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

Malware detection report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	wazuh_agent_ubuntu	172.20.0.8	Wazuh v4.9.0	wazuh-manager-4.9.0-7102	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 16, 2024 @ 15:11:37.000

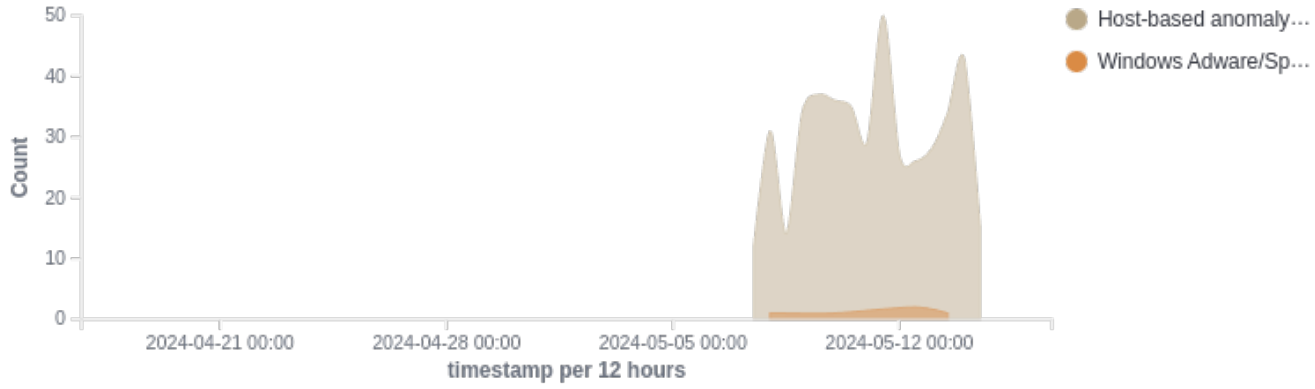
Group: default

Verify that your systems are configured according to your security policies baseline.

2024-04-16T17:11:37 to 2024-05-16T17:11:37

rule.groups: rootcheck AND cluster.name: wazuh AND agent.id: 001

Alerts over time



Rule distribution

Events per control type evolution

Alerts summary

Description	Control	Count
Host-based anomaly detection event (rootcheck).	Trojaned version of file detected.	192
Host-based anomaly detection event (rootcheck).	Rootkit 'Omega' detected by the presence of file '/dev/chr'.	25
Host-based anomaly detection event (rootcheck).	Rootkit 'Monkit' detected by the presence of file '/lib/defs'.	15
Host-based anomaly detection event (rootcheck).	Rootkit 'LDP' detected by the presence of file '/dev/.kork'.	12
Host-based anomaly detection event (rootcheck).	Rootkit 'Volc' detected by the presence of file '/usr/bin/volc'.	11
Host-based anomaly detection event (rootcheck).	Rootkit 'Knark' detected by the presence of file '/proc/knark'.	9
Host-based anomaly detection event (rootcheck).	Rootkit 'Monkit' detected by the presence of file '/usr/lib/libpikapp.a'.	9
Host-based anomaly detection event (rootcheck).	Rootkit 'Rh-Sharpe' detected by the presence of file '/bin/lkillall'.	9
Host-based anomaly detection event (rootcheck).	Rootkit 'Rh-Sharpe' detected by the presence of file '/usr/bin/.ps'.	9
Host-based anomaly detection event (rootcheck).	Rootkit 'Volc' detected by the presence of file '/usr/lib/volc'.	9
Windows Adware/Spyware application found.	-	6