info@wazuh.com
https://wazuh.com

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

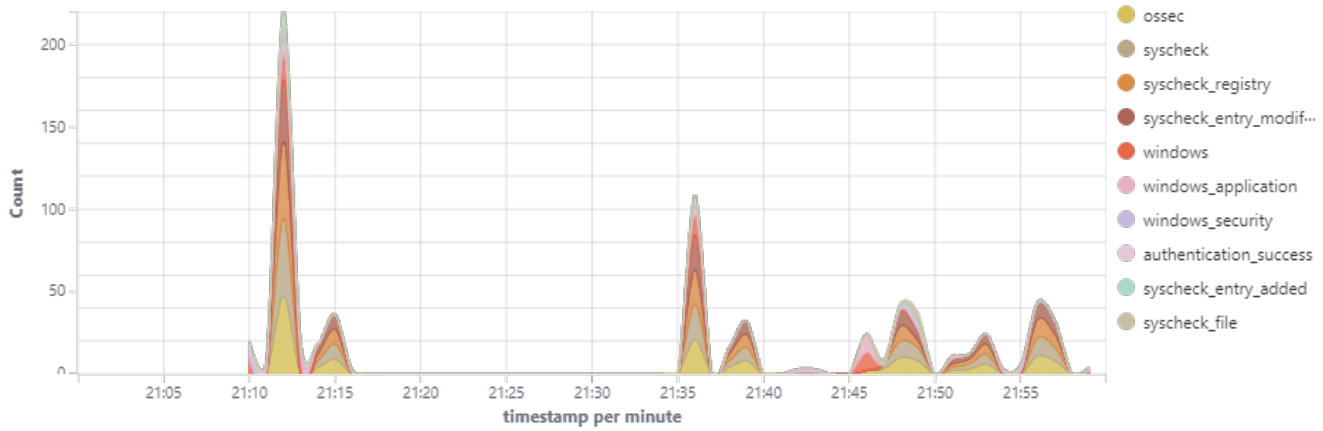
Group: default

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

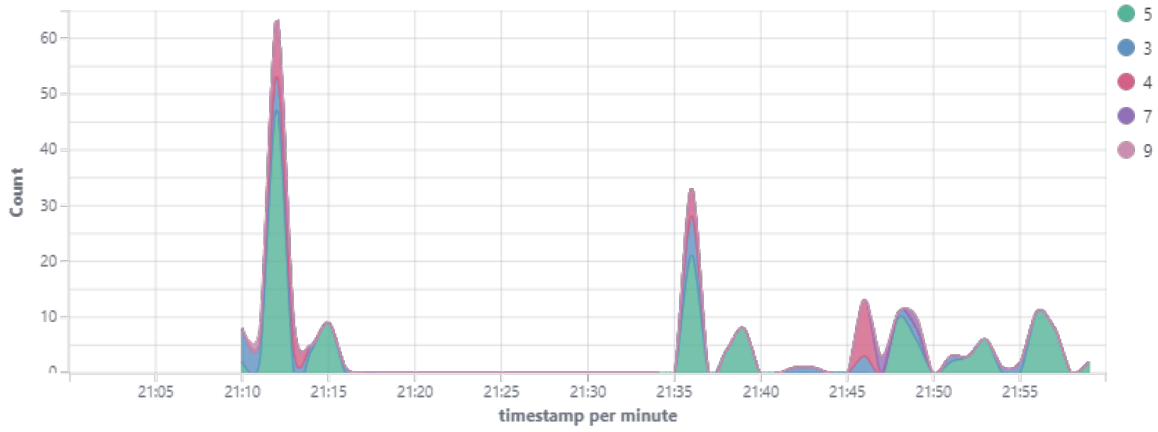
2024-11-04T21:00:00 to 2024-11-04T22:00:00

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

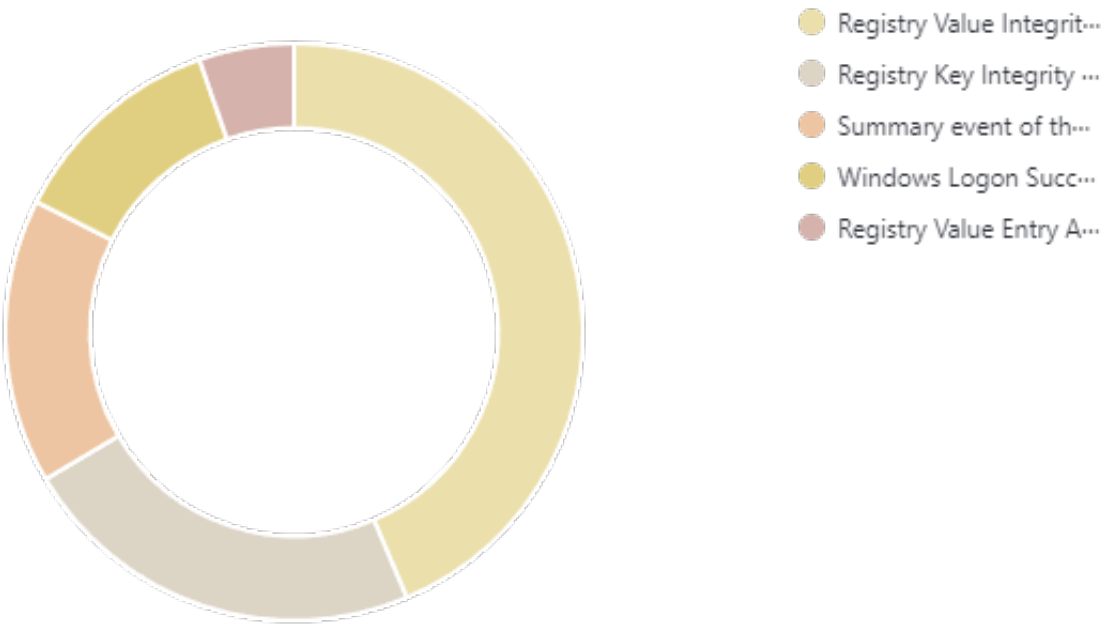
Top 10 Alert groups evolution



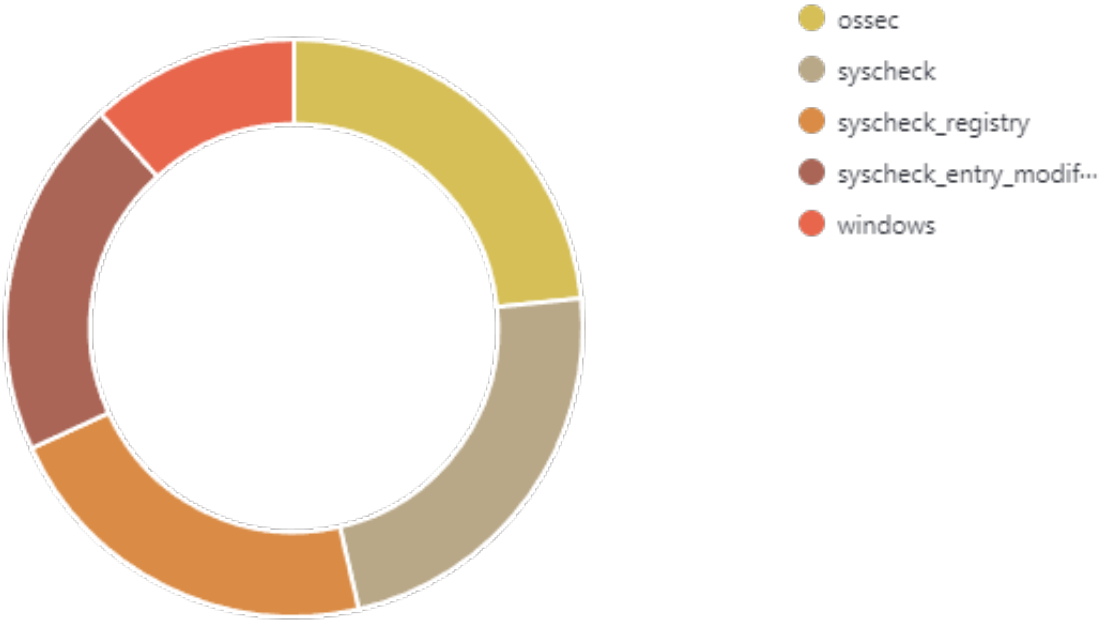
Alerts



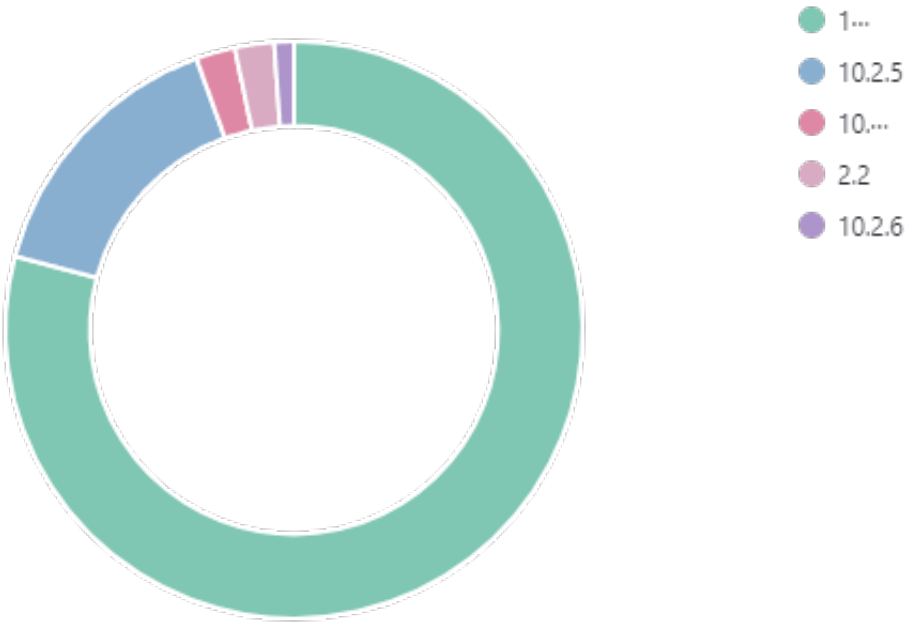
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



223
- Total -

0
- Level 12 or above alerts -

1
- Authentication failure -

27
- Authentication success -

Alerts summary

Rule ID	Description	Level	Count
750	Registry Value Integrity Checksum Changed	5	82
594	Registry Key Integrity Checksum Changed	5	43
60608	Summary event of the report's signatures.	4	30
60106	Windows Logon Success	3	23
752	Registry Value Entry Added to the System	5	10
60642	Software protection service scheduled successfully.	3	5
553	File deleted.	7	4
60118	Windows Workstation Logon Success	3	4
67023	Non service account logged off.	3	4
554	File added to the system.	5	3
19005	SCA summary: CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Score less than 30% (29)	9	2
60104	Windows audit failure event	5	2
67028	Special privileges assigned to new logon.	3	2
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.: Status changed from passed to 'not applicable'	5	1
19015	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.: Status changed from 'not applicable' to passed	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1
550	Integrity checksum changed.	7	1
598	Registry Key Entry Added to the System	5	1
60122	Logon Failure - Unknown user or bad password	5	1
61102	Windows System error event	5	1
61138	New Windows Service Created	5	1

Groups summary

Groups	Count
ossec	146
syscheck	144
syscheck_registry	136
syscheck_entry_modified	126
windows	73
windows_application	35
windows_security	30
authentication_success	27
syscheck_entry_added	14
syscheck_file	8
WEF	6
sca	4
syscheck_entry_deleted	4
windows_system	2
authentication_failed	1
system_error	1