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

Threat hunting report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	WIN-3KH74N2U82B	10.10.10.6	Wazuh v4.11.2	mail.strayerraptors.com	Microsoft Windows Server 2019 Standard 10.0.17763.7136	May 2, 2025 @ 23:13:38.000	May 7, 2025 @ 22:03:56.000

Group: default

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

2025-05-06T22:04:02 to 2025-05-07T22:04:02

manager.name: mail.strayerraptors.com AND agent.id: 001

972

- Total -

0

- Level 12 or above alerts -

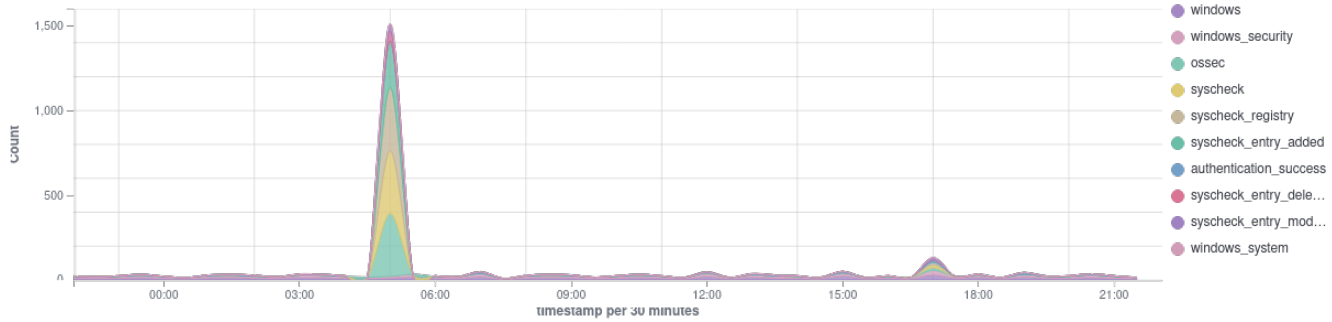
0

- Authentication failure -

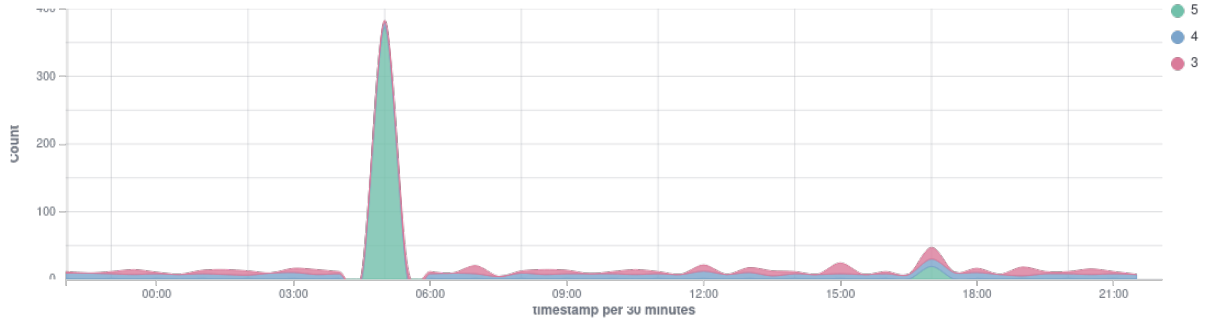
157

- Authentication success -

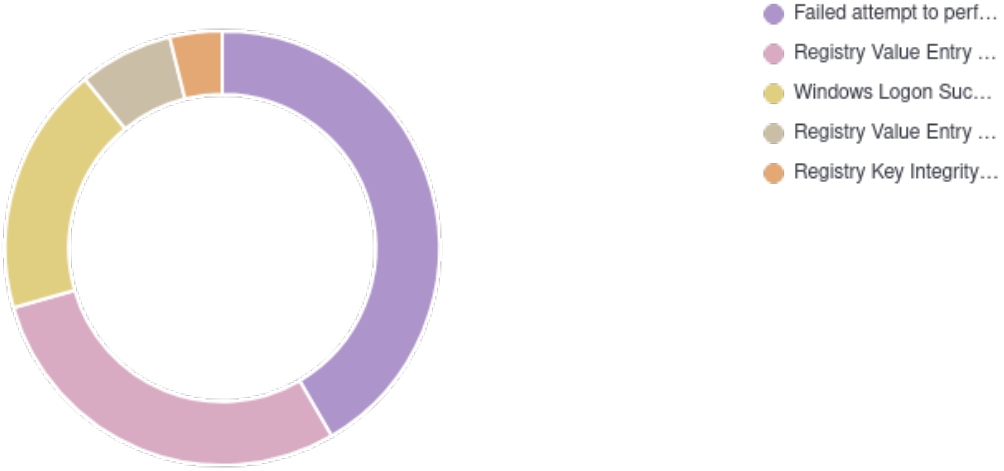
Top 10 Alert groups evolution



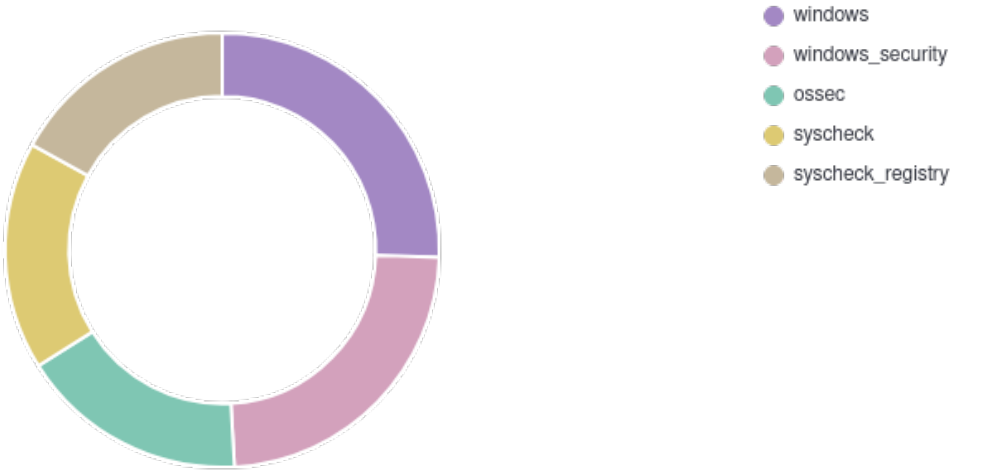
Alerts



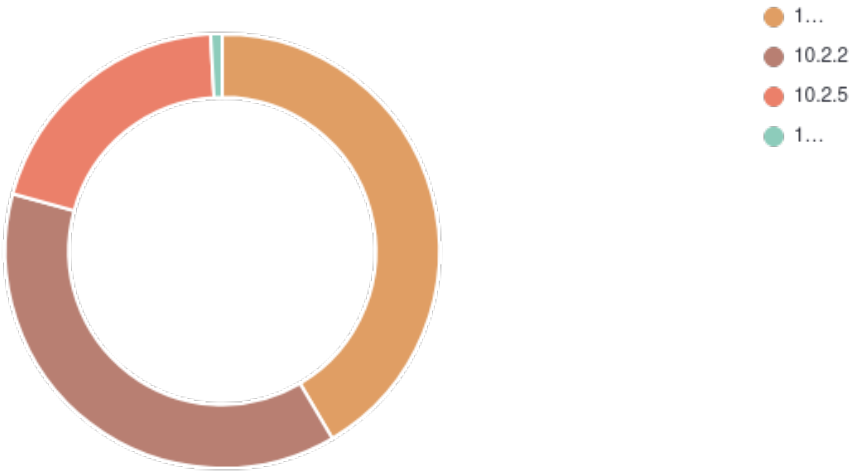
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
60107	Failed attempt to perform a privileged operation	4	352
752	Registry Value Entry Added to the System	5	245
60106	Windows Logon Success	3	157
751	Registry Value Entry Deleted.	5	59
594	Registry Key Integrity Checksum Changed	5	33
60137	Windows User Logoff	3	29
598	Registry Key Entry Added to the System	5	27
61102	Windows System error event	5	25
750	Registry Value Integrity Checksum Changed	5	24
61104	Service startup type was changed	3	8
60642	Software protection service scheduled successfully.	3	6
60228	A scheduled task was created	4	1
60646	License activation (slui.exe) failed.	5	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

Groups summary

Groups	Count
windows	584
windows_security	539
ossec	388
syscheck	388
syscheck_registry	388
syscheck_entry_added	272
authentication_success	157
syscheck_entry_deleted	59
syscheck_entry_modified	57
windows_system	33
system_error	25
windows_application	12
policy_changed	8
ipsec	1