Threat hunting report

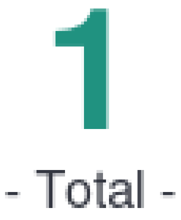
ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
004	Secretary-Windows	10.0.40.13	Wazuh v4.14.1	wazuh-server	Microsoft Windows 11 Enterprise Evaluation 10.0.22621.6060	Jan 2, 2026 @ 18:31:27.000	Feb 9, 2026 @ 22:44:36.000

Group: Secretary

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

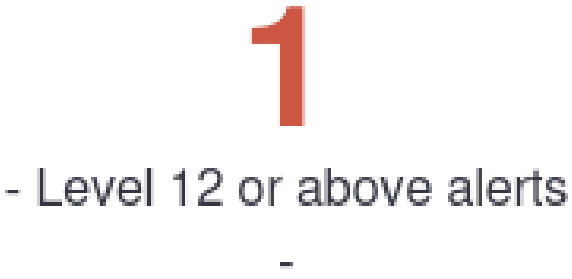
🕘 2026-02-09T22:00:00 to 2026-02-09T23:00:00

🔍 manager.name: wazuh-server AND agent.id: 004 AND query: {"bool":{"filter":[{"bool":{"minimum_should_match":1,"should":[{"range":{"rule.level":{"gte":12}}}]}}],"must":[],"must_not":[],"should":[]}} AND rule.level: 12



1

- Total -



1

- Level 12 or above alerts -

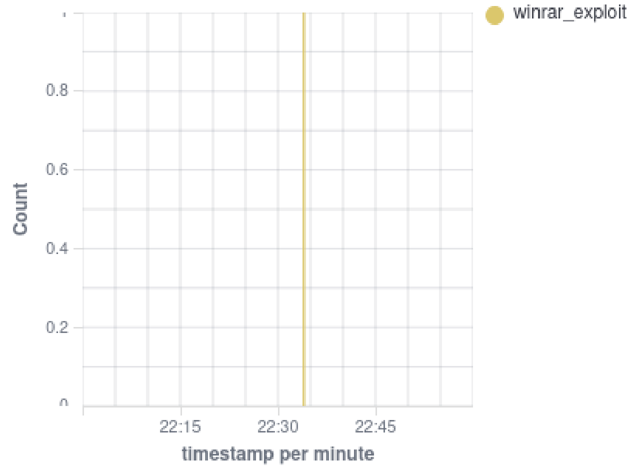
0

- Authentication failure -

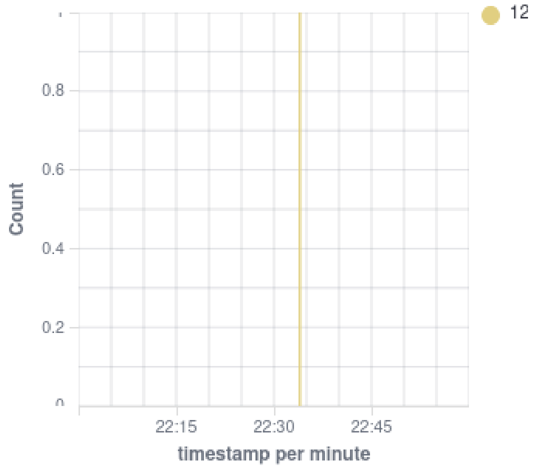
0

- Authentication success -

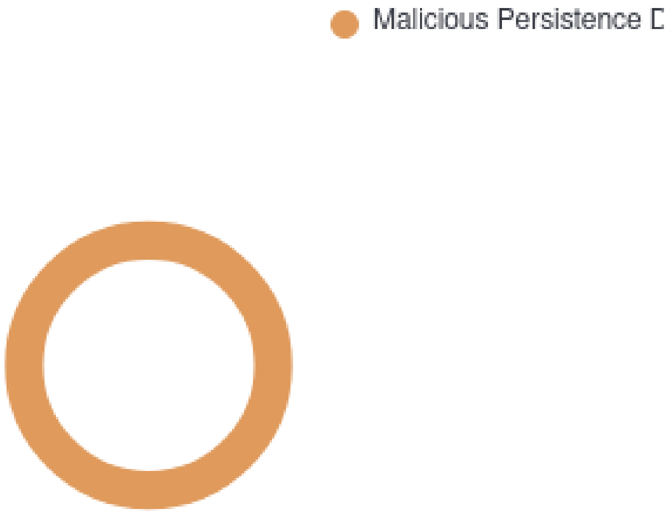
Top 10 Alert groups evolution



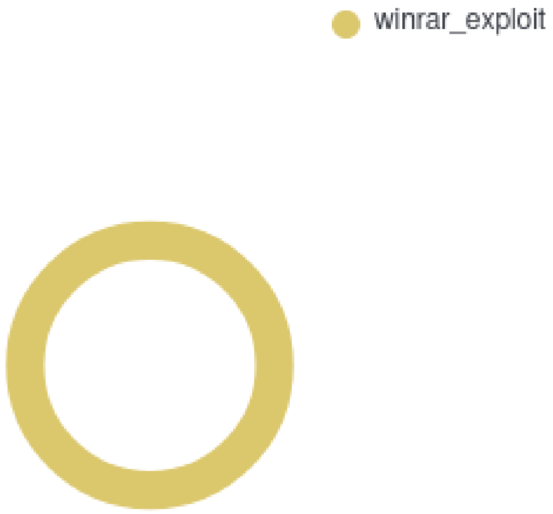
Alerts



Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements

No results found

Alerts summary

Rule ID	Description	Level	Count
100010	Malicious Persistence Detected in Startup folder (WinRAR CVE Detection)	12	1

Groups summary

Groups	Count
winrar_exploit	1