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

Threat hunting report

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 @ 15:14:19.000

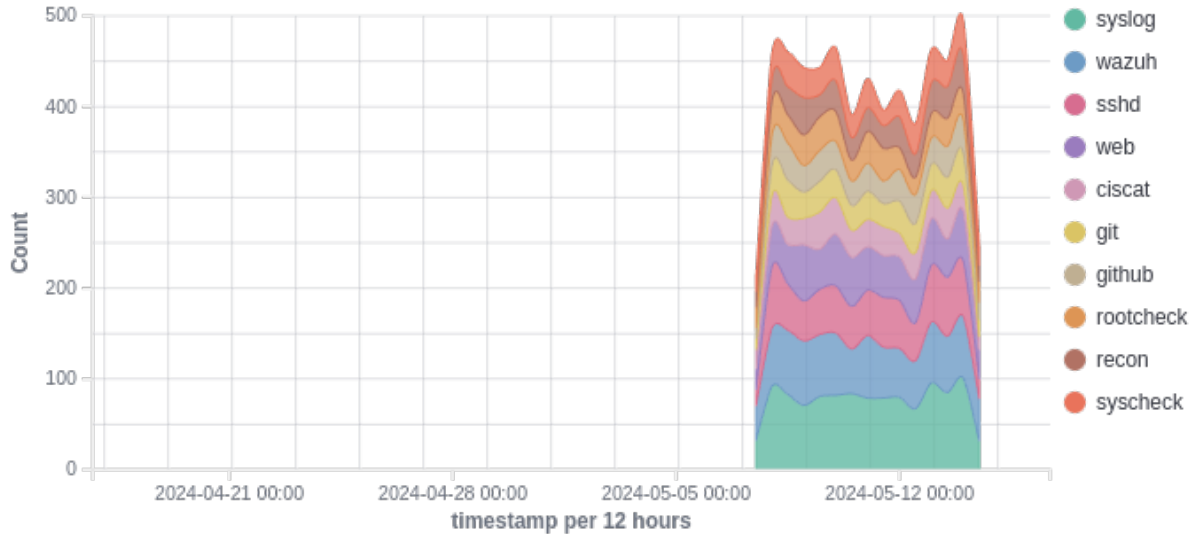
Group: default

Browse through your security alerts, identifying issues and threats in your environment.

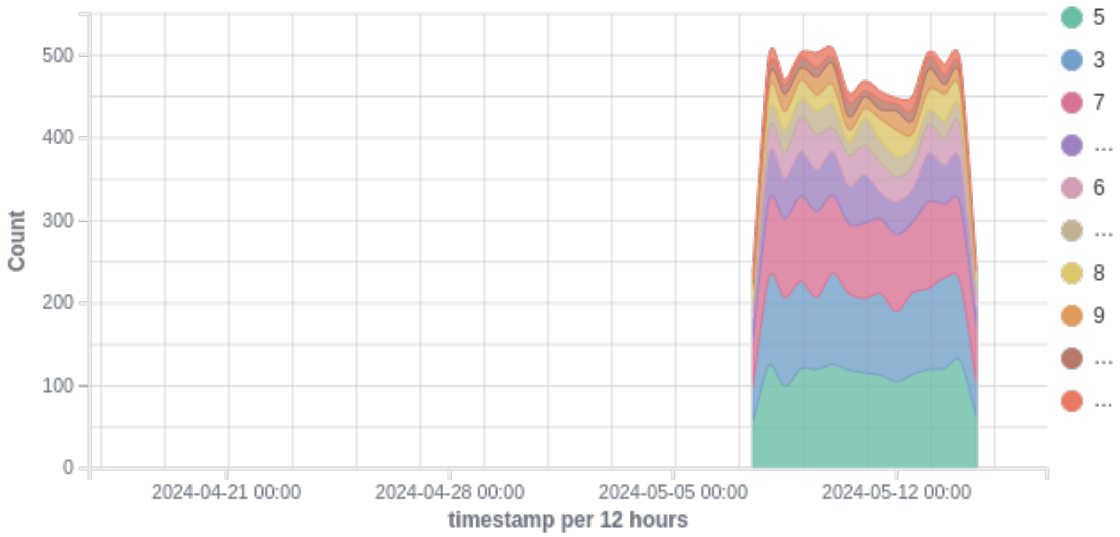
2024-04-16T17:14:23 to 2024-05-16T17:14:23

cluster.name: wazuh AND agent.id: 002

Top 10 Alert groups evolution



Alerts



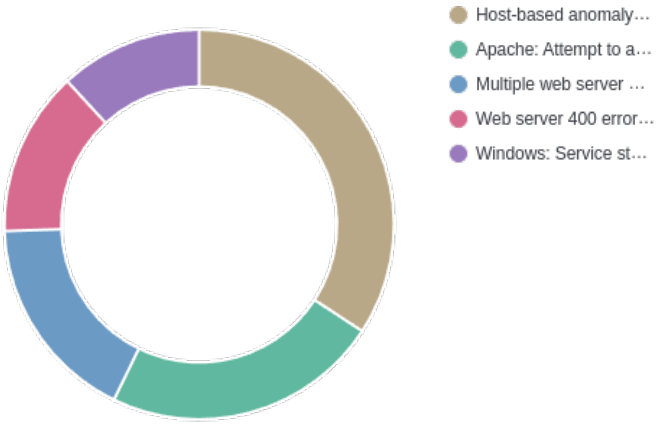
7,175
- Total -

645
- Level 12 or above alerts -

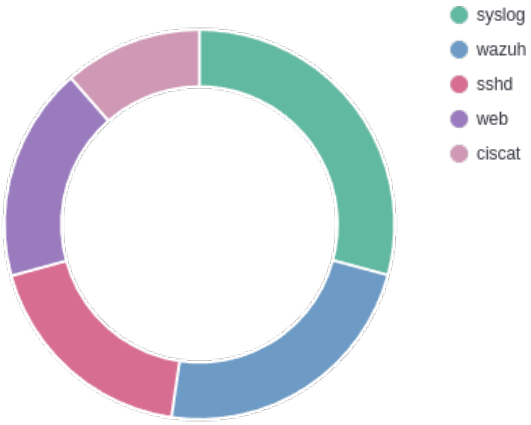
464
- Authentication failure -

57
- Authentication success -

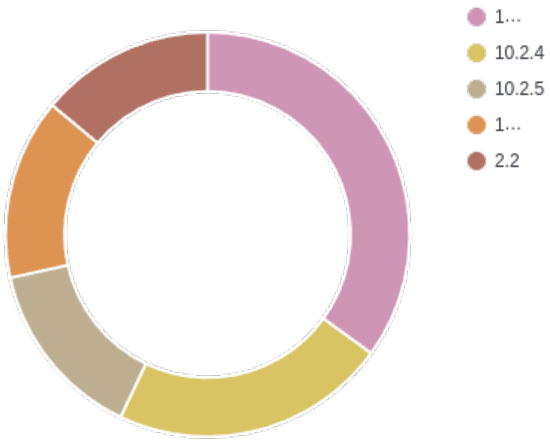
Top 5 alerts



Top 5 rule groups



Top 5 PCI DSS Requirements



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	442
30306	Apache: Attempt to access forbidden directory index.	5	297
31151	Multiple web server 400 error codes from same source ip.	10	223
31101	Web server 400 error code.	5	177
550	Integrity checksum changed.	7	150
553	File deleted.	7	146
554	File added to the system.	5	141
5703	sshd: Possible breakin attempt (high number of reverse lookup errors).	10	121
5706	sshd: insecure connection attempt (scan).	6	108
80355	AWS Macie CRITICAL: S3 Bucket IAM policy grants global read rights - S3 Bucket uses IAM policy to grant read rights to Everyone. Your IAM policy contains a clause that effectively grants read access to any user. Please audit this bucket, and data contained within and confirm that this is intentional. If intentional, please use the alert whitelist feature to prevent future alerts	12	108
5702	sshd: Reverse lookup error (bad ISP or attack).	5	104
91158	GitHub Git clone.	3	99
5701	sshd: Possible attack on the ssh server (or version gathering).	8	96
5710	sshd: Attempt to login using a non-existent user	5	93
5758	Maximum authentication attempts exceeded.	8	88
80302	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0cab4a083d57dc400 on server port 5060.	6	55
80781	Audit: Command: /usr/sbin/ls	3	50
80784	Audit: Command: /usr/sbin/crond	3	46
80302	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0b0b8b34a48c8f1c4 on server port 5060.	6	42
80784	Audit: Command: /usr/sbin/grep	3	41
80781	Audit: Command: /usr/sbin/sudo	3	40
80781	Audit: Command: /usr/sbin/consoletype	3	36
80784	Audit: Command: /usr/sbin/hostname	3	34
87928	Docker: Container test_container received the action: die	3	33
87928	Docker: Network bridge connected	3	31
80781	Audit: Command: /usr/sbin/id	3	30
80784	Audit: Command: /usr/sbin/bash	3	29
87932	Docker: Image or repository wazuh/wazuh-nginx pulled	3	29
87928	Docker: Container test_container started	3	29
81529	OpenSCAP: Record Events that Modify User/Group Information (not passed)	5	27
87932	Docker: Image or repository wazuh/wazuh-elasticsearch pulled	3	27
81530	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)	7	26
87932	Docker: Image or repository wazuh/wazuh-kibana pulled	3	23
81530	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)	7	22
87932	Docker: Image or repository wazuh/wazuh pulled	3	21

Rule ID	Description	Level	Count
81530	OpenSCAP: Set Password Strength Minimum Lowercase Characters (not passed)	7	18
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal SYSTEM.	6	18
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 160.0.14.40] [Port: 80]	3	18
81530	OpenSCAP: Ensure auditd Collects Information on the Use of Privileged Commands (not passed)	7	17
81530	OpenSCAP: Set Lockout Time For Failed Password Attempts (not passed)	7	16
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 160.0.14.40] [Port: 80]	3	15
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 75.0.101.245] [Port: 80]	3	15
81529	OpenSCAP: Record Attempts to Alter Time Through clock_settime (not passed)	5	15
81530	OpenSCAP: Enable Smart Card Login (not passed)	7	14
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal suricata.	6	14
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal wazuh.	6	14
23504	CVE-2020-1927 affects apache2	7	14
81529	OpenSCAP: Ensure auditd Collects System Administrator Actions (not passed)	5	14
23503	CVE-2013-4235 affects login	5	14
81530	OpenSCAP: Install AIDE (not passed)	7	13
81530	OpenSCAP: Set Password Minimum Length (not passed)	7	13
81529	OpenSCAP: Record Attempts to Alter the localtime File (not passed)	5	13
81529	OpenSCAP: Record attempts to alter time through settimeofday (not passed)	5	13
23503	CVE-2019-1552 affects openssl	5	13
81530	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)	7	12
81530	OpenSCAP: Record Attempts to Alter Logon and Logout Events (not passed)	7	12
81530	OpenSCAP: Record Events that Modify the System's Discretionary Access Controls - removexattr (not passed)	7	12
81530	OpenSCAP: Set Deny For Failed Password Attempts (not passed)	7	12
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal Administrators.	6	12
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal ec2-user.	6	12
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal root.	6	12
23503	CVE-2015-2987 affects ed	5	12
81530	OpenSCAP: Limit Password Reuse (not passed)	7	11
81530	OpenSCAP: Set Password Maximum Age (not passed)	7	11
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal NETWORK Service.	6	11
23504	CVE-2018-15919 affects openssh-client	7	11
23504	CVE-2019-1003010 affects git	7	11
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 2.25.80.45] [Port: 80]	3	11
81529	OpenSCAP: Record Events that Modify the System's Network Environment (not passed)	5	11
81530	OpenSCAP: Configure auditd to use audispd's syslog plugin (not passed)	7	10
81530	OpenSCAP: Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful) (not passed)	7	10
23504	CVE-2016-4484 affects cryptsetup	7	10
23504	CVE-2017-18018 affects coreutils	7	10

Rule ID	Description	Level	Count
23504	CVE-2018-20217 affects libkrb5-3	7	10
23504	CVE-2020-1927 affects apache2-data	7	10
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 70.24.101.214] [Port: 80]	3	10
23504	CVE-2019-18684 affects sudo	7	9
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 75.0.101.245] [Port: 80]	3	9
81529	OpenSCAP: Record Events that Modify the System's Discretionary Access Controls - chown (not passed)	5	9
81530	OpenSCAP: Set Password Strength Minimum Uppercase Characters (not passed)	7	8
23504	CVE-2018-14036 affects accountsservice	7	8
23504	CVE-2019-1010204 affects binutils	7	8
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 70.24.101.214] [Port: 80]	3	8
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 187.234.16.206] [Port: 80]	3	8
81530	OpenSCAP: Set Password Strength Minimum Digit Characters (not passed)	7	7
23504	CVE-2016-5011 affects uuid-runtime	7	7
23504	CVE-2018-8975 affects netpbm	7	7
23504	CVE-2019-11727 affects thunderbird	7	7
81530	OpenSCAP: Configure Periodic Execution of AIDE (not passed)	7	6
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal LOCAL Service.	6	6
23504	CVE-2017-14988 affects libopenexr22	7	6
23504	CVE-2019-17543 affects liblz4-1	7	6
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 187.234.16.206] [Port: 80]	3	6
23504	CVE-2017-7244 affects libpcre3	7	5
23504	CVE-2017-9502 affects curl	7	5
23504	CVE-2019-17540 affects imagemagick	7	5
23504	CVE-2019-17595 affects ncurses-base	7	5
23504	CVE-2020-1927 affects apache2-bin	7	5
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 2.25.80.45] [Port: 80]	3	5

Groups summary

Groups	Count
syslog	1143
wazuh	906
sshd	741
web	697
ciscat	449
git	448
github	448
syscheck	447
rootcheck	444
recon	439
virustotal	432
oscap	431
gcp	425
osquery	419
amazon	409
aws	409
vulnerability-detector	401
accesslog	400
oscap-result	397
audit	392
audit_command	392
docker	383
authentication_failed	320
aws_guardduty	301
access_denied	300
apache	297
web_scan	223
windows	201
attack	177
policy_changed	153
invalid_login	141
git_git	129
git_org	110
aws_macie	108
authentication_failures	96
pam	91
multiple_spam	73
git_team	71
postfix	69

Groups	Count
spam	60
sendmail	59
authentication_success	57
win_authentication_failed	48
windows_security	48
oscap-report	34
pix	32
netscreenfw	30
git_repo	27
docker-error	26
git_dependency_graph_new_repos	24