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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	MSI	10.206.79.43	Wazuh v4.12.0	wazuh-server	Microsoft Windows 11 Home 10.0.26100.4946	Aug 26, 2025 @ 00:29:56.000	Aug 26, 2025 @ 20:38:10.000

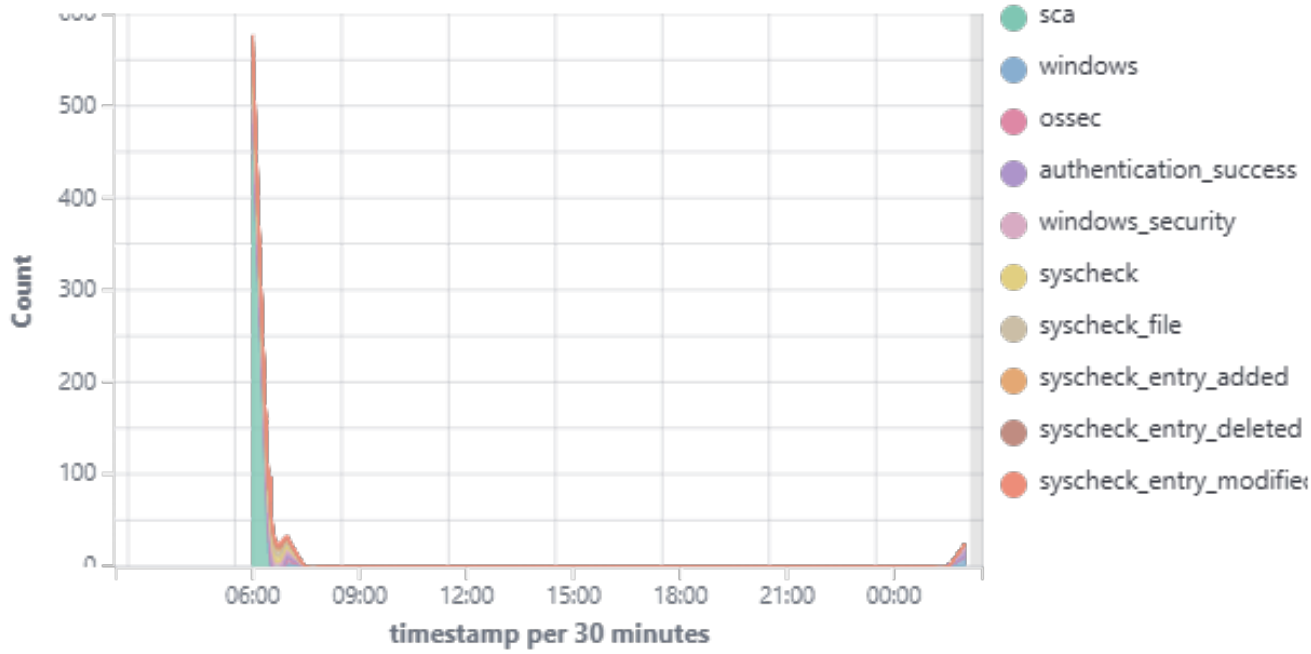
Group: default

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

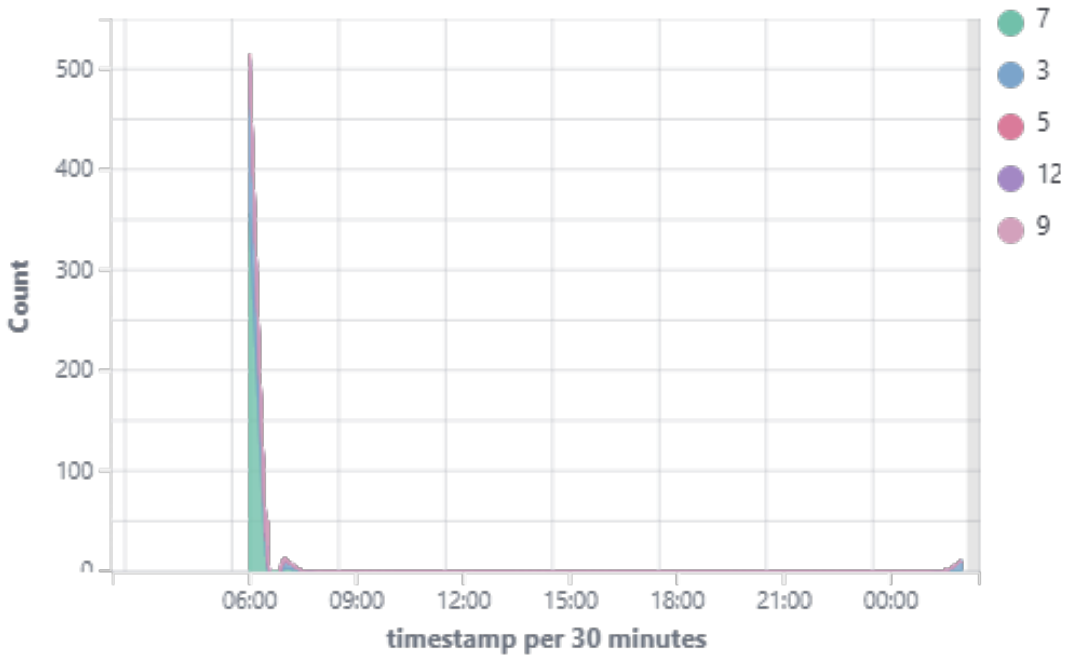
2025-08-26T02:08:13 to 2025-08-27T02:08:13

manager.name: wazuh-server AND agent.id: 001

Top 10 Alert groups evolution



Alerts



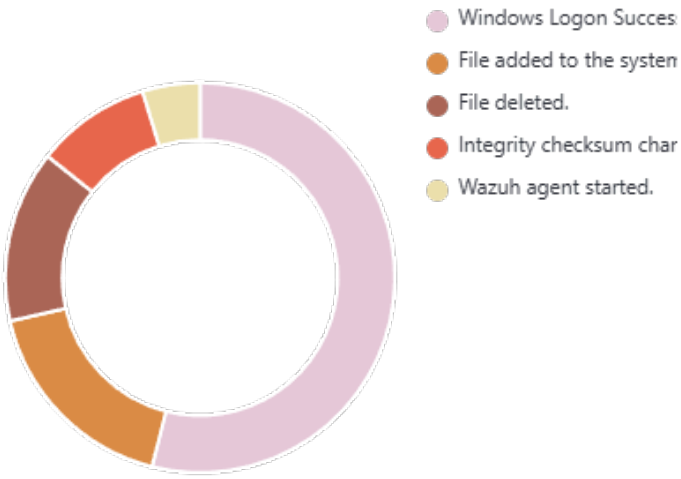
563
- Total -

5
- Level 12 or above alerts -

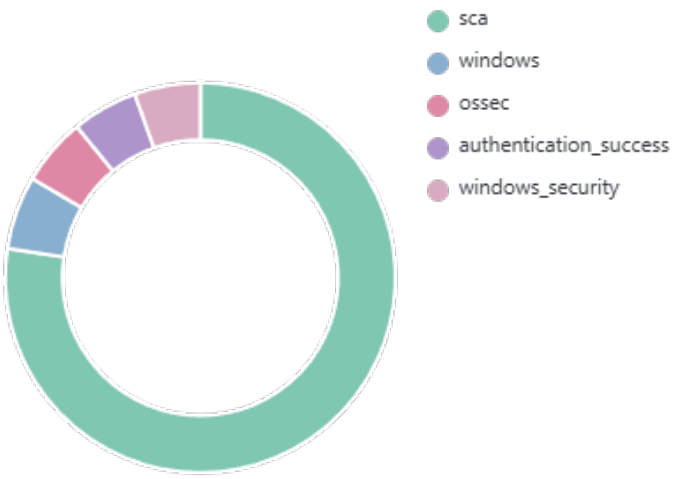
0
- Authentication failure -

34
- Authentication success -

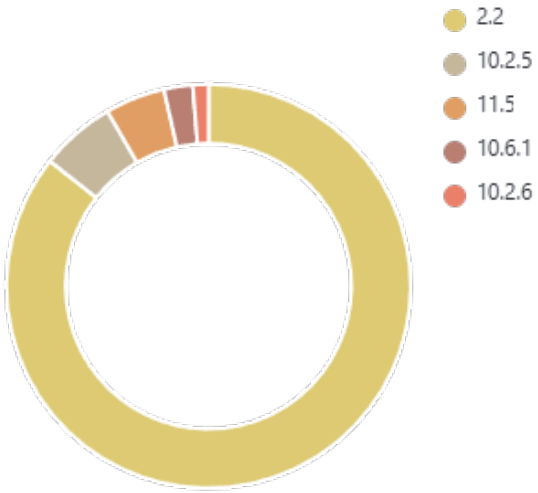
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	34
554	File added to the system.	5	11
553	File deleted.	7	9
550	Integrity checksum changed.	7	7
503	Wazuh agent started.	3	4
506	Wazuh agent stopped.	3	3
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False'.	7	2
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Basic authentication' is set to 'Disabled'.	3	2
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow unencrypted traffic' is set to 'Disabled'.	3	2
87105	VirusTotal: Alert - c:\users\swast\downloads\6340f7f8-7837-4fb3-abcc-fe747d1b8df4.tmp - 36 engines detected this file	12	2
87105	VirusTotal: Alert - c:\users\swast\downloads\unconfirmed 409694.crdownload - 36 engines detected this file	12	2
60642	Software protection service scheduled successfully.	3	2
61104	Service startup type was changed	3	2
87104	VirusTotal: Alert - c:\users\swast\downloads\malware detection.pdf - No positives found	3	2
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Configure 'Accounts: Rename administrator account'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Configure 'Accounts: Rename guest account'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Configure 'Interactive logon: Message text for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Configure 'Interactive logon: Message title for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Accounts: Guest account status' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Cortana above lock screen' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Cortana' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Message Service Cloud Sync' is set to	7	1

Rule ID	Description	Level	Count
	'Disabled'.		
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Online Tips' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'.	7	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow user control over installs' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Always install with elevated privileges' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Audit Policy Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Authentication Policy Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Logoff' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Logon' is set to 'Success and Failure'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Other System Events' is set to 'Success and Failure'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Security Group Management' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Security State Change' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit Special Logon' is set to include 'Success'.	3	1
19008	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Audit System Integrity' is set to 'Success and Failure'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Computer Browser (Browser)' is set to 'Disabled' or 'Not Installed'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Download Mode' is NOT set to 'Enabled: Internet'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'PNRP Machine Name Publication Service (PNRPAutoReg)' is set to 'Disabled'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Peer Name Resolution Protocol (PNRPsvc)' is set to 'Disabled'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Peer Networking Grouping (p2psvc)' is set to 'Disabled'.	3	1

Rule ID	Description	Level	Count
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Peer Networking Identity Manager (p2pimsvc)' is set to 'Disabled'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'.	3	1
19009	CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'.	3	1
87105	VirusTotal: Alert - c:\users\swast\downloads\madman.exe - 36 engines detected this file	12	1
19005	SCA summary: CIS Microsoft Windows 11 Enterprise Benchmark v3.0.0: Score less than 30% (26)	9	1
501	New wazuh agent connected.	3	1

Groups summary

Groups	Count
sca	483
windows	38
ossec	35
authentication_success	34
windows_security	34
syscheck	27
syscheck_file	27
syscheck_entry_added	11
syscheck_entry_deleted	9
syscheck_entry_modified	7
virustotal	7
policy_changed	2
windows_application	2
windows_system	2