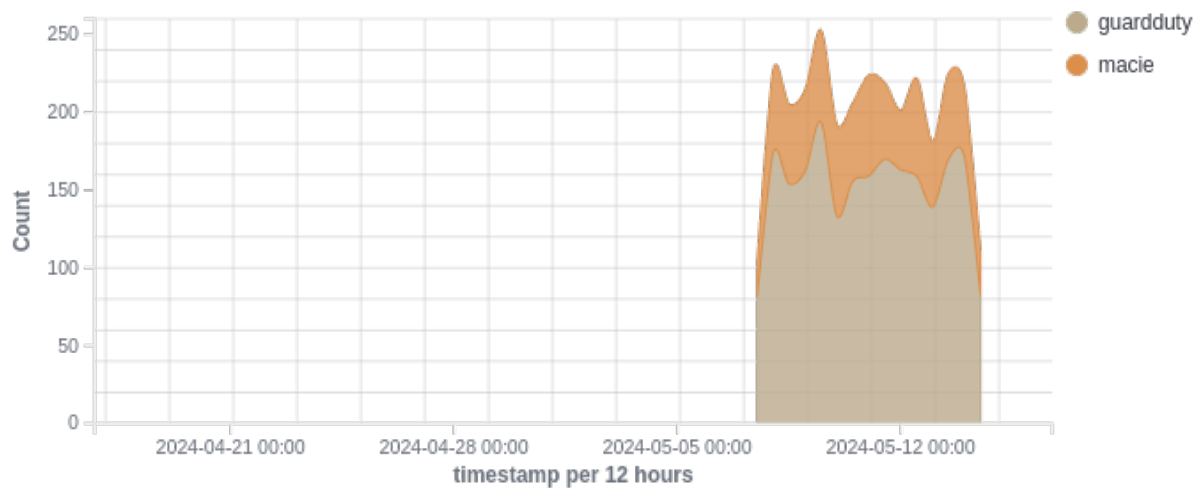# wazuh.

AWS report

Security events related to your Amazon AWS services, collected directly via AWS API.
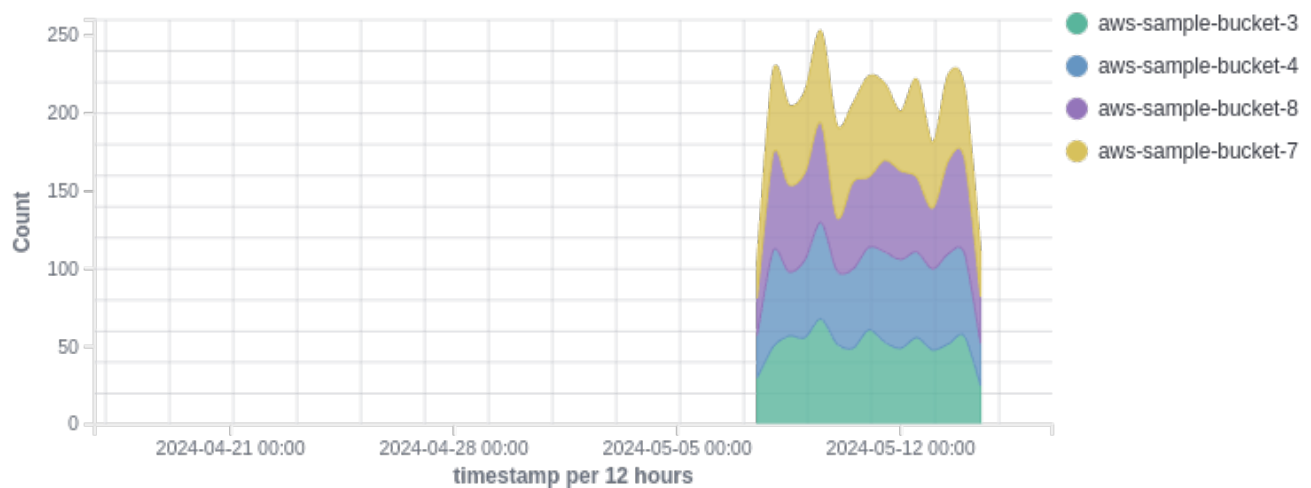
🕐 2024-04-16T17:48:21 to 2024-05-16T17:48:21

🔍 rule.groups: amazon AND cluster.name: wazuh
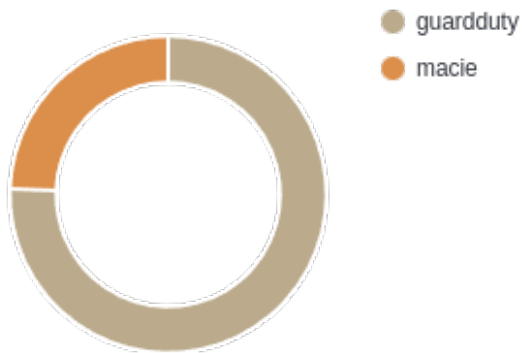
Events by source over time

Events by S3 bucket over time

wazuh.

Geolocation map

Count
- 276 – 289.75
- 289.75 – 303.5
- 303.5 – 317.25
- 317.25 – 331

Map data © OpenStreetMap contributors

Sources

- guardduty
- macie

Accounts

- 1861541717…
- 117521235382
- 186157501624

Buckets

- aws-sample-bucket-3
- aws-sample-bucket-4
- aws-sample-bucket-8
- aws-sample-bucket-7

Regions

- eu-central-1
- eu-west-1
- ap-east-2
- ap-east-1
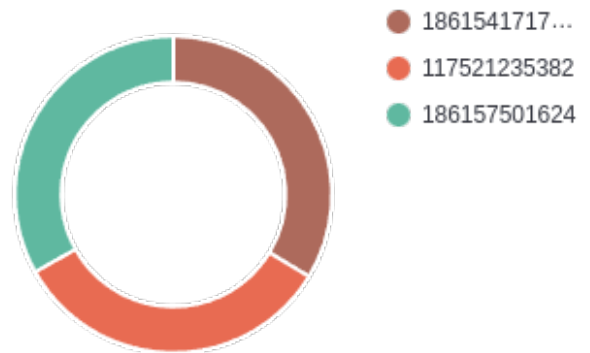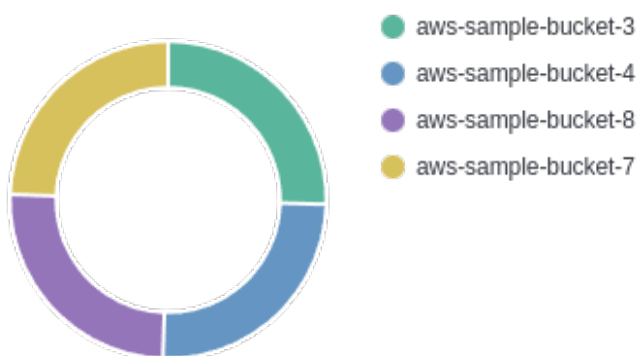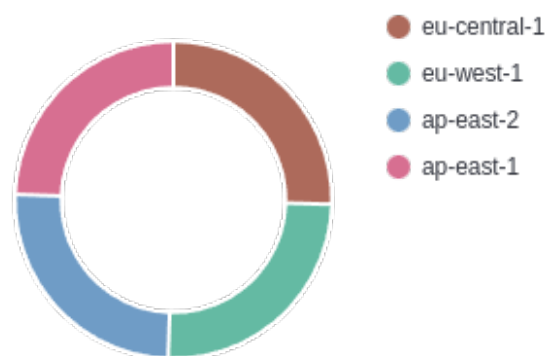
Alerts summary

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	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
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
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
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
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal root.	6	94
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal SYSTEM.	6	93
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal Administrators.	6	89
80302	AWS GuardDuty: AWS_API_CALL - Unusual console login was seen for principal NETWORK Service.	6	87
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0b0b8b34a48c8f1c4 is being probed. [IP: 75.0.101.245] [Port: 80]	3	74
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
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
80305	AWS GuardDuty: PORT_PROBE - Unprotected port on EC2 instance i-0cab4a083d57dc400 is being probed. [IP: 2.25.80.45] [Port: 80]	3	49