

MITRE ATT&CK report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	Mr-Chandan-Prasad-indian	192.168.1.101	Wazuh v4.7.2	wazuh.manager	Microsoft Windows 11 Home Single Language 10.0.26200.7171	Nov 19, 2025 @ 15:10:21.000	Nov 19, 2025 @ 18:54:54.000

Group: default

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

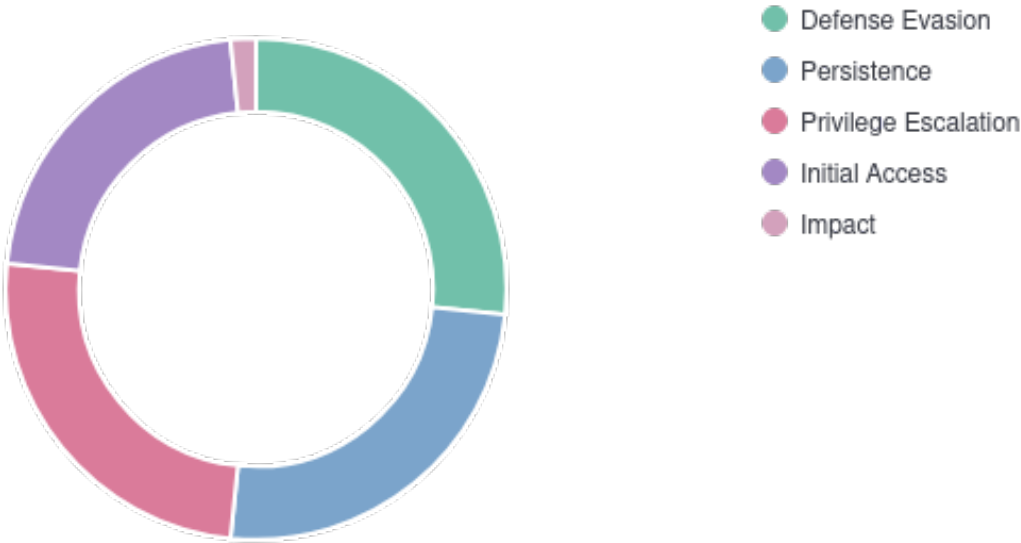
🕒 2025-11-18T13:55:02 to 2025-11-19T13:55:02

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

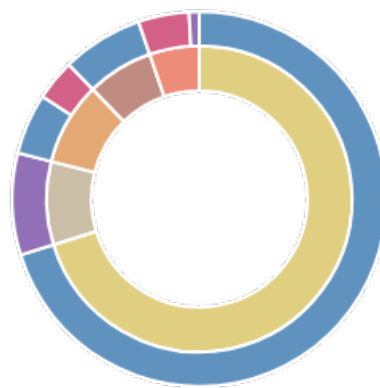
Alerts evolution over time



Top tactics

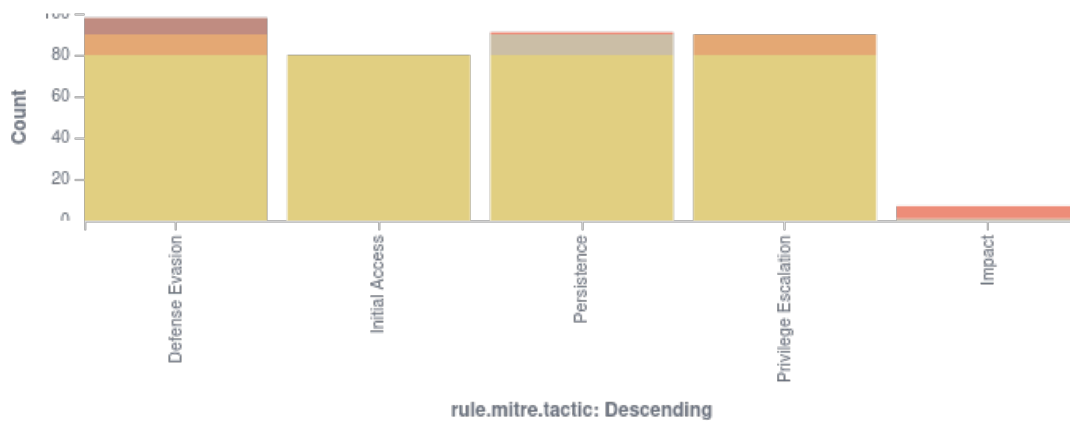


## Rule level by attack



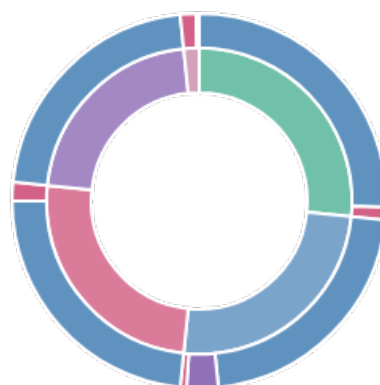
- Valid Accounts
- Account Manipulation
- Domain Policy Modifi...
- Disable or Modify Tools
- Account Access Re...
- 3
- 8
- 5

## MITRE attacks by tactic



- Valid Accounts
- Account Manipulation
- Domain Policy Modifi...
- Disable or Modify Tools
- Account Access Re...

## Rule level by tactic



- Defense Evasion
- Persistence
- Privilege Escalation
- Initial Access
- Impact
- 3
- 5
- 8

## Alerts summary

Rule ID	Description	Level	Count
60106	Windows Logon Success	3	80
506	Wazuh agent stopped.	3	8
60110	User account changed	8	7
67028	Special privileges assigned to new logon.	3	6
60122	Logon Failure - Unknown user or bad password	5	5
60109	User account enabled or created	8	2
60160	Domain Users Group Changed	5	2
60170	Users Group Changed	5	2
61138	New Windows Service Created	5	2
60111	User account disabled or deleted	8	1