

MITRE ATT&CK 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

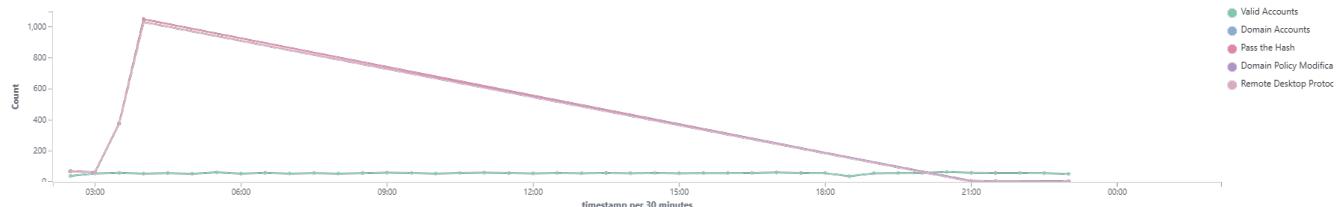
Group: default

Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

⌚ 2026-01-05T02:08:20 to 2026-01-06T02:08:20

🔍 manager.name: wazuh.manager AND rule.mitre.id: * AND agent.id: 001

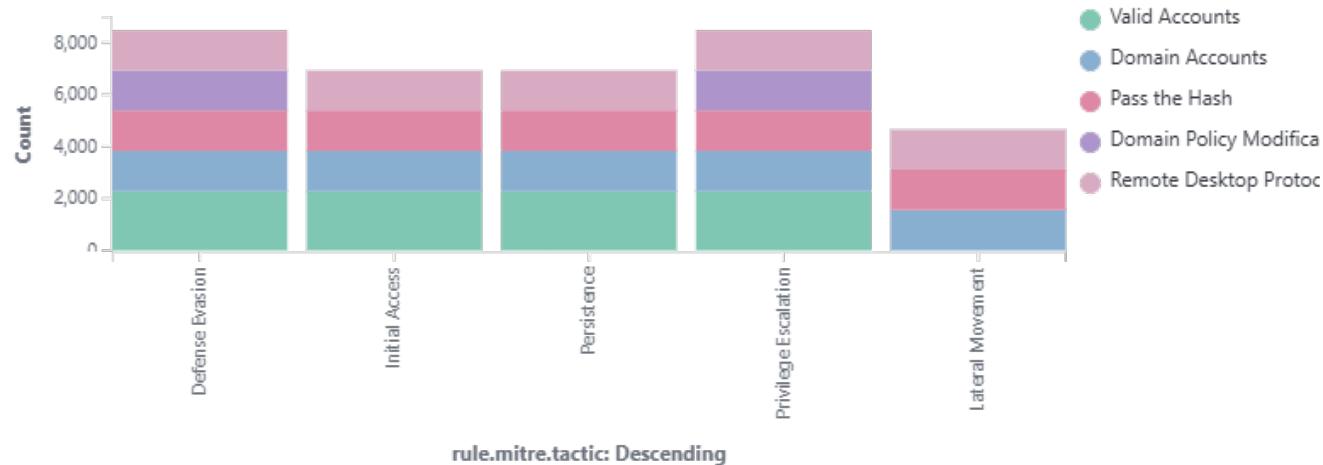
Alerts evolution over time



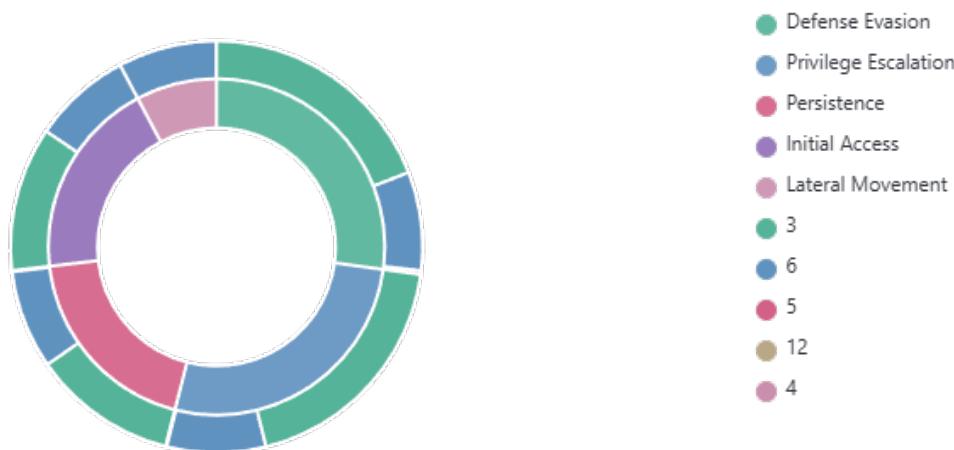
Rule level by attack



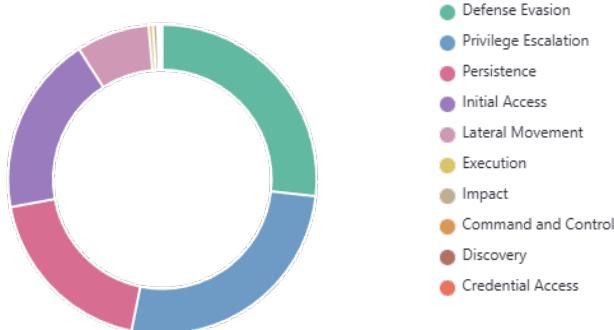
MITRE attacks by tactic



Rule level by tactic



Top tactics



Alerts summary

Rule ID	Description	Level	Count
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
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
92031	Discovery activity executed	3	15
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
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
91820	Powershell script recursively collected files from a filesystem search	4	3
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_i se.exe	3	2
92110	Detected WinRM activity from 0:0:0:0:0:0:1 to 0:0:0:0:0:0:1	4	2
504	Wazuh agent disconnected.	3	1

Rule ID	Description	Level	Count
506	Wazuh agent stopped.	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
92203	Executable file created by powershell: C:\\SecurityLab\\Demo\\lateral-movement-demo.ps1	6	1
92217	Executable dropped in Windows root folder	6	1
92653	User: SOCSERVER\\Administrator logged using Remote Desktop Connection (RDP) from ip:0.0.0.0.	3	1