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

File integrity monitoring report

Alerts related to file changes, including permissions, content, ownership and attributes.

2024-04-16T17:12:44 to 2024-05-16T17:12:44

rule.groups: syscheck AND cluster.name: wazuh

Top 3 FIM rules

Top 3 rules that are generating most alerts.

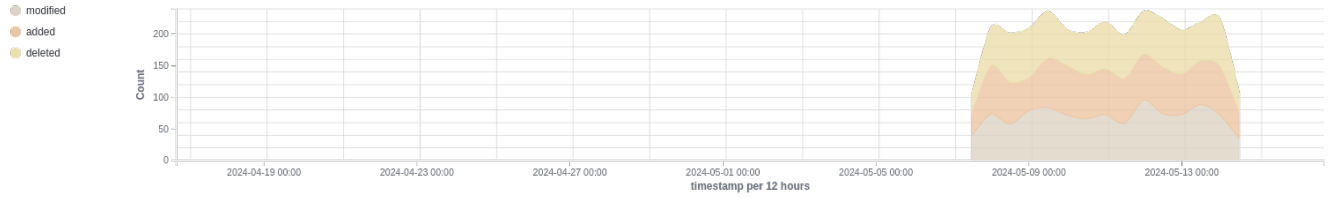
Rule ID	Description
550	Integrity checksum changed.
554	File added to the system.
553	File deleted.

Agents with suspicious FIM activity

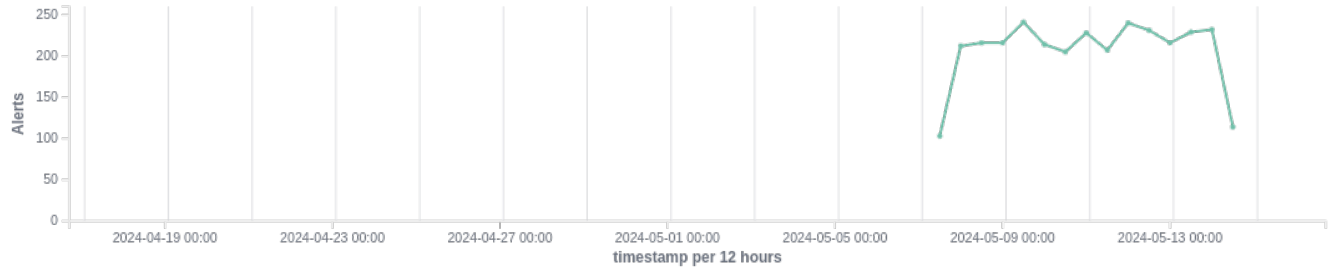
Top 3 agents that have most FIM alerts from level 7 to level 15. Take care about them.

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	wazuh_agent_ubuntu_2	172.20.0.7	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 @ 15:12:39.000

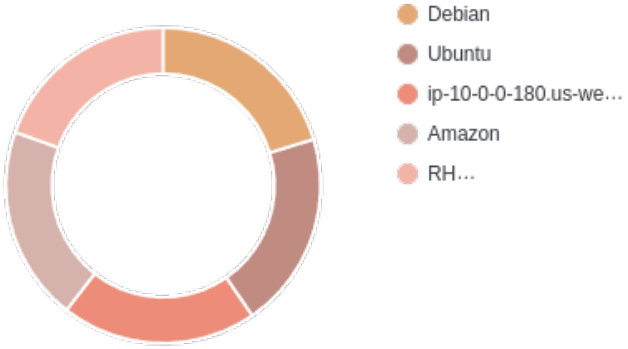
Alerts by action over time



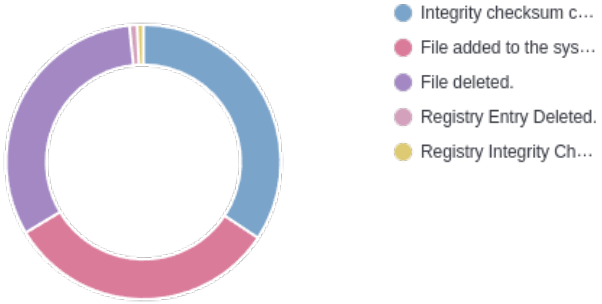
Events summary



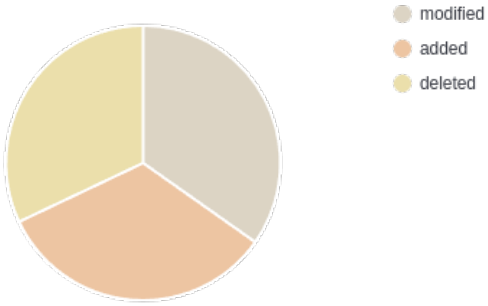
Top 5 agents



Rule distribution



Actions



Top 5 users

Top user	Agent ID	Agent name	Count
Administrators	002	Amazon	64
Administrators	004	Ubuntu	59
Administrators	007	Debian	58
Administrators	005	Centos	55

Alerts summary

Agent name	Path	Action	Count
Debian	/var/wazuh/queue/fim/db/fim.db	modified	24
Ubuntu	/run/utmp	added	24
Debian	/run/utmp	modified	23
Ubuntu	/var/wazuh/queue/fim/db/fim.db	added	23
Debian	/etc/resolv.conf	deleted	22
Ubuntu	/var/wazuh/queue/fim/db/fim.db	deleted	22
Ubuntu	/var/wazuh/queue/fim/db/fim.db	modified	22
ip-10-0-0-180.us-west-1.compute.internal	/var/osquery/osquery.db/CURRENT	modified	22
Debian	/etc/resolv.conf	added	20
Debian	/var/wazuh/queue/fim/db/fim.db	added	20
Debian	/var/osquery/osquery.db/CURRENT	modified	20
Debian	/var/osquery/osquery.db/CURRENT	added	19
Ubuntu	/var/osquery/osquery.db/CURRENT	deleted	19
Debian	/etc/resolv.conf	modified	18
Ubuntu	/run/utmp	deleted	18
Ubuntu	/run/utmp	modified	18
ip-10-0-0-180.us-west-1.compute.internal	/var/wazuh/queue/fim/db/fim.db	deleted	18
ip-10-0-0-180.us-west-1.compute.internal	/var/wazuh/queue/fim/db/fim.db	modified	18
ip-10-0-0-180.us-west-1.compute.internal	/etc/resolv.conf	added	18
ip-10-0-0-180.us-west-1.compute.internal	/var/osquery/osquery.db/CURRENT	deleted	17
ip-10-0-0-180.us-west-1.compute.internal	/etc/resolv.conf	modified	17
Ubuntu	/var/osquery/osquery.db/CURRENT	modified	16
ip-10-0-0-180.us-west-1.compute.internal	/var/wazuh/queue/fim/db/fim.db	added	16
ip-10-0-0-180.us-west-1.compute.internal	/run/utmp	modified	16
ip-10-0-0-180.us-west-1.compute.internal	/etc/filebeat/fields.yml	added	16
Debian	/var/wazuh/queue/fim/db/fim.db	deleted	15
Debian	-	-	15
Ubuntu	/etc/resolv.conf	deleted	15
ip-10-0-0-180.us-west-1.compute.internal	/etc/resolv.conf	deleted	15
ip-10-0-0-180.us-west-1.compute.internal	/run/utmp	deleted	15
ip-10-0-0-180.us-west-1.compute.internal	/etc/elasticsearch/users	modified	15
Debian	/var/osquery/osquery.db/CURRENT	deleted	14
Ubuntu	/etc/resolv.conf	added	14
Ubuntu	/etc/filebeat/fields.yml	deleted	14
ip-10-0-0-180.us-west-1.compute.internal	/var/osquery/osquery.db/CURRENT	added	14
Debian	/run/utmp	deleted	13
Debian	/var/wazuh/queue/fim/db/fim.db-journal	deleted	13
Ubuntu	/tmp/agent.conf	modified	13
ip-10-0-0-180.us-west-1.compute.internal	/run/utmp	added	13

Agent name	Path	Action	Count
ip-10-0-0-180.us-west-1.compute.internal	/etc/elasticsearch/elasticsearch.yml	modified	13
Debian	/tmp/wazuh-config	modified	12
Ubuntu	/var/osquery/osquery.db/CURRENT	added	12
Ubuntu	/etc/resolv.conf	modified	12
Ubuntu	/etc/elasticsearch/config	deleted	12
Ubuntu	-	-	12
Debian	/run/utmp	added	11
Debian	/etc/filebeat/fields.yml	modified	11
Debian	/etc/elasticsearch/config	added	11
Ubuntu	/etc/filebeat/fields.yml	modified	11
Ubuntu	/etc/elasticsearch/elasticsearch.yml	added	11
ip-10-0-0-180.us-west-1.compute.internal	/etc/filebeat/fields.yml	deleted	11
Debian	/etc/filebeat/fields.yml	added	10
Debian	/etc/elasticsearch/config	modified	10
Debian	/tmp/agent.conf	added	10
Ubuntu	/etc/elasticsearch/config	modified	10
Ubuntu	/tmp/agent.conf	added	10
ip-10-0-0-180.us-west-1.compute.internal	/etc/elasticsearch/elasticsearch.yml	added	10
Debian	/var/wazuh/queue/fim/db/fim.db-journal	added	9
Debian	/tmp/agent.conf	modified	9
Debian	/var/log/lastlog	added	9
Ubuntu	/etc/elasticsearch/config	added	9
Ubuntu	/etc/elasticsearch/elasticsearch.yml	deleted	9
Ubuntu	/tmp/wazuh-config	modified	9
Ubuntu	/etc/elasticsearch/users	added	9
Ubuntu	/etc/sysconfig/network-scripts/ifcfg-eth1	deleted	9
Ubuntu	/var/wazuh/queue/fim/db/fim.db-journal	modified	9
ip-10-0-0-180.us-west-1.compute.internal	/etc/elasticsearch/elasticsearch.yml	deleted	9
Debian	/var/wazuh/queue/fim/db/fim.db-journal	modified	8
Debian	/etc/filebeat/fields.yml	deleted	8
Debian	/tmp/agent.conf	deleted	8
Debian	/etc/sysconfig/network-scripts/ifcfg-eth1	deleted	8
Debian	/etc/elasticsearch/users	added	8
Ubuntu	/etc/filebeat/fields.yml	added	8
Ubuntu	/tmp/agent.conf	deleted	8
Ubuntu	/tmp/wazuh-config	added	8
Ubuntu	/etc/sysconfig/network-scripts/ifcfg-eth1	added	8
Ubuntu	/var/log/lastlog	deleted	8
Debian	/tmp/wazuh-config	deleted	7
Debian	/var/log/lastlog	deleted	7
Debian	/etc/sysconfig/network-scripts/ifcfg-eth1	modified	7

Agent name	Path	Action	Count
Debian	/etc/elasticsearch/elasticsearch.yml	added	7
Debian	/etc/elasticsearch/elasticsearch.yml	deleted	7
Ubuntu	/tmp/wazuh-config	deleted	7
Ubuntu	/var/log/lastlog	added	7
Debian	/etc/elasticsearch/config	deleted	6
Debian	/tmp/wazuh-config	added	6
Debian	/var/log/lastlog	modified	6
Debian	/etc/sysconfig/network-scripts/ifcfg-eth1	added	6
Debian	/etc/elasticsearch/elasticsearch.yml	modified	6
Debian	/etc/elasticsearch/users	deleted	6
Ubuntu	/etc/elasticsearch/users	deleted	6
Ubuntu	/etc/elasticsearch/users	modified	6
Ubuntu	/var/wazuh/queue/fim/db/fim.db-journal	added	6
ip-10-0-0-180.us-west-1.compute.internal	/etc/filebeat/fields.yml	modified	6
Debian	/etc/elasticsearch/users	modified	5
Ubuntu	/etc/elasticsearch/elasticsearch.yml	modified	5
Ubuntu	/var/wazuh/queue/fim/db/fim.db-journal	deleted	5
Ubuntu	/etc/sysconfig/network-scripts/ifcfg-eth1	modified	4
Ubuntu	/var/log/lastlog	modified	3