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

MITRE ATT&CK report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	DC-Server	192.168.50.5	Wazuh v4.7.5	ubuntu	Microsoft Windows Server 2019 Standard 10.0.17763.3650	Jul 10, 2025 @ 07:59:07.000	Jul 10, 2025 @ 21:41:54.000

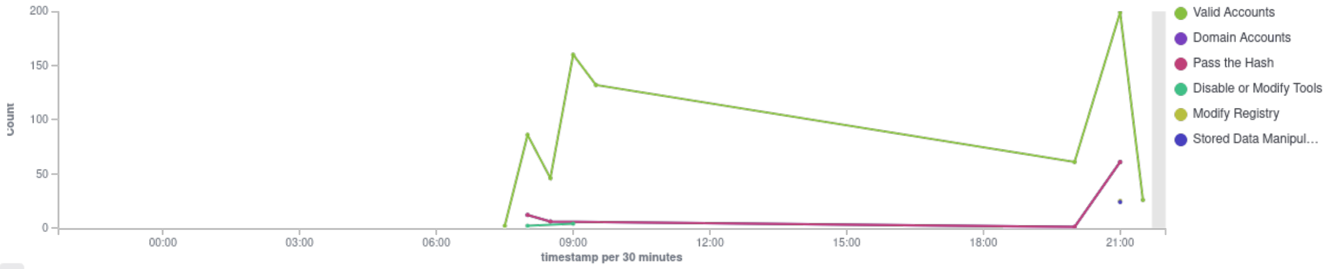
Group: default

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

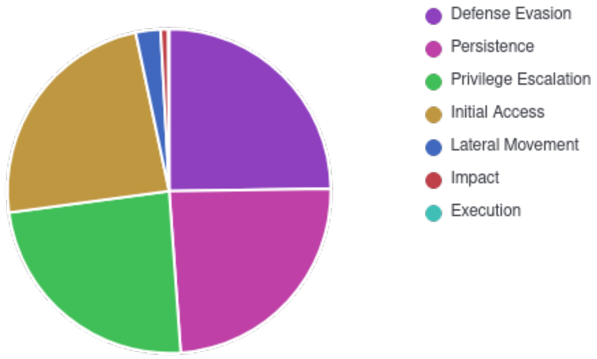
2025-07-09T21:41:56 to 2025-07-10T21:41:56

manager.name: ubuntu AND rule.mitre.id: * AND agent.id: 001

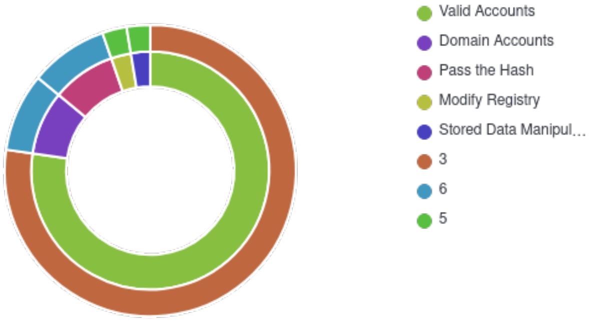
Mitre alerts evolution



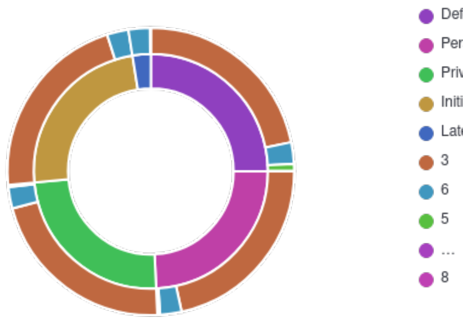
Top tactics pie



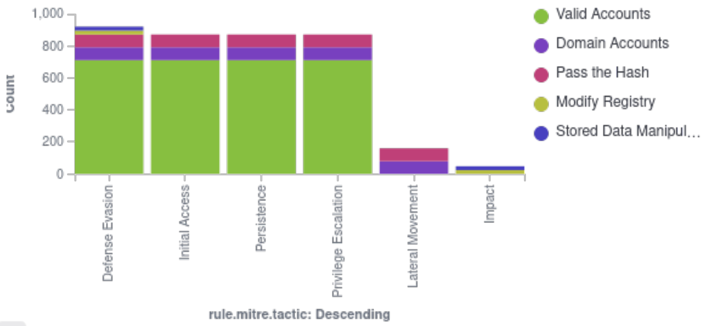
Alerts level by attack



Alerts level by tactic



Top tactics



Alerts summary

Rule ID	Description	Level	Count
60106	Windows logon success.	3	712
92652	Successful Remote Logon Detected - User:\Administrator - NTLM authentication, possible pass-the-hash attack.	6	50
92652	Successful Remote Logon Detected - User:\bob - NTLM authentication, possible pass-the-hash attack.	6	27
750	Registry Value Integrity Checksum Changed	5	15
594	Registry Key Integrity Checksum Changed	5	9
506	Wazuh agent stopped.	3	6
61138	New Windows Service Created	5	6
92652	Successful Remote Logon Detected - User:\ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack.	6	3
92650	New Windows Service Created to start from windows root path. Suspicious event as the binary may have been dropped using Windows Admin Shares.	12	3
60109	User account enabled or created.	8	2
60110	User account changed.	8	2
60147	Security enabled local group changed.	5	1
60154	Administrators group changed.	12	1
60778	The shell stopped unexpectedly.	5	1
752	Registry Value Entry Added to the System	5	1