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

Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	DC-Server	192.168.50.5	Wazuh v4.7.5	ubuntu	Microsoft Windows Server 2019 Standard 10.0.17763.3650	Jul 10, 2025 @ 07:59:07.000	Jul 10, 2025 @ 09:50:26.000

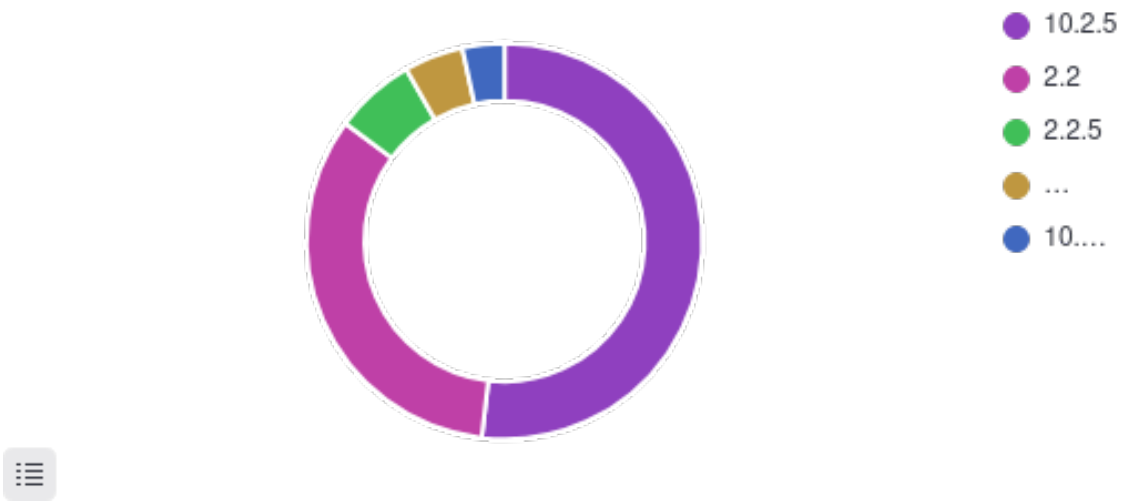
Group: default

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

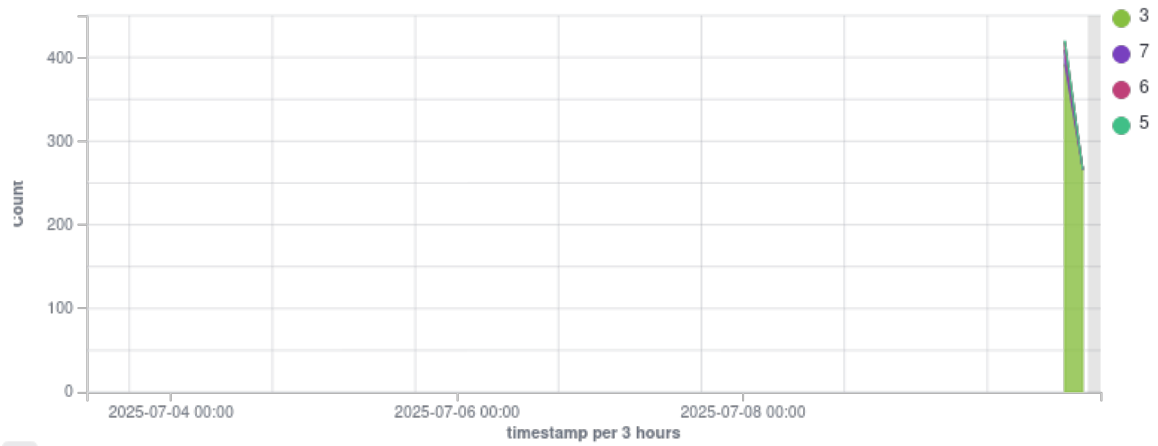
2025-07-03T09:50:26 to 2025-07-10T09:50:26

manager.name: ubuntu AND agent.id: 001

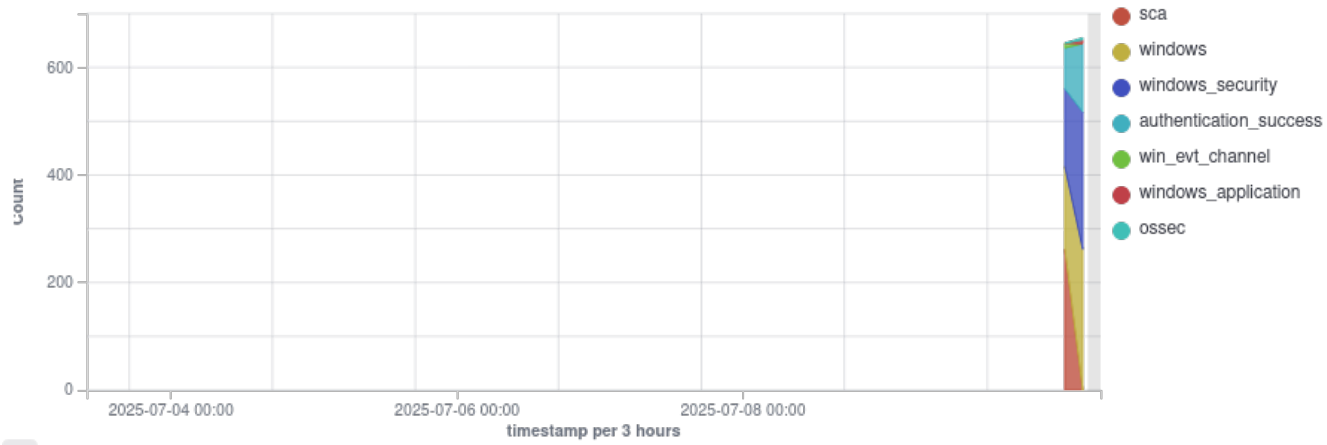
Top 5 PCI DSS requirements



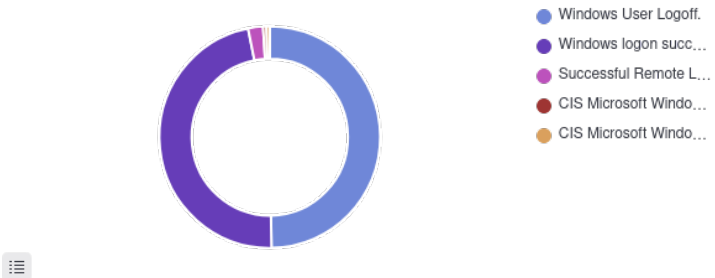
Alerts



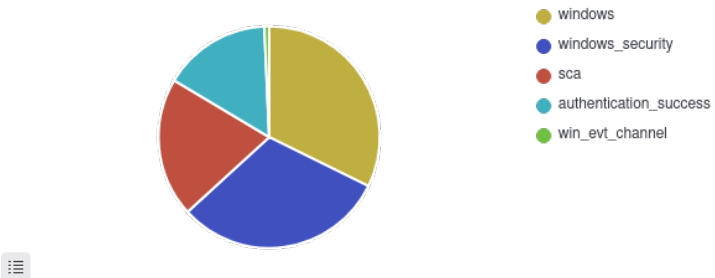
Alert groups evolution



Top 5 alerts



Top 5 rule groups



Alerts summary

Rule ID	Description	Level	Count
60137	Windows User Logoff.	3	205
60106	Windows logon success.	3	194
92652	Successful Remote Logon Detected - User:\Administrator - NTLM authentication, possible pass-the-hash attack.	6	9
503	Wazuh agent started.	3	3
506	Wazuh agent stopped.	3	3
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Basic authentication' is set to 'Disabled'	3	2
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow unencrypted traffic' is set to 'Disabled'	3	2
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Online Tips' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Remote Shell Access' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' or 'Enabled: 1 - Basic'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Use of Camera' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow input personalization' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'	3	1
19009	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Configure 'Network access: Remotely accessible registry paths and sub-paths'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Configure 'Network access: Remotely accessible registry paths'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	3	1

Rule ID	Description	Level	Count
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	3	1
19008	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	3	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Configure 'Network access: Named Pipes that can be accessed anonymously'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn and prevent bypass'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	7	1

Rule ID	Description	Level	Count
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	7	1
19007	CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Ensure LAPS AdmPwd GPO Extension / CSE is installed	7	1
19003	SCA summary: CIS Microsoft Windows Server 2019 Benchmark v1.0.1: Score less than 80% (69)	5	1
501	New wazuh agent connected.	3	1
60610	Windows installer began an installation process.	3	1
60635	Windows installer reconfigured the product.	3	1
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
61109	Name resolution for the name v10.events.data.microsoft.com timed out	5	1
657	Active response: restart-wazuh.exe - add	3	1

Groups summary

Groups	Count
windows	416
windows_security	399
sca	262
authentication_success	203
win_evt_channel	9
ossec	8
windows_application	7
active_response	1
windows_system	1