wazuh.

MITRE ATT&CK report

Warning. Agent is disconnected

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	●	●	Wazuh v4.10.1	ubantu-VMware-Virtual-Platform	Microsoft Windows 10 Home Single Language 10.0.19045.5440	Feb 1, 2025 @ ●	Feb 2, 2025 @ ●

Group: default

Explore security alerts mapped to adversary tactics and techniques for better threat understanding.
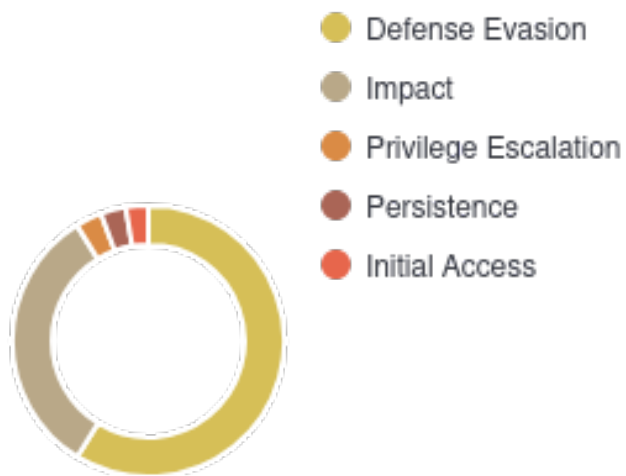
🕐 2025-02-02T11:00:00 to 2025-02-02T11:30:00

🔍 manager.name: ubantu-VMware-Virtual-Platform AND rule.mitre.id: * AND agent.id: 001
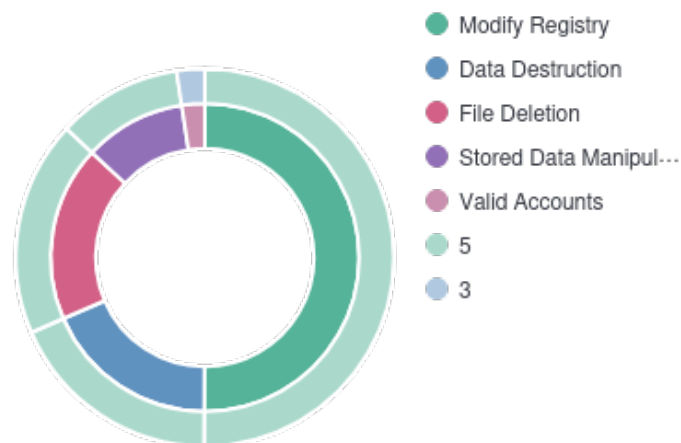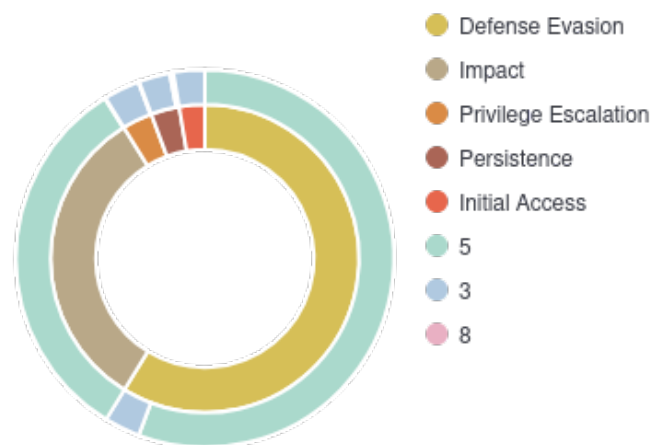
Alerts evolution over time

Top tactics

- Defense Evasion
- Impact
- Privilege Escalation
- Persistence
- Initial Access

Rule level by attack

- Modify Registry
- Data Destruction
- File Deletion
- Stored Data Manipul···
- Valid Accounts
- 5
- 3

MITRE attacks by tactic

- Modify Registry
- Data Destruction
- File Deletion
- Stored Data Manipul···
- Valid Accounts

rule.mitre.tactic: Descending

Rule level by tactic

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

Alerts summary

Rule ID	Description	Level	Count
752	Registry Value Entry Added to the System	5	482
751	Registry Value Entry Deleted.	5	426
750	Registry Value Integrity Checksum Changed	5	186
594	Registry Key Integrity Checksum Changed	5	116
598	Registry Key Entry Added to the System	5	112
597	Registry Key Entry Deleted.	5	96
60106	Windows Logon Success	3	68
67028	Special privileges assigned to new logon.	3	10
60110	User account changed	8	6
61138	New Windows Service Created	5	2
67018	System shutdown initiated.	3	2