# Threat hunting report

Warning. Agent is disconnected

| ID | Name | IP address | Version | Manager | Operating system | Registration date | Last keep alive |
|---|---|---|---|---|---|---|---|
| 001 | Windows-Server-2022 | 172.17.179.5 | Wazuh v4.14.1 | wazuh.manager | Microsoft Windows Server 2025 Datacenter Evaluation 10.0.26100.4946 | Jan 5, 2026 @ 00:41:57.000 | Jan 5, 2026 @ 21:25:06.000 |

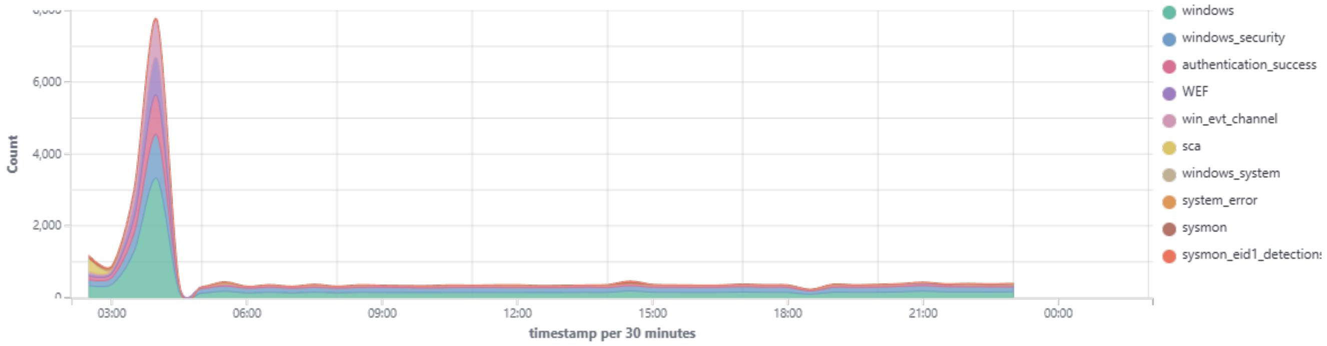
Group: default

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

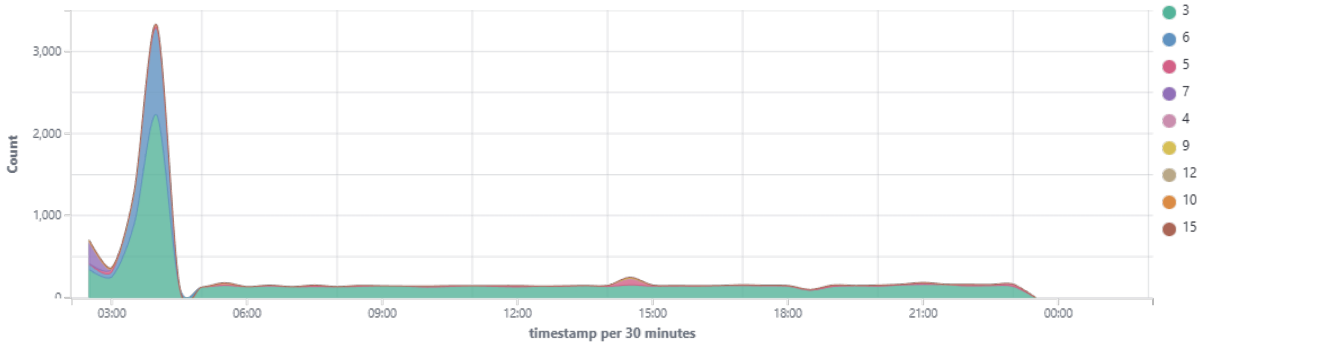
🕘 2026-01-05T02:06:19 to 2026-01-06T02:06:19

🔍 manager.name: wazuh.manager AND agent.id: 001

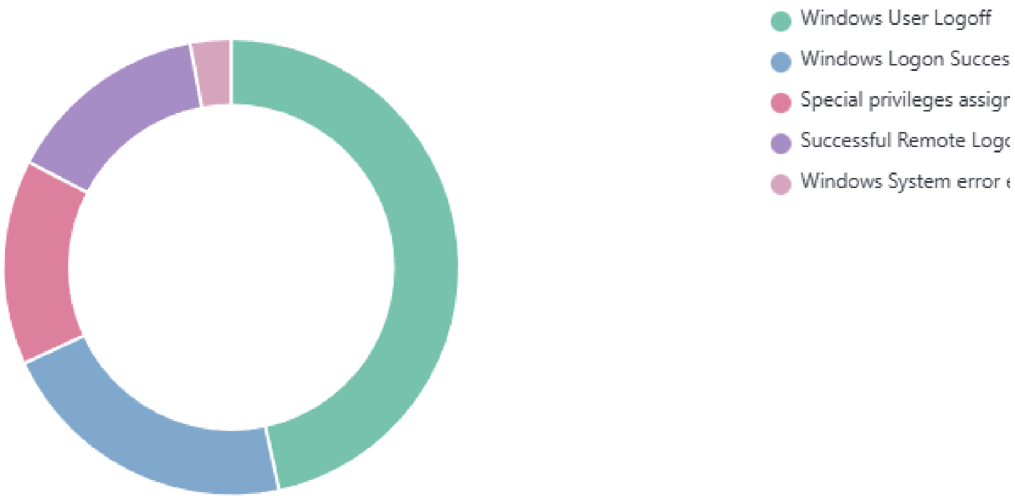
## Top 10 Alert groups evolution



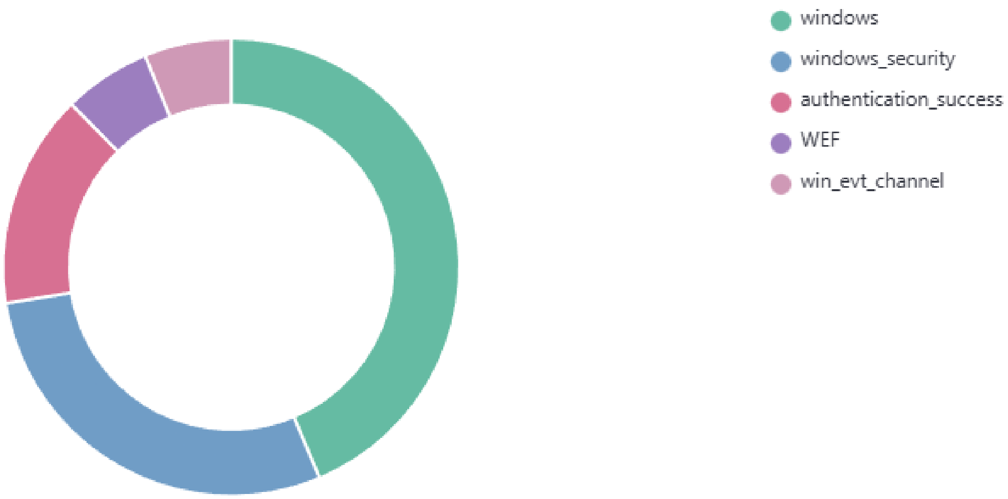
## Alerts



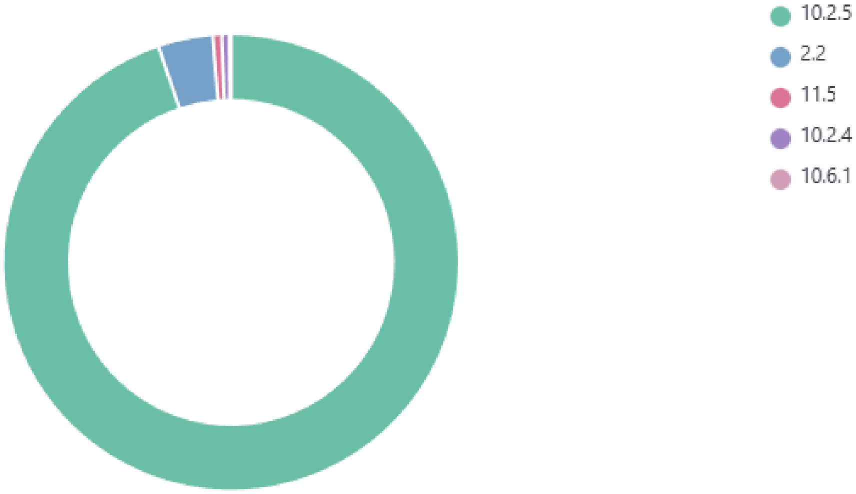
## Top 5 alerts



## Top 5 rule groups



## Top 5 PCI DSS Requirements



**11,462**
- Total -

**25**
- Level 12 or above alerts -

**49**
- Authentication failure -

**3,833**
- Authentication success -

## Alerts summary

| Rule ID | Description | Level | Count |
|---|---|---|---|
| 60137 | Windows User Logoff | 3 | 4944 |
| 60106 | Windows Logon Success | 3 | 2277 |
| 67028 | Special privileges assigned to new logon. | 3 | 1541 |
| 92657 | Successful Remote Logon Detected - User:\labuser - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that linuxserver24 is allowed to perform RDP connections | 6 | 1534 |
| 61102 | Windows System error event | 5 | 308 |
| 60642 | Software protection service scheduled successfully. | 3 | 97 |
| 60122 | Logon Failure - Unknown user or bad password | 5 | 44 |
| 750 | Registry Value Integrity Checksum Changed | 5 | 31 |
| 92205 | Powershell process created an executable file in Windows root folder | 9 | 28 |
| 92032 | Suspicious Windows cmd shell execution | 3 | 23 |
| 92052 | Windows command prompt started by an abnormal process | 4 | 22 |
| 92652 | Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack. | 6 | 22 |
| 92066 | C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe | 4 | 21 |
| 92058 | Application Compatibility Database launched | 12 | 20 |
| 594 | Registry Key Integrity Checksum Changed | 5 | 19 |
| 92021 | Powershell was used to delete files or directories | 3 | 18 |
| 60608 | Summary event of the report's signatures. | 4 | 16 |
| 92031 | Discovery activity executed | 3 | 15 |
| 67023 | Non service account logged off. | 3 | 13 |
| 61110 | Multiple System error events | 10 | 12 |
| 67022 | Non network or service local logon. | 3 | 12 |
| 92201 | C:\\WINDOWS\\System32\\WindowsPowershell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder | 9 | 11 |
| 598 | Registry Key Entry Added to the System | 5 | 8 |
| 92201 | C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder | 9 | 6 |
| 60104 | Windows audit failure event | 5 | 6 |
| 60204 | Multiple Windows Logon Failures | 10 | 5 |
| 92027 | Powershell process spawned powershell instance | 4 | 5 |
| 91816 | Powershell script querying system environment variables | 4 | 4 |
| 92033 | Discovery activity spawned via powershell execution | 3 | 4 |
| 92213 | Executable file dropped in folder commonly used by malware | 15 | 4 |
| 60776 | TrustedInstaller was unavailable to handle a critical | 7 | 3 |

| Rule ID | Description | Level | Count |
|---|---|---|---|
| | notification event. | | |
| 91820 | Powershell script recursively collected files from a filesystem search | 4 | 3 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Basic authentication' is set to 'Disabled'. | 3 | 2 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow unencrypted traffic' is set to 'Disabled'. | 3 | 2 |
| 92037 | A net.exe connection to a remote resource was started by C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe | 3 | 2 |
| 92037 | A net.exe connection to a remote resource was started by C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell_ise.exe | 3 | 2 |
| 19005 | SCA summary: CIS Microsoft Windows Server 2025 Benchmark: Score less than 30% (27) | 9 | 2 |
| 60602 | Windows application error event. | 9 | 2 |
| 61104 | Service startup type was changed | 3 | 2 |
| 92110 | Detected WinRM activity from 0:0:0:0:0:0:0:1 to 0:0:0:0:0:0:0:1 | 4 | 2 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Accounts: Rename administrator account'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Accounts: Rename guest account'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Interactive logon: Message text for users attempting to log on'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Interactive logon: Message title for users attempting to log on'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Network access: Named Pipes that can be accessed anonymously' (DC only). | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Network access: Named Pipes that can be accessed anonymously' (MS only). | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)'). | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Account lockout duration' is set to '15 or more minute(s)'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Accounts: Guest account status' is set to 'Disabled' (MS only). | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow | 7 | 1 |

| Rule ID | Description | Level | Count |
|---|---|---|---|
| | Clipboard synchronization across devices' is set to 'Disabled'. | | |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Custom SSPs and APs to be loaded into LSASS' is set to 'Disabled'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Online Tips' is set to 'Disabled'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'. | 7 | 1 |
| 19007 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow Remote Shell Access' is set to 'Disabled'. | 7 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Network access: Remotely accessible registry paths and sub-paths' is configured. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Configure 'Network access: Remotely accessible registry paths' is configured. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow remote server management through WinRM' is set to 'Disabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Allow user control over installs' is set to 'Disabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Always install with elevated privileges' is set to 'Disabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only). | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Audit Policy Change' is set to include 'Success'. | 3 | 1 |

| Rule ID | Description | Level | Count |
|---|---|---|---|
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Authentication Policy Change' is set to include 'Success'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Computer Account Management' is set to include 'Success' (DC only). | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Logoff' is set to include 'Success'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Logon' is set to 'Success and Failure'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Other System Events' is set to 'Success and Failure'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Security Group Management' is set to include 'Success'. | 3 | 1 |
| 19008 | CIS Microsoft Windows Server 2025 Benchmark: Ensure 'Audit Security State Change' is set to include 'Success'. | 3 | 1 |
| 501 | New wazuh agent connected. | 3 | 1 |
| 503 | Wazuh agent started. | 3 | 1 |
| 504 | Wazuh agent disconnected. | 3 | 1 |
| 506 | Wazuh agent stopped. | 3 | 1 |
| 61107 | Remote Desktop Services terminated unexpectedly | 5 | 1 |
| 61109 | Name resolution for the name client.wns.windows.com timed out | 5 | 1 |
| 62107 | Windows Defender: Antimalware scan started | 3 | 1 |
| 62108 | Windows Defender: Antimalware scan finished | 3 | 1 |
| 62154 | Windows Defender: Antimalware platform feature configuration changed | 5 | 1 |
| 657 | Active response: restart-wazuh.exe - add | 3 | 1 |
| 92036 | A C:\\Windows\\System32\\net.exe binary was started by a Windows cmd shell | 3 | 1 |
| 92071 | A powershell process created by WMI executed a base64 encoded command | 12 | 1 |

## Groups summary

| Groups | Count |
|---|---|
| windows | 11038 |
| windows_security | 7276 |
| authentication_success | 3833 |
| WEF | 1566 |
| win_evt_channel | 1557 |
| sca | 361 |
| windows_system | 324 |
| system_error | 310 |
| sysmon | 187 |
| sysmon_eid1_detections | 134 |
| windows_application | 118 |
| ossec | 63 |
| syscheck | 58 |
| syscheck_registry | 58 |
| sysmon_eid11_detections | 51 |
| syscheck_entry_modified | 50 |
| authentication_failed | 44 |
| syscheck_entry_added | 8 |
| powershell | 7 |
| authentication_failures | 5 |
| windows_defender | 3 |
| policy_changed | 2 |
| sysmon_eid3_detections | 2 |
| active_response | 1 |