wazuh.

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

Malware detection report

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

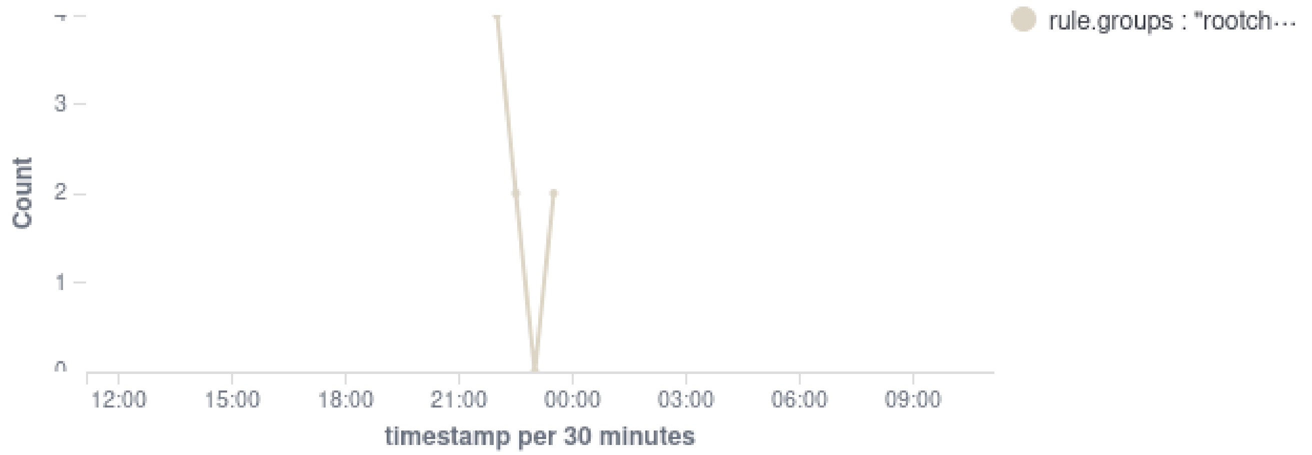
2024-10-19T11:08:30 to 2024-10-20T11:08:30

manager.name: reem-VMware AND rule.groups: rootcheck

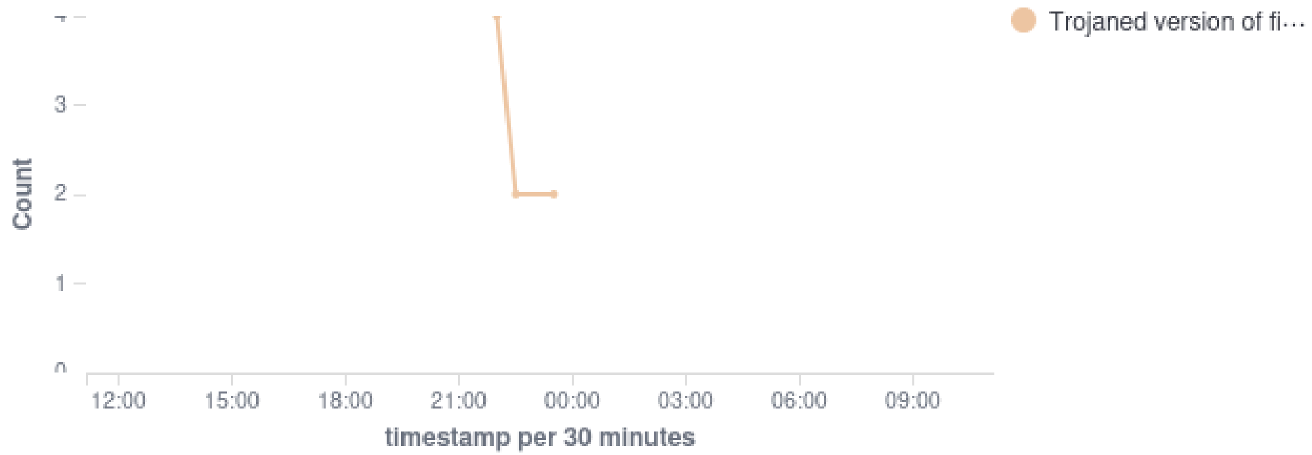
No agents have hidden processes

No agents have hidden ports

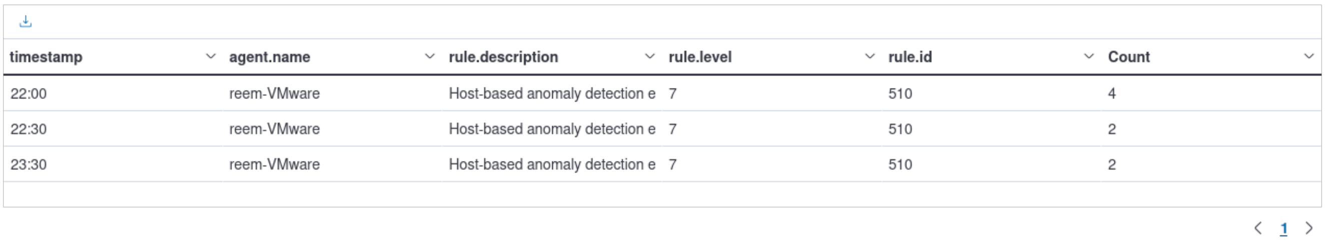
Emotet malware activity



Rootkits malware activity



Security alerts



timestamp	agent.name	rule.description	rule.level	rule.id	Count
22:00	reem-VMware	Host-based anomaly detection e	7	510	4
22:30	reem-VMware	Host-based anomaly detection e	7	510	2
23:30	reem-VMware	Host-based anomaly detection e	7	510	2

Alerts summary

Description	Control	Count
Host-based anomaly detection event (rootcheck).	Trojaned version of file detected.	8