



Analyzing the CSV results with Excel and Timeline Explorer

Zach Mathis (2021/12/25)

Excel

It will look like this when you open the CSV file.

A1	Time	Computername	Eventid	Level	Alert	Details	Rulepath	Filepath						
1	2013-10-24 03:37L4247D28-	037L4247D28-	4624	informational	Logon Type 0	Bootup	../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						
2	2013-10-24 03:37L4247D28-	037L4247D28-	4625	medium	Failed Logon From Public		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx						
4	2013-10-24 03:37L4247D28-	037L4247D28-	1	high	Execution Of Not Existing		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
5	2013-10-24 03:37L4247D28-	037L4247D28-	1	high	Execution Of Other File Ty		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
6	2013-10-24 03:37L4247D28-	037L4247D28-	2003	low	USB Device Plugged		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
7	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Not Existing		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
8	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Other File Ty		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
9	2013-10-24 01:IE8Win7	01:IE8Win7	4624	informational	Logon Type 0	Bootup	../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						
10	2013-10-24 01:IE8Win7	01:IE8Win7	4625	medium	Failed Logon From Public		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx						
11	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Not Existing		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
12	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Other File Ty		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
13	2013-10-24 01:IE8Win7	01:IE8Win7	4616	medium	Unauthorized System Tim		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						
14	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Not Existing		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
15	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Other File Ty		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
16	2013-10-24 01:IE8Win7	01:IE8Win7	4616	medium	Unauthorized System Tim		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						
17	2013-10-24 01:IE8Win7	01:IE8Win7	4720	medium	Local user ac User: IEUser		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx						
18	2013-10-24 01:IE8Win7	01:IE8Win7	4720	medium	Local user ac User: IEUser		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						
19	2013-10-24 01:IE8Win7	01:IE8Win7	4732	high	User added t User: - : SID		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx						
20	2013-10-24 01:IE8Win7	01:IE8Win7	4732	high	User added t User: - : SID		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						
21	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Not Existing		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
22	2013-10-24 01:IE8Win7	01:IE8Win7	1	high	Execution Of Other File Ty		../hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx						
23	2013-10-24 01:IE8Win7	01:IE8Win7	4648	informational	Explicit Logo	Source User:/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx						

It is pretty hard to read so first click on the upper-left corner to select all of the cells.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Time	ComputerName	EventId	Level	Alert	Details	Rulepath	Filepath					
2	2013-10-24 03:37:42.4728	DEEPBLUE	4624	informational	Logon Type C	Bootup/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
3	2013-10-24 03:37:42.4728	DEEPBLUE	4625	medium	Failed Logon From Public	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx					
4	2013-10-24 03:37:42.4728	DEEPBLUE	1	high	Execution Of Not Existing	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
5	2013-10-24 03:37:42.4728	DEEPBLUE	1	high	Execution Of Other File Ty	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
6	2013-10-24 03:37:42.4728	DEEPBLUE	2003	low	USB Device Plugged	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
7	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Not Existing/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
8	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Other File Ty/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
9	2013-10-24 01:48:05.187	IE8Win7		4624	informational	Logon Type C	Bootup/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx				
10	2013-10-24 01:48:05.187	IE8Win7		4625	medium	Failed Logon From Public	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx				
11	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Not Existing	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx				
12	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Other File Ty	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx				
13	2013-10-24 01:48:05.187	IE8Win7		4616	medium	Unauthorized System Tim	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx				
14	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Not Existing	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx				
15	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Other File Ty	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx				
16	2013-10-24 01:48:05.187	IE8Win7		4616	medium	Unauthorized System Tim	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx				
17	2013-10-24 01:48:05.187	IE8Win7		4720	medium	Local user ac User: IEUser	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx				
18	2013-10-24 01:48:05.187	IE8Win7		4720	medium	Local user ac User: IEUser	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx				
19	2013-10-24 01:48:05.187	IE8Win7		4732	high	User added t User: - : SID	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx				
20	2013-10-24 01:48:05.187	IE8Win7		4732	high	User added t User: - : SID	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx				
21	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Not Existing	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx				
22	2013-10-24 01:48:05.187	IE8Win7		1	high	Execution Of Other File Ty	/hayabusa-/hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx				

Then double click on the line between A and B to adjust to the optimal row width:

A	B	C	D	E	
1 Time	Computername	Eventid	Level	Alert	Details
2 2013-10-24 01:16:13.843 +09:00	37L4247D28-05	4624	informational	Logon Type 0 - System	Bootup
3 2013-10-24 01:16:29.000 +09:00	37L4247D28-05	4625	medium	Failed Logon From Public IP	
4 2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Not Existing File	
5 2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Other File Type Than .exe	
6 2013-10-24 01:18:09.203 +09:00	37L4247D28-05	2003	low	USB Device Plugged	
7 2013-10-24 01:18:33.828 +09:00	IE8Win7	1	high	Execution Of Not Existing File	
8 2013-10-24 01:18:33.828 +09:00	IE8Win7	1	high	Execution Of Other File Type Than .exe	
9 2013-10-24 01:18:50.500 +09:00	IE8Win7	4624	informational	Logon Type 0 - System	Bootup
10 2013-10-24 01:21:30.000 +09:00	IE8Win7	4625	medium	Failed Logon From Public IP	
11 2013-10-24 01:21:33.630 +09:00	IE8Win7	1	high	Execution Of Not Existing File	
12 2013-10-24 01:21:33.630 +09:00	IE8Win7	1	high	Execution Of Other File Type Than .exe	
13 2013-10-24 01:21:33.630 +09:00	IE8Win7	4616	medium	Unauthorized System Time Modification	
14 2013-10-24 01:22:39.911 +09:00	IE8Win7	1	high	Execution Of Not Existing File	
15 2013-10-24 01:22:39.911 +09:00	IE8Win7	1	high	Execution Of Other File Type Than .exe	
16 2013-10-24 01:22:39.911 +09:00	IE8Win7	4616	medium	Unauthorized System Time Modification	
17 2013-10-24 01:22:39.973 +09:00	IE8Win7	4720	medium	Local user account created	User: IEUser : SID:S-1-5-21-3463664321-2923530833-3546627382-1000
18 2013-10-24 01:22:39.973 +09:00	IE8Win7	4720	medium	Local user account created	User: IEUser : SID:S-1-5-21-3463664321-2923530833-3546627382-1000
19 2013-10-24 01:22:40.004 +09:00	IE8Win7	4732	high	User added to local Administrators group	User: - : SID: S-1-5-21-3463664321-2923530833-3546627382-1000 : Group: Administrators
20 2013-10-24 01:22:40.004 +09:00	IE8Win7	4732	high	User added to local Administrators group	User: - : SID: S-1-5-21-3463664321-2923530833-3546627382-1000 : Group: Administrators
21 2013-10-24 01:22:40.005 +09:00	IE8Win7	1	high	Execution Of Not Existing File	

The results will be pretty wide so a wide monitor is recommended.

Click on the B2 cell and then View→Freeze Panes. This will let you scroll while still seeing the headers and timestamps:

The screenshot shows the Microsoft Excel ribbon with the 'View' tab selected (indicated by a red box). The 'Freeze Panes' button in the 'Window' group is also highlighted with a red box. The formula bar shows the cell reference B2. Below the ribbon, a table is displayed with five columns labeled A through E. The first row contains column headers: Time, Computername, Eventid, Level, Alert, and Details. The second row contains data: 2013-10-24 01:16:13.843 +09:00, 37L4247D28-05, 4624, informational, Logon Type 0 - System, Bootup. The third row contains: 2013-10-24 01:16:29.000 +09:00, 37L4247D28-05, 4625, medium, Failed Logon From Public IP, . The fourth row contains: 2013-10-24 01:17:44.109 +09:00, 37L4247D28-05, 1, high, Execution Of Not Existing File, . The 'Computername' cell in the second row is highlighted with a red box.

A	B	C	D	E	Details
1 Time	Computername	Eventid	Level	Alert	
2 2013-10-24 01:16:13.843 +09:00	37L4247D28-05	4624	informational	Logon Type 0 - System	Bootup
3 2013-10-24 01:16:29.000 +09:00	37L4247D28-05	4625	medium	Failed Logon From Public IP	
4 2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Not Existing File	

1. Select all of the cells in row 1.
2. Click Data→Filter.

The screenshot shows the Microsoft Excel ribbon with the 'Data' tab selected, indicated by a red box. On the far right of the ribbon, there is a 'Sort & Filter' group containing icons for 'Clear', 'Reapply', 'Sort', and 'Filter'. The 'Filter' icon, which looks like a funnel, is also highlighted with a red box. Below the ribbon, the Excel interface includes a formula bar with cell reference A1, and a main worksheet area with a table of log event data. The first row of the table is highlighted in green, and the 'Time' column header is also highlighted in green, indicating it is the active cell.

1	Time	Computername	Eventid	Level	Alert	Details
2	2013-10-24 01:16:13.843 +09:00	37L4247D28-05	4624	informational	Logon Type 0 - System	Bootup
3	2013-10-24 01:16:29.000 +09:00	37L4247D28-05	4625	medium	Failed Logon From Public IP	
4	2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Not Existing File	
5	2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Other File Type Than .exe	
6	2013-10-24 01:18:09.203 +09:00	37L4247D28-05	2003	low	USB Device Plugged	

This will let you filter by severity level, Event IDs, alerts, etc..

The screenshot shows a software interface for managing event logs. On the left, there is a table with columns labeled B, C, and D. Column B contains event names like 'ername', '7D28-05', and '7'. Column C contains Event IDs such as '4624', '4625', '1', '1', '2003', '1', '4624', '4625', '1', '1', '4616', '1', '4616', '4720', '4720', '4732', '4732', '1', '1', and '4648'. Column D contains levels like 'informational', 'medium', 'high', 'high', 'low', 'high', 'high', 'medium', 'medium', 'high', 'medium', 'medium', 'high', 'high', 'high', 'high', 'informational', 'informational', 'informational', and 'informational'. A red box highlights the dropdown menu in column D.

A central modal dialog is titled 'Alert' and has a red dot icon. It includes a 'Sort' section with 'A Z Ascending' and 'Z A Descending' buttons, and a 'Filter' section with a dropdown set to 'Choose One'. A search bar with a magnifying glass icon and the word 'Search' is also present. A large red box highlights the 'Filter' dropdown, which lists the following options:

- (Select All)
- critical
- high
- informational
- low
- medium

At the bottom of the dialog, there is an 'Auto Apply' checkbox and two buttons: 'Apply Filter' and 'Clear Filter'. The status bar at the bottom of the window displays the message 'Execution of NOT EXISTING file'.

There will be false-positives, but we recommend to search from critical alerts first and go down from there.

It will be easier to see if you apply background colors to each level:

The screenshot shows a Microsoft Excel spreadsheet with a table containing log data. The table has columns labeled 'Time', 'Computername', 'Event', 'Level', and 'Alert'. The rows are color-coded: the first row is light gray, and subsequent rows alternate between red and green. The 'Time' column contains dates and times, the 'Computername' column contains computer names, the 'Event' column contains event IDs, the 'Level' column contains severity levels, and the 'Alert' column contains descriptive text. The Excel ribbon is visible at the top, with the 'Home' tab selected. The status bar at the bottom shows the cell reference 'F5535'.

Time	Computername	Event	Level	Alert
4284 2019-02-02 18:17:27.629 +09:00	ICORP-DC.internal.corp	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
4285 2019-02-02 18:17:27.629 +09:00	ICORP-DC.internal.corp	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
4353 2019-03-18 04:37:11.661 +09:00	PC04.example.corp	10	critical	Mimikatz Use
4562 2019-03-18 23:23:23.937 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
4563 2019-03-18 23:23:23.937 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
4564 2019-03-18 23:23:23.937 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5115 2019-03-18 23:23:25.529 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5116 2019-03-18 23:23:25.529 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5117 2019-03-18 23:23:25.529 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5150 2019-03-18 23:23:25.589 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5151 2019-03-18 23:23:25.589 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5160 2019-03-18 23:23:25.599 +09:00	PC01.example.corp	5145	critical	Mimikatz Use
5524 2019-03-26 06:28:45.022 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
5525 2019-03-26 06:28:45.022 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right

After adding color:

A	B	C	D	E	
Time	Computername	EventID	Level	Alert	Details
2021-05-03 17:58:38.774 +09:00	webiis01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : Port: 6
2021-05-03 17:58:38.775 +09:00	webiis01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : Port: 6
2021-05-03 17:58:38.775 +09:00	webiis01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : Port: 6
2021-05-03 21:06:57.954 +09:00	win10-02.offsec.lan	1	high	Process Creation Sysmon Rule Alert	Rule: technique_id=T1059,technique_name=Command-Line Interfa
2021-05-03 21:06:57.954 +09:00	win10-02.offsec.lan	1	critical	Sticky Key Like Backdoor Usage	
2021-05-15 05:39:33.214 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-05-19 06:18:40.607 +09:00	rootdc1.offsec.lan	150	critical	DNS Server Error Failed Loading the ServerLevelPluginDLL	
2021-05-19 06:18:40.607 +09:00	rootdc1.offsec.lan	150	high	Possible CVE-2021-1675 Print Spooler Exploitation	
2021-05-19 06:18:40.607 +09:00	rootdc1.offsec.lan	150	critical	Mimikatz Use	
2021-05-19 06:23:27.038 +09:00	rootdc1.offsec.lan	150	critical	DNS Server Error Failed Loading the ServerLevelPluginDLL	
2021-05-19 06:23:27.038 +09:00	rootdc1.offsec.lan	150	high	Possible CVE-2021-1675 Print Spooler Exploitation	
2021-05-19 06:23:27.038 +09:00	rootdc1.offsec.lan	150	critical	Mimikatz Use	
2021-05-19 06:30:17.318 +09:00	rootdc1.offsec.lan	4688	high	Possible CVE-2021-1675 Print Spooler Exploitation	
2021-05-19 06:30:17.318 +09:00	rootdc1.offsec.lan	4688	critical	Mimikatz Use	
2021-05-19 06:30:17.318 +09:00	rootdc1.offsec.lan	4688	high	Relevant Anti-Virus Event	
2021-05-19 06:33:49.548 +09:00	rootdc1.offsec.lan	770	critical	DNS Server Error Failed Loading the ServerLevelPluginDLL	
2021-05-19 06:33:49.548 +09:00	rootdc1.offsec.lan	770	high	Possible CVE-2021-1675 Print Spooler Exploitation	
2021-05-19 06:33:49.548 +09:00	rootdc1.offsec.lan	770	high	Relevant Anti-Virus Event	
2021-05-19 06:33:49.548 +09:00	rootdc1.offsec.lan	770	critical	Mimikatz Use	
2021-05-20 21:49:31.863 +09:00	fs01.offsec.lan	1102	high	Security log was cleared	User: admmig
2021-05-20 21:49:46.875 +09:00	fs01.offsec.lan	4648	informational	Explicit Logon	Source User: FS01\$: Target User: sshd_5848 : IP Address: - : Pr
2021-05-20 21:49:46.876 +09:00	fs01.offsec.lan	4624	low	Logon Type 5 - Service	User: sshd_5848 : Workstation: - : IP Address: - : Port: - : Logo
2021-05-20 21:49:46.876 +09:00	fs01.offsec.lan	4672	informational	Admin Logon	User: sshd_5848 : LogonID: 0x3c569ed
2021-05-20 21:49:52.315 +09:00	fs01.offsec.lan	4776	informational	NTLM Logon to Local Account	User: NOUSER : Workstation FS01 : Status: 0xc0000064
2021-05-20 21:49:52.315 +09:00	fs01.offsec.lan	4625	informational	Logon Failure - Username does not exist	User: NOUSER : Type: 8 : Workstation: FS01 : IP Address: - : S

Timeline Explorer

Highly recommended over Excel.

A CSV timeline analysis tool written in C# by Eric Zimmerman.

It is faster than Excel and has more useful features for forensic analysis.

You can download it from:

<https://ericzimmerman.github.io/#!index.md>

※The only downside is that it runs on Windows only.

Timeline Explorer

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

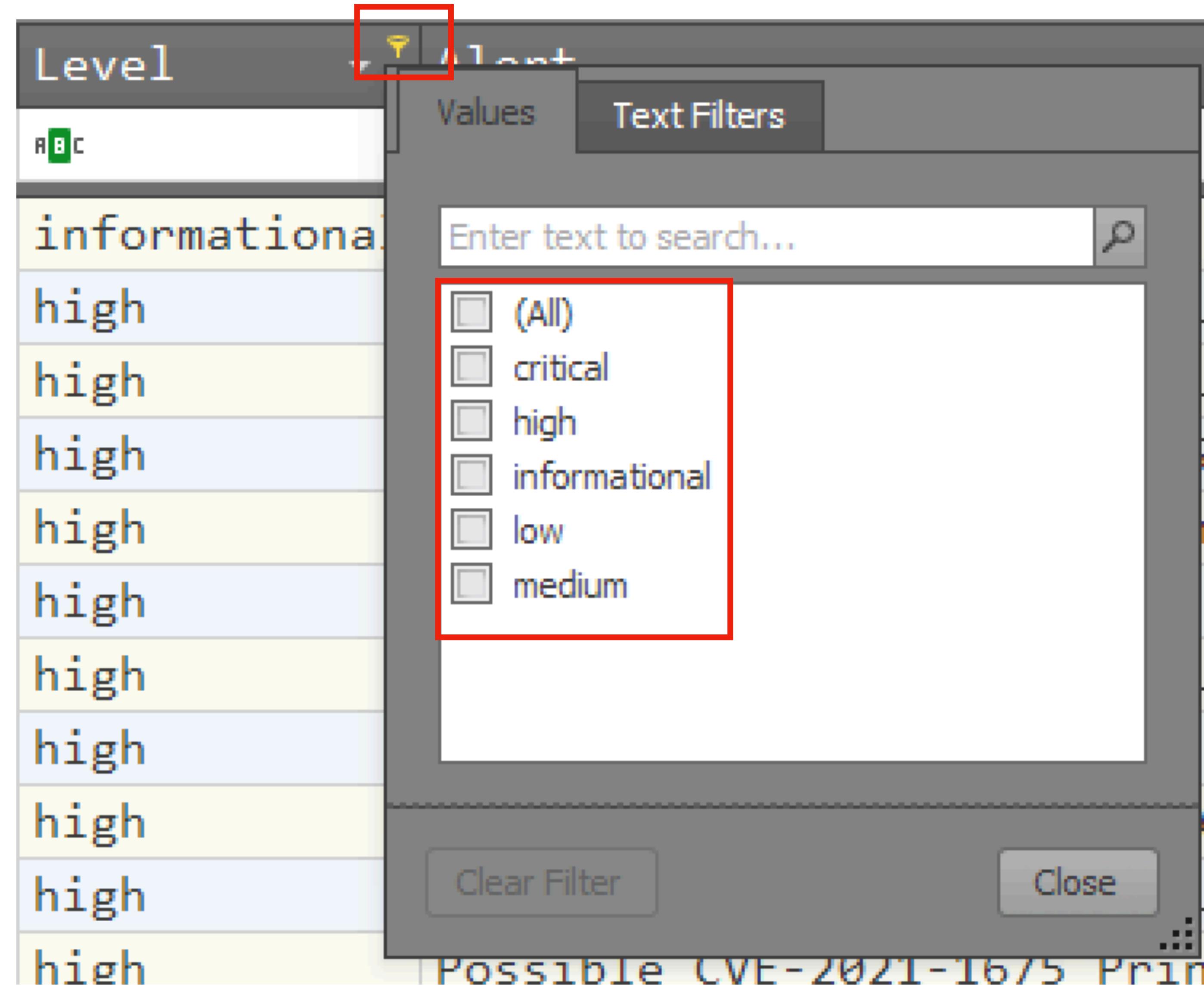
2021-12-20-sample-evtx-results.csv

Drag a column header here to group by that column

Enter text to search... Find

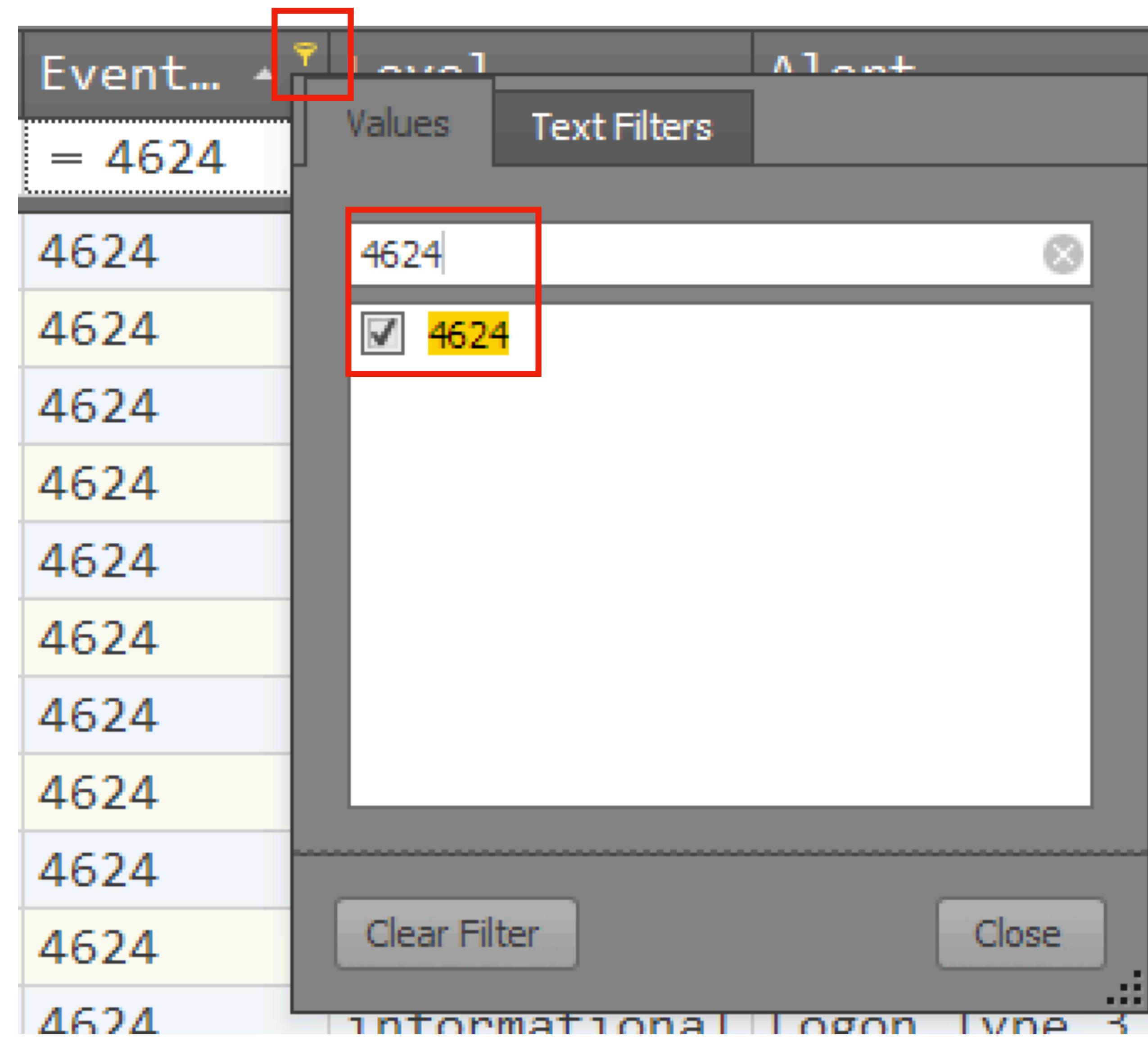
Time	Computername	Eventid	Level	Alert
2013-10-24 01:16:13.843 +09:00	37L4247D28-05	4624	informational	Logon Type 0 - System
2013-10-24 01:16:29.000 +09:00	37L4247D28-05	4625	medium	Failed Logon From Public IP
2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Not Existing File
2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution Of Other File Type Than .exe
2013-10-24 01:18:09.203 +09:00	37L4247D28-05	2003	low	USB Device Plugged
2013-10-24 01:18:33.828 +09:00	IE8Win7	1	high	Execution Of Not Existing File
2013-10-24 01:18:33.828 +09:00	IE8Win7	1	high	Execution Of Other File Type Than .exe
2013-10-24 01:18:50.500 +09:00	IE8Win7	4624	informational	Logon Type 0 - System
2013-10-24 01:21:30.000 +09:00	IE8Win7	4625	medium	Failed Logon From Public IP
2013-10-24 01:21:33.630 +09:00	IE8Win7	1	high	Execution Of Not Existing File
2013-10-24 01:21:33.630 +09:00	IE8Win7	1	high	Execution Of Other File Type Than .exe
2013-10-24 01:21:33.630 +09:00	IE8Win7	4616	medium	Unauthorized System Time Modification
2013-10-24 01:22:39.911 +09:00	IE8Win7	1	high	Execution Of Not Existing File
2013-10-24 01:22:39.911 +09:00	IE8Win7	1	high	Execution Of Other File Type Than .exe
2013-10-24 01:22:39.911 +09:00	IE8Win7	4616	medium	Unauthorized System Time Modification
2013-10-24 01:22:39.973 +09:00	IE8Win7	4720	medium	Local user account created
2013-10-24 01:22:39.973 +09:00	IE8Win7	4720	medium	Local user account created
2013-10-24 01:22:40.004 +09:00	IE8Win7	4732	high	User added to local Administrators gro

Filtering by Level:



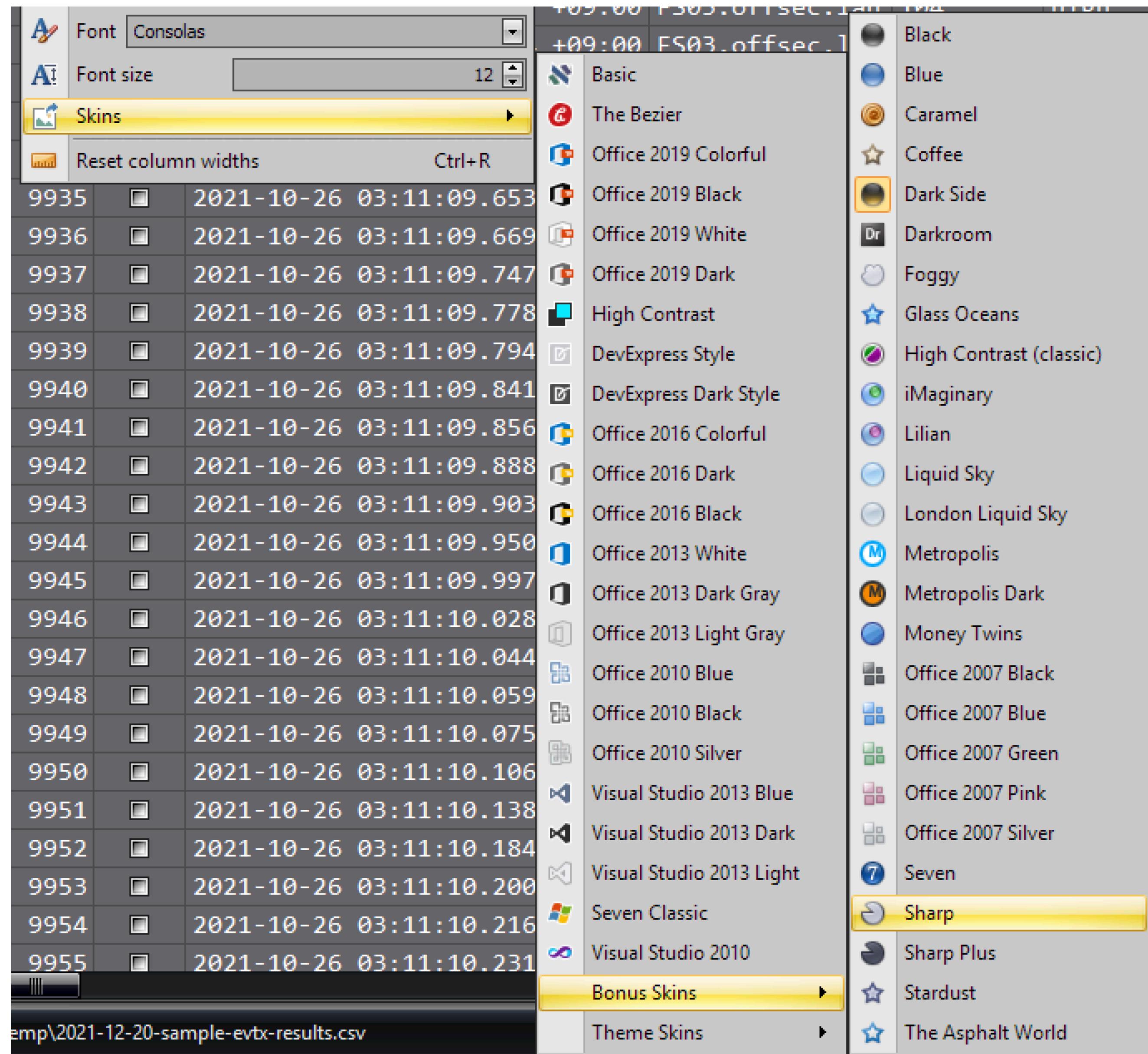
Time	Computername	Eventid	Level	Alert
			= critical	
2019-03-26 06:28:45.025 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.025 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.026 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.026 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.026 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.026 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.026 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-04-29 01:29:42.988 +09:00	IEWIN7	10	critical	Mimikatz Use
2019-04-30 05:59:14.447 +09:00	IEWIN7	18	critical	Malicious Named Pipe
2019-05-01 03:08:29.138 +09:00	Sec504Student	4673	critical	Mimikatz Use
2019-05-01 03:08:29.138 +09:00	Sec504Student	4673	critical	Mimikatz Use
2019-05-01 03:08:29.138 +09:00	Sec504Student	4673	critical	Mimikatz Use
2019-05-01 03:08:29.138 +09:00	Sec504Student	4673	critical	Mimikatz Use
2019-05-01 05:26:51.981 +09:00	IEWIN7	13	critical	CobaltStrike Service Installations in Registry
2019-05-09 10:59:29.090 +09:00	IEWIN7	1	critical	UAC Bypass via Event Viewer
2019-05-26 13:01:43.567 +09:00	IEWIN7	1	critical	Suspect Svchost Activity
2019-06-20 02:22:41.709 +09:00	IEWIN7	13	critical	Registry Persistence Mechanisms
2019-06-20 02:22:43.944 +09:00	IEWIN7	13	critical	Registry Persistence Mechanisms
2019-06-20 02:22:45.694 +09:00	IEWIN7	13	critical	Registry Persistence Mechanisms
2019-06-21 16:35:37.329 +09:00	alice.insecurebank.local	11	critical	Dumpert Process Dumper
2019-06-21 16:35:50.259 +09:00	alice.insecurebank.local	11	critical	Dumpert Process Dumper
2019-06-21 16:35:50.729 +09:00	alice.insecurebank.local	11	critical	Dumpert Process Dumper
2019-07-19 23:47:40.706 +09:00	MSEdgeWIN10	1	critical	Shadow Copies Deletion Using Operating Systems Utilities
2019-07-19 23:47:45.585 +09:00	MSEdgeWIN10	1	critical	WannaCry Ransomware
2019-07-19 23:47:45.624 +09:00	MSEdgeWIN10	1	critical	Shadow Copies Deletion Using Operating Systems Utilities
2019-07-19 23:47:45.624 +09:00	MSEdgeWIN10	1	critical	WannaCry Ransomware

Filtering by Event ID:



Time	Computername	Event ID	Level	Alert	Details
		= 4624	=		
2021-05-03 17:58:38.752 +09:00	prtg-mon.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.753 +09:00	prtg-mon.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.753 +09:00	prtg-mon.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.762 +09:00	adfs01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.762 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.771 +09:00	adfs01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.771 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.772 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.773 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.773 +09:00	adfs01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.773 +09:00	adfs01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.774 +09:00	webiis01.offse...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.775 +09:00	webiis01.offse...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-03 17:58:38.775 +09:00	webiis01.offse...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-20 21:49:46.876 +09:00	fs01.offsec.lan	4624	low	Logon Type 5 - Service	User: sshd_5848 : Workstation: - : IP Address: - : Port: -
2021-05-22 05:43:07.153 +09:00	fs01.offsec.lan	4624	low	Logon Type 5 - Service	User: sshd_4332 : Workstation: - : IP Address: - : Port: -
2021-05-26 22:02:27.149 +09:00	mssql01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-05-26 22:02:29.726 +09:00	mssql01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-05-26 22:02:34.373 +09:00	mssql01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-26 22:02:34.379 +09:00	mssql01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-26 22:02:34.379 +09:00	mssql01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-05-26 22:02:34.380 +09:00	mssql01.offsec...	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-06-03 21:18:12.942 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-06-11 06:21:20.636 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : F
2021-06-11 06:21:26.357 +09:00	fs01.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-10-20 22:39:17.315 +09:00	FS03.offsec.lan	4624	informational	Logon Type 9 - NewCredentials	User: admmig : Workstation: - : IP Address: ::1 : Port: 0
2021-10-20 22:39:17.315 +09:00	FS03.offsec.lan	4624	medium	Pass the Hash Activity 2	
2021-10-20 22:39:17.315 +09:00	FS03.offsec.lan	4624	high	Successful Overpass the Hash Attempt	
2021-10-20 23:29:09.758 +09:00	FS03.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-10-20 23:29:09.773 +09:00	FS03.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-10-20 23:29:09.836 +09:00	FS03.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-10-20 23:29:09.898 +09:00	FS03.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F
2021-10-20 23:29:09.961 +09:00	FS03.offsec.lan	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.123.11 : F

Lots of skins!



Group by Computer Name:

Drag a column header here to group by that column

Line	Tag	Computername	Time	Eventid	Level	Alert
		ドラッグ & ドロップ	+09:00	1	high	WMI Spawning Windows PowerShell
			+09:00	1	low	Non Interactive PowerShell
10062	fs03vuln.offse...	2021-11-09 00:01:27.604	+09:00	1	high	Suspicious PowerShell Parent Process
10061	fs03vuln.offse...	2021-11-09 00:01:27.604	+09:00	1	high	Wmiprvse Spawning Process
10060	fs03vuln.offse...	2021-11-09 00:01:27.604	+09:00	1	high	Process Creation Sysmon Rule Alert
10059	fs03vuln.offse...	2021-11-02 23:15:23.676	+09:00	1102	high	Security log was cleared
10058	FS03.offsec.lan	2021-10-28 22:41:21.325	+09:00	1	high	Abused Debug Privilege by Arbitrary ...
10057	FS03.offsec.lan	2021-10-28 22:41:21.325	+09:00	1	high	Process Creation Sysmon Rule Alert
10056	FS03.offsec.lan	2021-10-27 19:34:50.024	+09:00	4674	critical	Mimikatz Use
10055	FS03.offsec.lan	2021-10-27 19:34:49.837	+09:00	6416	critical	Mimikatz Use
10054	FS03.offsec.lan	2021-10-27 19:28:26.307	+09:00	823	critical	Mimikatz Use
10053	FS03.offsec.lan	2021-10-27 19:28:26.260	+09:00	354	critical	Mimikatz Use
10052	FS03.offsec.lan	2021-10-27 19:28:26.260	+09:00	354	high	Possible CVE-2021-1675 Print Spooler...
10051	fs03vuln.offse...	2021-10-27 19:14:27.559	+09:00	300	critical	Mimikatz Use
10050	fs03vuln.offse...	2021-10-27 19:14:27.559	+09:00	823	critical	Mimikatz Use
10049	fs03vuln.offse...	2021-10-27 19:14:27.466	+09:00	5142	critical	Mimikatz Use
10048	fs03vuln.offse...	2021-10-27 19:14:27.466	+09:00	848	critical	Mimikatz Use
10047	fs03vuln.offse...	2021-10-27 19:14:27.403	+09:00	4674	critical	Mimikatz Use
10046	fs03vuln.offse...	2021-10-27 19:14:27.403	+09:00	823	critical	Mimikatz Use

Grouping by Computer Name:

Computername						
Line	Tag	Time	Eventid	Level	Alert	Details
7	=	■ RBC	=	=	RBC	RBC
	+ Computername: 2012r2srv.maincorp.local (Count: 1)					
	+ Computername: 2016dc.hqcorp.local (Count: 1)					
➤	⊖ Computername: 37L4247D28-05 (Count: 5)					
5	□	2013-10-24 01:18:09.203 +09:00	2003	low	USB Device Plugged	
4	□	2013-10-24 01:17:44.109 +09:00	1	high	Execution Of Other File Type Than .e...	
3	□	2013-10-24 01:17:44.109 +09:00	1	high	Execution Of Not Existing File	
2	□	2013-10-24 01:16:29.000 +09:00	4625	medium	Failed Logon From Public IP	
1	□	2013-10-24 01:16:13.843 +09:00	4624	informational	Logon Type 0 - System	Bootup
	+ Computername: adfs01.offsec.lan (Count: 6)					
	+ Computername: alice.insecurebank.local (Count: 18)					
	+ Computername: atacore01.offsec.lan (Count: 6)					
	+ Computername: atanids01.offsec.lan (Count: 6)					
	+ Computername: DC1.insecurebank.local (Count: 35)					
	+ Computername: DC-Server-1.labcorp.local (Count: 24)					

Grouping by Event ID:

Eventid	Line	Tag	Computername	Time	Level	Alert
+	=	■	RBC	RBC	=	RBC
+	Eventid: 1 (Count: 2,370)					
+	Eventid: 10 (Count: 118)					
+	Eventid: 104 (Count: 97)					
+	Eventid: 11 (Count: 20)					
+	Eventid: 1102 (Count: 55)					
+	Eventid: 1116 (Count: 35)					
+	Eventid: 1117 (Count: 9)					
+	Eventid: 12 (Count: 34)					
+	Eventid: 13 (Count: 60)					
+	Eventid: 150 (Count: 6)					
+	Eventid: 17 (Count: 4)					
+	Eventid: 18 (Count: 6)					
>	Eventid: 20 (Count: 1)	5542	PC04.example.c...	2019-04-04 03:11:54.178 +09:00	high	Suspicious Scripting in a WMI Consumer
+	Eventid: 2003 (Count: 4)					

Grouping by Level:

A screenshot of a log viewer application. At the top, there is a header bar with a search field containing the text "Level" and an upward arrow icon, which is highlighted with a red box. Below the header is a table with four columns: "Line", "Tag", "Computername", and "Eventid". The first row shows a magnifying glass icon, an equals sign, an orange square icon, and a green square icon. The second row is expanded, showing a plus sign, the text "Level: critical (Count: 134)", and two additional collapsed items: "Level: high (Count: 1,350)" and "Level: informational (Count: 4,414)". The third row is collapsed, showing a plus sign and the text "Level: low (Count: 3,725)". The fourth row is collapsed, showing a plus sign and the text "Level: medium (Count: 444)".

Line	Tag	Computername	Eventid
≡ =	■	ABC	=
➤ +	Level: critical (Count: 134)		
	+ Level: high (Count: 1,350)		
	+ Level: informational (Count: 4,414)		
	+ Level: low (Count: 3,725)		
	+ Level: medium (Count: 444)		

Grouping by Alert:

Alert					
	Line	Tag	Computername	Level	Eventid
					Time
▼	=	■ ABC		=	= ABC
▶	+ Alert: Abused Debug Privilege by Arbitrary Parent Processes	(Count: 11)			
	+ Alert: Accessing WinAPI in PowerShell	(Count: 2)			
	+ Alert: Accessing WinAPI in PowerShell for Credentials Dumping	(Count: 4)			
	+ Alert: Accessing WinAPI in PowerShell. Code Injection.	(Count: 93)			
	+ Alert: Active Directory User Backdoors	(Count: 16)			
	+ Alert: AD Privileged Users or Groups Reconnaissance	(Count: 11)			
	+ Alert: AD User Enumeration	(Count: 18)			
	+ Alert: Addition of SID History to Active Directory Object	(Count: 1)			
	+ Alert: Admin Logon	(Count: 76)			
	+ Alert: Admin User Remote Logon	(Count: 1)			
	+ Alert: Always Install Elevated MSI Spawns Cmd And Powershell	(Count: 1)			

Tag alerts and events that relevant to your investigation:

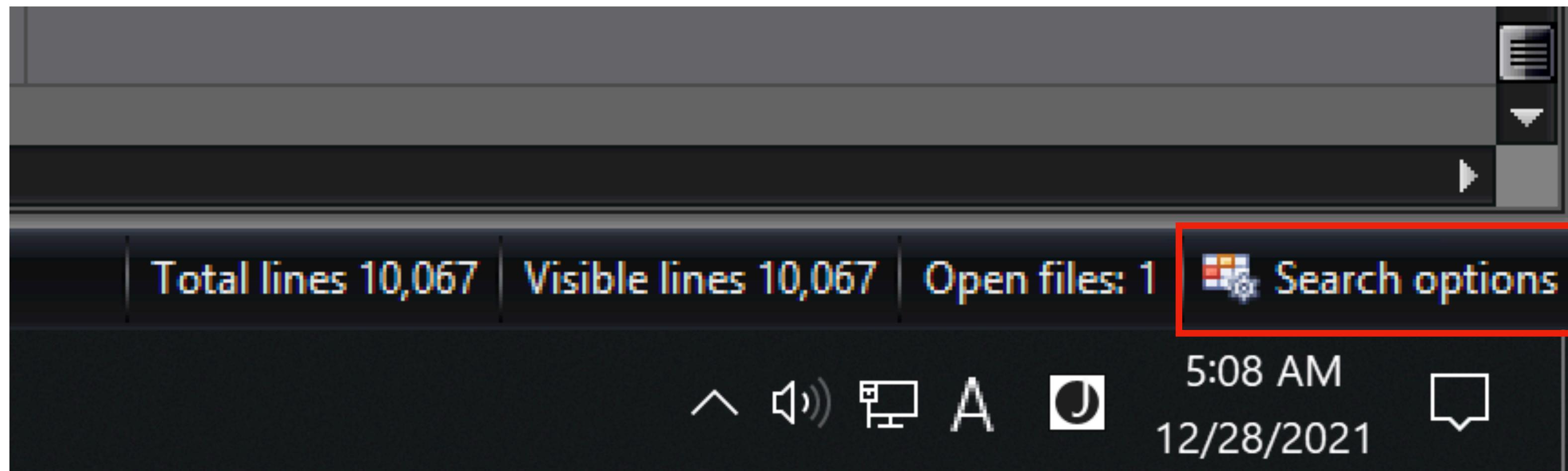
Drag a column header here to group by that column

Line	Tag	Computername	Time	Eventid	Level	Alert
10064	fs03vuln.offsec.lan	2021-11-09 00:01:27.604 +09:00	1	high	WMI Spawning Windows PowerShell	
10063	fs03vuln.offsec.lan	2021-11-09 00:01:27.604 +09:00	1	low	Non Interactive PowerShell	
10062	fs03vuln.offsec.lan	2021-11-09 00:01:27.604 +09:00	1	high	Suspicious PowerShell Parent Process	
10061	fs03vuln.offsec.lan	2021-11-09 00:01:27.604 +09:00	1	high	Wmiprvse Spawning Process	
10060	fs03vuln.offsec.lan	2021-11-09 00:01:27.604 +09:00	1	high	Process Creation Sysmon Rule Alert	
10059	fs03vuln.offsec.lan	2021-11-02 23:15:23.676 +09:00	1102	high	Security log was cleared	
10058	FS03.offsec.lan	2021-10-28 22:41:21.325 +09:00	1	high	Abused Debug Privilege by Arbitrary ...	
10057	FS03.offsec.lan	2021-10-28 22:41:21.325 +09:00	1	high	Process Creation Sysmon Rule Alert	
10056	FS03.offsec.lan	2021-10-27 19:34:50.024 +09:00	4674	critical	Mimikatz Use	
10055	FS03.offsec.lan	2021-10-27 19:34:49.837 +09:00	6416	critical	Mimikatz Use	
10054	FS03.offsec.lan	2021-10-27 19:28:26.307 +09:00	823	critical	Mimikatz Use	
10053	FS03.offsec.lan	2021-10-27 19:28:26.260 +09:00	354	critical	Mimikatz Use	
10052	FS03.offsec.lan	2021-10-27 19:28:26.260 +09:00	354	high	Possible CVE-2021-1675 Print Spooler...	
10051	fs03vuln.offsec.lan	2021-10-27 19:14:27.559 +09:00	300	critical	Mimikatz Use	
10050	fs03vuln.offsec.lan	2021-10-27 19:14:27.559 +09:00	823	critical	Mimikatz Use	
10049	fs03vuln.offsec.lan	2021-10-27 19:14:27.466 +09:00	5142	critical	Mimikatz Use	
10048	fs03vuln.offsec.lan	2021-10-27 19:14:27.466 +09:00	848	critical	Mimikatz Use	
10047	fs03vuln.offsec.lan	2021-10-27 19:14:27.403 +09:00	4674	critical	Mimikatz Use	
10046	fs03vuln.offsec.lan	2021-10-27 19:14:27.403 +09:00	823	critical	Mimikatz Use	

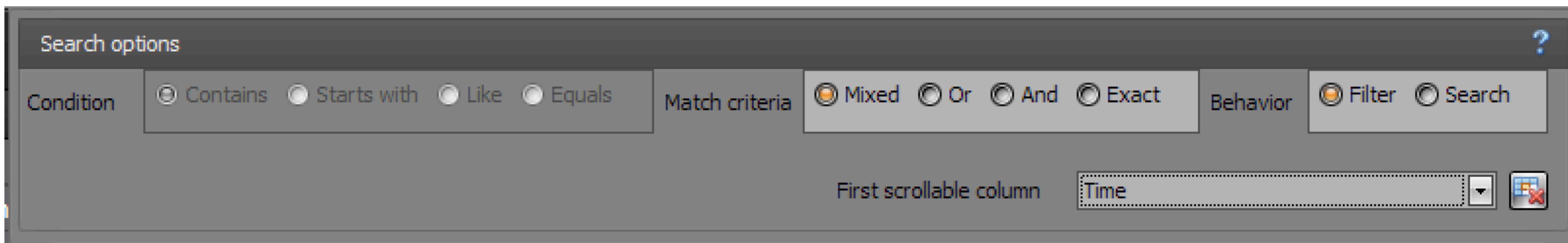
Grouping by Tags:

Freezing rows

1. Click on "Search options" in the bottom right corner:



2. Change "First scrollable column" to "Time":



The Time row will now be frozen:

Time	Level	Eventid	Alert	Details
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Not Existing File	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Other File Type Than .exe	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Not Existing File	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Other File Type Than .exe	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Not Existing File	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Other File Type Than .exe	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Not Existing File	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Other File Type Than .exe	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Not Existing File	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Other File Type Than .exe	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Not Existing File	
2021-08-17 21:26:51.409 +09:00	high	1	Execution Of Other File Type Than .exe	
2021-08-17 21:26:51.409 +09:00	medium	9	Raw Disk Access Using Illegitimate Tools	
2021-08-23 04:33:38.725 +09:00	informational	1	Process Creation	Command: c:\temp\EfsPotato.exe whoami
2021-08-23 04:33:38.844 +09:00	critical	17	EfsPotato Named Pipe	
2021-08-23 04:33:38.884 +09:00	critical	18	EfsPotato Named Pipe	
2021-08-23 04:33:38.905 +09:00	informational	1	Process Creation	Command: whoami : Path: C:\Windows\Sys
2021-08-23 04:33:38.905 +09:00	high	1	Run Whoami as SYSTEM	
2021-08-23 04:33:38.905 +09:00	medium	1	Whoami Execution	
2021-08-23 04:33:38.905 +09:00	low	1	Local Accounts Discovery	

Please check out this page to learn more about Timeline Explorer:

<https://aboutdfir.com/toolsandartifacts/windows/timeline-explorer/2/>