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

# AWS 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 @ 15:48:59.000 |

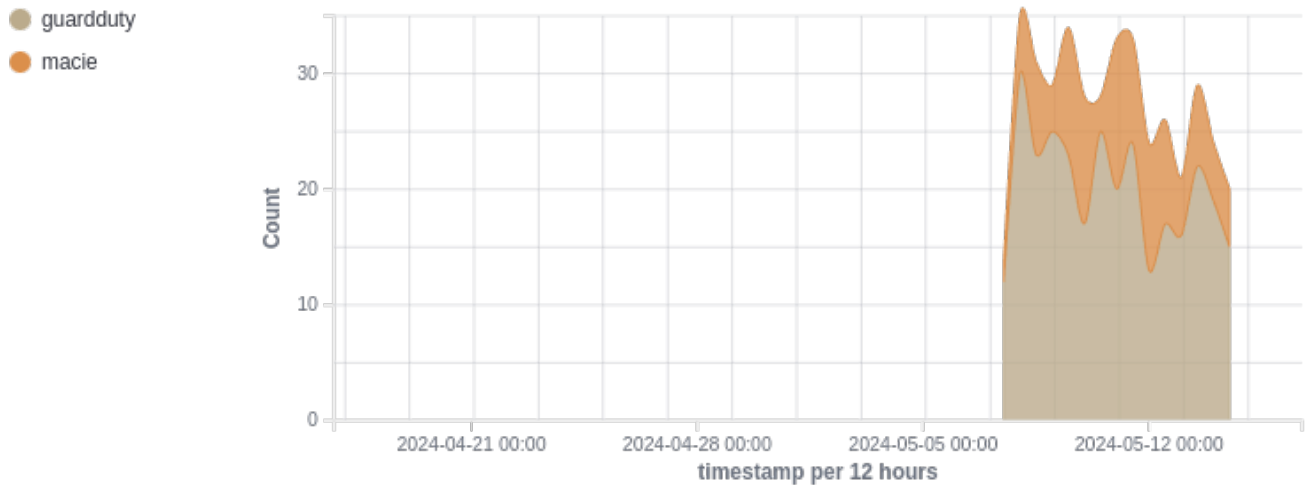
Group: default

Security events related to your Amazon AWS services, collected directly via AWS API.

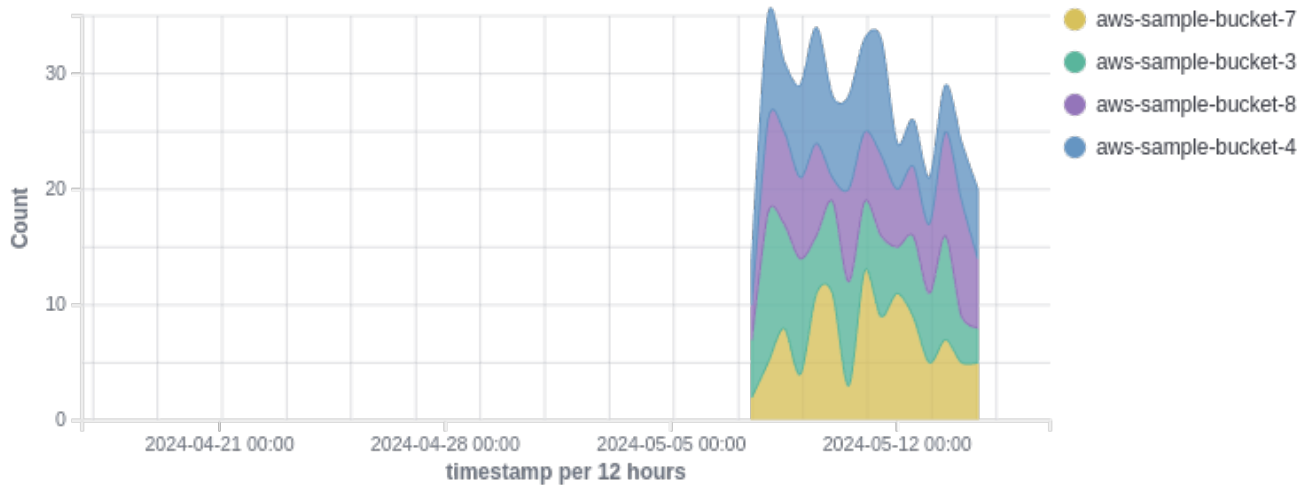
2024-04-16T17:49:01 to 2024-05-16T17:49:01

rule.groups: amazon AND cluster.name: wazuh AND agent.id: 002

## Events by source over time

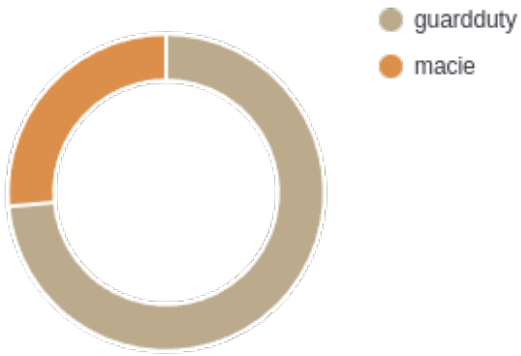


## Events by S3 bucket over time

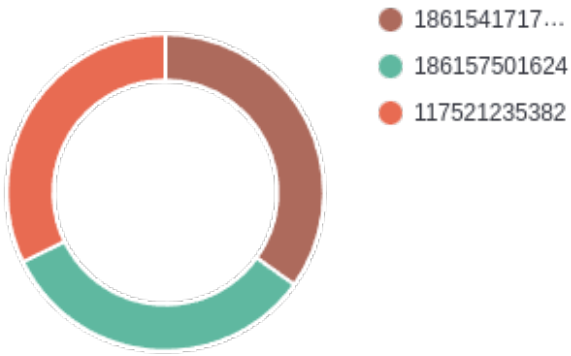



## Geolocation map

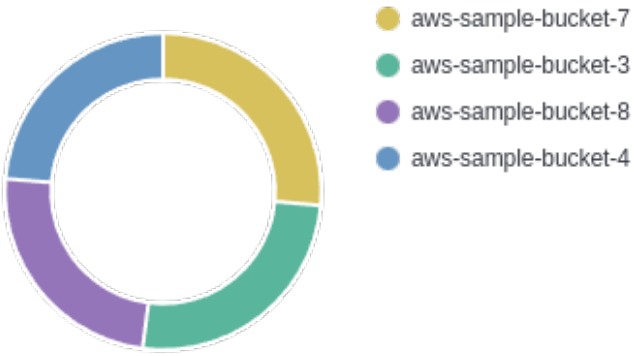

## Sources



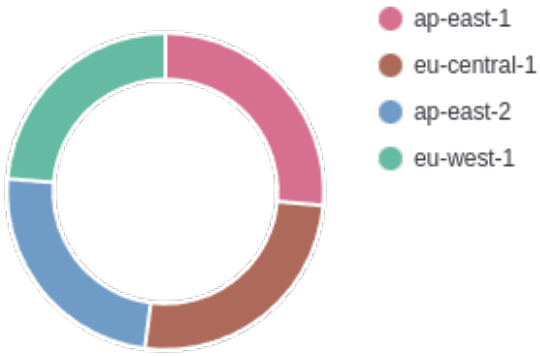

## Accounts



## Buckets




## Regions



# Alerts summary

| Rule ID | Description | Level | Count |
|---|---|---|---|
| 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 |
| 80302 | AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0cab4a083d57dc400 on server port 5060. | 6 | 55 |
| 80302 | AWS GuardDuty: NETWORK_CONNECTION - Unusual outbound communication seen from EC2 instance i-0b0b8b34a48c8f1c4 on server port 5060. | 6 | 42 |
| 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 |
| 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 |
| 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 |
| 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 |
| 80302 | AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal NETWORK Service. | 6 | 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 |
| 80305 | AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 70.24.101.214] [Port: 80] | 3 | 10 |
| 80305 | AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 75.0.101.245] [Port: 80] | 3 | 9 |
| 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 |
| 80302 | AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal LOCAL Service. | 6 | 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 |
| 80305 | AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 2.25.80.45] [Port: 80] | 3 | 5 |