

## 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 @ 19:05:35.000

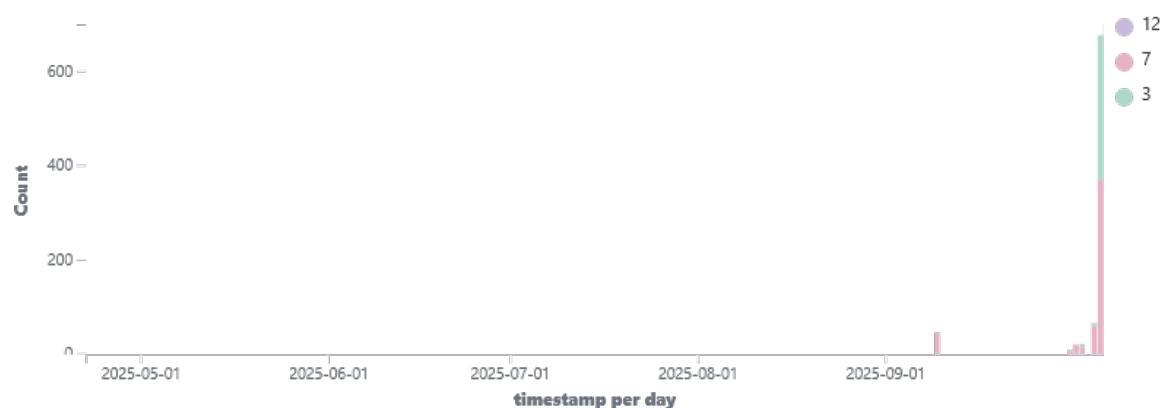
Group: default

Check indicators of compromise triggered by malware infections or cyberattacks.

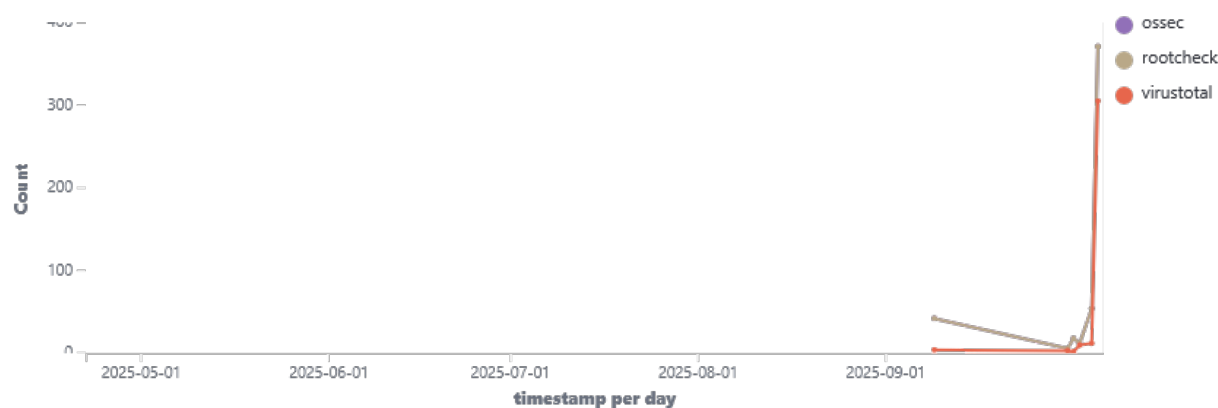
🕒 2025-04-21T19:05:36 to 2025-10-06T19:05:36

🔍 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 @ 19:05:24.513
/home/kali/Desktop/Diamorphine/.git/hooks/push-to-checkout	Oct 6, 2025 @ 19:03:05.676
/home/kali/Desktop/Diamorphine/.git/hooks/post-update.s	Oct 6, 2025 @ 19:03:04.306
/home/kali/Desktop/Diamorphine/.git/hooks/update.sample	Oct 6, 2025 @ 19:03:02.929
/home/kali/Desktop/Diamorphine/.git/hooks/commit-msg.s	Oct 6, 2025 @ 19:03:01.358

&lt; 1 &gt;

## Latest yara scanned files



No results found

## Latest rootcheck file

	
Rootcheck file	Timestamp
/etc/suricata/rules/dhcp-events.rules	Oct 6, 2025 @ 18:56:39.245
/etc/suricata/rules/pgsql-events.rules	Oct 6, 2025 @ 18:56:39.245
/etc/suricata/rules/stream-events.rules	Oct 6, 2025 @ 18:56:39.245
/etc/suricata/rules/websocket-events.rules	Oct 6, 2025 @ 18:56:39.195
/etc/suricata/rules/app-layer-events.rules	Oct 6, 2025 @ 18:56:39.194

< **1** >

## Alerts summary

Description	Control	Count
Host-based anomaly detection event (rootcheck).	File is owned by root and has written permissions to anyone.	297
VirusTotal: Alert - No records in VirusTotal database	-	284
Host-based anomaly detection event (rootcheck).	Trojaned version of file detected.	206
VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file	-	6
VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-shm - No positives found	-	4
VirusTotal: Alert - /home/kali/.local/share/nautilus/tags/meta.db-wal - No positives found	-	4
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/.cache/mozilla/firefox/cs2lwm8z.default-esr/.startup-incomplete - No positives found	-	2
VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/cache2/ce_T151c2VyQ29udGV4dElkPTUs - No positives found	-	2
VirusTotal: Alert - /home/kali/.mozilla/firefox/cs2lwm8z.default-esr/lock - No positives found	-	2
VirusTotal: Alert - /home/kali/Desktop/Diamorphine/.git/hooks/push-to-checkout.sample - No positives found	-	2
VirusTotal: Alert - /home/kali/Desktop/Diamorphine/.git/hooks/update.sample - No positives found	-	2
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/mesa_shader_cache_db/marker - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/activity-stream.weather_feed.json - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/cache2/ce_T151c2VyQ29udGV4dElkPTUsYSw= - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/safebrowsing/ads-track-digest256.vlpset - No positives found	-	1
VirusTotal: Alert - /home/kali/.cache/mozilla/firefox/cs2lwm8z.default-esr/safebrowsing/social-tracking-protection-twitter-digest256.vlpset - No positives found	-	1