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

Malware detection report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	kali	192.168.84.135	Wazuh v4.12.0	siem-VMware-Virtual-Platform	Kali GNU/Linux 2025.3	Sep 9, 2025 @ 15:07:31.000	Oct 6, 2025 @ 07:36:54.000

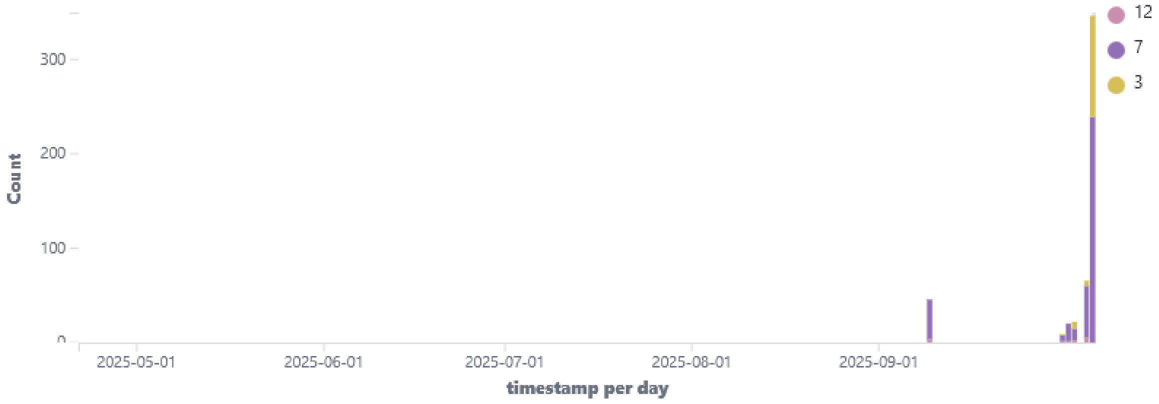
Group: default

Check indicators of compromise triggered by malware infections or cyberattacks.

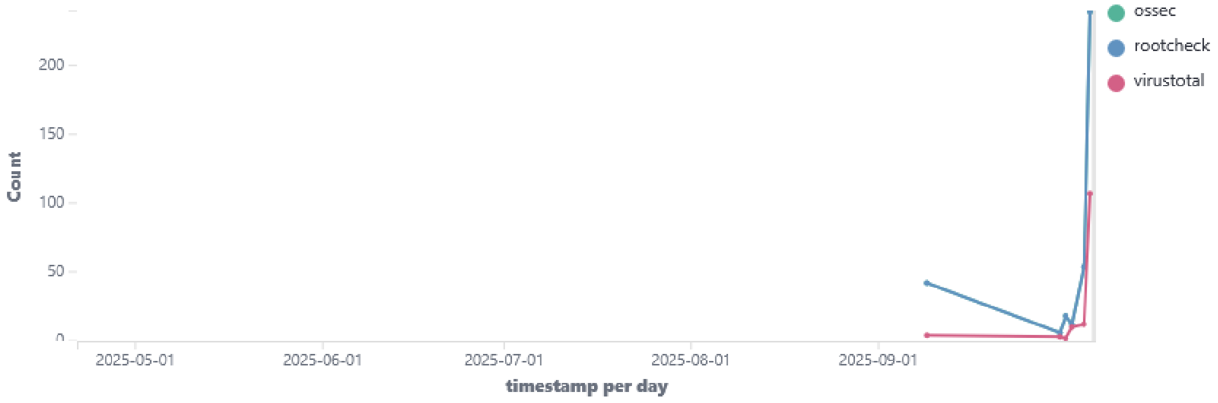
2025-04-21T07:36:56 to 2025-10-06T07:36:56

manager.name: siem-VMware-Virtual-Platform AND rule.groups: (rootcheck OR virustotal OR yara) AND agent.id: 001

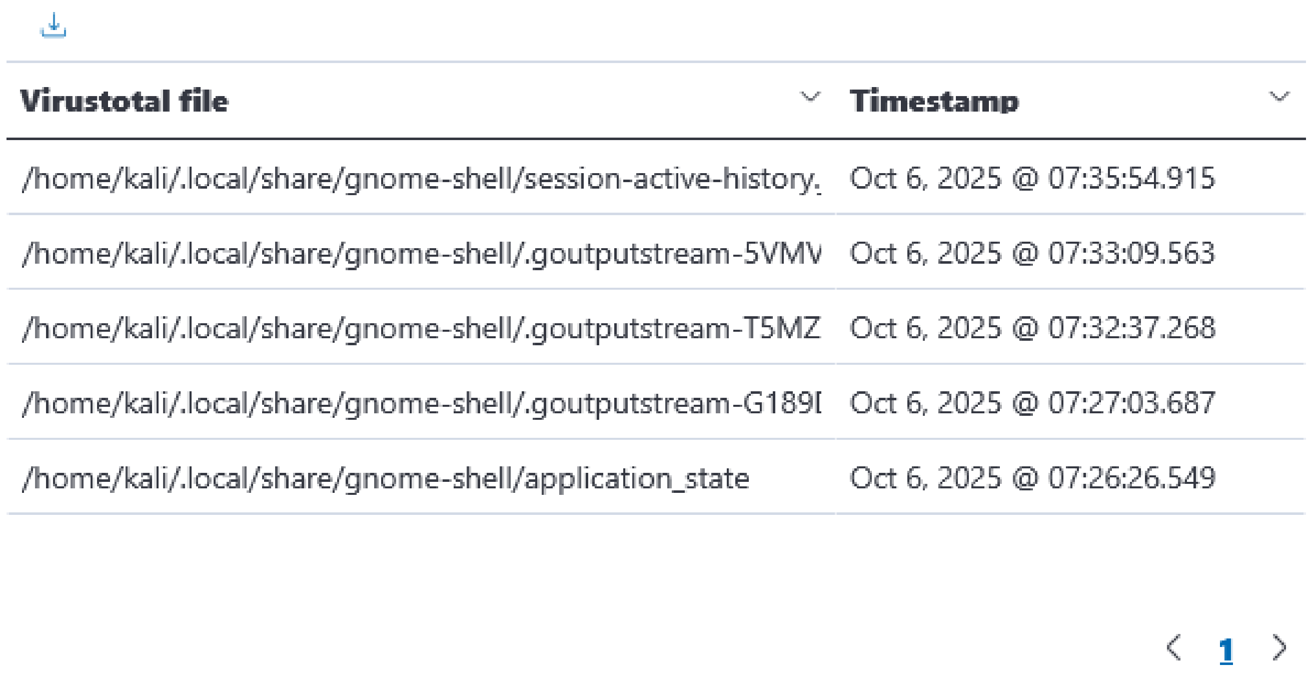
Rule level histogram



Events by rule group



Latest virustotal files

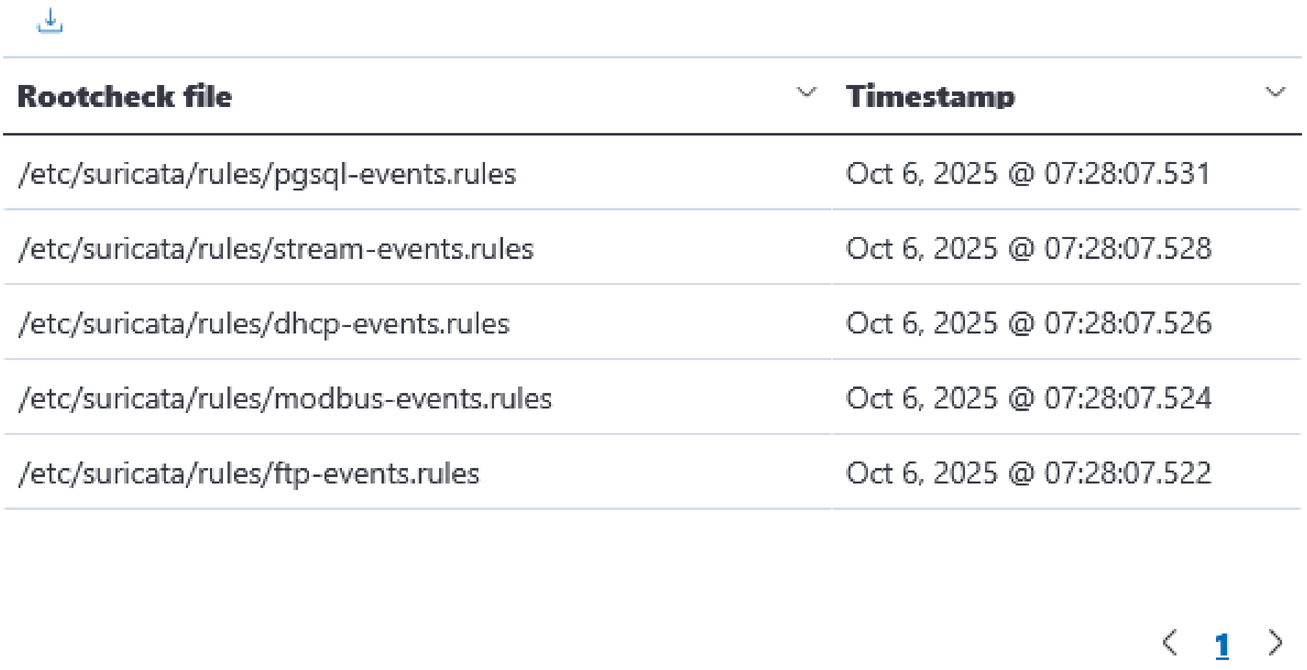


Virustotal file	Timestamp
/home/kali/.local/share/gnome-shell/session-active-history.	Oct 6, 2025 @ 07:35:54.915
/home/kali/.local/share/gnome-shell/.goutputstream-5VMV	Oct 6, 2025 @ 07:33:09.563
/home/kali/.local/share/gnome-shell/.goutputstream-T5MZ	Oct 6, 2025 @ 07:32:37.268
/home/kali/.local/share/gnome-shell/.goutputstream-G189I	Oct 6, 2025 @ 07:27:03.687
/home/kali/.local/share/gnome-shell/application_state	Oct 6, 2025 @ 07:26:26.549

Latest yara scanned files

No results found

Latest rootcheck file



Rootcheck file	Timestamp
/etc/suricata/rules/pgsql-events.rules	Oct 6, 2025 @ 07:28:07.531
/etc/suricata/rules/stream-events.rules	Oct 6, 2025 @ 07:28:07.528
/etc/suricata/rules/dhcp-events.rules	Oct 6, 2025 @ 07:28:07.526
/etc/suricata/rules/modbus-events.rules	Oct 6, 2025 @ 07:28:07.524
/etc/suricata/rules/ftp-events.rules	Oct 6, 2025 @ 07:28:07.522

Alerts summary

Description	Control	Count
Host-based anomaly detection event (rootcheck).	File is owned by root and has written permissions to anyone.	189
Host-based anomaly detection event (rootcheck).	Trojaned version of file detected.	182
VirusTotal: Alert - No records in VirusTotal database	-	112
VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file	-	6
VirusTotal: Alert - /home/kali/malware/ecir - 64 engines detected this file	-	3
VirusTotal: Alert - /home/kali/malware/eicar - 65 engines detected this file	-	3
active-response/bin/remove-threat.sh removed threat located at /home/kali/malware/eicar	-	3
VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found	-	2
VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file	-	2
VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-shm - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Pictures.db-wal - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-shm - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/tracker3/files/http%3A%2F%2Ftracker.api.gnome.org%2Fontology%2Fv3%2Ftracker%23Software.db-wal - No positives found	-	1
VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-shm - No positives found	-	1
VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-wal - No positives found	-	1
VirusTotal: Alert - /root/.cache/dconf/user - No positives found	-	1