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
004	aditys-agent	192.168.1.46	Wazuh v4.14.1	wazuh-server	Microsoft Windows 10 Pro 10.0.19045.6466	Jan 8, 2026 @ 02:45:52.000	Jan 9, 2026 @ 10:16:34.000

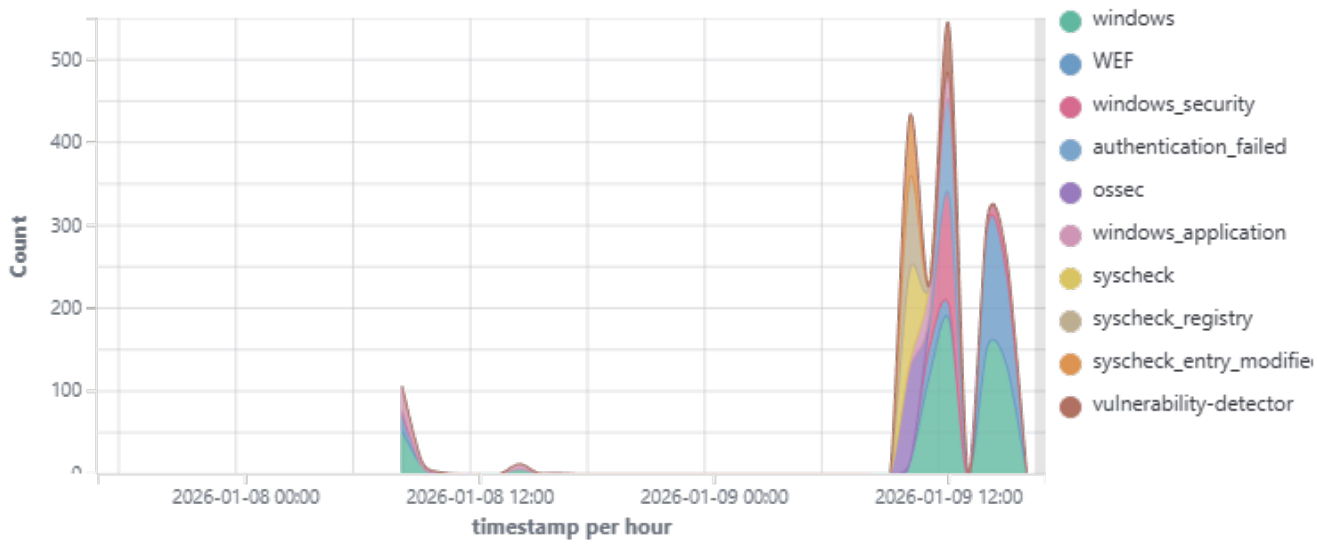
Group: default

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

2026-01-07T16:24:06 to 2026-01-09T16:24:06

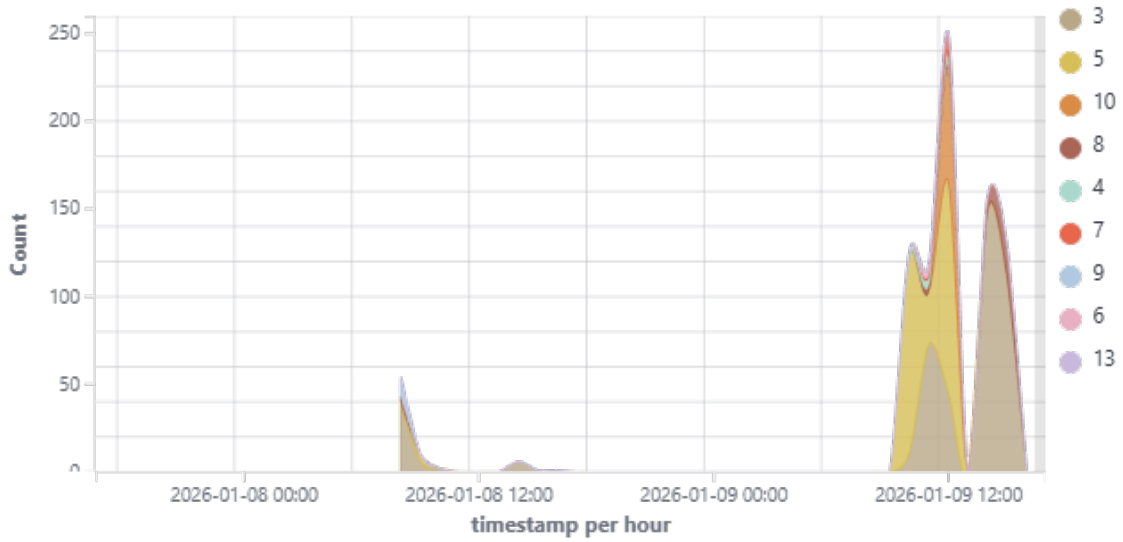
manager.name: wazuh-server AND agent.id: 004

Top 10 Alert groups evolution



Copyright © Wazuh, Inc.

Alerts



856
- Total -

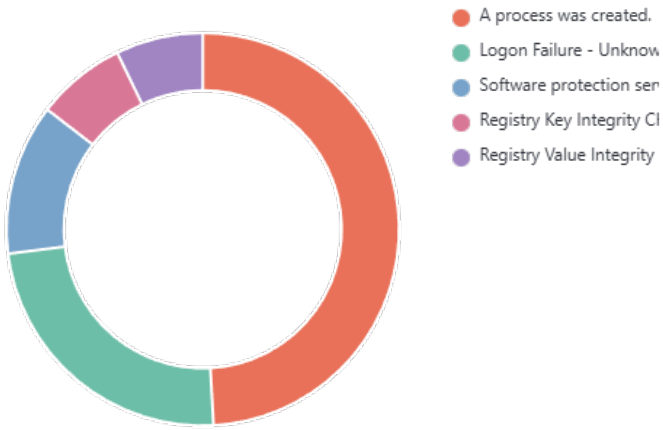
1
- Level 12 or above alerts -

138
- Authentication failure -

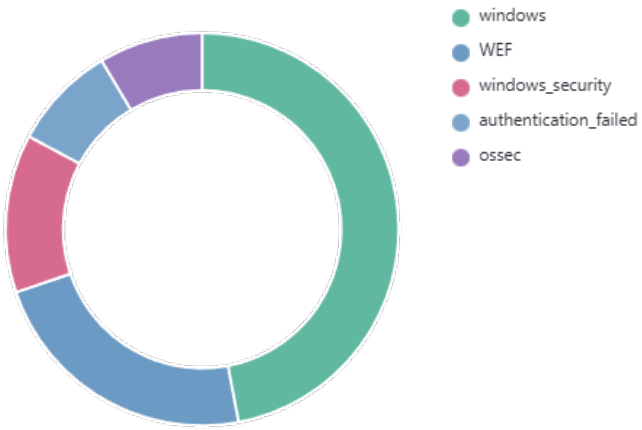
8
- Authentication success -

Copyright © Wazuh, Inc.

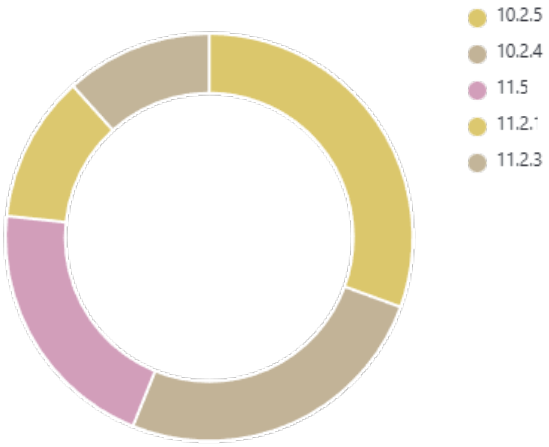
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Copyright © Wazuh, Inc.

Alerts summary

Rule ID	Description	Level	Count
67027	A process was created.	3	253
60122	Logon Failure - Unknown user or bad password	5	123
60642	Software protection service scheduled successfully.	3	64
594	Registry Key Integrity Checksum Changed	5	38
750	Registry Value Integrity Checksum Changed	5	37
67022	Non network or service local logon.	3	28
598	Registry Key Entry Added to the System	5	24
60112	Windows Audit Policy changed	8	24
67023	Non service account logged off.	3	24
61104	Service startup type was changed	3	23
67028	Special privileges assigned to new logon.	3	17
60204	Multiple Windows Logon Failures	10	15
752	Registry Value Entry Added to the System	5	12
60110	User account changed	8	11
60608	Summary event of the report's signatures.	4	11
60602	Windows application error event.	9	10
60702	The VSS service is shutting down due to idle timeout.	5	10
60775	SessionEnv was unavailable to handle a notification event.	5	9
60137	Windows User Logoff	3	8
61102	Windows System error event	5	7
60775	WSearch was unavailable to handle a notification event.	5	5
503	Wazuh agent started.	3	5
504	Wazuh agent disconnected.	3	5
60118	Windows Workstation Logon Success	3	4
67018	System shutdown initiated.	3	3
61109	Name resolution for the name client.wns.windows.com timed out	5	2
61109	Name resolution for the name v20.events.data.microsoft.com timed out	5	2
60716	Skipped creation of restore point for C:\\Windows\\winsxs\\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.6151_none_7e2f7fd67c740ce3\\TiWorker.exe -Embedding, Windows Modules Installer as there is a previous restore point available.	4	2
60776	SessionEnv was unavailable to handle a critical notification event.	7	2
92652	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	6	2
92657	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that WINDOWS is allowed to perform RDP connections	6	2

Copyright © Wazuh, Inc.

Rule ID	Description	Level	Count
23505	CVE-2025-54100 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-55233 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59505 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59506 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59507 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59508 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59511 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59512 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59514 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59515 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59516 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-59517 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60703 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60704 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60705 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60707 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60709 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60714 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60715 affects Microsoft Windows 10 Pro	10	1
23505	CVE-2025-60716 affects Microsoft Windows 10 Pro	10	1
23504	CVE-2025-59509 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-59510 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-59513 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-60706 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-60708 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-60723 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-62453 affects Microsoft Visual Studio Code (User)	7	1
23504	CVE-2025-62463 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-62473 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-62567 affects Microsoft Windows 10 Pro	7	1
23504	CVE-2025-64670 affects Microsoft Windows 10 Pro	7	1
60716	Skipped creation of restore point for C:\\Windows\\winsxs\\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.6465_none_7e0fb53c7c8be091\\TiWorker.exe -Embedding, Windows Modules Installer as there is a previous restore point available.	4	1
23506	CVE-2025-60724 affects Microsoft Windows 10 Pro	13	1
506	Wazuh agent stopped.	3	1
60132	System time changed	5	1
60668	The Windows search service started.	3	1
60703	The VSS service is shutting down due to a shutdown event from the service control manager.	3	1
60718	Restore point successfully created.	3	1

Copyright © Wazuh, Inc.

Rule ID	Description	Level	Count
60798	The database engine attached a database.	3	1
60805	The database engine is starting a new instance.	3	1
60807	The database engine is initiating recovery steps.	3	1
60808	The database engine is replaying log file C:\Winnt\system32\wins\j50.log.	3	1
60809	The database engine has completed recovery steps.	3	1

Copyright © Wazuh, Inc.

Groups summary

Groups	Count
windows	671
WEF	325
windows_security	186
authentication_failed	123
ossec	122
windows_application	122
syscheck	111
syscheck_registry	111
syscheck_entry_modified	75
vulnerability-detector	63
policy_changed	47
syscheck_entry_added	36
windows_system	34
system_error	17
authentication_failures	15
account_changed	11
authentication_success	8
win_evt_channel	4
time_changed	1

Copyright © Wazuh, Inc.