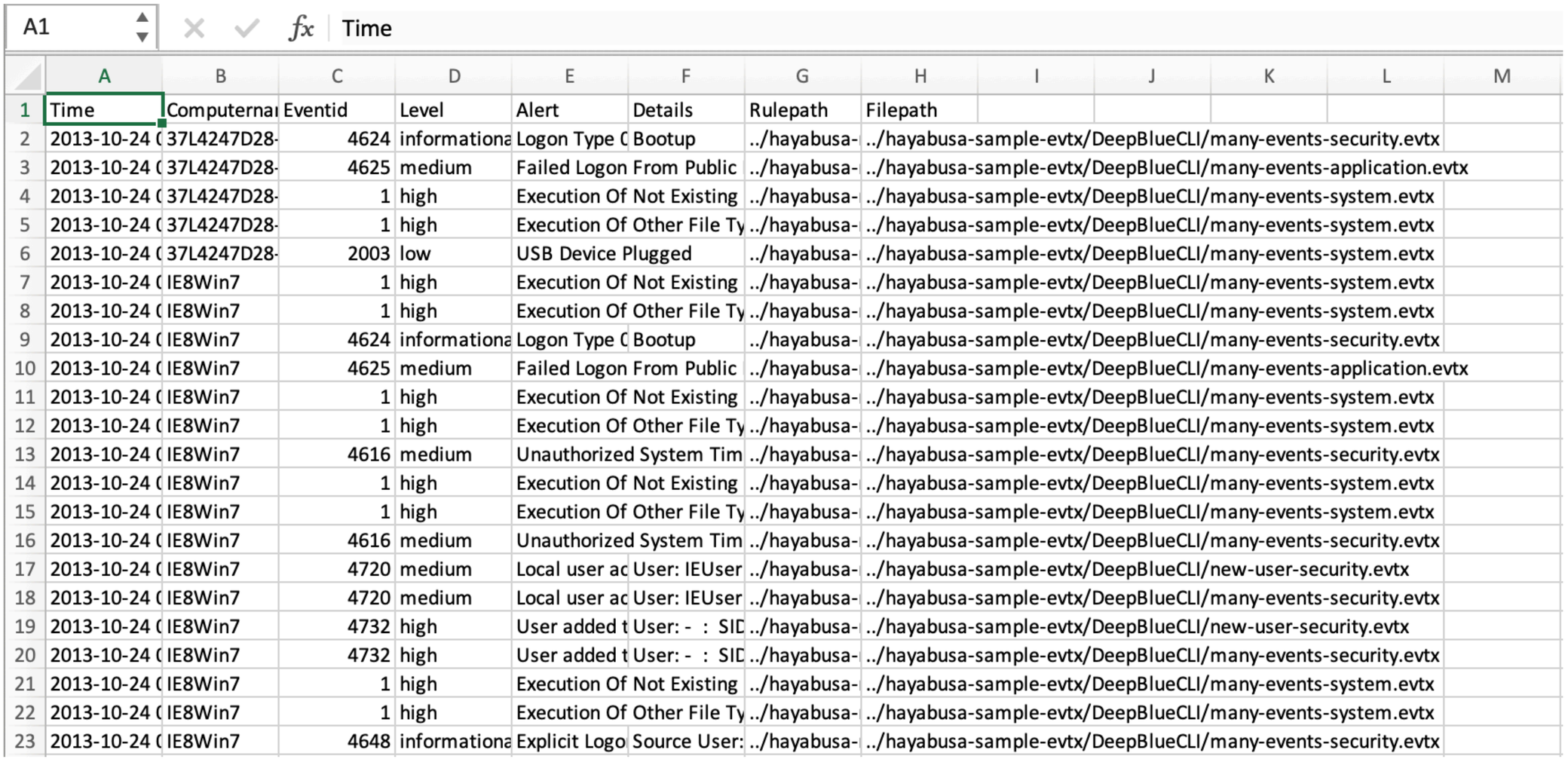
CSV結果をExcelとTimeline Explorerで解析する方法

田中ザック (2021/12/25)

Excel

CSVを開くと、このように表示される：



A1 | Time

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Time	Computernai	Eventid	Level	Alert	Details	Rulepath	Filepath					
2	2013-10-24 (	37L4247D28-	4624	informationa	Logon Type (	Bootup	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
3	2013-10-24 (	37L4247D28-	4625	medium	Failed Logon	From Public	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx					
4	2013-10-24 (	37L4247D28-	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
5	2013-10-24 (	37L4247D28-	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
6	2013-10-24 (	37L4247D28-	2003	low	USB Device	Plugged	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
7	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
8	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
9	2013-10-24 (	IE8Win7	4624	informationa	Logon Type (	Bootup	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
10	2013-10-24 (	IE8Win7	4625	medium	Failed Logon	From Public	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx					
11	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
12	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
13	2013-10-24 (	IE8Win7	4616	medium	Unauthorized	System Tim	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
14	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
15	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
16	2013-10-24 (	IE8Win7	4616	medium	Unauthorized	System Tim	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
17	2013-10-24 (	IE8Win7	4720	medium	Local user ac	User: IEUser	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx					
18	2013-10-24 (	IE8Win7	4720	medium	Local user ac	User: IEUser	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
19	2013-10-24 (	IE8Win7	4732	high	User added t	User: - ： SID	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx					
20	2013-10-24 (	IE8Win7	4732	high	User added t	User: - ： SID	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
21	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
22	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
23	2013-10-24 (	IE8Win7	4648	informationa	Explicit Logo	Source User:	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					

見にくいので左上をクリックして、まず全セルを選択します：

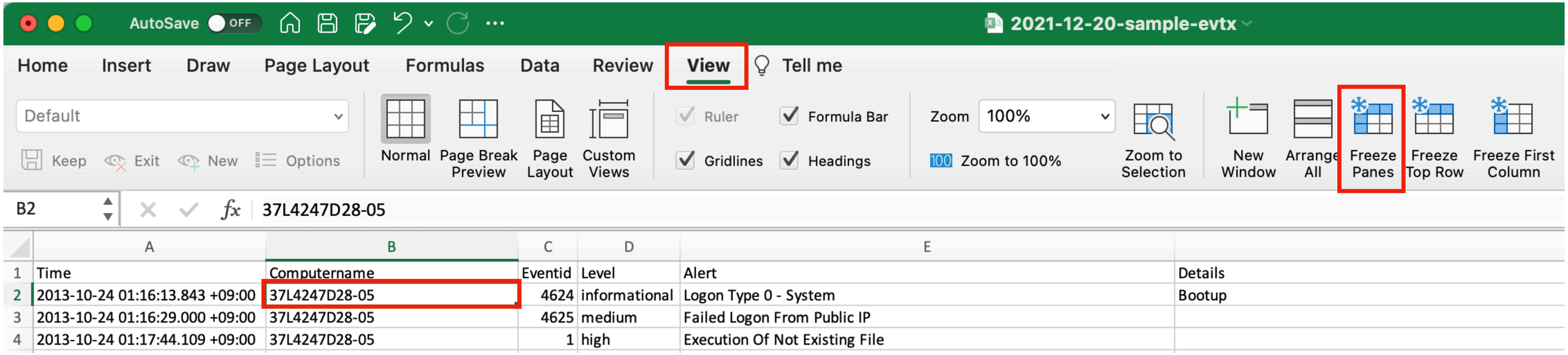
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Time	Computernai	Eventid	Level	Alert	Details	Rulepath	Filepath					
2	2013-10-24 (	37L4247D28-	4624	informationa	Logon Type (	Bootup	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
3	2013-10-24 (	37L4247D28-	4625	medium	Failed Logon	From Public	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx					
4	2013-10-24 (	37L4247D28-	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
5	2013-10-24 (	37L4247D28-	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
6	2013-10-24 (	37L4247D28-	2003	low	USB Device	Plugged	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
7	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
8	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
9	2013-10-24 (	IE8Win7	4624	informationa	Logon Type (	Bootup	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
10	2013-10-24 (	IE8Win7	4625	medium	Failed Logon	From Public	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-application.evtx					
11	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
12	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
13	2013-10-24 (	IE8Win7	4616	medium	Unauthorized	System Tim	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
14	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
15	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
16	2013-10-24 (	IE8Win7	4616	medium	Unauthorized	System Tim	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
17	2013-10-24 (	IE8Win7	4720	medium	Local user ac	User: IEUser	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx					
18	2013-10-24 (	IE8Win7	4720	medium	Local user ac	User: IEUser	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
19	2013-10-24 (	IE8Win7	4732	high	User added t	User: - : SID	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/new-user-security.evtx					
20	2013-10-24 (	IE8Win7	4732	high	User added t	User: - : SID	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-security.evtx					
21	2013-10-24 (	IE8Win7	1	high	Execution Of	Not Existing	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					
22	2013-10-24 (	IE8Win7	1	high	Execution Of	Other File Ty	../hayabusa-	../hayabusa-sample-evtx/DeepBlueCLI/many-events-system.evtx					

AとBの間の線をダブルクリックすると、列の幅が自動的に調整されます：

	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	

幅が広いので、なるべくワイドな
モニターをおすすめします！

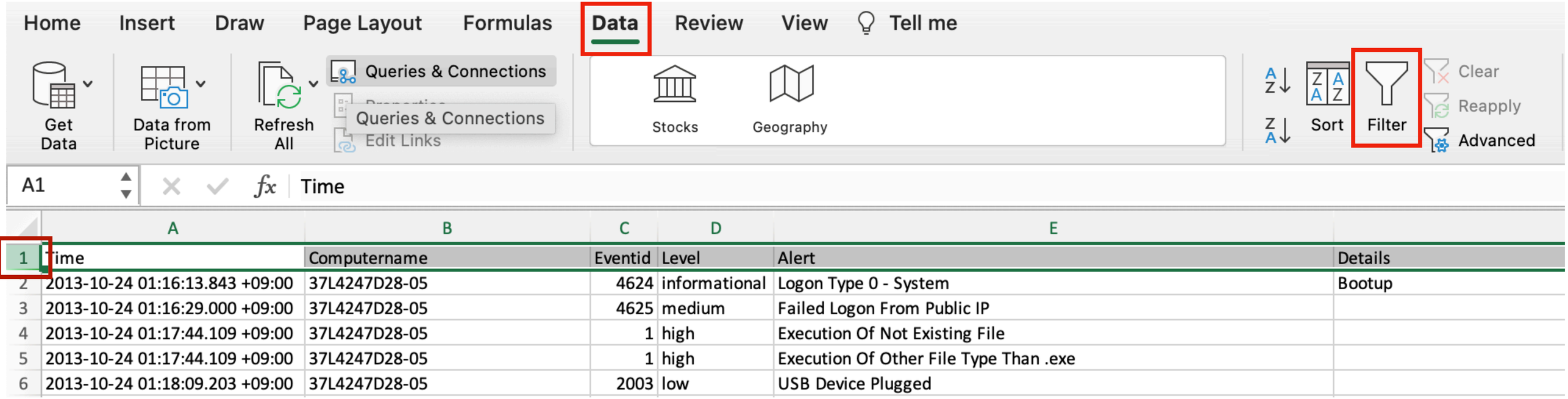
B2セルを選択してから、View→Freeze Panesをクリックすると、タイムスタンプと見出しが固定されるのでおすすめします：



	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	

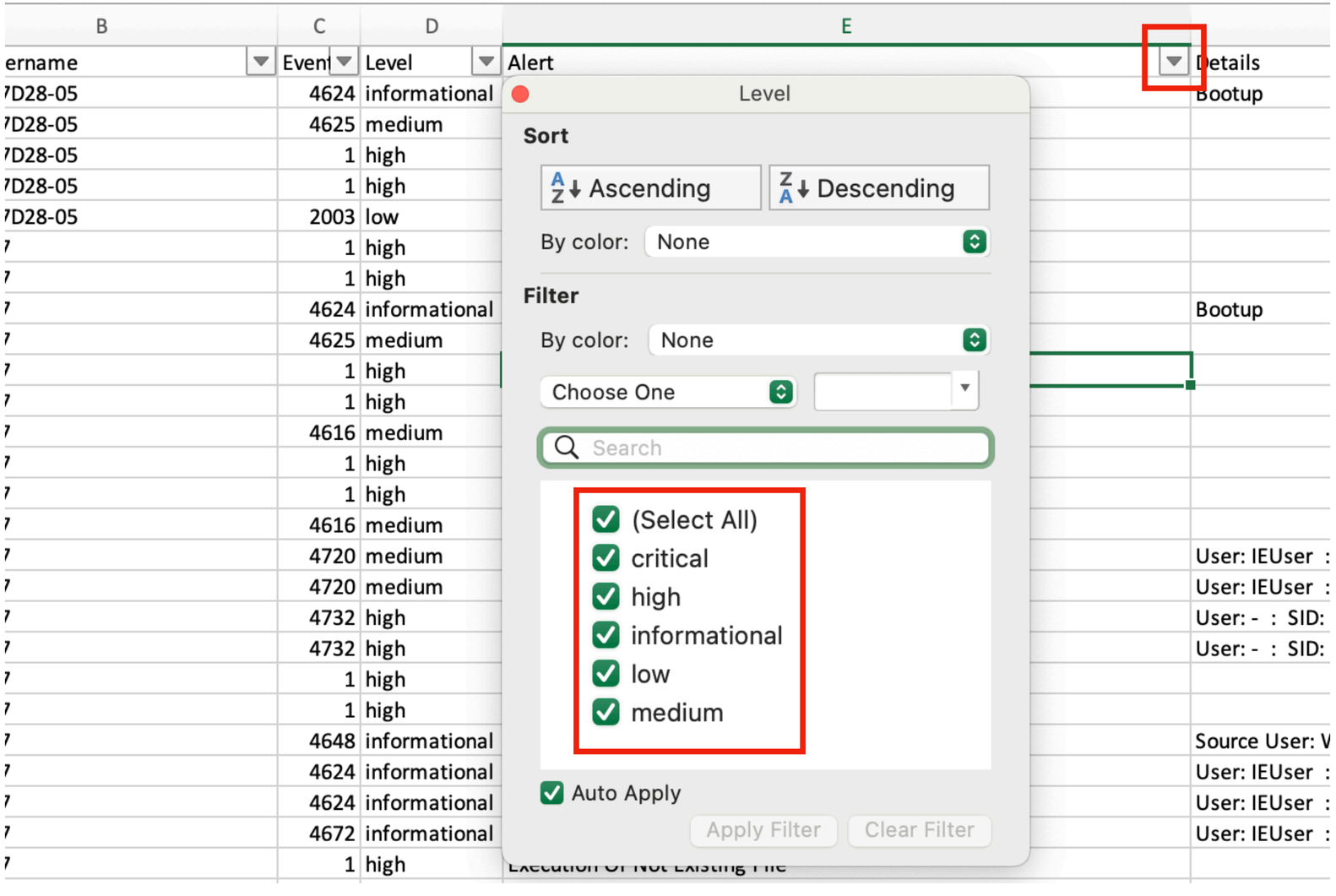
1. 1番目の行を全部選択します

2. Data→Filterをクリックします

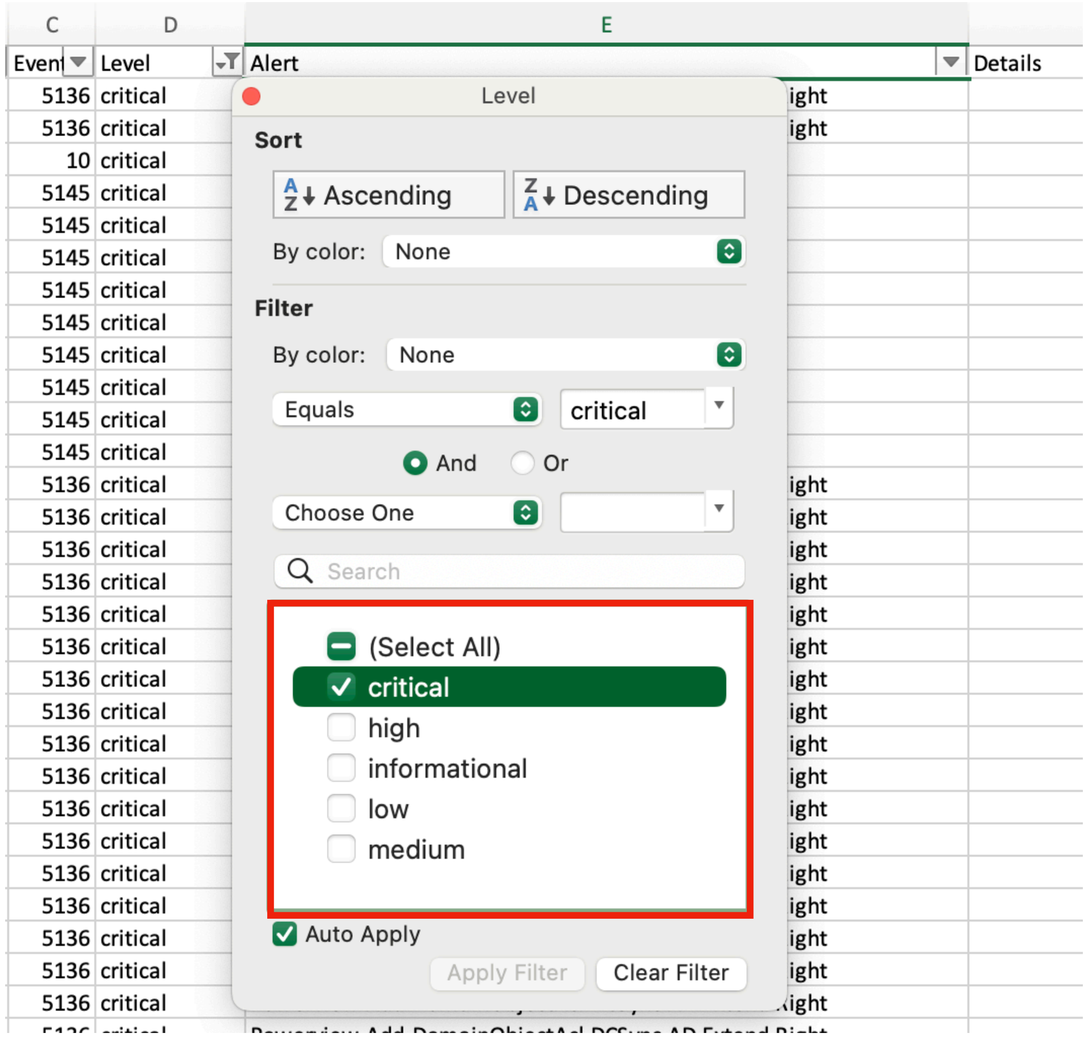


	A	B	C	D	E	
1	Time	Computername	Eventid	Level	Alert	Details
2	2013-10-24 01:16:13.843 +09:00	37L4247D28-05	4624	informational	Logon Type 0 - System	Bootup
3	2013-10-24 01:16:29.000 +09:00	37L4247D28-05	4625	medium	Failed Logon From Public IP	
4	2013-10-24 01:17:44.109 +09:00	37L4247D28-05	1	high	Execution 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	

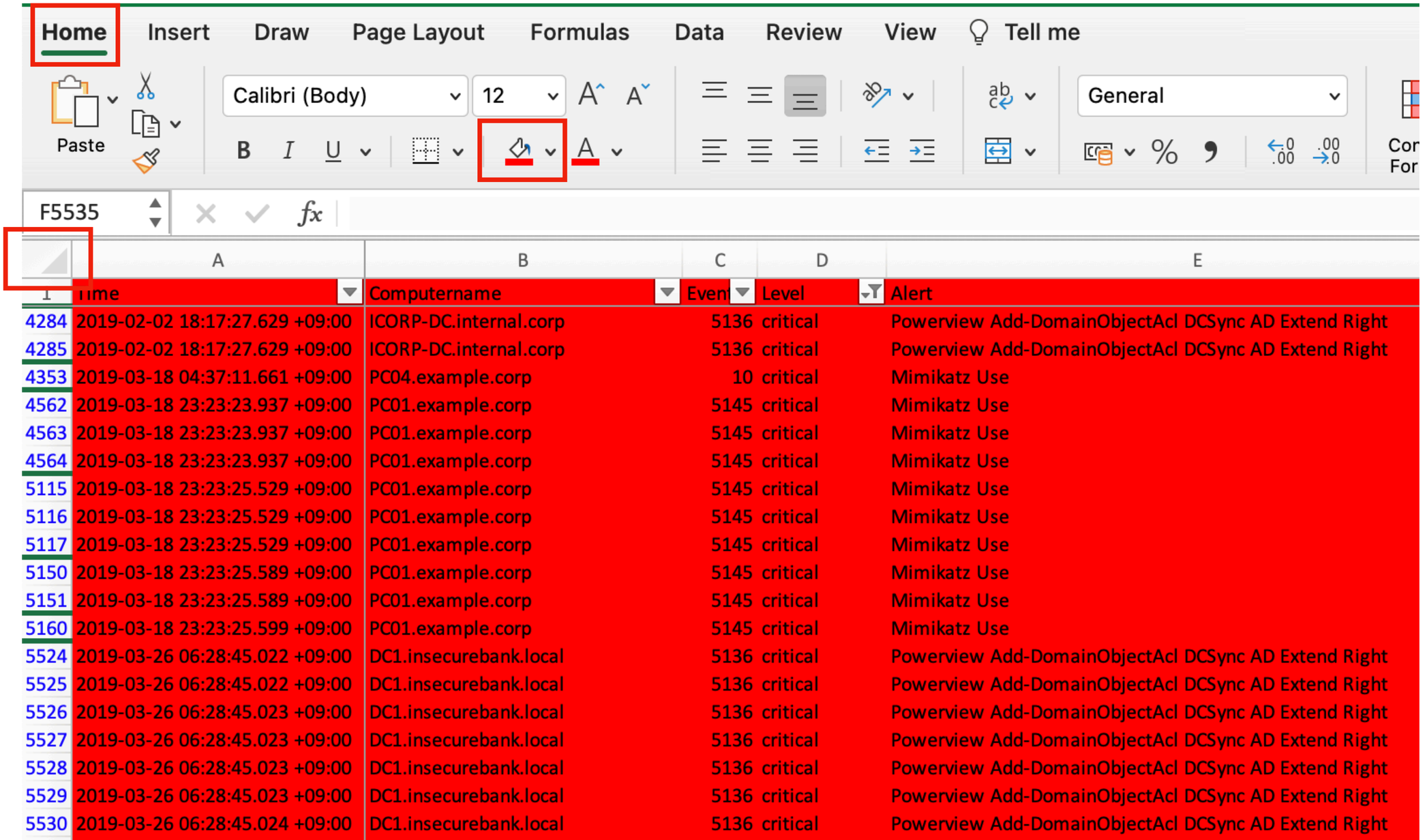
そうすると、深刻度のレベル等でフィルタすることができます。



誤検知もありますが、criticalから順番にアラートを調べることをおすすめします。



各レベルに色を付けるとより分かりやすくなります：



	A	B	C	D	E
1	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
5526	2019-03-26 06:28:45.023 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
5527	2019-03-26 06:28:45.023 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
5528	2019-03-26 06:28:45.023 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
5529	2019-03-26 06:28:45.023 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
5530	2019-03-26 06:28:45.024 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right

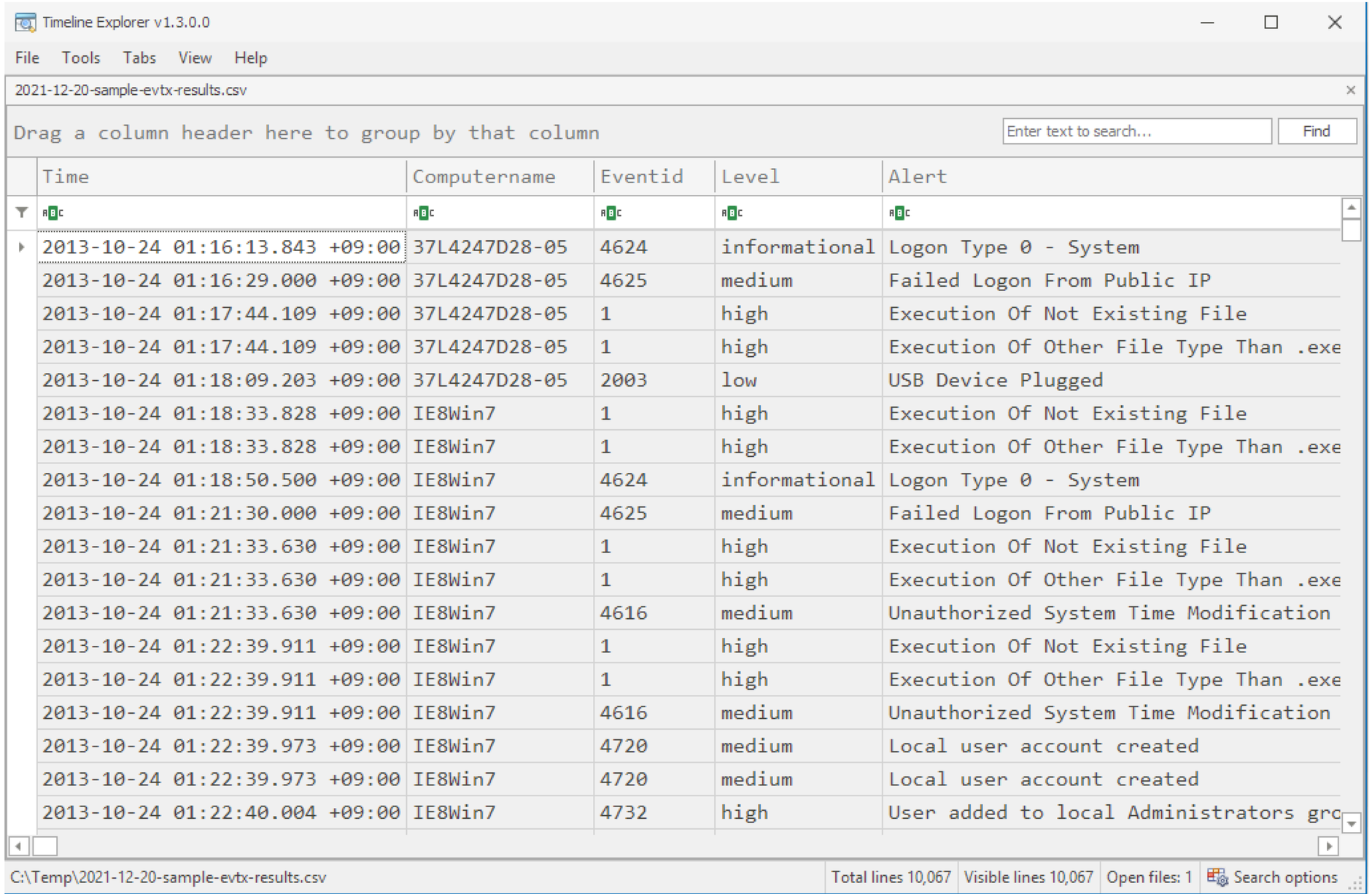
色付け完了

A	B	C	D	E	
Time	Computername	Eventi	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

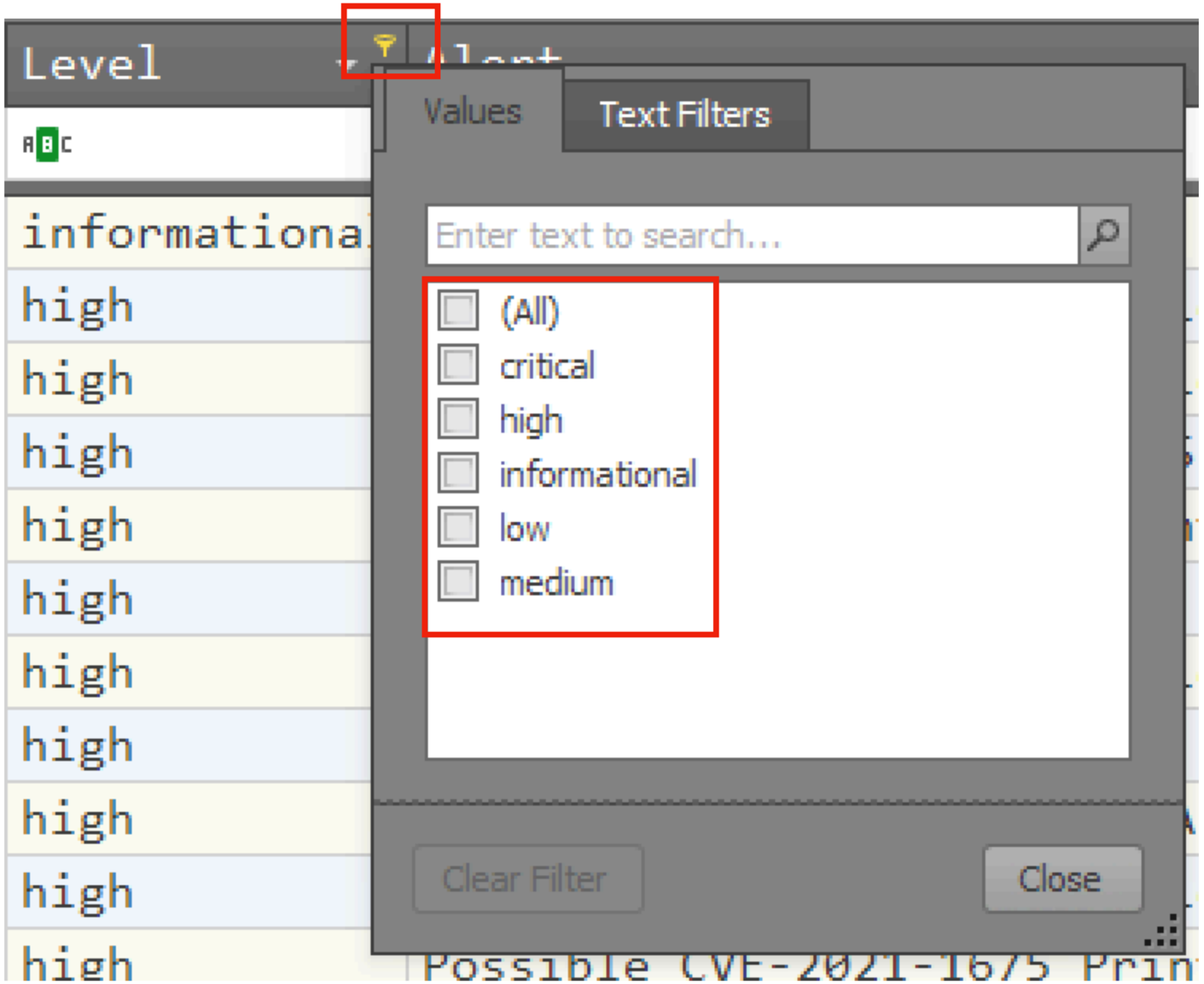
Timeline Explorer

イチオシ！！！
Eric Zimmermanが作ったCSV解析ツール
C#で開発され、Excelより速くて、便利！！
https://ericzimmerman.github.io/#!index.md
からダウンロードできます。
※残念ながら、Windowsのみ・・

Timeline Explorer

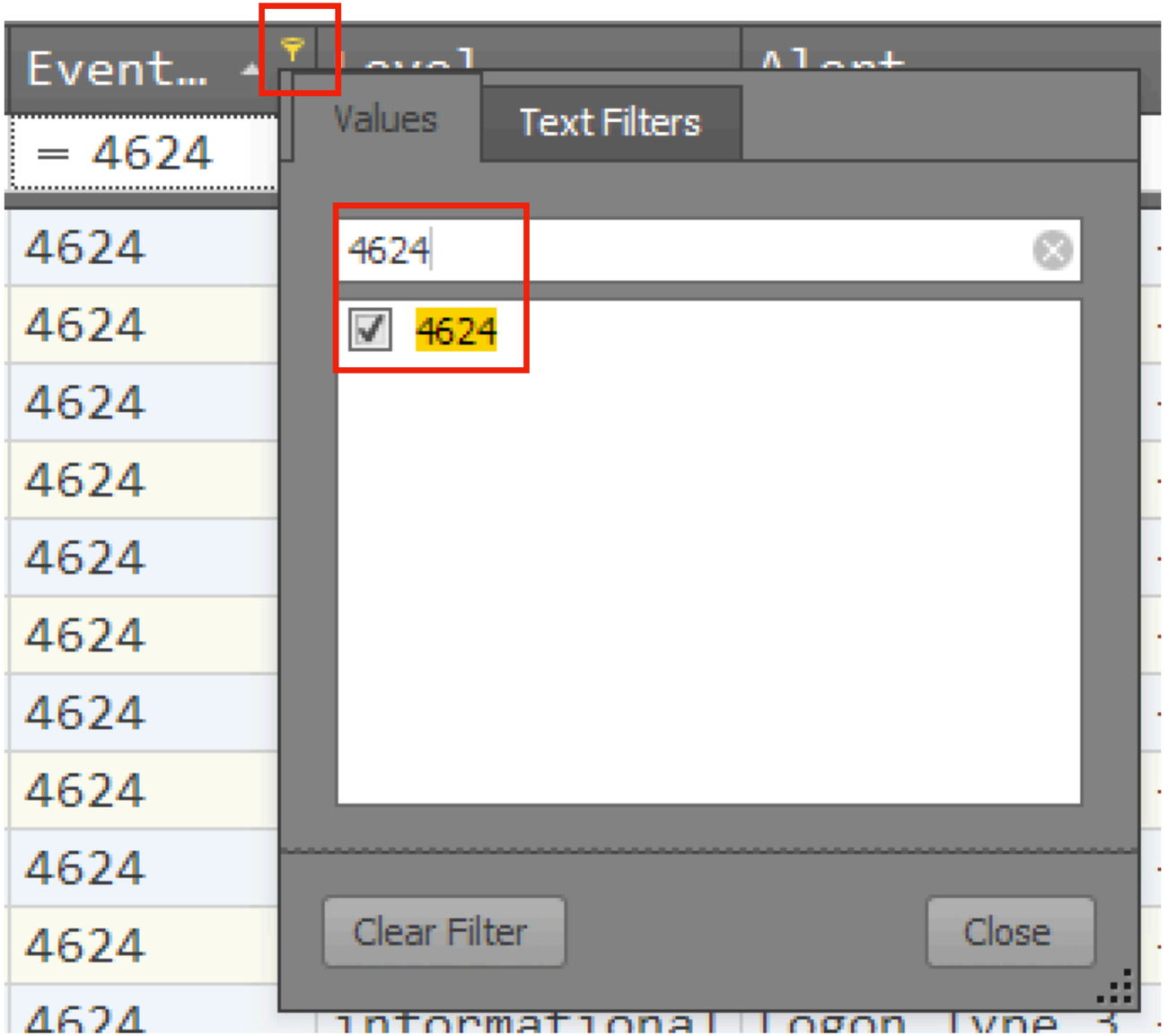


Levelでのフィルタリング



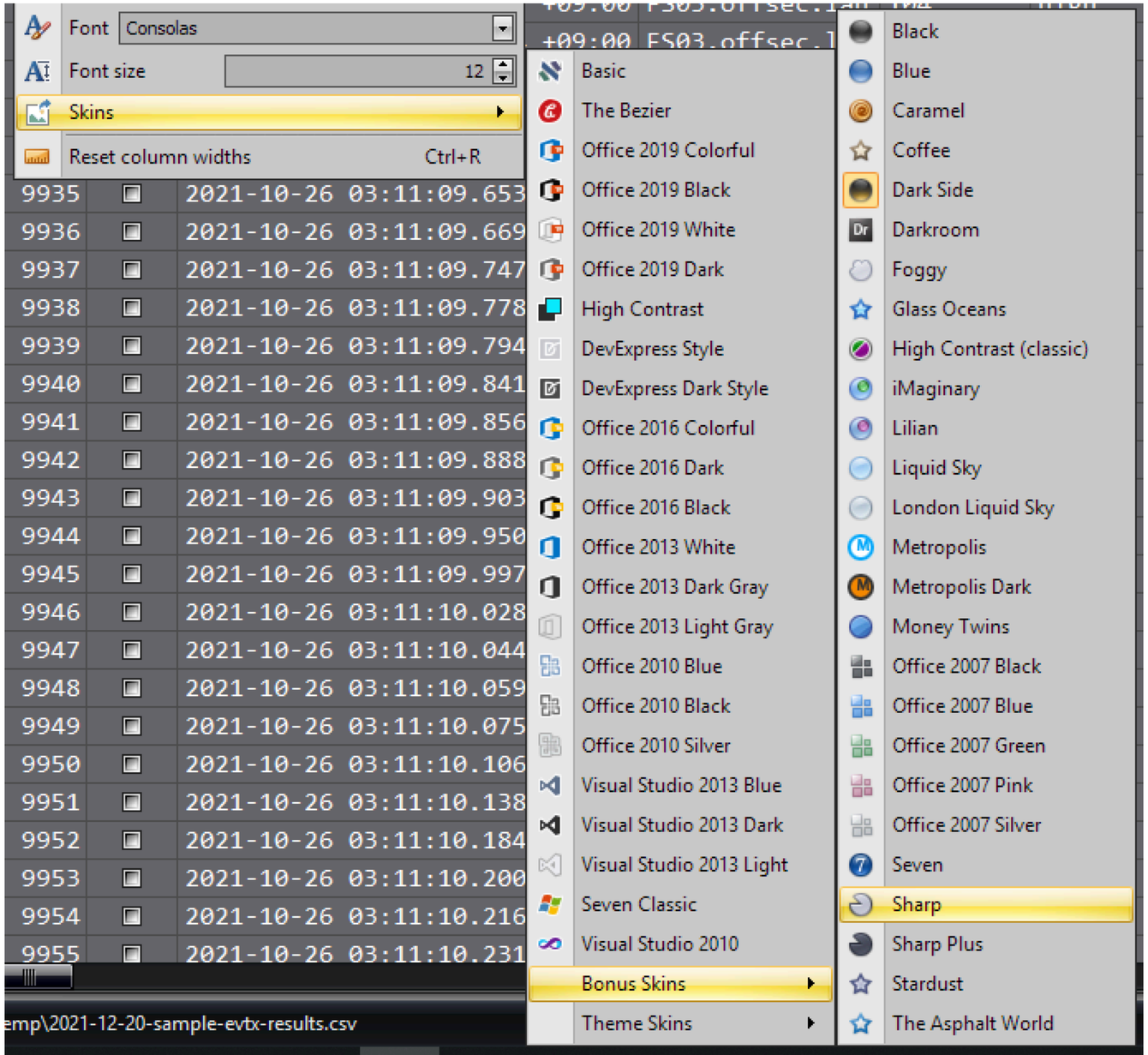
Time	Computername	Eventid	Level	Alert
			= critical	
2019-03-26 06:28:45.025 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 06:28:45.025 +09:00	DC1.insecurebank.local	5136	critical	Powerview Add-DomainObjectAcl DCSync AD Extend Right
2019-03-26 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
2019-04-29 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

イベントIDでのフィルタリング

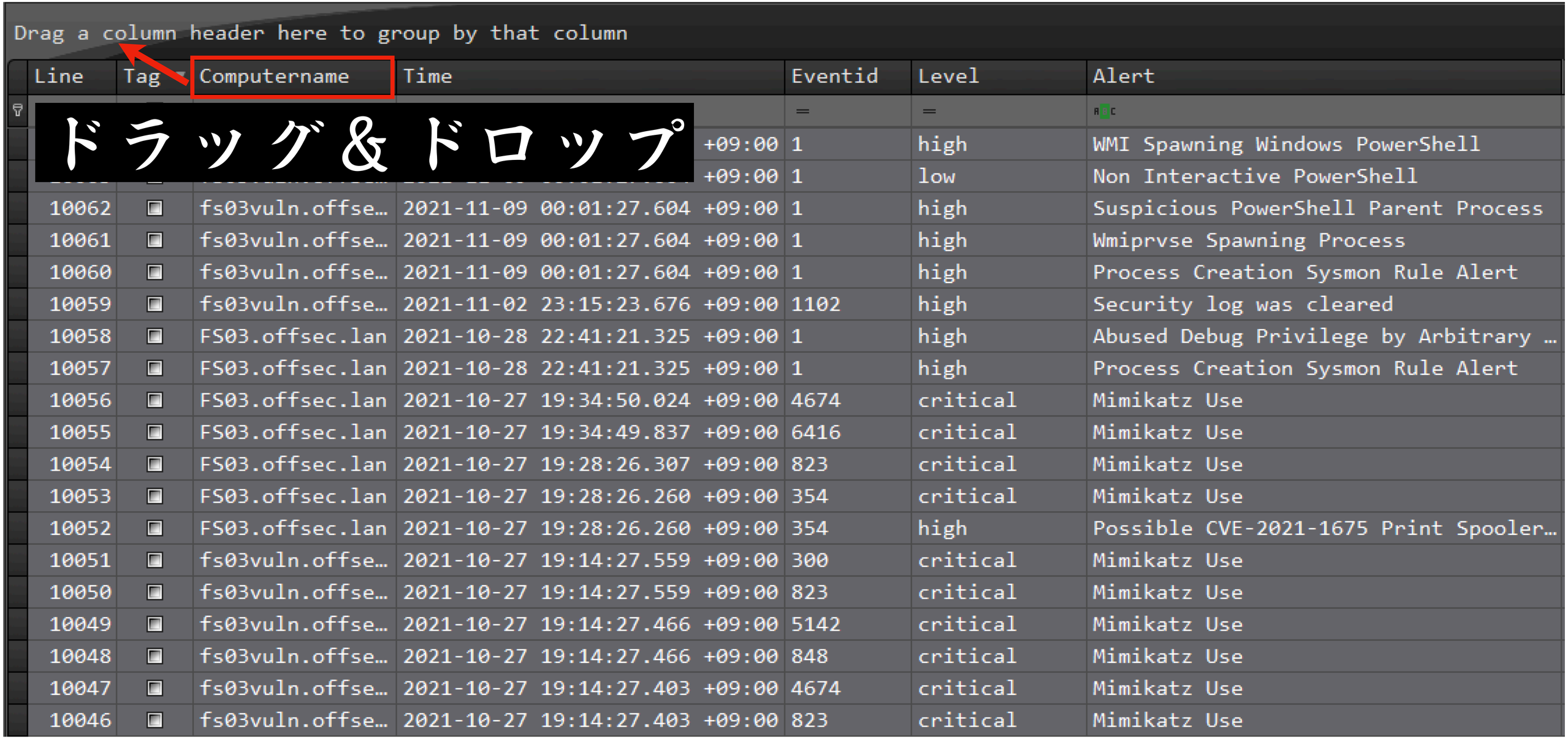


Time	Computername	Event…	Level	Alert	Details
		= 4624	=		
2021-05-03 17:58:38.752 +09:00	prtg-mon.offse…	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : P
2021-05-03 17:58:38.753 +09:00	prtg-mon.offse…	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : P
2021-05-03 17:58:38.753 +09:00	prtg-mon.offse…	4624	informational	Logon Type 3 - Network	User: admmig : Workstation: - : IP Address: 10.23.23.9 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 :
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 :
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 : P
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 : P
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 : P
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 : P
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 : P
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 : P
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 :
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 :
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 :
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 :
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 :
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 :

Skinが沢山！！


Font
Consolas
Font size
12
Skins
Reset column widths
Ctrl+R
9935 2021-10-26 03:11:09.653
9936 2021-10-26 03:11:09.669
9937 2021-10-26 03:11:09.747
9938 2021-10-26 03:11:09.778
9939 2021-10-26 03:11:09.794
9940 2021-10-26 03:11:09.841
9941 2021-10-26 03:11:09.856
9942 2021-10-26 03:11:09.888
9943 2021-10-26 03:11:09.903
9944 2021-10-26 03:11:09.950
9945 2021-10-26 03:11:09.997
9946 2021-10-26 03:11:10.028
9947 2021-10-26 03:11:10.044
9948 2021-10-26 03:11:10.059
9949 2021-10-26 03:11:10.075
9950 2021-10-26 03:11:10.106
9951 2021-10-26 03:11:10.138
9952 2021-10-26 03:11:10.184
9953 2021-10-26 03:11:10.200
9954 2021-10-26 03:11:10.216
9955 2021-10-26 03:11:10.231
emp\2021-12-20-sample-evtx-results.csv
Basic
The Bezier
Office 2019 Colorful
Office 2019 Black
Office 2019 White
Office 2019 Dark
High Contrast
DevExpress Style
DevExpress Dark Style
Office 2016 Colorful
Office 2016 Dark
Office 2016 Black
Office 2013 White
Office 2013 Dark Gray
Office 2013 Light Gray
Office 2010 Blue
Office 2010 Black
Office 2010 Silver
Visual Studio 2013 Blue
Visual Studio 2013 Dark
Visual Studio 2013 Light
Seven Classic
Visual Studio 2010
Bonus Skins
Theme Skins
Black
Blue
Caramel
Coffee
Dark Side
Darkroom
Foggy
Glass Oceans
High Contrast (classic)
iMaginary
Lilian
Liquid Sky
London Liquid Sky
Metropolis
Metropolis Dark
Money Twins
Office 2007 Black
Office 2007 Blue
Office 2007 Green
Office 2007 Pink
Office 2007 Silver
Seven
Sharp
Sharp Plus
Stardust
The Asphalt World

コンピュータ名でのグルーピング



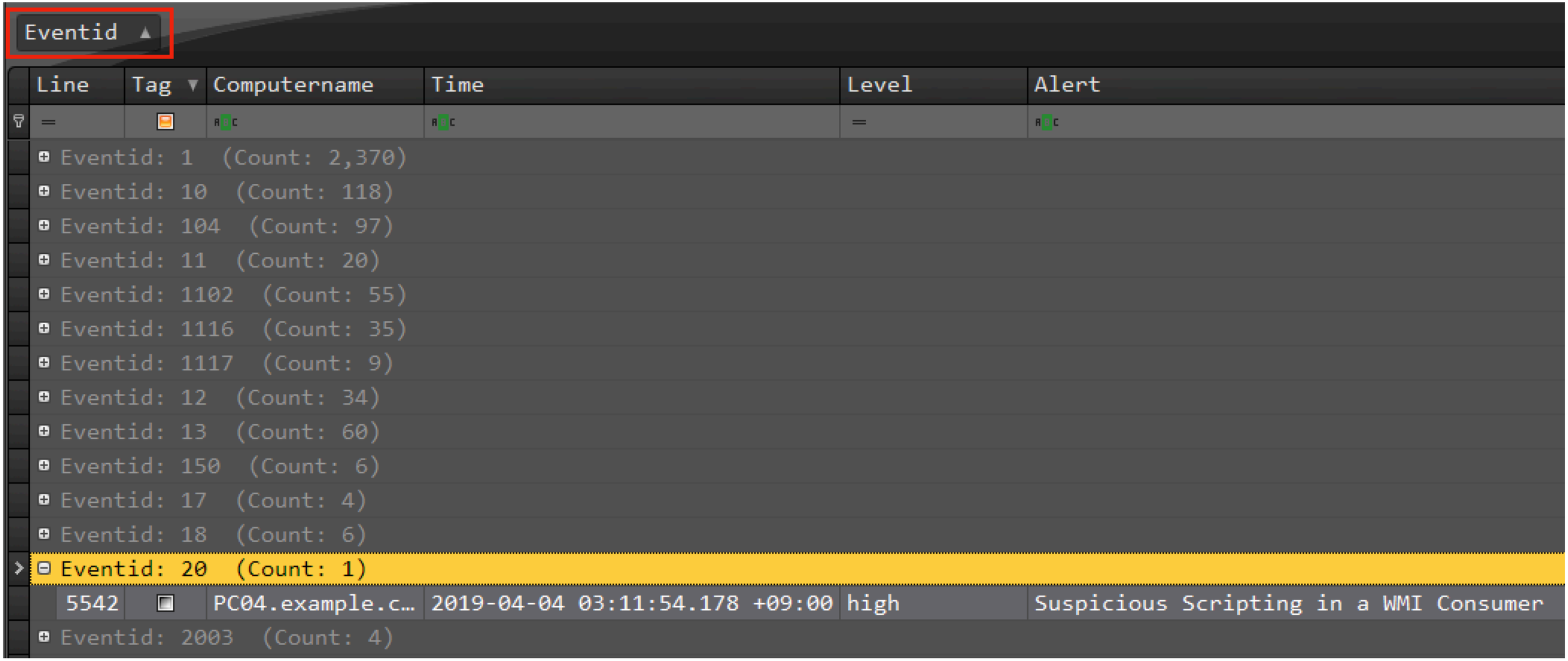
Line	Tag	Computername	Time	Eventid	Level	Alert
				=	=	
			+09:00	1	high	WMI Spawning Windows PowerShell
			+09:00	1	low	Non Interactive PowerShell
10062	☐	fs03vuln.offse…	2021-11-09 00:01:27.604 +09:00	1	high	Suspicious PowerShell Parent Process
10061	☐	fs03vuln.offse…	2021-11-09 00:01:27.604 +09:00	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

コンピュータ名でのグルーピング

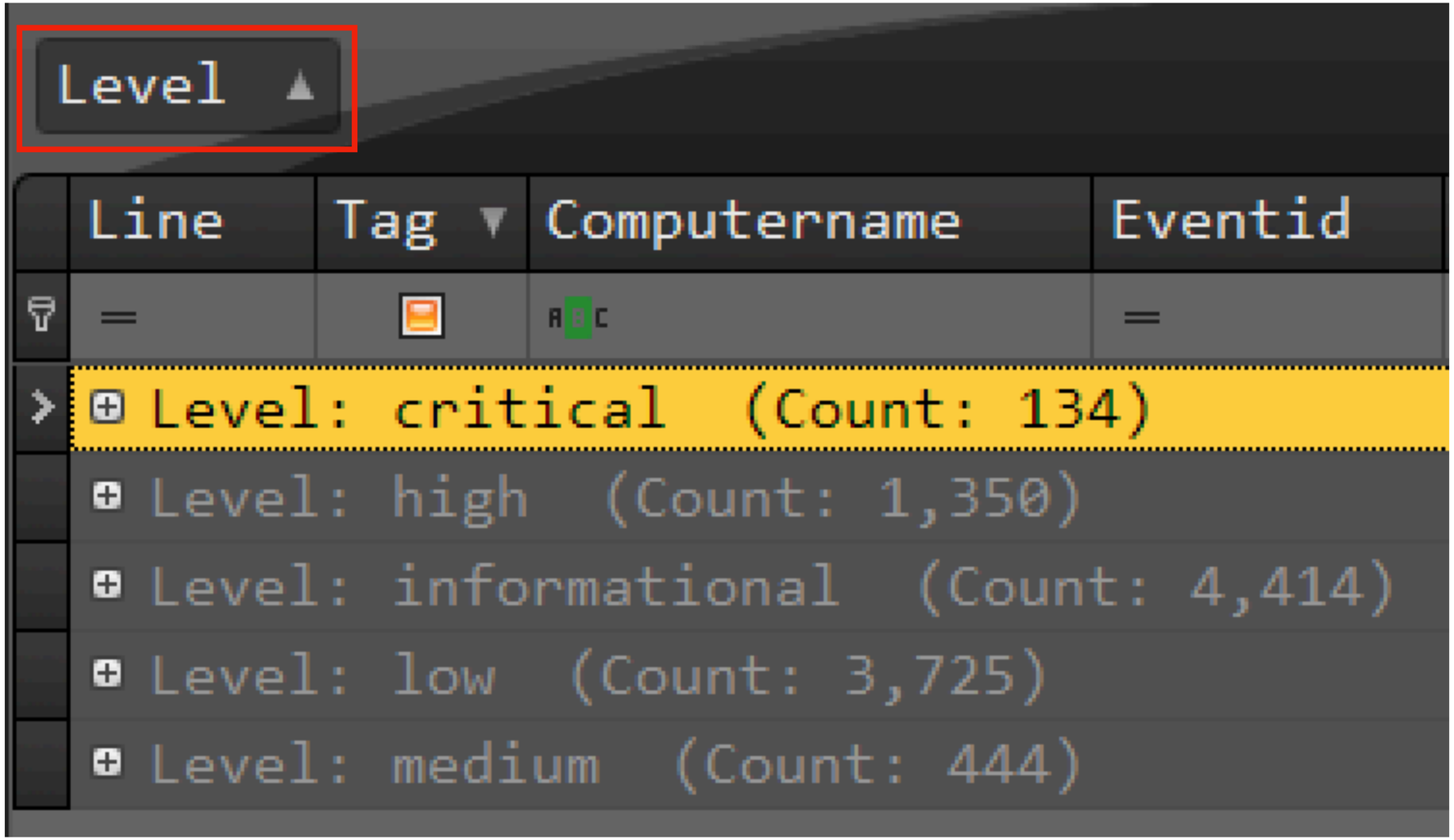
Computername ▲

Line	Tag	Time	Eventid	Level	Alert	Details
=		ABC	=	=	ABC	ABC
⊞ 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)						

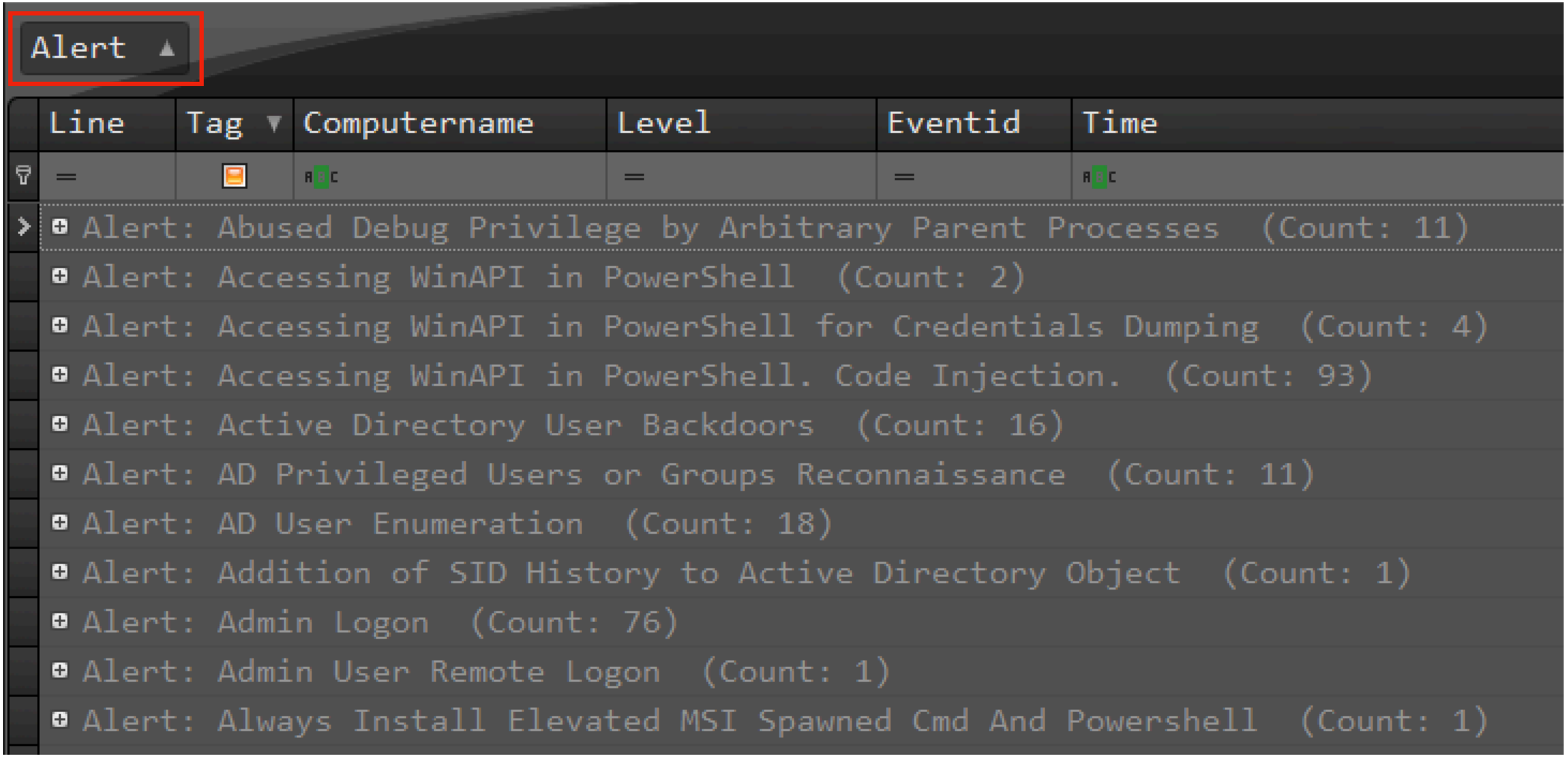
イベントIDでのグルーピング



レベルでのグルーピング



アラートでのグルーピング



タグ機能
調査に関係しているアラートとイベントに
タグを付ける

Drag a column header here to group by that column

Line	Tag	Computername	Time	Eventid	Level	Alert
10064	☐	fs03vuln.offse…	2021-11-09 00:01:27.604 +09:00	1	high	WMI Spawning Windows PowerShell
10063	☐	fs03vuln.offse…	2021-11-09 00:01:27.604 +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

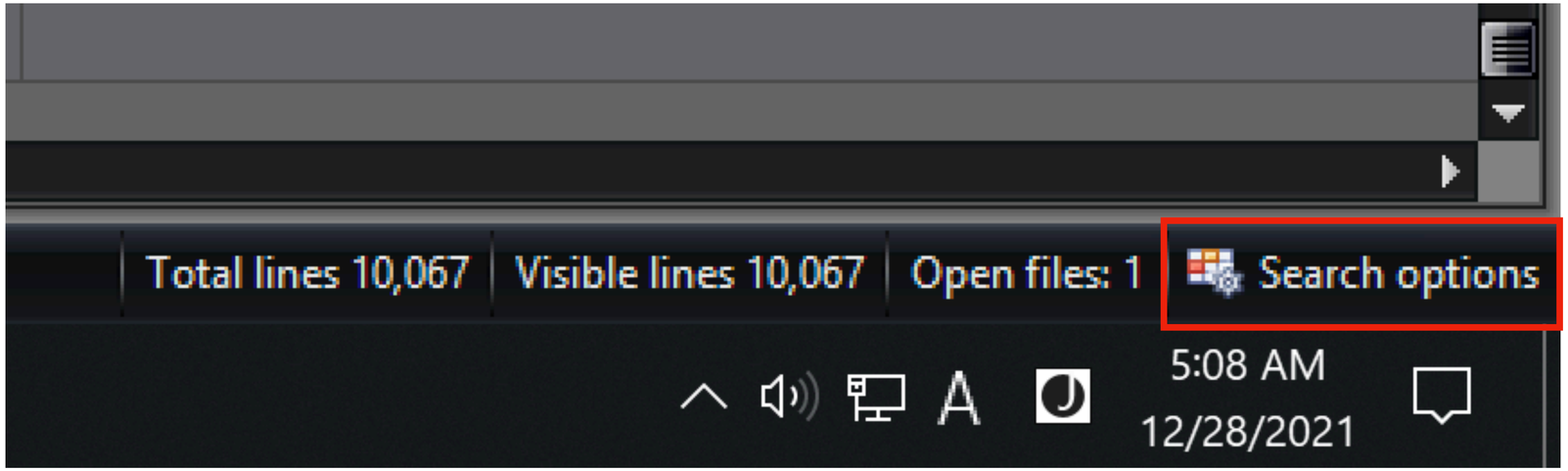
タグでのグルーピング

Tag ▼

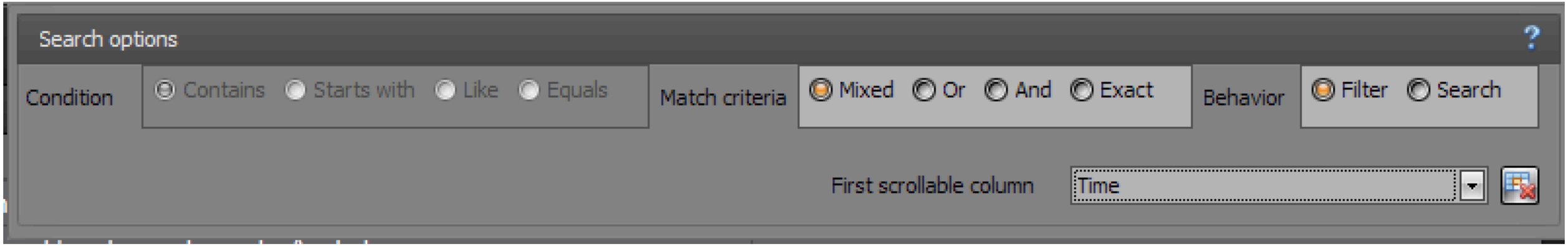
Line	Time	Computername	Level	Eventid	Alert
Tag: Checked (Count: 10)					
100…	2021-11-02 23:15:23.676 +09:00	fs03vuln.offse…	high	1102	Security log was cleared
100…	2021-10-28 22:41:21.325 +09:00	FS03.offsec.lan	high	1	Abused Debug Privilege by Arbitrary Parent Proces…
100…	2021-10-28 22:41:21.325 +09:00	FS03.offsec.lan	high	1	Process Creation Sysmon Rule Alert
100…	2021-10-27 19:28:26.260 +09:00	FS03.offsec.lan	high	354	Possible CVE-2021-1675 Print Spooler Exploitation
100…	2021-10-27 19:14:27.559 +09:00	fs03vuln.offse…	critical	823	Mimikatz Use
100…	2021-10-27 19:14:27.466 +09:00	fs03vuln.offse…	critical	5142	Mimikatz Use
9780	2021-05-22 05:43:50.607 +09:00	fs01.offsec.lan	low	4625	Logon Failure - Wrong Password
9776	2021-05-22 05:43:18.227 +09:00	fs01.offsec.lan	informational	4648	Explicit Logon
9772	2021-05-20 21:49:54.945 +09:00	fs01.offsec.lan	informational	4776	NTLM Logon to Local Account
9770	2021-05-20 21:49:54.662 +09:00	fs01.offsec.lan	informational	4776	NTLM Logon to Local Account
Tag: Unchecked (Count: 10,057)					

列の固定

1. 右下の「Search options」をクリックします



2. 「First scrollable column」を「Time」に設定します：



Time列が固定される

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	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	

Timeline Explorerをもっと使いこなしたい方へ
この記事をおすすめします：

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