Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	victima-windows	192.168.1.73	Wazuh v4.9.1	instance-20241026-022758	Microsoft Windows 10 Pro 10.0.19041.450	Oct 28, 2024 @ 03:39:10.000	Nov 5, 2024 @ 17:49:08.000

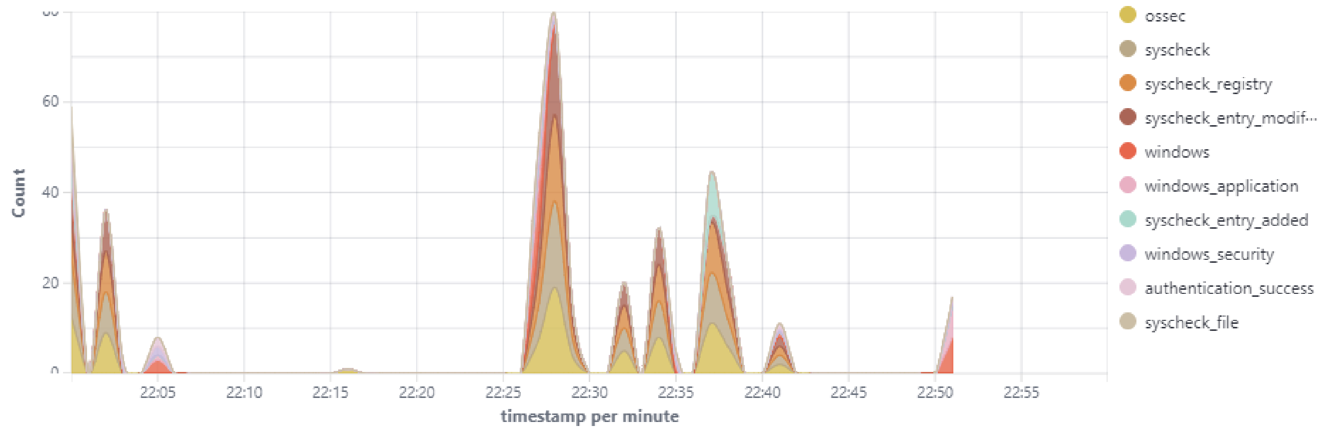
Group: default

Browse through your security alerts, identifying issues and threats in your environment.

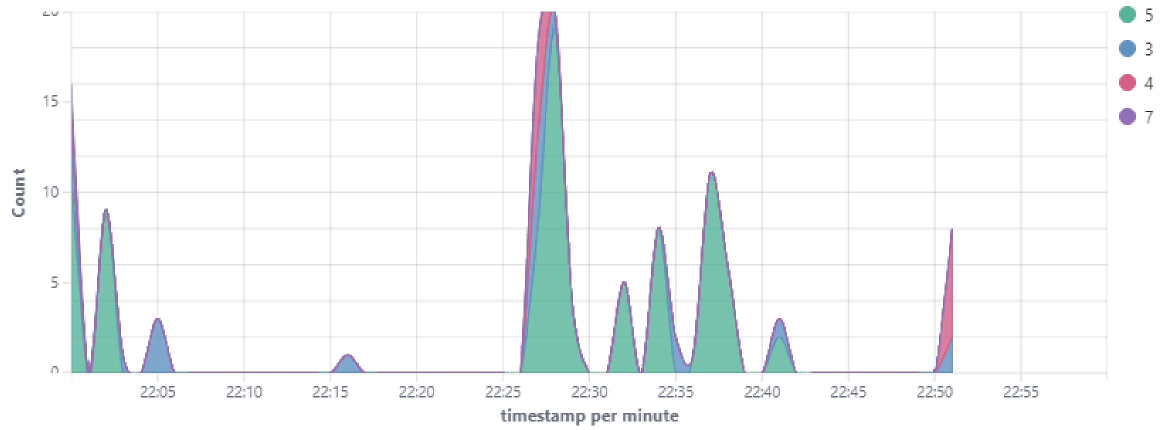
2024-11-04T22:00:00 to 2024-11-04T23:00:00

manager.name: instance-20241026-022758 AND agent.id: 002

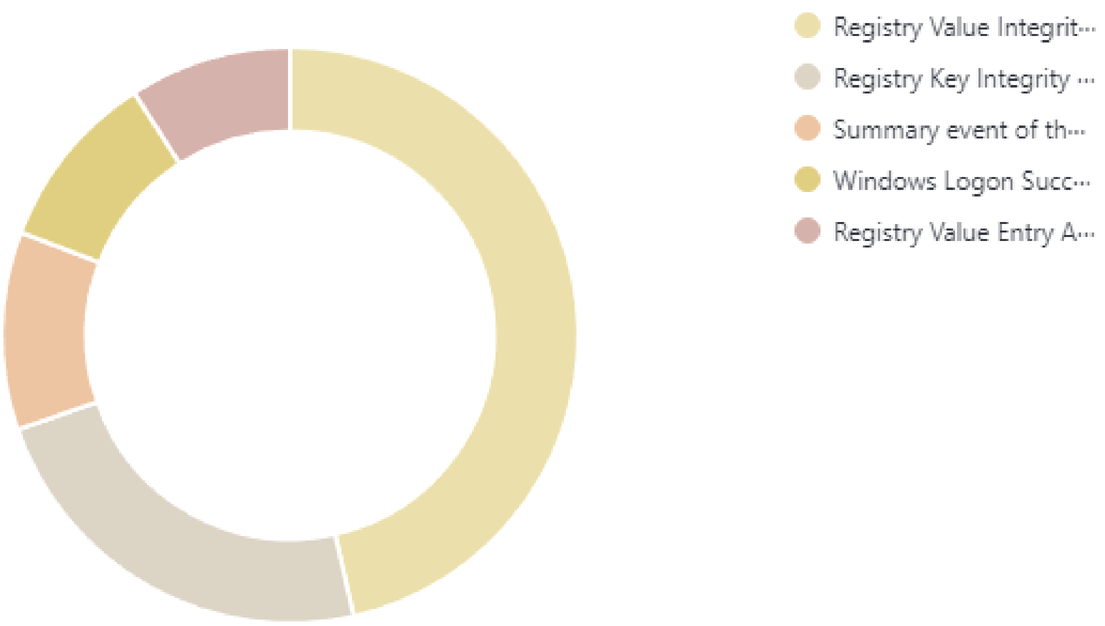
Top 10 Alert groups evolution



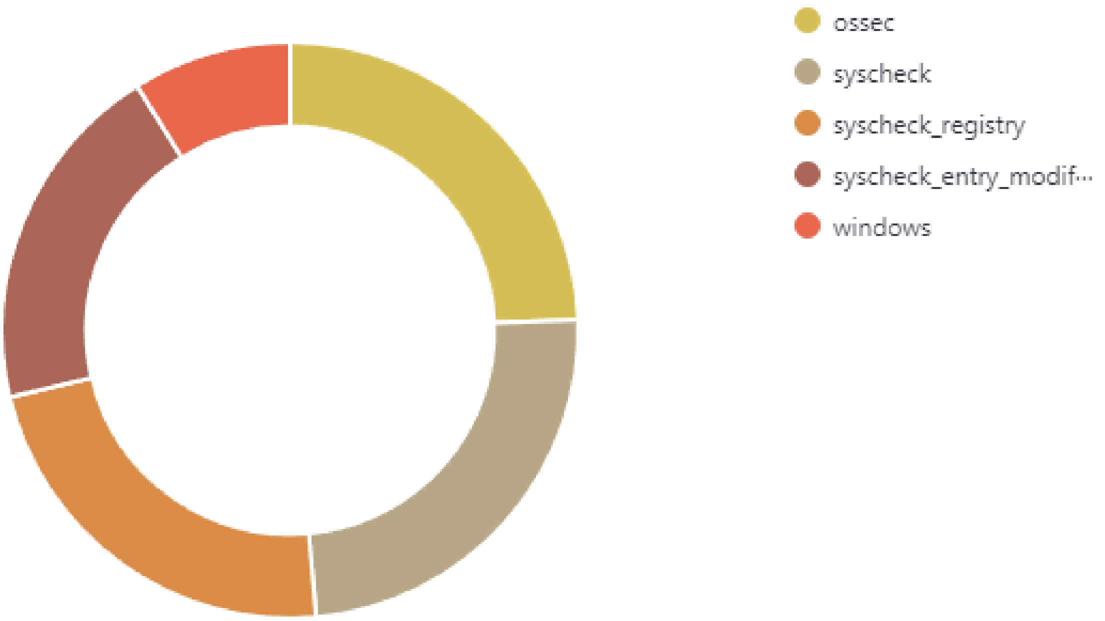
Alerts



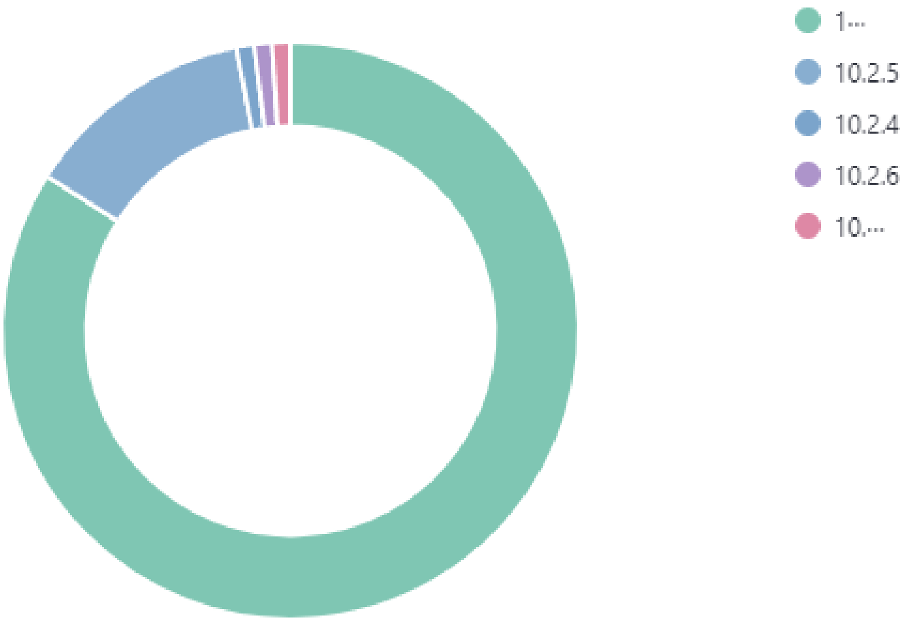
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



1...
- Total -

0
- Level 12 or above alerts -

1
- Authentication failure -

12
- Authentication success -

Alerts summary

Rule ID	Description	Level	Count
750	Registry Value Integrity Checksum Changed	5	46
594	Registry Key Integrity Checksum Changed	5	23
60608	Summary event of the report's signatures.	4	11
60106	Windows Logon Success	3	10
752	Registry Value Entry Added to the System	5	9
554	File added to the system.	5	3
60642	Software protection service scheduled successfully.	3	3
553	File deleted.	7	2
60118	Windows Workstation Logon Success	3	2
67023	Non service account logged off.	3	2
504	Wazuh agent disconnected.	3	1
598	Registry Key Entry Added to the System	5	1
60122	Logon Failure - Unknown user or bad password	5	1
61138	New Windows Service Created	5	1
67028	Special privileges assigned to new logon.	3	1

Groups summary

Groups	Count
ossec	85
syscheck	84
syscheck_registry	79
syscheck_entry_modified	69
windows	31
windows_application	14
syscheck_entry_added	13
windows_security	13
authentication_success	12
syscheck_file	5
WEF	3
syscheck_entry_deleted	2
authentication_failed	1
windows_system	1