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

Threat hunting report

Warning. Agent is disconnected

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
003	jamod-win10	192.168.1.49	Wazuh v4.14.1	wazuh-server	Microsoft Windows 10 Home 10.0.19045.3803	Jan 8, 2026 @ 01:27:53.000	Jan 8, 2026 @ 11:53:29.000

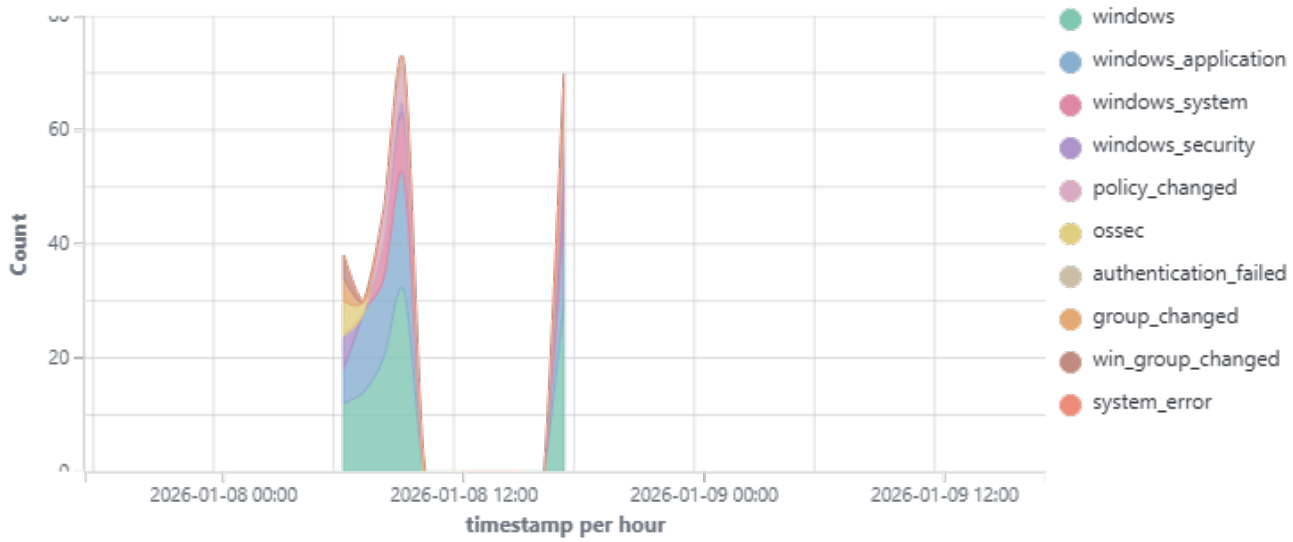
Group: default

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

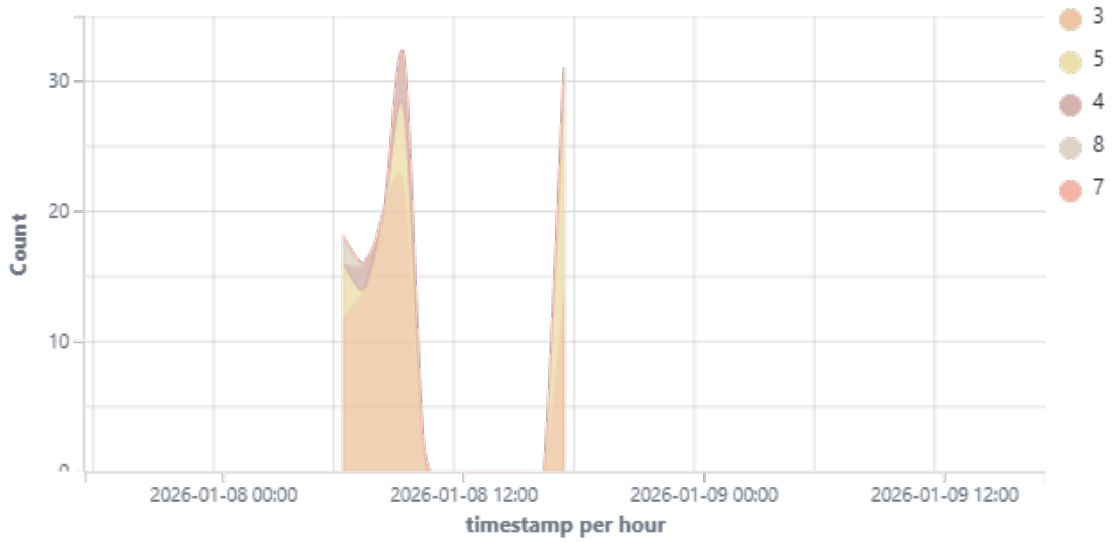
2026-01-07T17:04:57 to 2026-01-09T17:04:57

manager.name: wazuh-server AND agent.id: 003

Top 10 Alert groups evolution



Alerts



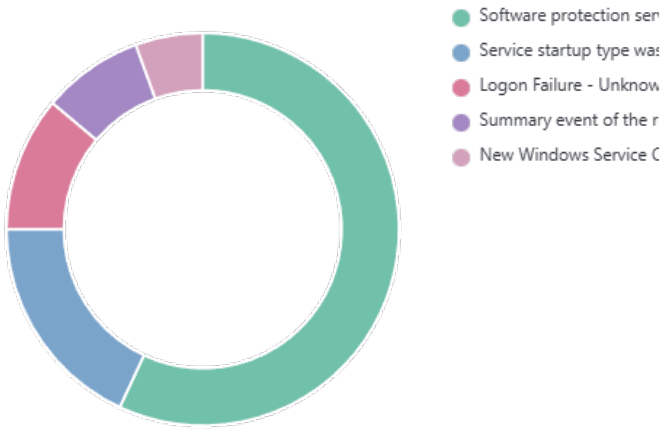
1...
- Total -

0
- Level 12 or above alerts -

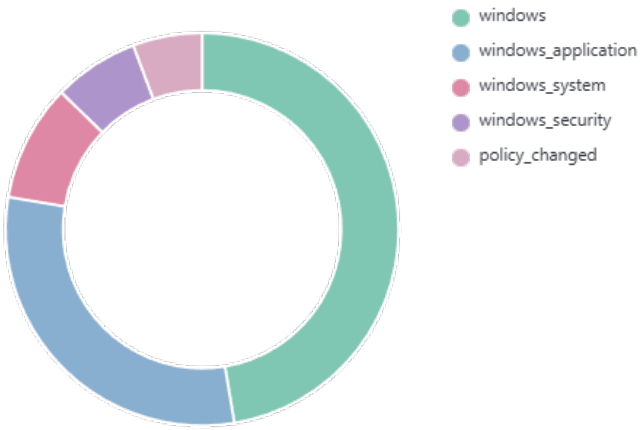
8
- Authentication failure -

2
- Authentication success -

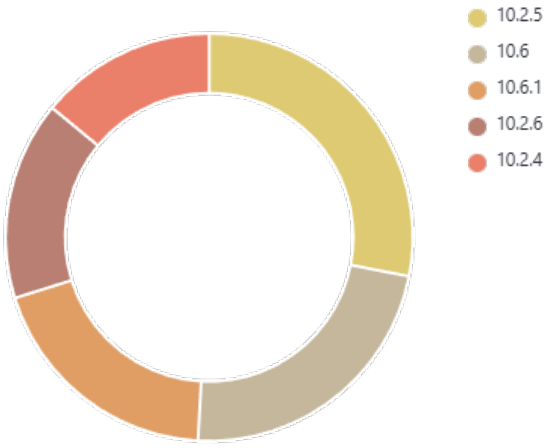
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
60642	Software protection service scheduled successfully.	3	41
61104	Service startup type was changed	3	13
60122	Logon Failure - Unknown user or bad password	5	8
60608	Summary event of the report's signatures.	4	6
504	Wazuh agent disconnected.	3	4
60610	Windows installer began an installation process.	3	4
60673	Windows Search Service indexed data for user successfully removed in response to user profile deletion.	3	4
61138	New Windows Service Created	5	4
503	Wazuh agent started.	3	3
61102	Windows System error event	5	3
60612	Application installed Microsoft Update Health Tools, 3.74.0.0, 0, 0, Microsoft Corporation.	3	2
60612	Application installed Product: Microsoft Update Health Tools -- Installation completed successfully..	3	2
60612	Application installed Product: Update for Windows 10 for x64-based Systems (KB5001716) -- Installation completed successfully..	3	2
60612	Application installed Update for Windows 10 for x64-based Systems (KB5001716), 8.94.0.0, 0, 0, Microsoft Corporation.	3	2
501	New wazuh agent connected.	3	2
506	Wazuh agent stopped.	3	2
60111	User account disabled or deleted	8	2
60118	Windows Workstation Logon Success	3	2
60160	Domain Users Group Changed	5	2
60170	Users Group Changed	5	2
60646	License activation (slui.exe) failed.	5	2
61109	Name resolution for the name 4.tlu.dl.delivery.mp.microsoft.com timed out	5	2
60702	The VSS service is shutting down due to idle timeout.	5	1
60730	Inconsistent system shutdown detected.	5	1
60775	SessionEnv was unavailable to handle a notification event.	5	1
60776	SessionEnv was unavailable to handle a critical notification event.	7	1
67028	Special privileges assigned to new logon.	3	1

Groups summary

Groups	Count
windows	108
windows_application	69
windows_system	22
windows_security	16
policy_changed	13
ossec	11
authentication_failed	8
group_changed	4
win_group_changed	4
system_error	3
account_changed	2
adduser	2
authentication_success	2
WEF	1