Malware detection report

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	MSI	10.22.137.43	Wazuh v4.12.0	wazuh-server	Microsoft Windows 11 Home 10.0.26100.4946	Aug 26, 2025 @ 00:29:56.000	Aug 26, 2025 @ 01:30:44.000

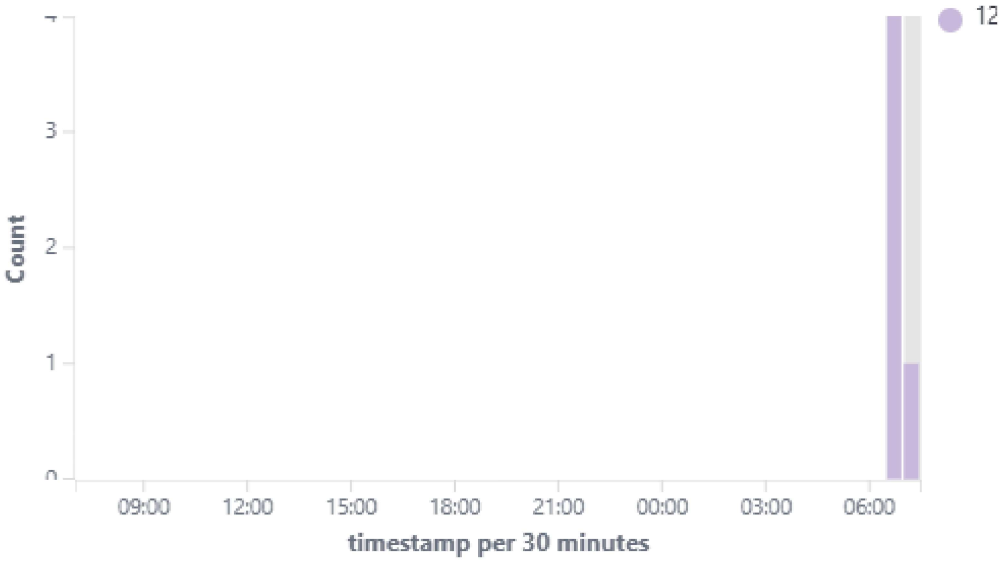
Group: default

Check indicators of compromise triggered by malware infections or cyberattacks.

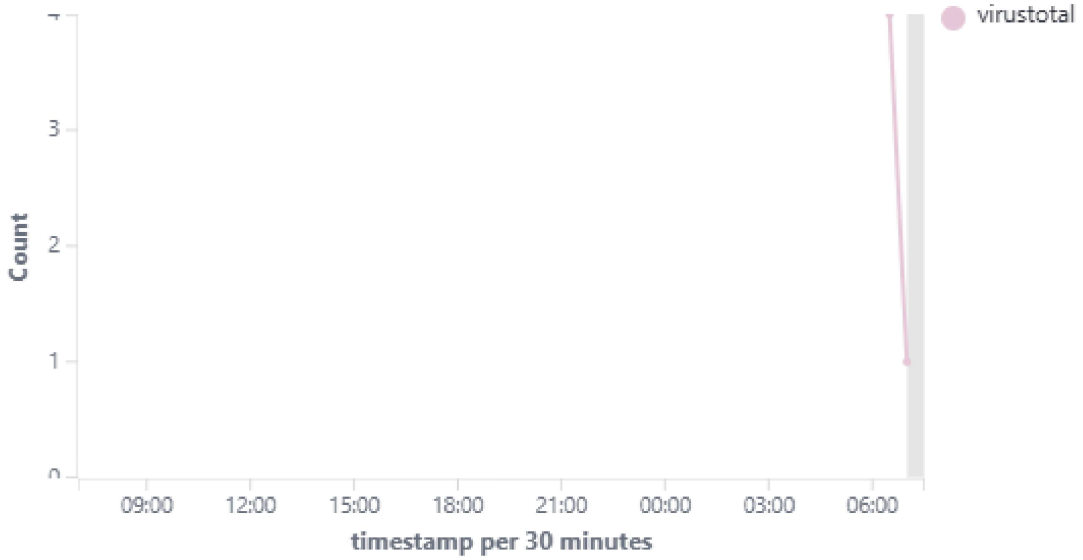
2025-08-25T07:00:49 to 2025-08-26T07:00:49

manager.name: wazuh-server 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
c:\users\swast\downloads\r	Aug 26, 2025 @ 07:00:34.937
c:\users\swast\downloads\u	Aug 26, 2025 @ 06:55:44.490
c:\users\swast\downloads\6	Aug 26, 2025 @ 06:55:42.526

Latest yara scanned files

No results found

‹ 1 ›

Latest rootcheck file

No results found

Alerts summary

Description	Control	Count
VirusTotal: Alert - c:\users\swast\downloads\6340f7f8-7837-4fb3-abcc-fe747d1b8df4.tmp - 36 engines detected this file	-	2
VirusTotal: Alert - c:\users\swast\downloads\unconfirmed 409694.crdownload - 36 engines detected this file	-	2
VirusTotal: Alert - c:\users\swast\downloads\madman.exe - 36 engines detected this file	-	1