File integrity monitoring report

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

2025-11-27T17:44:45 to 2025-11-28T17:44:45

manager.name: ip-172-31-16-30 AND rule.groups: syscheck

Top 3 FIM rules

Top 3 rules that are generating most alerts.

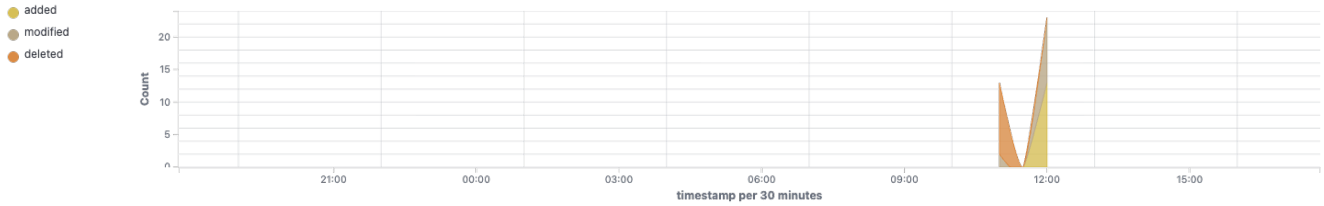
Rule ID	Description
554	File added to the system.
550	Integrity checksum changed.
553	File deleted.

Agents with suspicious FIM activity

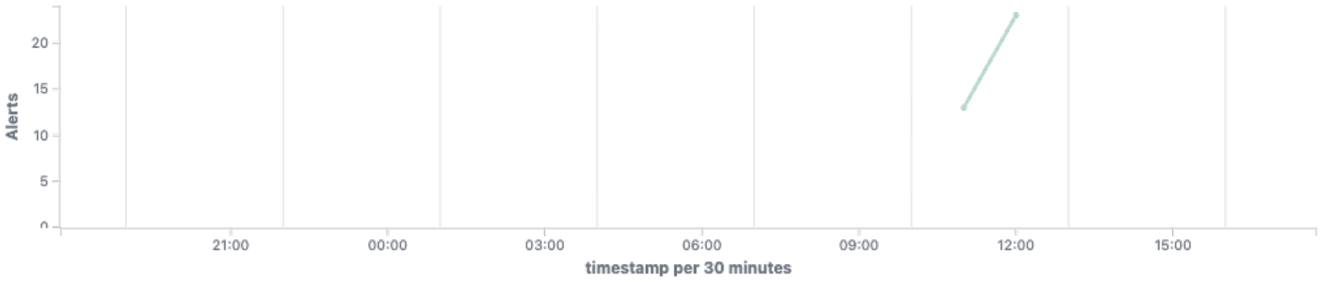
Top 3 agents that have most FIM alerts from level 7 to level 15. Take care about them.

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
000	ip-172-31-16-30	127.0.0.1	Wazuh v4.14.1	ip-172-31-16-30	Ubuntu 22.04.5 LTS	Nov 28, 2025 @ 03:59:37.000	Dec 31, 9999 @ 23:59:59.000
002	ubuntu-agent2	172.31.5.228	Wazuh v4.14.1	ip-172-31-16-30	Ubuntu 22.04.5 LTS	Nov 28, 2025 @ 04:46:56.000	Nov 28, 2025 @ 22:44:42.000

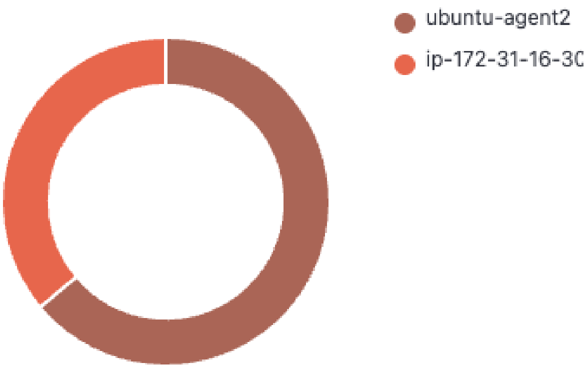
Alerts by action over time



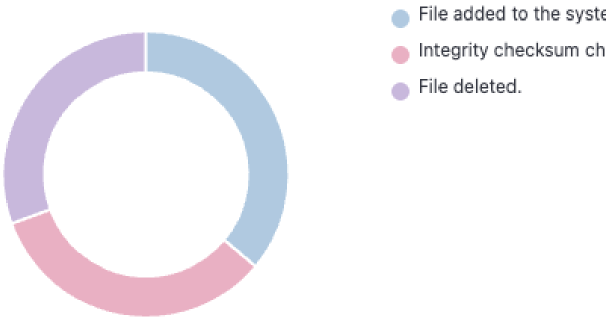
Events summary



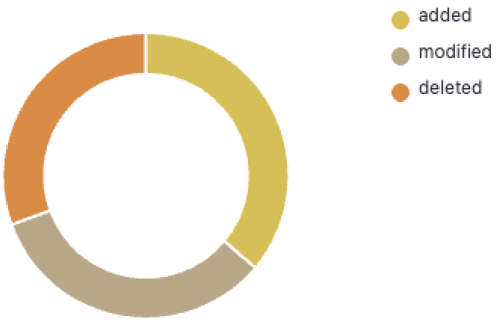
Top 5 agents



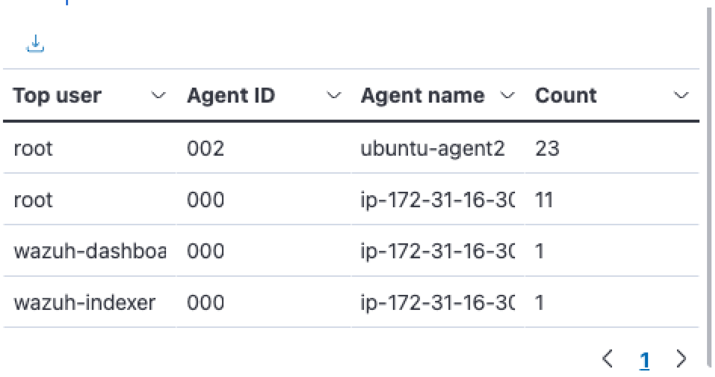
Rule distribution



Actions



Top 5 users



Top user	Agent ID	Agent name	Count
root	002	ubuntu-agent2	23
root	000	ip-172-31-16-3(	11
wazuh-dashboa	000	ip-172-31-16-3(	1
wazuh-indexer	000	ip-172-31-16-3(	1

Alerts summary

Agent name	Path	Action	Count
ubuntu-agent2	/etc/WAZUH_CRITICAL_TEST	added	1
ubuntu-agent2	/etc/passwd	modified	1
ubuntu-agent2	/etc/ssh/sshd_config	modified	1
ubuntu-agent2	/etc/systemd/system/multi-user.target.wants/snap-core20-2682.mount	added	1
ubuntu-agent2	/etc/systemd/system/multi-user.target.wants/snap-core22-2163.mount	added	1
ubuntu-agent2	/etc/systemd/system/multi-user.target.wants/snap-lxd-36558.mount	added	1
ubuntu-agent2	/etc/systemd/system/multi-user.target.wants/snap-snapd-25577.mount	added	1
ubuntu-agent2	/etc/systemd/system/multi-user.target.wants/snap.lxd.activate.service	modified	1
ubuntu-agent2	/etc/systemd/system/snap-core20-2682.mount	added	1
ubuntu-agent2	/etc/systemd/system/snap-core22-2163.mount	added	1
ubuntu-agent2	/etc/systemd/system/snap-lxd-36558.mount	added	1
ubuntu-agent2	/etc/systemd/system/snap-snapd-25577.mount	added	1
ubuntu-agent2	/etc/systemd/system/snap.lxd.activate.service	modified	1
ubuntu-agent2	/etc/systemd/system/snap.lxd.daemon.service	modified	1
ubuntu-agent2	/etc/systemd/system/snap.lxd.daemon.unix.socket	modified	1
ubuntu-agent2	/etc/systemd/system/snap.lxd.user-daemon.service	modified	1
ubuntu-agent2	/etc/systemd/system/snap.lxd.user-daemon.unix.socket	modified	1
ubuntu-agent2	/etc/systemd/system/snapd.mounts.target.wants/snap-core20-2682.mount	added	1
ubuntu-agent2	/etc/systemd/system/snapd.mounts.target.wants/snap-core22-2163.mount	added	1
ubuntu-agent2	/etc/systemd/system/snapd.mounts.target.wants/snap-lxd-36558.mount	added	1
ip-172-31-16-30	/etc/wazuh-dashboard/opensearch_dashboards.keystore	modified	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/action_groups.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/allowlist.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/audit.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/config.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/internal_users.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/nodes_dn.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/opensearch.yml.example	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/roles.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/roles_mapping.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/tenants.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/backup/whitelist.yml	deleted	1
ip-172-31-16-30	/etc/wazuh-indexer/opensearch-security/internal_users.yml	modified	1