Security events report

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

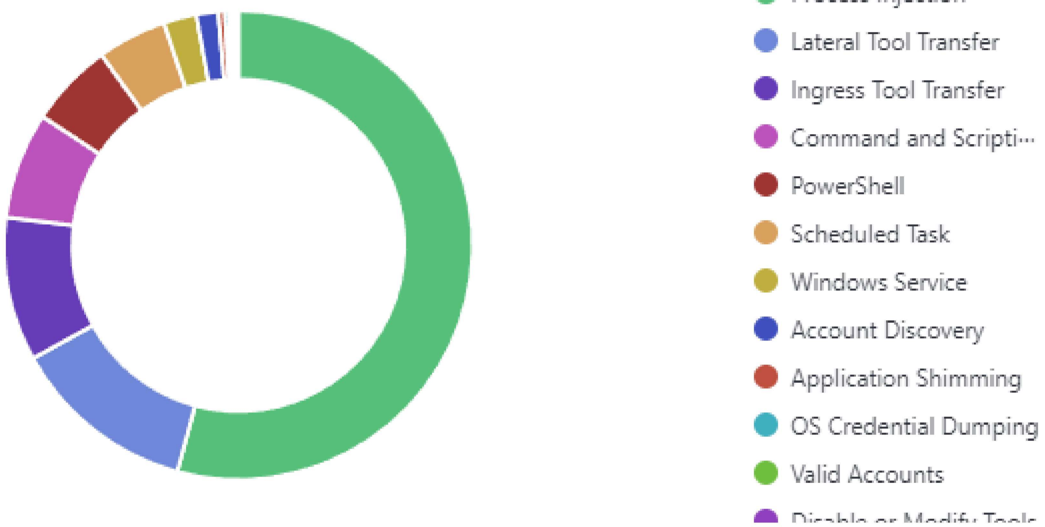
🕘 2024-04-24T17:53:31 to 2024-04-25T17:53:31

🔍 manager.name: Wazuh

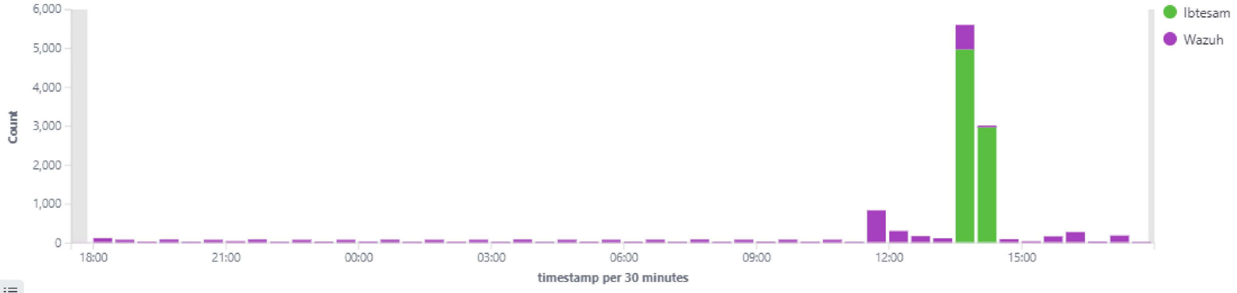
Top 3 agents with level 15 alerts

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	Ibtesam	192.168.96.132	Wazuh v4.7.3	Wazuh	Microsoft Windows 10 Pro 10.0.19045.3803	Apr 24, 2024 @ 00:21:45.000	Apr 25, 2024 @ 20:22:32.000

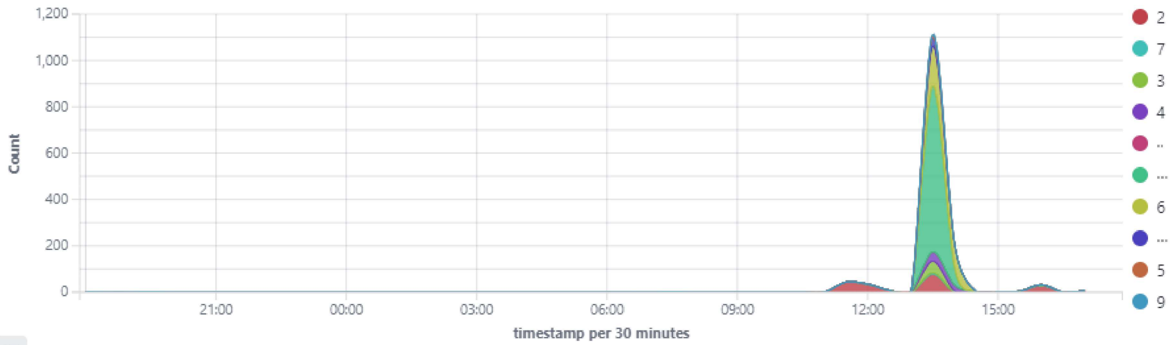
Alerts



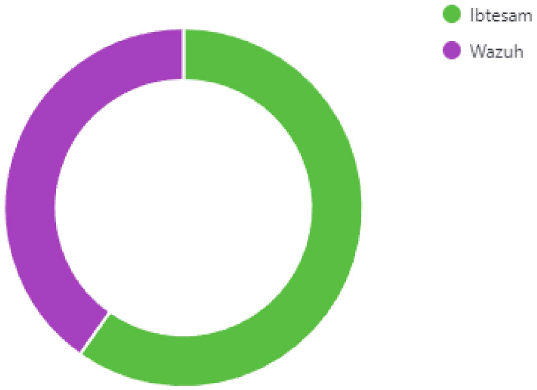
Alerts evolution Top 5 agents



Alert level evolution



Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
92910	Explorer process was accessed by C:\\Users\\Sam\\AppData\\Local\\Microsoft\\OneDrive\\Update\ \OneDriveSetup.exe, possible process injection	12	619
1002	Unknown problem somewhere in the system.	2	203
92217	Executable dropped in Windows root folder	6	169
92200	Scripting file created under Windows Temp or User folder	6	96
92151	Binary loaded PowerShell automation library - Possible unmanaged Powershell execution by suspicious process	12	77
92154	Process loaded taskschd.dll module. May be used to create delayed malware execution	4	63
92910	Explorer process was accessed by C:\\Users\\Sam\\AppData\\Local\\Microsoft\\OneDrive\\OneDrive.exe, possible process injection	12	43
92213	Executable file dropped in folder commonly used by malware	15	34
92910	Explorer process was accessed by C:\\Users\\Sam\\AppData\\Local\\Microsoft\\OneDrive\\21.220.1024.0005\ \Microsoft.SharePoint.exe, possible process injection	12	27
92910	Explorer process was accessed by C:\\Users\\Sam\\AppData\\Local\\Microsoft\\OneDrive\\24.070.0407.0003\ \FileSyncConfig.exe, possible process injection	12	27
510	Host-based anomaly detection event (rootcheck).	7	12
92031	Discovery activity executed	3	11
92039	A net.exe account discovery command was initiated	3	9
100002	Mimikatz Detected	15	4
502	Wazuh server started.	3	4
19009	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.	3	2
5501	PAM: Login session opened.	3	2
651	Host Blocked by firewall-drop Active Response	3	2
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \AarSvc_6064b\\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_6064b\\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\ \BluetoothUserService_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k BthAppGroup -p	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \CDPUserSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k UnistackSvcGroup	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \CaptureService_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k LocalService -p	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \ConsentUxUserSvc_6064b\\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\ \CredentialEnrollmentManagerUserSvc_6064b\\Description binary is: @%%SystemRoot%%\\system32\ \CredentialEnrollmentManager.exe,-101	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \CredentialEnrollmentManagerUserSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\ \CredentialEnrollmentManager.exe	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\ \DeviceAssociationBrokerSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k DevicesFlow -p	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\	3	1

Rule ID	Description	Level	Count
	\\DevicePickerUserSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k DevicesFlow		
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\DevicesFlowUserSvc_6064b\\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\\MessagingService_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k UnistackSvcGroup	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\OneSyncSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k UnistackSvcGroup	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\PimIndexMaintenanceSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k UnistackSvcGroup	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\PrintWorkflowUserSvc_6064b\\ImagePath binary is: C:\\Windows\\system32\\svchost.exe -k PrintWorkflow	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules\\{30228356-B0B2-4579-AEAC-A8FF33AF379B} binary is: v2.30|Action=Allow|Active=TRUE|Dir=In|Protocol=17|App=C:\\Program Files\\WindowsApps\\Microsoft.SkypeApp_15.118.3205.0_x64__kzf8qxf38zg5c\\Skype\\Skype.exe|Name=Skype|Desc=Skype|EmbedCtxt={78E1CD88-49E3-476E-B926-580E596AD309}|	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules\\{B01CC168-EBEC-49A5-B8EA-76103F12892F} binary is: v2.30|Action=Allow|Active=TRUE|Dir=Out|Protocol=6|App=C:\\Program Files\\WindowsApps\\Microsoft.SkypeApp_15.118.3205.0_x64__kzf8qxf38zg5c\\Skype\\Skype.exe|Name=Skype|Desc=Skype|EmbedCtxt={78E1CD88-49E3-476E-B926-580E596AD309}|	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules\\{B84F1D1B-8EA7-4570-80DD-98DE1D3506A7} binary is: v2.30|Action=Allow|Active=TRUE|Dir=Out|Protocol=17|App=C:\\Program Files\\WindowsApps\\Microsoft.SkypeApp_15.118.3205.0_x64__kzf8qxf38zg5c\\Skype\\Skype.exe|Name=Skype|Desc=Skype|EmbedCtxt={78E1CD88-49E3-476E-B926-580E596AD309}|	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\FirewallRules\\{D8F95BA5-05B6-46B8-85AA-90FBBBB61AE7} binary is: v2.30|Action=Allow|Active=TRUE|Dir=In|Protocol=6|App=C:\\Program Files\\WindowsApps\\Microsoft.SkypeApp_15.118.3205.0_x64__kzf8qxf38zg5c\\Skype\\Skype.exe|Name=Skype|Desc=Skype|EmbedCtxt={78E1CD88-49E3-476E-B926-580E596AD309}|	3	1
92307	Evidence of new service creation found in registry under HKLM\\System\\CurrentControlSet\\Services\\SharedAccess\\Parameters\\FirewallPolicy\\RestrictedServices\\Configurable\\System\\0adcb3b6-3900-423a-8d13-6ac2769f598e binary is: v2.30|Action=Block|Active=TRUE|Dir=In|App=%%ProgramData%%\\Microsoft\\Windows Defender\\platform\\4.18.24030.9-0\\MsMpEng.exe|Svc=WinDefend|Name=Inbound service restriction rule for WinDefend|Desc=Block all inbound traffic to service WinDefend|	3	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout duration' is set to '15 or more minute(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Application Group Management' is set to 'Success and Failure'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Credential Validation' is set to 'Success and Failure'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Enforce password history' is set to '24 or more password(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password age' is set to '1 or more day(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Minimum password length' is set to '14 or more character(s)'.: Status changed from failed to 'not applicable'	5	1
19013	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'.: Status changed from failed to 'not applicable'	5	1

Rule ID	Description	Level	Count
92157	An executable - C:\\Program Files\\Windows Defender\\MsMpEng.exe - loaded C:\\Windows\\Temp\\7C5D49B0-92EF-4BD9-9E79-41B94528B802\\MpUpdate.dll from the Temp directory.	6	1
92157	An executable - C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismHost.exe - loaded C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\CbsProvider.dll from the Temp directory.	6	1
92157	An executable - C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismHost.exe - loaded C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismCorePS.dll from the Temp directory.	6	1
92157	An executable - C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismHost.exe - loaded C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismProv.dll from the Temp directory.	6	1
92157	An executable - C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismHost.exe - loaded C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\LogProvider.dll from the Temp directory.	6	1
92157	An executable - C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\DismHost.exe - loaded C:\\Windows\\Temp\\5396DED4-49A8-4974-9A5B-4E77F62950AA\\OSProvider.dll from the Temp directory.	6	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Administrator account status' is set to 'Disabled'.: Status changed from passed to 'not applicable'	5	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Audit Security Group Management' is set to include 'Success'.: Status changed from passed to 'not applicable'	5	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.: Status changed from passed to 'not applicable'	5	1
19012	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'.: Status changed from passed to 'not applicable'	5	1
19004	SCA summary: CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Score less than 50% (32)	7	1
503	Wazuh agent started.	3	1
504	Wazuh agent disconnected.	3	1
535	List of the last logged in users.	1	1
5715	sshd: authentication success.	3	1
5762	sshd: connection reset	4	1
92021	Powershell was used to delete files or directories	3	1
92052	Windows command prompt started by an abnormal process	4	1
92152	Printer spooler service loaded a dll file. Possible PrintNightmare exploit: CVE-2021-34527	6	1
92201	C:\\Windows\\SysWOW64\\WindowsPowerShell\\v1.0\\powershell.exe created a new scripting file under Windows Temp or User data folder	9	1