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

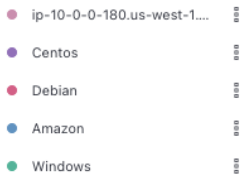
Security events report

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

2022-02-07T11:33:12 to 2022-02-14T11:44:30

cluster.name: wazuh

Alerts evolution Top 5 agents



Alert level evolution

Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	1711
30306	Apache: Attempt to access forbidden directory index.	5	1130
31101	Web server 400 error code.	5	875
31151	Multiple web server 400 error codes from same source ip.	10	871
553	File deleted.	7	594
554	File added to the system.	5	567
550	Integrity checksum changed.	7	542
80302	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0cab4a083d57dc400 on server port 5060.	6	219
80302	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0b0b8b34a48c8f1c4 on server port 5060.	6	204
80790	Audit: Command: /usr/sbin/bash	3	189
80790	Audit: Command: /usr/sbin/crond	3	183
80784	Audit: Command: /usr/sbin/ls	3	177
80790	Audit: Command: /usr/sbin/id	3	166
80784	Audit: Command: /usr/sbin/sudo	3	166
80790	Audit: Command: /usr/sbin/grep	3	162
80784	Audit: Command: /usr/sbin/sh	3	162
81530	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)	7	106
81530	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)	7	102
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal NETWORK Service.	6	65
81530	OpenSCAP: Limit Password Reuse (not passed)	7	60
81530	OpenSCAP: Set Password Maximum Age (not passed)	7	59
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal LOCAL Service.	6	59
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal root.	6	59
81530	OpenSCAP: Set Lockout Time For Failed Password Attempts (not passed)	7	57
81530	OpenSCAP: Configure Periodic Execution of AIDE (not passed)	7	55
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal wazuh.	6	54
81530	OpenSCAP: Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful) (not passed)	7	53
81530	OpenSCAP: Install AIDE (not passed)	7	53
81530	OpenSCAP: Record Events that Modify the System's Discretionary Access Controls - removexattr (not passed)	7	52
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal Administrators.	6	52
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal SYSTEM.	6	52
81530	OpenSCAP: Ensure auditd Collects Information on the Use of Privileged Commands (not passed)	7	51
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal suricata.	6	51
81530	OpenSCAP: Set Password Strength Minimum Digit Characters (not passed)	7	48
81530	OpenSCAP: Configure auditd to use audispd's syslog plugin (not passed)	7	47
81530	OpenSCAP: Record Attempts to Alter Logon and Logout Events (not passed)	7	47
81530	OpenSCAP: Set Password Minimum Length (not passed)	7	47

Rule ID	Description	Level	Count
81530	OpenSCAP: Set Password Strength Minimum Uppercase Characters (not passed)	7	47
81530	OpenSCAP: Set Deny For Failed Password Attempts (not passed)	7	46
81530	OpenSCAP: Set Password Strength Minimum Lowercase Characters (not passed)	7	44
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal ec2-user.	6	43
81530	OpenSCAP: Enable Smart Card Login (not passed)	7	42
81530	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)	7	40
23504	CVE-2020-1927 affects apache2-bin	7	36
23504	CVE-2019-1003010 affects git	7	35
23504	CVE-2020-1927 affects apache2	7	35
23504	CVE-2016-5011 affects uuid-runtime	7	34
23504	CVE-2016-4484 affects cryptsetup	7	32
23504	CVE-2019-17540 affects imagemagick	7	32
23504	CVE-2019-1010204 affects binutils	7	31
23504	CVE-2017-14988 affects libopenexr22	7	30
23504	CVE-2018-14036 affects accountsservice	7	30
23504	CVE-2019-11727 affects thunderbird	7	30
23504	CVE-2019-19232 affects sudo	7	29
23504	CVE-2015-5191 affects open-vm-tools	7	28
23504	CVE-2019-17595 affects ncurses-base	7	28
23504	CVE-2020-1927 affects apache2-data	7	28
23504	CVE-2018-15919 affects openssh-server	7	27
23504	CVE-2017-18018 affects coreutils	7	25
23504	CVE-2018-15919 affects openssh-client	7	25
23504	CVE-2019-14855 affects dirmngr	7	24
23504	CVE-2019-17540 affects libmagickcore-6.q16-3	7	24
23504	CVE-2017-7244 affects libpcre3	7	23
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure default deny firewall policy	3	18
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure loopback traffic is configured	3	12
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure DNS Server is not enabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure FTP Server is not enabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure LDAP server is not enabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure NFS and RPC are not enabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure SSH IgnoreRhosts is enabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure SSH LoginGraceTime is set to one minute or less	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure SSH MaxAuthTries is set to 4 or less	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure SSH MaxSessions is set to 4 or less	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure all AppArmor Profiles are in enforce or complain mode	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure base chains exist	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure mounting of cramfs filesystems is disabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure mounting of freevxfs filesystems is disabled	3	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure mounting of squashfs filesystems is disabled	3	6

Rule ID	Description	Level	Count
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure /etc/hosts.allow is configured	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure /etc/hosts.deny is configured	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure AppArmor is installed	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure IPv6 router advertisements are not accepted	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure address space layout randomization (ASLR) is enabled	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure authentication required for single user mode	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure default user shell timeout is 900 seconds or less	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure events that modify user/group information are collected	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure nodev option set on /var/tmp partition	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure noexec option set on /var/tmp partition	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure nosuid option set on /tmp partition	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure permissions on /etc/crontab are configured	7	6
19007	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure permissions on SSH public host key files are configured	7	6
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Disable Automounting	3	5
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Disable IPv6	3	5
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Disable USB Storage	3	5
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure AppArmor is enabled in the bootloader configuration	3	5
19009	CIS benchmark for Ubuntu Linux 18.04 LTS: Ensure Avahi Server is not enabled	3	5
510	Sample alert 4	1	1
553	Windows: Service startup type was changed.	3	1
553	osquery: incident-response process_env: Process 26151 Environment variable GENERATION value 244	12	1