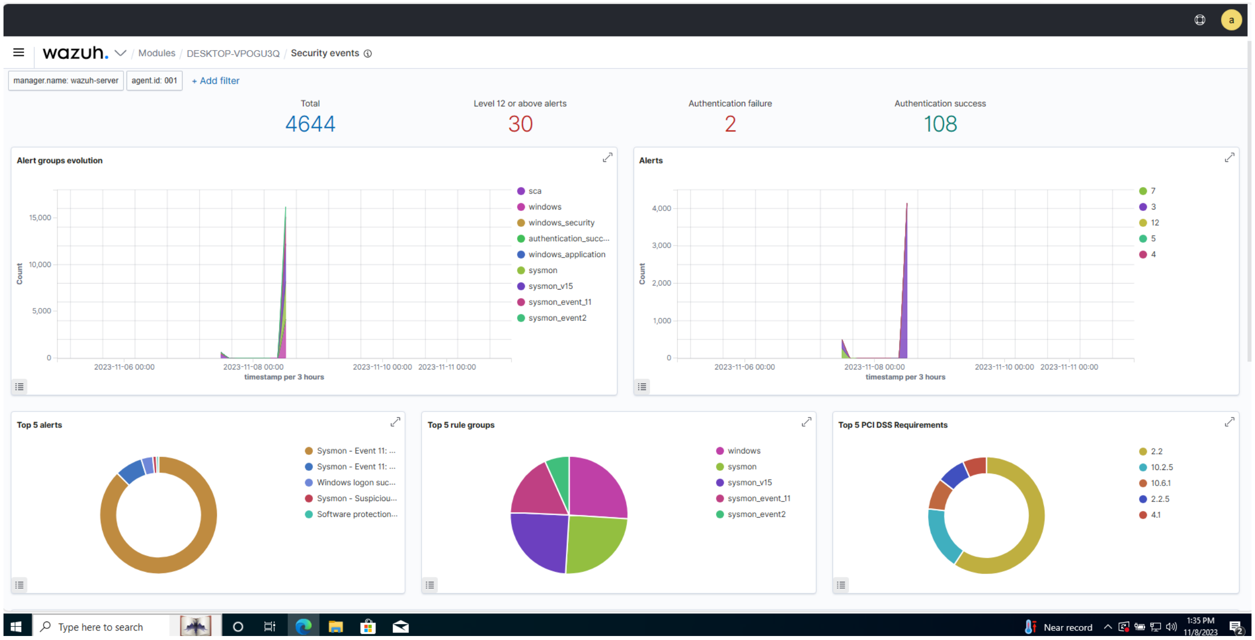
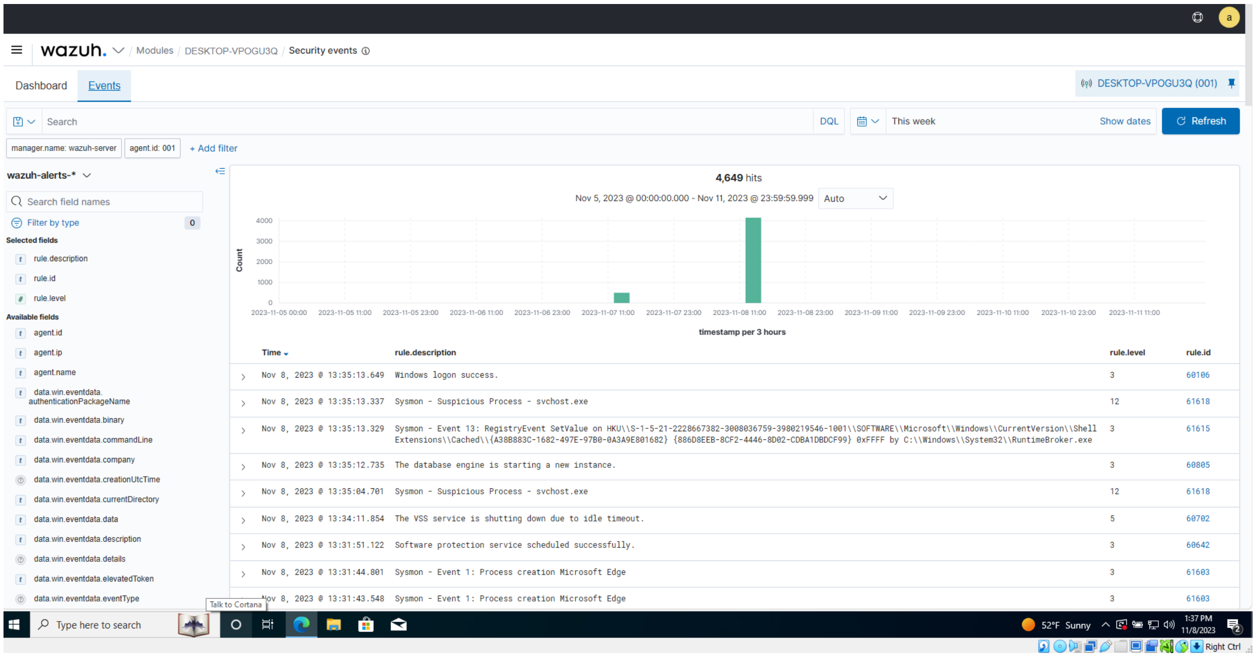


wazuh. / Modules / DESKTOP-VPOGU3Q / Security events

manager.name: wazuh-server | agent.id: 001 | + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
4644	30	2	108



wazuh. / Modules / DESKTOP-VPOGU3Q / Security events

Dashboard | Events

DESKTOP-VPOGU3Q (001)

Search | DQL | This week | Show dates | Refresh

manager.name: wazuh-server | agent.id: 001 | + Add filter

wazuh-alerts-*

Search field names

Filter by type 0

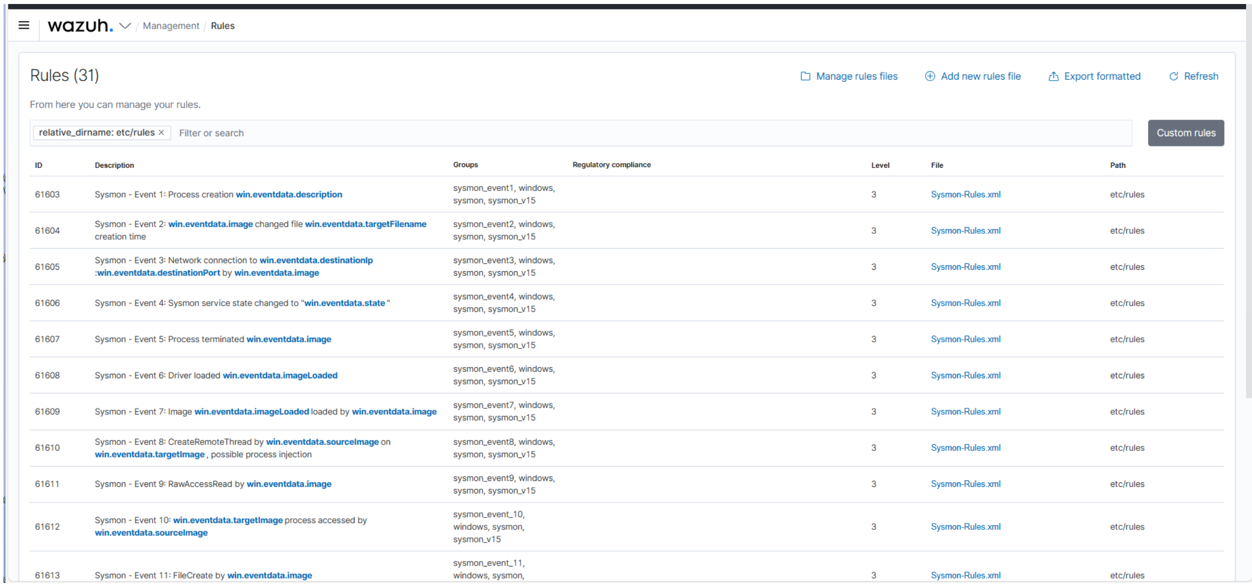
Selected fields
- rule.description
- rule.id
- rule.level

Available fields
- agent.id
- agent.ip
- agent.name
- data.win.eventdata.authenticationPackageName
- data.win.eventdata.binary
- data.win.eventdata.commandLine
- data.win.eventdata.company
- data.win.eventdata.creationUtcTime
- data.win.eventdata.currentDirectory
- data.win.eventdata.data
- data.win.eventdata.description
- data.win.eventdata.details
- data.win.eventdata.elevatedToken
- data.win.eventdata.eventType

4,649 hits

Nov 5, 2023 @ 00:00:00.000 - Nov 11, 2023 @ 23:59:59.999 Auto

Time	rule.description	rule.level	rule.id
Nov 8, 2023 @ 13:35:13.649	Windows logon success.	3	60106
Nov 8, 2023 @ 13:35:13.337	Sysmon - Suspicious Process - svchost.exe	12	61618
Nov 8, 2023 @ 13:35:13.329	Sysmon - Event 13: RegistryEvent SetValue on HKU\\S-1-5-21-2228667382-3008036759-3980219546-1001\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Shell Extensions\\Cached\\{A38B883C-1682-497E-97B0-0A3A9E801682} {886D8EEB-8CF2-4446-8D02-CDBA1DBDCF99} 0xFFFF by C:\\Windows\\System32\\RuntimeBroker.exe	3	61615
Nov 8, 2023 @ 13:35:12.735	The database engine is starting a new instance.	3	60805
Nov 8, 2023 @ 13:35:04.701	Sysmon - Suspicious Process - svchost.exe	12	61618
Nov 8, 2023 @ 13:34:11.854	The VSS service is shutting down due to idle timeout.	5	60702
Nov 8, 2023 @ 13:31:51.122	Software protection service scheduled successfully.	3	60642
Nov 8, 2023 @ 13:31:44.801	Sysmon - Event 1: Process creation Microsoft Edge	3	61603
Nov 8, 2023 @ 13:31:43.548	Sysmon - Event 1: Process creation Microsoft Edge	3	61603



Rules (31)

From here you can manage your rules.

ID	Description	Groups	Regulatory compliance	Level	File	Path
61603	Sysmon - Event 1: Process creation **win.eventdata.description**	sysmon_event1, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61604	Sysmon - Event 2: **win.eventdata.image** changed file **win.eventdata.targetFilename** creation time	sysmon_event2, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61605	Sysmon - Event 3: Network connection to **win.eventdata.destinationIp** :**win.eventdata.destinationPort** by **win.eventdata.image**	sysmon_event3, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61606	Sysmon - Event 4: Sysmon service state changed to "**win.eventdata.state** "	sysmon_event4, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61607	Sysmon - Event 5: Process terminated **win.eventdata.image**	sysmon_event5, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61608	Sysmon - Event 6: Driver loaded **win.eventdata.imageLoaded**	sysmon_event6, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61609	Sysmon - Event 7: Image **win.eventdata.imageLoaded** loaded by **win.eventdata.image**	sysmon_event7, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61610	Sysmon - Event 8: CreateRemoteThread by **win.eventdata.sourceImage** on **win.eventdata.targetImage** , possible process injection	sysmon_event8, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61611	Sysmon - Event 9: RawAccessRead by **win.eventdata.image**	sysmon_event9, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61612	Sysmon - Event 10: **win.eventdata.targetImage** process accessed by **win.eventdata.sourceImage**	sysmon_event_10, windows, sysmon, sysmon_v15		3	Sysmon-Rules.xml	etc/rules
61613	Sysmon - Event 11: FileCreate by **win.eventdata.image**	sysmon_event_11, windows, sysmon,		3	Sysmon-Rules.xml	etc/rules