

Security events report

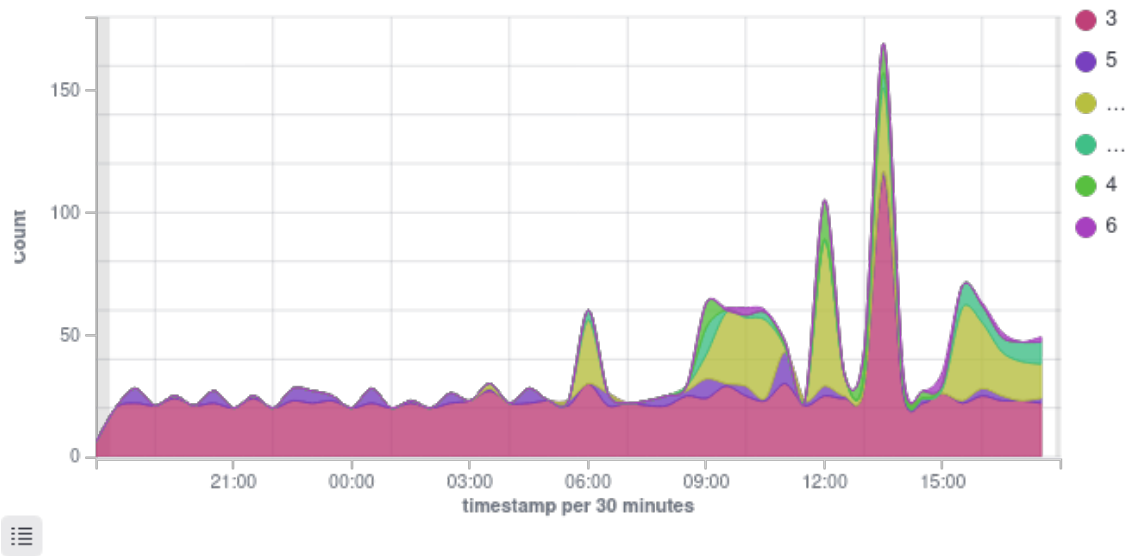
ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
020	hq06	134.23.3.16	Wazuh v4.2.2	wazuh	Microsoft Windows 10 IoT Enterprise LTSC 2021 10.0.19044	May 20, 2024 @ 16:19:20.000	Dec 30, 2024 @ 17:51:40.000

Group: default

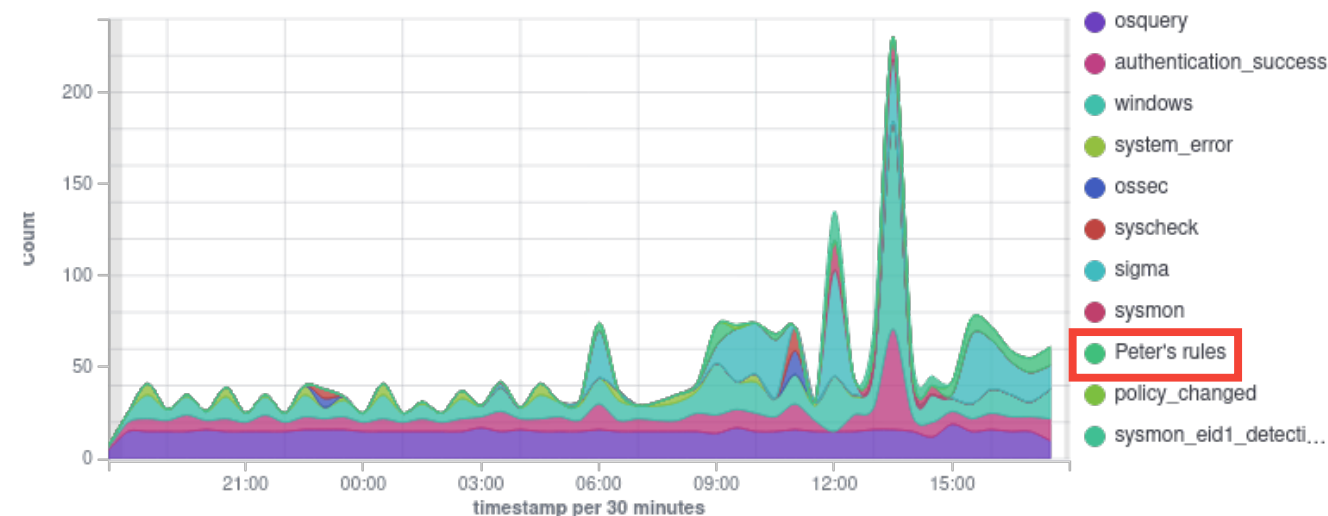
Browse through your security alerts, identifying issues and threats in your environment.

🕒 2024-12-29T17:51:42 to 2024-12-30T17:51:42
🔍 manager.name: wazuh AND agent.id: 020

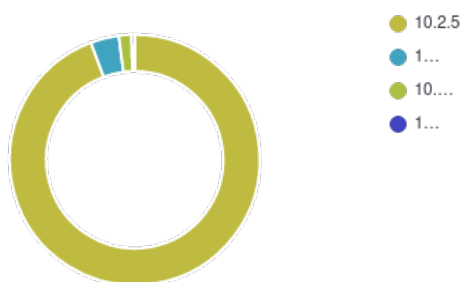
Alerts



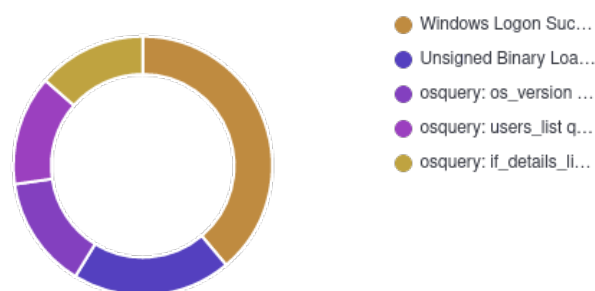
Alert groups evolution



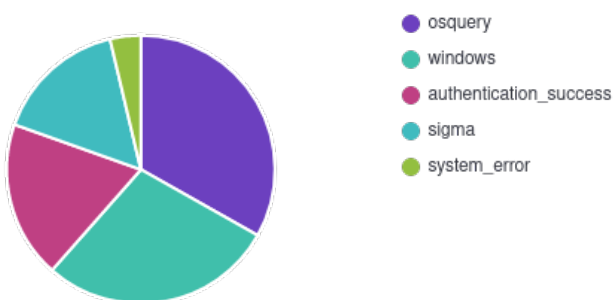
Top 5 PCI DSS requirements



Top 5 alerts



Top 5 rule groups



Alerts summary

Rule ID	Description	Level	Count
18107	Windows Logon Success.	3	420
900228	Unsigned Binary Loaded From Suspicious Location	13	214
24010	osquery: os_version query result	3	151
24010	osquery: users_list query result	3	148
24010	osquery: if_details_list query result	3	146
24010	osquery: system_info query result	3	146
24010	osquery: if_addr_list query result	3	143
900852	DNS TXT Answer with Possible Execution Strings	13	134
18103	Windows error event.	5	82
18149	Windows User Logoff.	3	44
92052	Windows command prompt started by an abnormal process	4	38
100011	Greedy File Deletion using Del	10	24
100009	File Decoded From Base64/Hex Via Certutil.EXE	10	19
92004	Powershell process spawned Windows command shell instance	4	16
100008	File Encoded To Base64 Via Certutil.EXE	10	10
750	Registry Value Integrity Checksum Changed	5	10
100004	Msiexec Quiet Installation	10	8
18147	Windows: Application Installed.	5	8
92073	Powershell executing certutil to decode a file	6	8
100012	File and SubFolder Enumeration via Dir Command	6	7
594	Registry Key Integrity Checksum Changed	5	6
92032	Suspicious Windows cmd shell execution	3	5
100005	MsiExec Web Install	10	4
100002	Potential PsExec Remote Execution	13	2
18145	Windows: Service startup type was changed.	3	2
751	Registry Value Entry Deleted.	5	2
900602	Suspicious Epmmap Connection	13	2
92027	Powershell process spawned powershell instance	4	2
92200	Scripting file created under Windows Temp or User folder	6	2
100006	Program Executed Using Proxy/Local Command Via SSH.EXE	10	1
100007	Port Forwarding Activity Via SSH.EXE	10	1
100010	New Root Certificate Installed Via Certutil.EXE	10	1
900400	Legitimate Application Dropped Executable	13	1
92021	Powershell was used to delete files or directories	3	1
92055	Known auto-elevated utility FodHelper.EXE may have been used to bypass UAC	12	1

Groups summary

Groups	Count
osquery	734
windows	629
authentication_success	420
sigma	351
system_error	82
Peter's rules	77
sysmon	73
sysmon_eid1_detections	71
ossec	18
syscheck	18
syscheck_registry	18
syscheck_entry_modified	16
policy_changed	2
syscheck_entry_deleted	2
sysmon_eid11_detections	2