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 @ 21:22:24.000

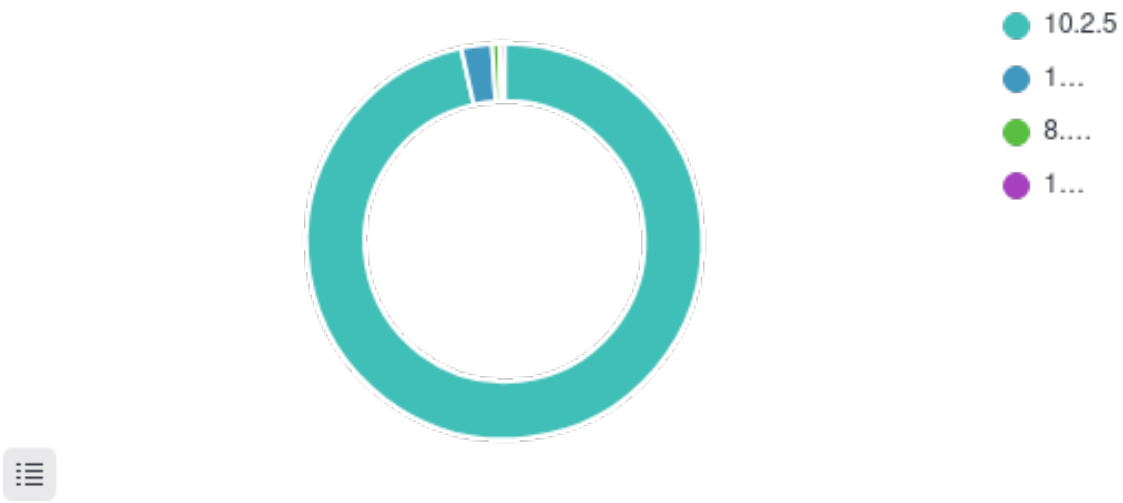
Group: default

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

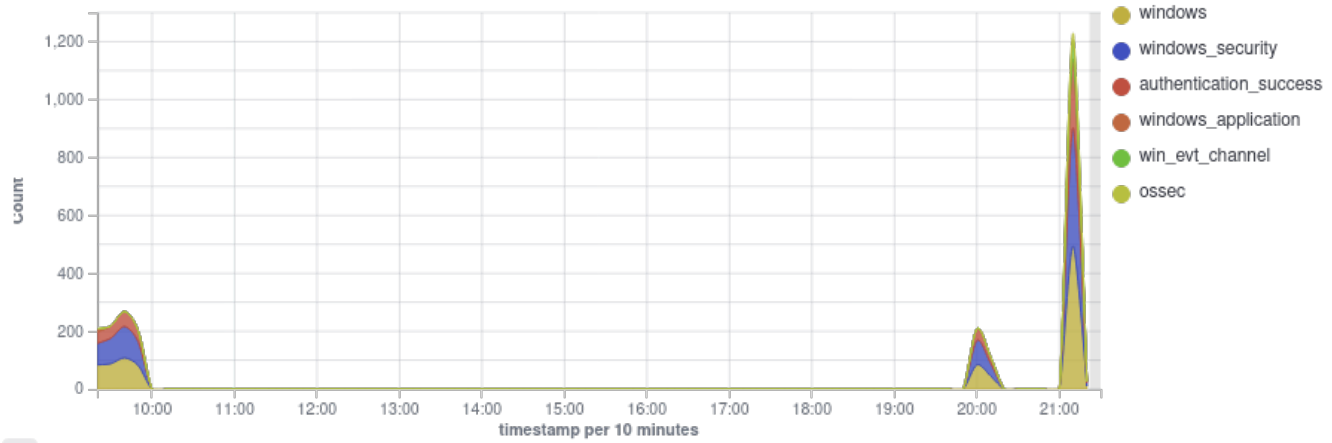
2025-07-10T09:22:25 to 2025-07-10T21:22:25

manager.name: ubuntu AND agent.id: 001

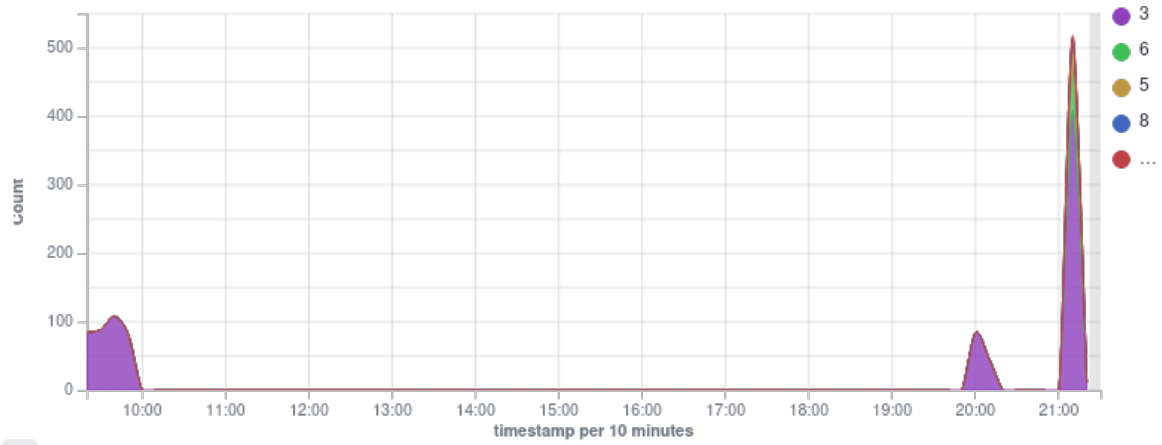
Top 5 PCI DSS requirements



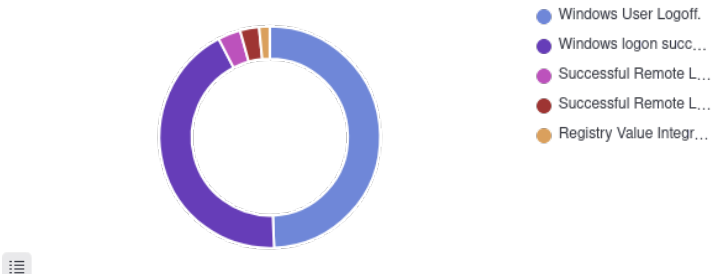
Alert groups evolution



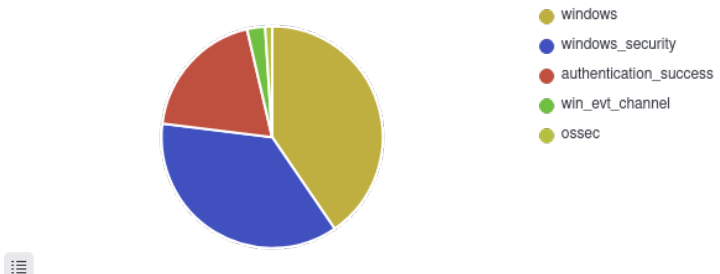
Alerts



Top 5 alerts



Top 5 rule groups



Alerts summary

Rule ID	Description	Level	Count
60137	Windows User Logoff.	3	478
60106	Windows logon success.	3	416
92652	Successful Remote Logon Detected - User:\Administrator - NTLM authentication, possible pass-the-hash attack.	6	32
92652	Successful Remote Logon Detected - User:\bob - NTLM authentication, possible pass-the-hash attack.	6	27
750	Registry Value Integrity Checksum Changed	5	15
594	Registry Key Integrity Checksum Changed	5	9
61102	Windows System error event	5	8
61138	New Windows Service Created	5	6
61104	Service startup type was changed	3	4
92652	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	6	3
92650	New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.	12	3
60109	User account enabled or created.	8	2
60110	User account changed.	8	2
60642	Software protection service scheduled successfully.	3	2
60798	The database engine attached a database.	3	2
60805	The database engine is starting a new instance.	3	2
60807	The database engine is initiating recovery steps.	3	2
60808	The database engine is replaying log file C:\Winnt\system32\wins\j50.log.	3	2
60809	The database engine has completed recovery steps.	3	2
60147	Security enabled local group changed.	5	1
60154	Administrators group changed.	12	1
60778	The shell stopped unexpectedly.	5	1
61110	Multiple System error events	10	1
752	Registry Value Entry Added to the System	5	1

Groups summary

Groups	Count
windows	997
windows_security	900
authentication_success	478
win_evt_channel	65
ossec	25
syscheck	25
syscheck_registry	25
syscheck_entry_modified	24
windows_system	19
windows_application	13
system_error	8
account_changed	4
policy_changed	4
adduser	2
group_changed	2
win_group_changed	2
syscheck_entry_added	1