

Security events report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
026	snort-srv	134.23.17.133	Wazuh v4.3.2	wazuh	Ubuntu 22.04.1 LTS	May 20, 2024 @ 17:03:32.000	Dec 17, 2024 @ 12:43:44.000

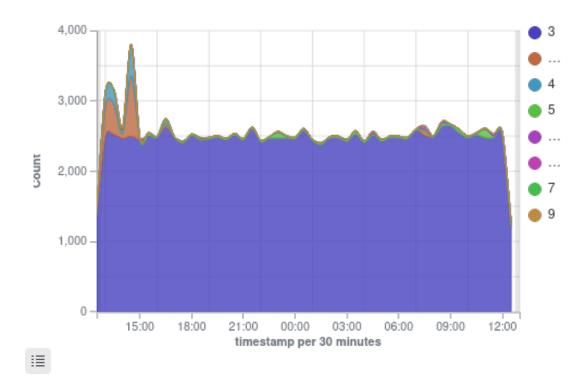
Group: default

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

② 2024-12-16T12:43:42 to 2024-12-17T12:43:42

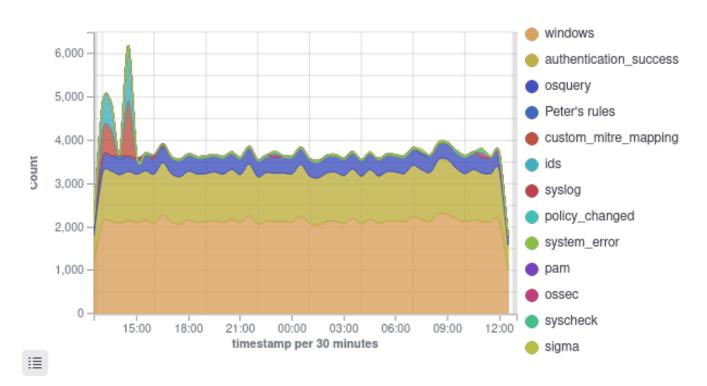
Q manager.name: wazuh

Alerts





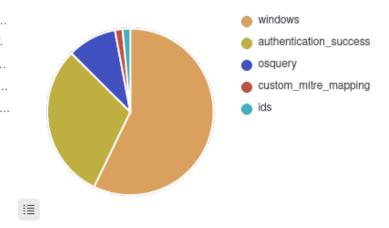
Alert groups evolution





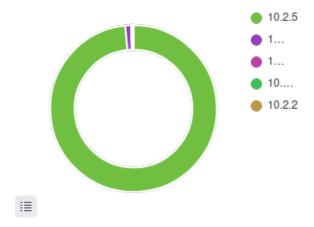
Windows Logon Suc... Windows User Logoff. osquery: if_details_li... osquery: if_addr_list ... osquery: system_info...

Top 5 rule groups





Top 5 PCI DSS requirements





Alerts summary

18107 Windows User Logoff. 3 54324 18149 Windows User Logoff. 3 45436 24010 osquery if details list query result 3 3461 24010 osquery, exident list query result 3 3462 24010 osquery, users list query result 3 3448 24010 osquery, users list query result 3 3448 24010 osquery, users list query result 3 3448 24010 osquery, osversion query result 3 3481 24010 osquery, system linfo query result 3 3171 24010 osquery, system linfo query result 3 3171 24010 osquery system linfo query result 3 3171 24010 osquery system linfo	Rule ID	Description	Level	Count
24010 osqueny; if, details: list query result 3 3477 24010 osqueny; if, addr list query result 3 3461 24010 osqueny; system_info query result 3 3452 24010 osqueny; system_info query result 3 3448 24010 osqueny; six erising query result 3 3848 24010 Souerey; os, version query result 3 3884 24010 Souerey; os, version query result 3 3884 24010 Snort alert of priority 1 concerning Potential Corporate Privacy Violation. Unknown mapping to Mitre tactics or techniques 10 1717 18163 Windows: Service startup type was changed. 3 1177 18103 Windows: Service startup type was changed. 3 1177 18103 Windows: Service startup type was changed. 3 1171 2000 Sond aller of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 Us NetworkCleartext Logon Success. 3 936 18260 Us NetworkCleartext Logon Success. 3 151	18107	Windows Logon Success.	3	54334
24010 osquery, if addr list query result 3 3461 24010 osquery, system info query result 3 3452 24010 osquery, users_list query result 3 3482 24010 osquery, users_list query result 3 3884 24010 source, os version query result 3 3884 24010 Snort alert of priority 1 concerning Potential Corporate Privacy Violation. Unknown mapping to Mitre tactics or techniques. 10 1717 18103 Windows service startup type was changed. 3 1177 18103 Windows error event. 5 1011 20200 Snort alert of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 Ilis NetworkCleartext Logon Success 3 936 900228 Unsigned Binary Loaded From Suspicious Location 13 218 180017 Teckedy File Deletion using Del 10 213 5501 PAM: Login session olosed. 3 151 5502 PAM: Login session closed. 3 113 5402	18149	Windows User Logoff.	3	45436
24010 osquery: system.info query result 3 3452 24010 osquery: users list query result 3 3448 24010 osquery: users list query result 3 3484 24010 osquery: users list query result 3 3384 240400 Short allert of priority 1 concerning Potential Corporate Privacy Violation. Unknown mapping to Mitre tactics or learning techniques. 10 1717 18163 Windows: Service startup type was changed. 3 1177 18103 Windows: Service startup type was changed. 3 1177 18260 IlS NetworkCleartext Logon Success 3 936 18260 IlS NetworkCleartext Logon Success 3 936 900228 Unsigned Rinary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Sysmon -	24010	osquery: if_details_list query result	3	3477
24010 osquery, users list query result 3 3448 24010 osquery, os, version query result 3 3884 24010 Shorr alert of priority 1 concerning Potential Corporate Privacy Violation. Unknown mapping to Mitre tactics or techniques. 10 1717 18145 Windows: Service startup type was changed. 3 1177 18103 Windows error event. 5 1011 20000 Shorr alert of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 IIS NeworkCleartext Logon Success 3 936 18200 Insigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session of closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 8402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618	24010	osquery: if_addr_list query result	3	3461
24010 asquery; as version query result 3 3384 20400 Short alert of priority 1 concerning Potential Corporate Privacy Violation, Unknown mapping to Mitre tactics or techniques. 10 1717 18145 Windows: Service startup type was changed. 3 1177 18103 Windows: Service startup type was changed. 5 1011 20200 Short alert of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 IIS NetworkCleartext Logon Success 3 936 902228 Unsigned Binary Loaded From Suspicious Location 13 218 900228 Unsigned Binary Loaded From Suspicious Location 10 213 5501 PAM: Login session opened. 10 213 5502 PAM: Login session closed. 3 113 7503 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 9 61618 Symnon - Suspicious Process - sychost exe 12 75 </td <td>24010</td> <td>osquery: system_info query result</td> <td>3</td> <td>3452</td>	24010	osquery: system_info query result	3	3452
20/000 Short alert of priority 1 concerning Potential Corporate Privacy Violation, Unknown mapping to Mitre tactics or techniques. 10 1717 18145 Windows: Service startup type was changed. 3 1177 182020 Short alert of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 IIS NetworkCleartext Logon Success 3 936 900228 Unsigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session olosed. 3 151 5502 PAM: Login session closed. 3 151 7503 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Symnor - Suspicious Process - sychost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Logifle rotated. 3 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14	24010	osquery: users_list query result	3	3448
techniques 3 117 181145 Windows: Service startup type was changed. 3 1171 18103 Windows: Service startup type was changed. 5 1011 20200 Snort alert of priority? Sconcerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 Ils Network/Cleartext Logon Success 3 936 900228 Unsigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 5501 PAM: Login session closed. 3 113 570 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - sychost exe 12 75 510 Host-based anomally detection event (rootcheck). 7 40	24010	osquery: os_version query result	3	3384
18103 Windows error event. 5 1011 20200 Snort alert of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 IIS NetworkCleartext Logon Success 3 936 900228 Unsigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - sychost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 3 4 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16	20400		10	1717
20200 Snort alert of priority 3 concerning. Unknown mapping to Mitre tactics or techniques. 4 960 18260 Ils NetworkCleartext Logon Success 3 936 900228 Unsigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 5715 sshd: duthentication success. 3 16	18145	Windows: Service startup type was changed.	3	1177
18260 IIS NetworkCleartext Logon Success 3 936 900228 Unsigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful Sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - sychost.eve 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 203 Agent event queue is full. Events may be lost. 9 13 18120 Wi	18103	Windows error event.	5	1011
900228 Unsigned Binary Loaded From Suspicious Location 13 218 100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 50% full. 7 14 205 Agent event queue is full. Events may be lost. 9 13 18140 Windows: Syste	20200	Snort alert of priority 3 concerning . Unknown mapping to Mitre tactics or techniques.	4	960
100017 Greedy File Deletion using Del 10 213 5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 203 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time chan	18260	IIS NetworkCleartext Logon Success	3	936
5501 PAM: Login session opened. 3 151 5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is book to normal load. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creati	900228	Unsigned Binary Loaded From Suspicious Location	13	218
5502 PAM: Login session closed. 3 113 750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 205 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 190738 Creation Of An User	100017	Greedy File Deletion using Del	10	213
750 Registry Value Integrity Checksum Changed 5 98 5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 205 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18275 Windows: TS Gateway login success. 3 12 200738 Creation Of An User Account 10 12 100014 File Encoded To B	5501	PAM: Login session opened.	3	151
5402 Successful sudo to ROOT executed. 3 97 594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 205 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service	5502	PAM: Login session closed.	3	113
594 Registry Key Integrity Checksum Changed 5 92 61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File D	750	Registry Value Integrity Checksum Changed	5	98
61618 Sysmon - Suspicious Process - svchost.exe 12 75 510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 203 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 <	5402	Successful sudo to ROOT executed.	3	97
510 Host-based anomaly detection event (rootcheck). 7 40 591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 <td>594</td> <td>Registry Key Integrity Checksum Changed</td> <td>5</td> <td>92</td>	594	Registry Key Integrity Checksum Changed	5	92
591 Log file rotated. 3 34 550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5 <td>61618</td> <td>Sysmon - Suspicious Process - svchost.exe</td> <td>12</td> <td>75</td>	61618	Sysmon - Suspicious Process - svchost.exe	12	75
550 Integrity checksum changed. 7 20 5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 10015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	510	Host-based anomaly detection event (rootcheck).	7	40
5715 sshd: authentication success. 3 16 18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	591	Log file rotated.	3	34
18154 Multiple Windows error events. 10 14 202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	550	Integrity checksum changed.	7	20
202 Agent event queue is 90% full. 7 14 205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	5715	sshd: authentication success.	3	16
205 Agent event queue is back to normal load. 3 14 203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	18154	Multiple Windows error events.	10	14
203 Agent event queue is full. Events may be lost. 9 13 18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	202	Agent event queue is 90% full.	7	14
18140 Windows: System time changed. 5 12 18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	205	Agent event queue is back to normal load.	3	14
18257 Windows: TS Gateway login success. 3 12 900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	203	Agent event queue is full. Events may be lost.	9	13
900738 Creation Of An User Account 10 12 100014 File Encoded To Base64 Via Certutil.EXE 10 11 40704 Systemd: Service exited due to a failure. 5 11 100015 File Decoded From Base64/Hex Via Certutil.EXE 10 10 533 Listened ports status (netstat) changed (new port opened or closed). 7 6 92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	18140	Windows: System time changed.	5	12
100014File Encoded To Base64 Via Certutil.EXE101140704Systemd: Service exited due to a failure.511100015File Decoded From Base64/Hex Via Certutil.EXE1010533Listened ports status (netstat) changed (new port opened or closed).7692021Powershell was used to delete files or directories36100005PsExec Service Execution105	18257	Windows: TS Gateway login success.	3	12
40704Systemd: Service exited due to a failure.511100015File Decoded From Base64/Hex Via Certutil.EXE1010533Listened ports status (netstat) changed (new port opened or closed).7692021Powershell was used to delete files or directories36100005PsExec Service Execution105	900738	Creation Of An User Account	10	12
100015File Decoded From Base64/Hex Via Certutil.EXE1010533Listened ports status (netstat) changed (new port opened or closed).7692021Powershell was used to delete files or directories36100005PsExec Service Execution105	100014	File Encoded To Base64 Via Certutil.EXE	10	11
533Listened ports status (netstat) changed (new port opened or closed).7692021Powershell was used to delete files or directories36100005PsExec Service Execution105	40704	Systemd: Service exited due to a failure.	5	11
92021 Powershell was used to delete files or directories 3 6 100005 PsExec Service Execution 10 5	100015	File Decoded From Base64/Hex Via Certutil.EXE	10	10
100005 PsExec Service Execution 10 5	533	Listened ports status (netstat) changed (new port opened or closed).	7	6
	92021	Powershell was used to delete files or directories	3	6
100006 Potential PsExec Remote Execution 13 5	100005	PsExec Service Execution	10	5
	100006	Potential PsExec Remote Execution	13	5



Rule ID	Description	Level	Count
100007	PsExec Service Child Process Execution as LOCAL SYSTEM	13	5
100010	Msiexec Quiet Installation	10	5
100012	Program Executed Using Proxy/Local Command Via SSH.EXE	10	5
100013	Port Forwarding Activity Via SSH.EXE	10	5
100016	New Root Certificate Installed Via Certutil.EXE	10	5
5503	PAM: User login failed.	5	5
900602	Suspicious Epmap Connection	13	5
92055	Known auto-elevated utility FodHelper.EXE may have been used to bypass UAC	12	4
900780	Persistence Via Cron Files	10	3
900852	DNS TXT Answer with Possible Execution Strings	13	3
20200	Snort alert of priority 3 concerning Misc activity. Unknown mapping to Mitre tactics or techniques.	4	2
752	Registry Value Entry Added to the System	5	2
900714	Antivirus Exploitation Framework Detection	15	2
100011	MsiExec Web Install	10	1
20101	Snort alert of priority 0 concerning .	3	1
5557	unix_chkpwd: Password check failed.	5	1



Groups summary

Groups	Count
windows	103017
authentication_success	54513
osquery	17222
custom_mitre_mapping	2680
ids	2680
policy_changed	1177
system_error	1011
syslog	383
ossec	292
Peter's rules	270
pam	270
sigma	243
syscheck	212
syscheck_entry_modified	210
syscheck_registry	192
sudo	97
sysmon	85
sysmon_process-anomalies	75
agent_flooding	41
wazuh	41
rootcheck	40
syscheck_file	20
sshd	16
time_changed	12
local	11
systemd	11
sysmon_eid1_detections	10
authentication_failed	6
syscheck_entry_added	2