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

Threat hunting report

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

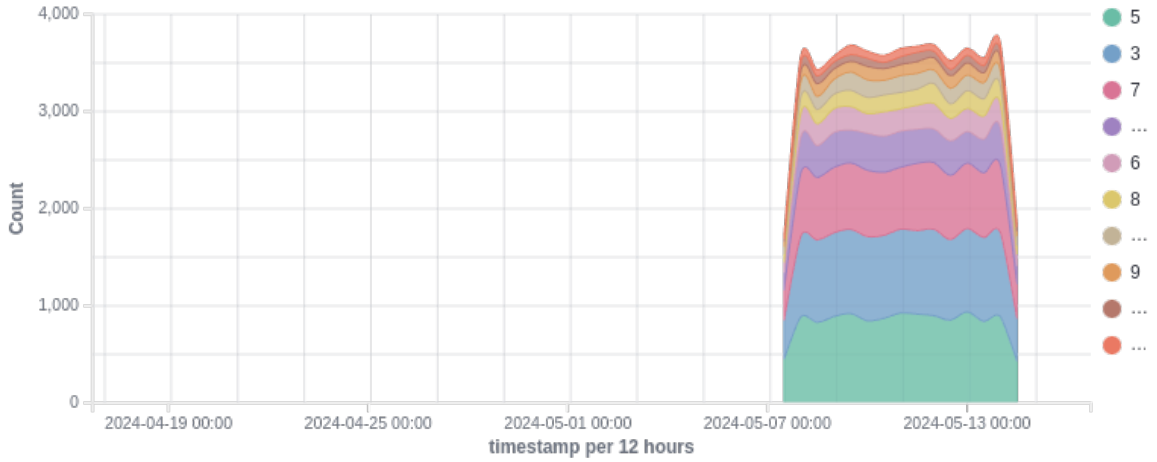
2024-04-16T17:13:15 to 2024-05-16T17:13:15

cluster.name: wazuh

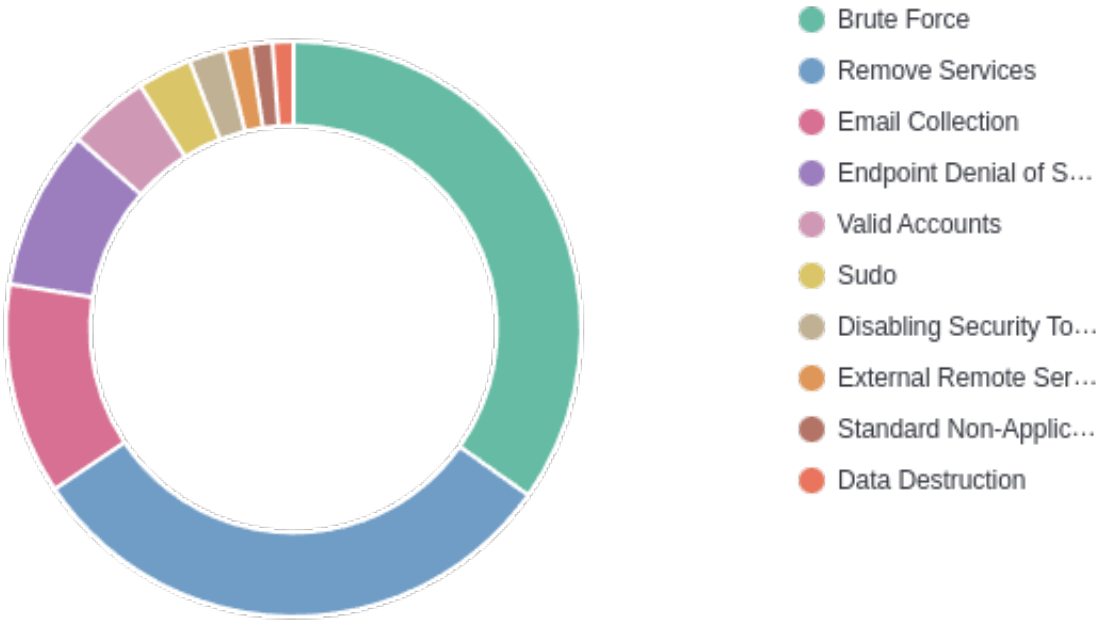
Top 3 agents with level 15 alerts

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	wazuh_agent_ubuntu	172.20.0.8	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 @ 15:13:07.000

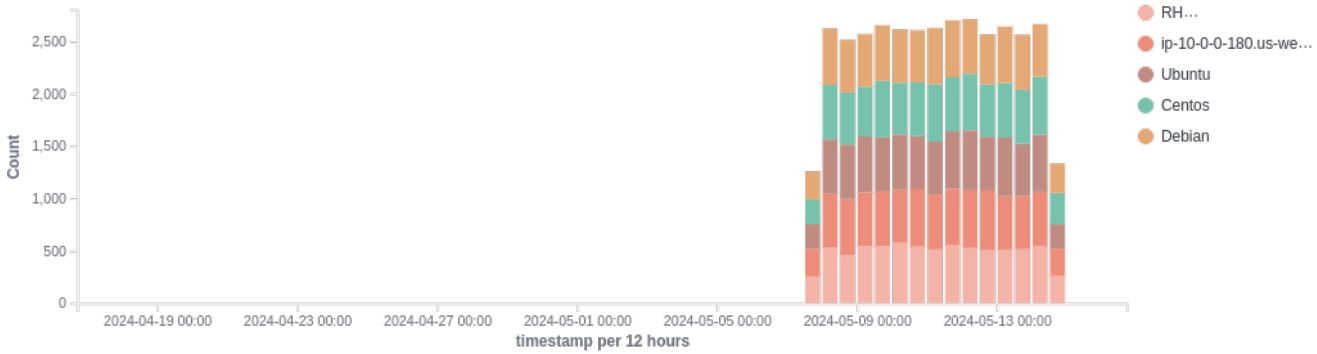
Top 10 Alert level evolution



Top 10 MITRE ATT&CKS



Alerts evolution - Top 5 agents



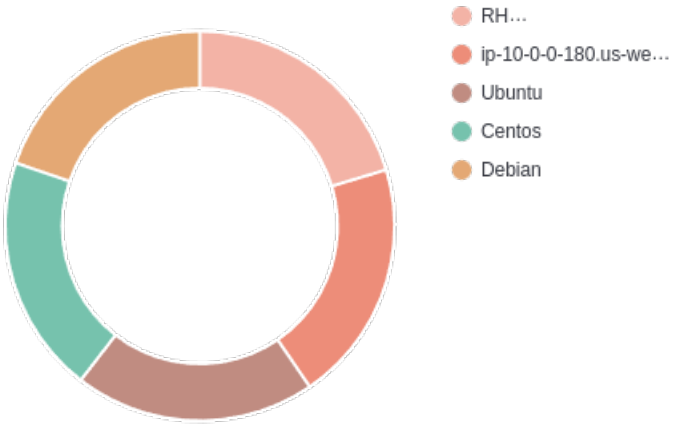
53,682
- Total -

4,491
- Level 12 or above alerts -

3,238
- Authentication failure -

365
- Authentication success -

Top 5 agents



Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	3000
30306	Apache: Attempt to access forbidden directory index.	5	2000
31151	Multiple web server 400 error codes from same source ip.	10	1530
31101	Web server 400 error code.	5	1470
550	Integrity checksum changed.	7	1043
554	File added to the system.	5	996
553	File deleted.	7	992
5702	sshd: Reverse lookup error (bad ISP or attack).	5	772
5703	sshd: Possible breakin attempt (high number of reverse lookup errors).	10	755
5706	sshd: insecure connection attempt (scan).	6	754
5701	sshd: Possible attack on the ssh server (or version gathering).	8	752
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	733
80302	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0b0b8b34a48c8f1c4 on server port 5060.	6	390
80302	AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0cab4a083d57dc400 on server port 5060.	6	363
80784	Audit: Command: /usr/sbin/hostname	3	317
80781	Audit: Command: /usr/sbin/sudo	3	314
80784	Audit: Command: /usr/sbin/crond	3	313
80781	Audit: Command: /usr/sbin/ls	3	312
80784	Audit: Command: /usr/sbin/bash	3	298
80781	Audit: Command: /usr/sbin/id	3	284
80784	Audit: Command: /usr/sbin/grep	3	273
80781	Audit: Command: /usr/sbin/consoletype	3	273
87932	Docker: Image or repository wazuh/wazuh-nginx pulled	3	227
87932	Docker: Image or repository wazuh/wazuh pulled	3	212
87932	Docker: Image or repository wazuh/wazuh-elasticsearch pulled	3	205
81529	OpenSCAP: Record Events that Modify User/Group Information (not passed)	5	193
87932	Docker: Image or repository wazuh/wazuh-kibana pulled	3	190
81530	OpenSCAP: Ensure auditd Collects Information on Kernel Module Loading and Unloading (not passed)	7	169
81530	OpenSCAP: Ensure auditd Collects File Deletion Events by User (not passed)	7	154
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 160.0.14.40] [Port: 80]	3	134
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 160.0.14.40] [Port: 80]	3	120
23505	CVE-2018-1000035 affects unzip	10	109
81530	OpenSCAP: Enable Smart Card Login (not passed)	7	107

Rule ID	Description	Level	Count
81530	OpenSCAP: Limit Password Reuse (not passed)	7	105
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal LOCAL Service.	6	99
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal ec2-user.	6	99
23505	CVE-2020-1747 affects python3-yaml	10	99
81530	OpenSCAP: Ensure auditd Collects Unauthorized Access Attempts to Files (unsuccessful) (not passed)	7	95
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal suricata.	6	95
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal wazuh.	6	95
81529	OpenSCAP: Record Events that Modify the System's Network Environment (not passed)	5	95
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal root.	6	94
81530	OpenSCAP: Ensure auditd Collects Information on Exporting to Media (successful) (not passed)	7	93
81530	OpenSCAP: Set Password Minimum Length (not passed)	7	93
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal SYSTEM.	6	93
81530	OpenSCAP: Set Password Maximum Age (not passed)	7	91
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal Administrators.	6	89
81529	OpenSCAP: Record Attempts to Alter the localtime File (not passed)	5	89
81530	OpenSCAP: Set Deny For Failed Password Attempts (not passed)	7	88
81530	OpenSCAP: Set Password Strength Minimum Lowercase Characters (not passed)	7	88
81530	OpenSCAP: Install AIDE (not passed)	7	87
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal NETWORK Service.	6	87
81529	OpenSCAP: Record Attempts to Alter Time Through clock_settime (not passed)	5	86
81530	OpenSCAP: Ensure auditd Collects Information on the Use of Privileged Commands (not passed)	7	83
81530	OpenSCAP: Record Attempts to Alter Logon and Logout Events (not passed)	7	83
81529	OpenSCAP: Ensure auditd Collects System Administrator Actions (not passed)	5	83
81530	OpenSCAP: Record Events that Modify the System's Discretionary Access Controls - removexattr (not passed)	7	82
81530	OpenSCAP: Set Lockout Time For Failed Password Attempts (not passed)	7	81
81529	OpenSCAP: Record attempts to alter time through settimeofday (not passed)	5	79
81530	OpenSCAP: Configure auditd to use audispd's syslog plugin (not passed)	7	76
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 75.0.101.245] [Port: 80]	3	74
81530	OpenSCAP: Set Password Strength Minimum Digit Characters (not passed)	7	73
81529	OpenSCAP: Record Events that Modify the System's Discretionary Access Controls - chown (not passed)	5	73
81530	OpenSCAP: Configure Periodic Execution of AIDE (not passed)	7	72
81530	OpenSCAP: Set Password Strength Minimum Uppercase Characters (not passed)	7	72
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 70.24.101.214] [Port: 80]	3	70
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 2.25.80.45] [Port: 80]	3	67
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 187.234.16.206] [Port: 80]	3	66
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 70.24.101.214] [Port: 80]	3	65
23504	CVE-2020-1927 affects apache2	7	64

Rule ID	Description	Level	Count
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 75.0.101.245] [Port: 80]	3	60
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 187.234.16.206] [Port: 80]	3	58
23504	CVE-2018-15919 affects openssh-client	7	57
23504	CVE-2016-4484 affects cryptsetup	7	54
23504	CVE-2017-9502 affects curl	7	54
23504	CVE-2020-1927 affects apache2-data	7	54
23505	CVE-2020-9366 affects screen	10	54
23504	CVE-2019-17543 affects liblz4-1	7	53
23504	CVE-2020-1927 affects apache2-bin	7	53
23504	CVE-2018-20217 affects libkrb5-3	7	52
23505	CVE-2019-15847 affects gcc	10	52
23504	CVE-2019-17540 affects imagemagick	7	51
23504	CVE-2019-18684 affects sudo	7	51
23504	CVE-2019-17595 affects ncurses-base	7	49
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 2.25.80.45] [Port: 80]	3	49
23504	CVE-2017-7244 affects libpcre3	7	48
23504	CVE-2019-17540 affects libmagickcore-6.q16-3	7	48
23505	CVE-2019-13050 affects gnupg	10	48
23504	CVE-2017-18018 affects coreutils	7	47
23504	CVE-2017-14988 affects libopenexr22	7	46
23504	CVE-2018-14036 affects accountsservice	7	46
23504	CVE-2018-15919 affects openssh-server	7	46
23504	CVE-2019-1003010 affects git	7	46
23505	CVE-2018-7738 affects mount	10	46
23505	CVE-2019-20079 affects vim	10	46
23504	CVE-2016-5011 affects uuid-runtime	7	44
23504	CVE-2019-1010204 affects binutils	7	44
550	Windows: Service startup type was changed.	3	1
5706	VirusTotal: Alert - /usr/share/sample/program - 32 engines detected this file	13	1