Type	Win-Sysmon-1-Create-Process

Win-Sysmon-1-Create-Process

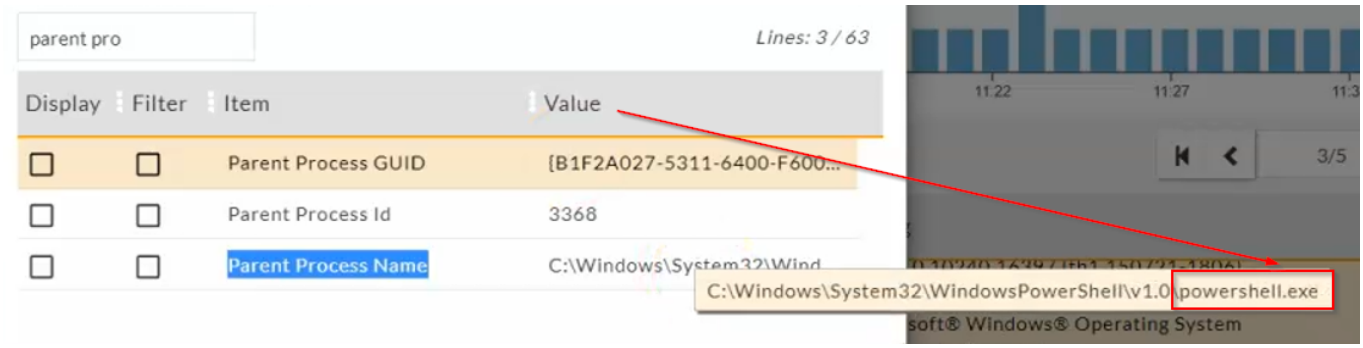
OK Close



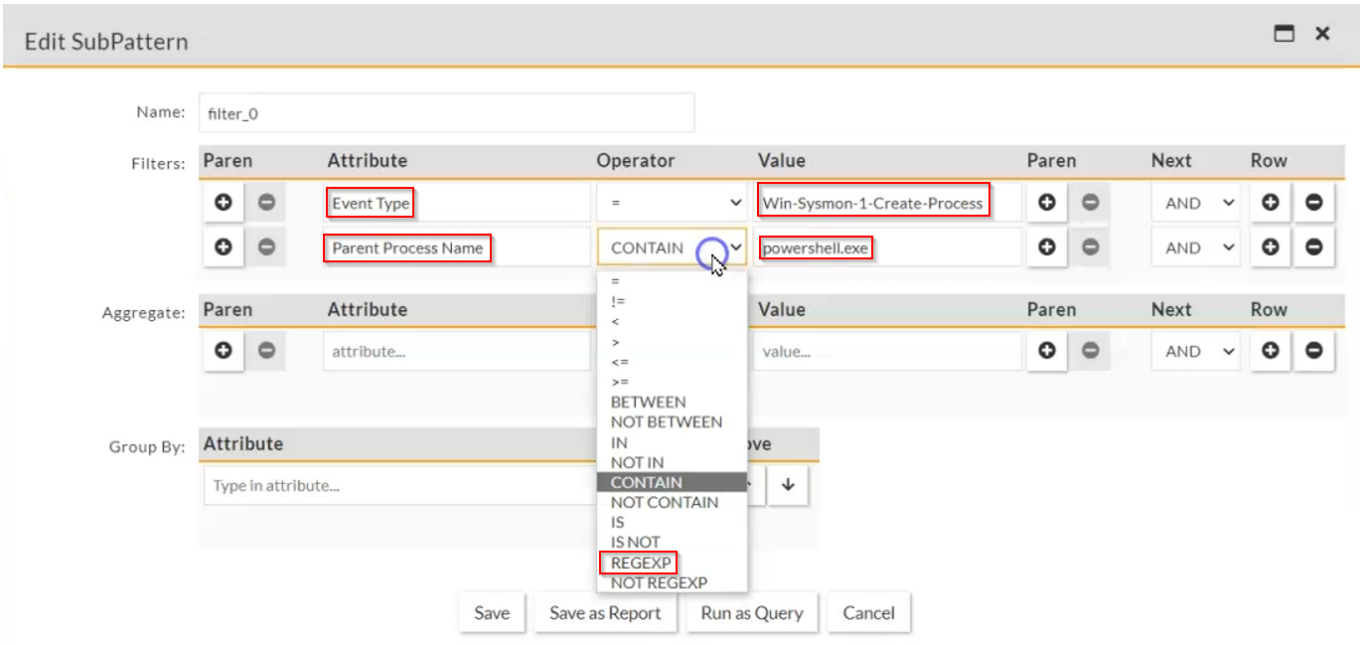
- You can check and validate value in `Express on Builder` option. and note that sometimes the `spaces` matters
- now we can add for parent process



- and the value should be `powershell.exe`

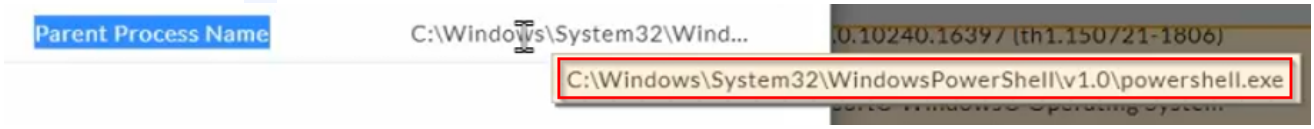


- we can also use the `regular expressions (REGEXP)` for complex filters

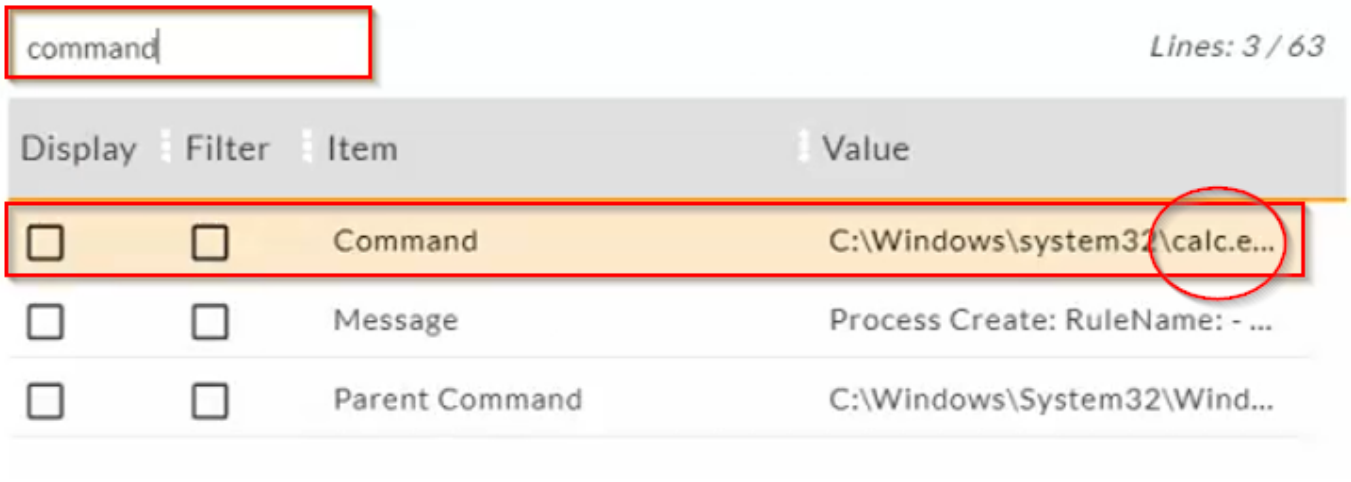


Note:

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

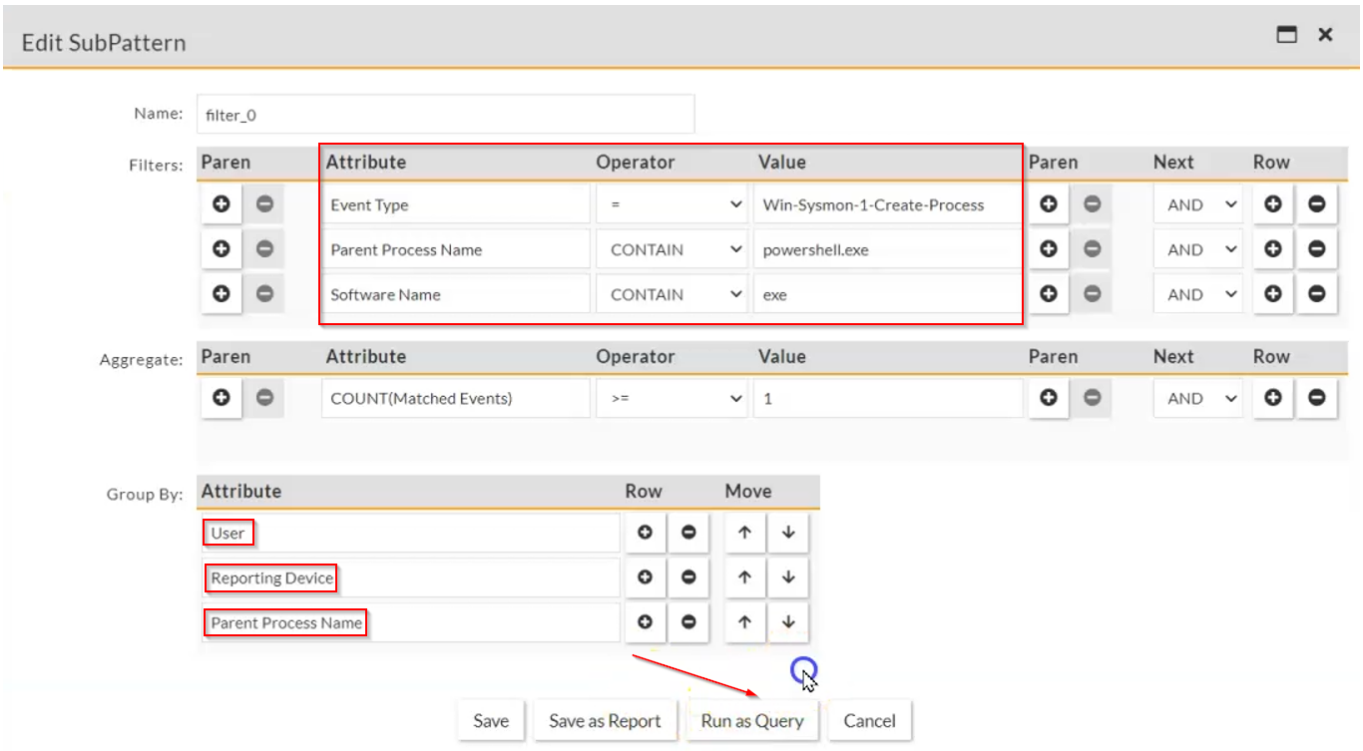


- Also we need to look for any executable in the `Command` (here `calc.exe`)

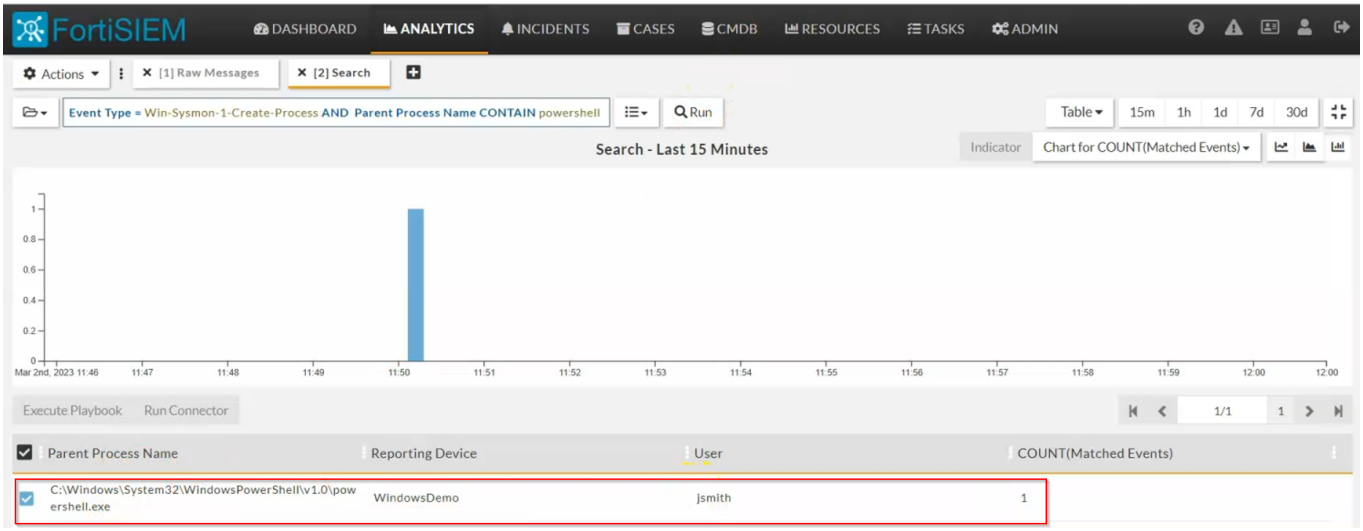


- And also software being called

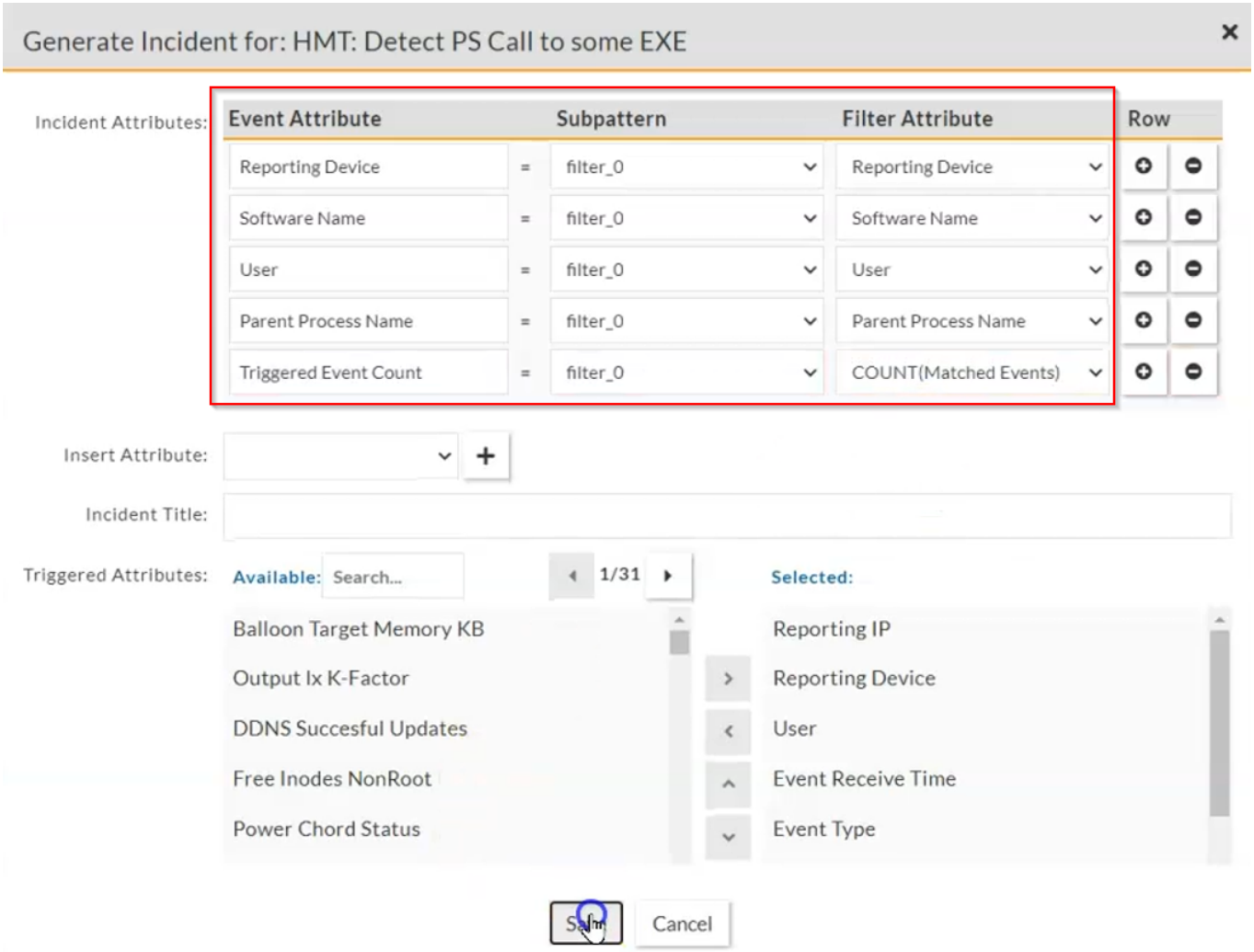
- we can `Run as Query` against historical data



- output



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



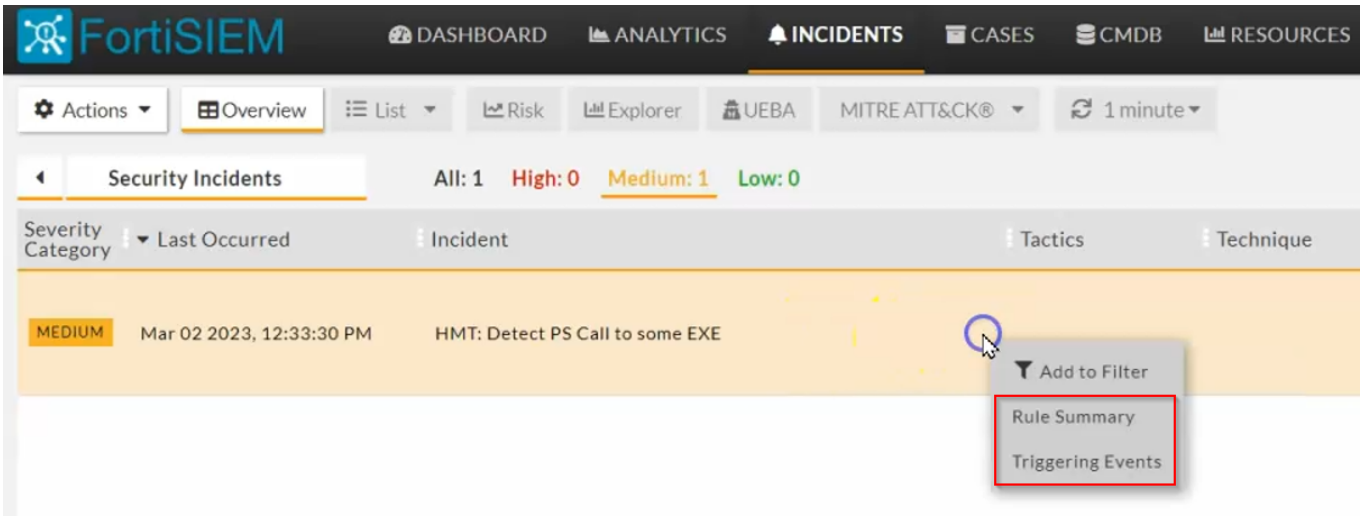
- finally save and review
- activate the rule and try to simulate the attack, and test the rule

- 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



- 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