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

Security events report

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

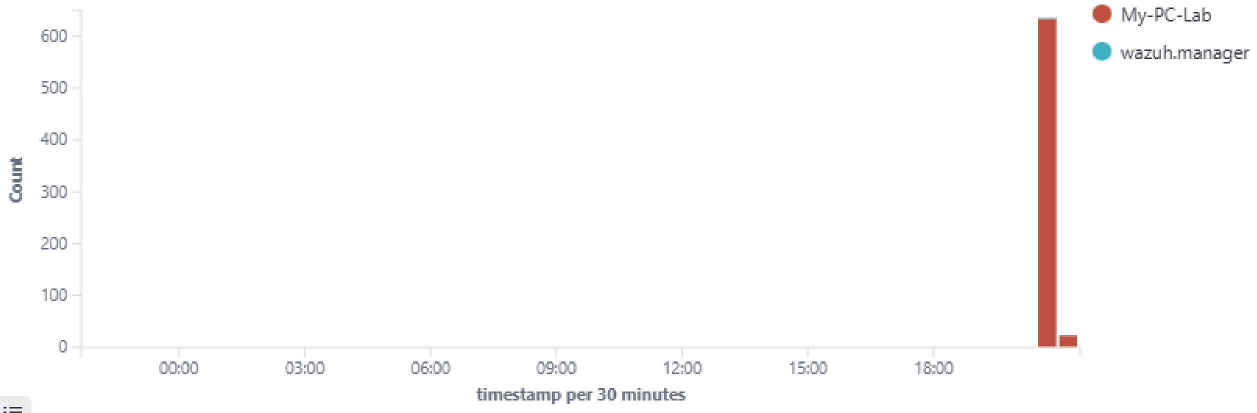
2026-01-27T21:40:15 to 2026-01-28T21:30:00

manager.name: wazuh.manager

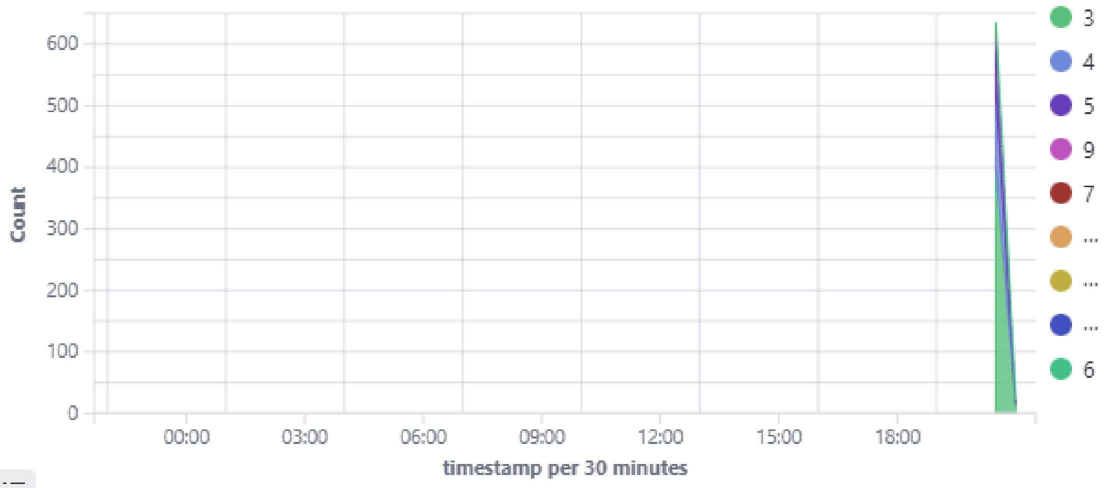
Top 3 agents with level 15 alerts

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	My-PC-Lab	192.168.208.1	Wazuh v4.7.2	wazuh.manager	Microsoft Windows 11 Home 10.0.26200.7628	Jan 27, 2026 @ 08:43:08.000	Jan 28, 2026 @ 14:23:05.000

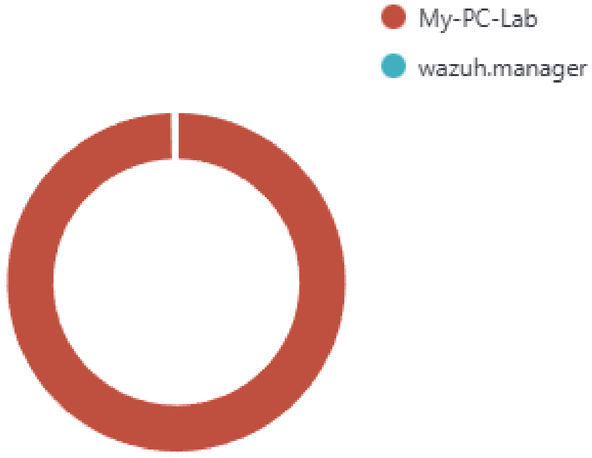
Alerts evolution Top 5 agents



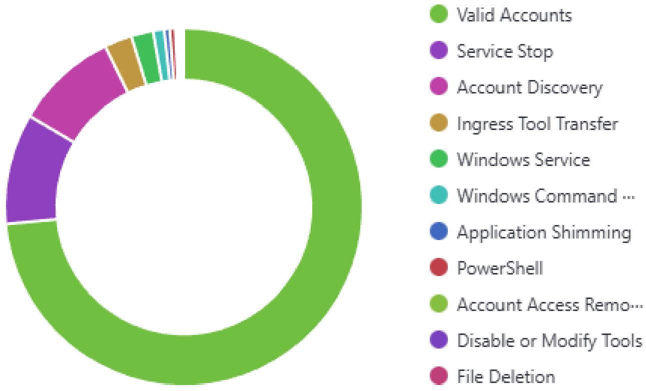
Alert level evolution



Top 5 agents



Alerts



Alerts summary

Rule ID	Description	Level	Count
60106	Windows logon success.	3	289
60608	Summary event of the report's signatures.	4	124
60642	Software protection service scheduled successfully.	3	43
61135	The browser has forced an election on network because a master browser was stopped	5	40
60104	Windows audit failure event.	5	23
92031	Discovery activity executed	3	23
61104	Service startup type was changed	3	17
92039	A net.exe account discovery command was initiated	3	11
61102	Windows System error event	5	9
60775	SessionEnv was unavailable to handle a notification event.	5	6
92205	Powershell process created an executable file in Windows root folder	9	5
60118	Windows workstation logon success.	3	4
60775	WSearch was unavailable to handle a notification event.	5	3
60137	Windows User Logoff.	3	3
60776	SessionEnv was unavailable to handle a critical notification event.	7	3
61021	.NET Runtime - Fatal execution engine error.	9	3
61060	The open procedure for service remote access failed.	5	3
92032	Suspicious Windows cmd shell execution	3	3
92213	Executable file dropped in folder commonly used by malware	15	3
502	Wazuh server started.	3	2
92058	Application Compatibility Database launched	12	2
92066	C:\\Windows\\SysWOW64\\SecEdit.exe binary in a suspicious location launched by C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe	4	2
61109	Name resolution for the name 0.9.3.d.0.5.7.b.0.0.0.0.0.0.0.0.0.0.0.0.b.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name 0.d.6.9.3.c.1.c.c.d.7.c.b.a.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. timed out	5	1
61109	Name resolution for the name 2.a.1.1.5.4.6.7.0.0.0.0.0.0.0.0.0.0.0.0.a.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name 2.a.3.d.0.5.7.b.0.0.0.0.0.0.0.0.0.0.0.0.b.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name 3.a.3.d.0.5.7.b.0.0.0.0.0.0.0.0.0.0.0.0.b.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name 8.9.1.1.5.4.6.7.0.0.0.0.0.0.0.0.0.0.0.0.a.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name 8.f.0.1.5.4.6.7.0.0.0.0.0.0.0.0.0.0.0.0.b.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name 9.0.0.1.5.4.6.7.0.0.0.0.0.0.0.0.0.0.0.0.b.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name b.a.1.1.5.4.6.7.0.0.0.0.0.0.0.0.0.0.0.0.a.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name d.c.0.1.5.4.6.7.0.0.0.0.0.0.0.0.0.0.0.0.b.0.1.0.0.0.8.4.5.0.4.2.ip6.arpa. timed out	5	1
61109	Name resolution for the name win1910.ipv6.microsoft.com. timed out	5	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\AarSvc_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\\svchost.exe -k AarSvcGroup -p	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\BcastDVRUserService_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\\svchost.exe -k BcastDVRUserService	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\	3	1

Rule ID	Description	Level	Count
	\ConsentUxUserSvc_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\\svchost.exe -k DevicesFlow		
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \CredentialEnrollmentManagerUserSvc_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\ \CredentialEnrollmentManager.exe	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \DevicePickerUserSvc_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\\svchost.exe -k DevicesFlow	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \P9RdrService_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\\svchost.exe -k P9RdrService -p	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \UdkUserSvc_3a063e63\\ImagePath binary is: C:\\WINDOWS\\system32\\svchost.exe -k UdkSvcGroup	3	1
92221	A screensaver executable C:\\Program Files\\WindowsApps\ \Microsoft.ScreenSketch_11.2511.31.0_x64__8wekyb3d8bbwe\\SnippingTool\\SnippingTool.exe created C:\\Users\ \Admin\\Downloads\\1.png	3	1
92221	A screensaver executable C:\\Program Files\\WindowsApps\ \Microsoft.ScreenSketch_11.2511.31.0_x64__8wekyb3d8bbwe\\SnippingTool\\SnippingTool.exe created C:\\Users\ \Admin\\Downloads\\2.png	3	1
202	Agent event queue is 90% full.	7	1
203	Agent event queue is full. Events may be lost.	9	1
204	Agent event queue is flooded. Check the agent configuration.	12	1
205	Agent event queue is back to normal load.	3	1
503	Wazuh agent started.	3	1
506	Wazuh agent stopped.	3	1
60122	Logon failure - Unknown user or bad password.	5	1
60702	The VSS service is shutting down due to idle timeout.	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
61110	Multiple System error events	10	1
61138	New Windows Service Created	5	1
657	Active response: restart-wazuh.exe - add	3	1
92002	Scripting interpreter spawned Windows command shell instance	6	1
92021	Powershell was used to delete files or directories	3	1