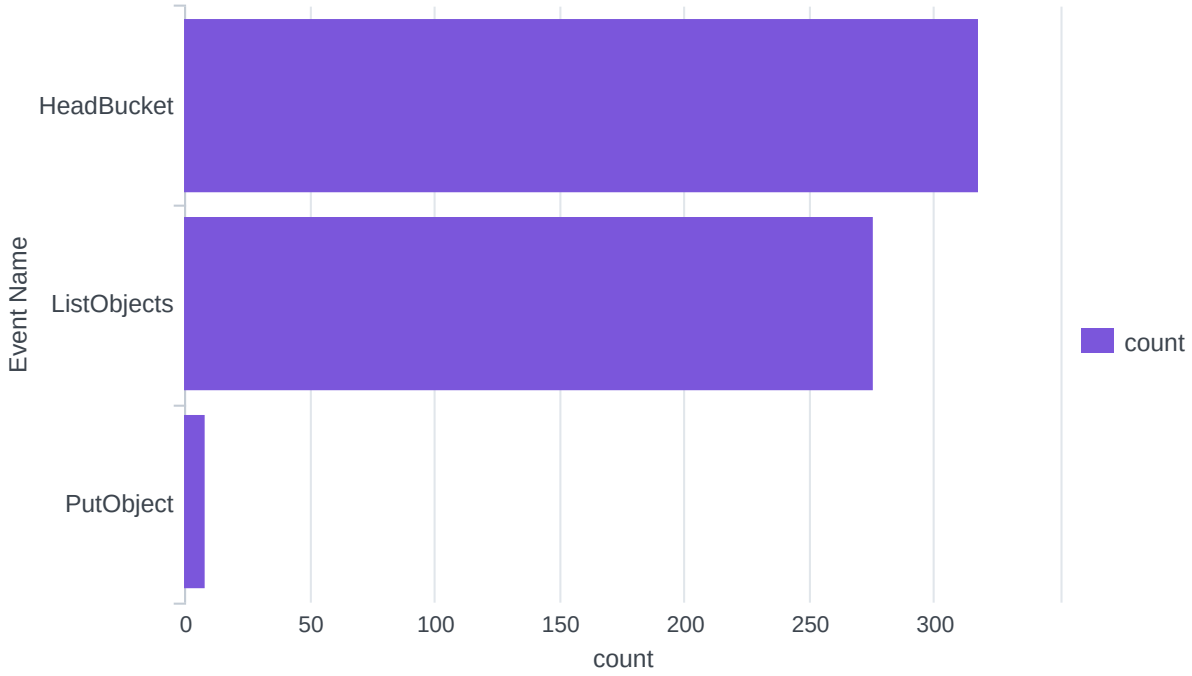
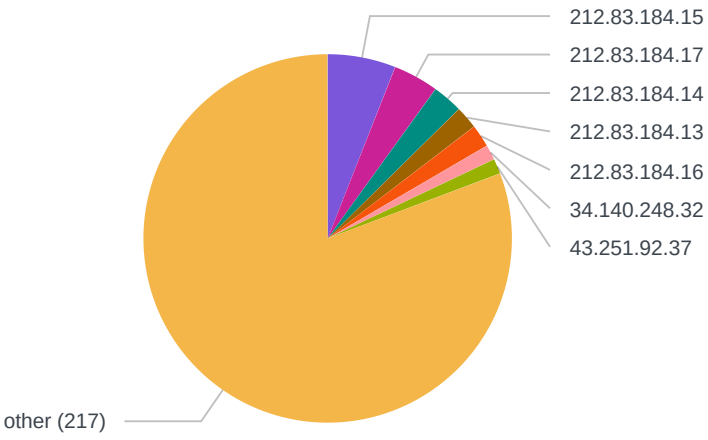
Event Name Count



Source IP Analysis

Panel Purpose: To track source IPs with the highest number of requests, which can alert you to potential sources of attack or unauthorized access.



Top User Agents

Panel Purpose: To monitor the most common user agents accessing your buckets, which can help identify automated tools or scripts.

Request User Agent	count
Go-http-client/1.1	264
Boto3/1.17.40 Python/3.6.12 Linux/3.10.0-1160.6.1.el7.x86_64 Botocore/1.20.112	110
Java/1.8.0_201	36
Ruby	14
Boto3/1.17.68 Python/3.9.4 Linux/5.4.0-1033-gke Botocore/1.20.68 Resource	8
Boto3/1.20.24 Python/3.9.9 Linux/5.4.0-1051-gke Botocore/1.23.24 Resource	8
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36	8
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0	8
python-requests/2.22.0	8
Boto3/1.17.68 Python/3.9.4 Linux/5.4.0-1036-gke Botocore/1.20.68 Resource	6
Boto3/1.18.53 Python/3.9.7 Linux/5.4.0-1049-gke Botocore/1.21.53 Resource	6
Boto3/1.9.85 Python/2.7.15 Darwin/17.7.0 Botocore/1.12.253 Resource	6
Java/11.0.11	6
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36	6
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36	6
aws-cli/1.17.9 Python/3.6.0 Windows/10 botocore/1.14.9	6
aws-sdk-go/1.40.9 (go1.15.8; linux; amd64)	6
Boto3/1.14.11 Python/3.5.6 Linux/4.19.112+ Botocore/1.17.11 Resource	4
Boto3/1.14.28 Python/3.6.9 Linux/4.15.0-66-generic Botocore/1.17.28	4
Boto3/1.15.15 Python/3.5.6 Linux/4.19.112+ Botocore/1.18.15 Resource	4
Boto3/1.16.18 Python/3.5.6 Linux/5.3.0-1036-gke Botocore/1.19.18 Resource	4
Boto3/1.16.59 Python/3.7.1 Linux/5.3.0-1036-gke Botocore/1.19.59 Resource	4
Boto3/1.17.17 Python/3.7.1 Linux/5.3.0-1038-gke Botocore/1.20.17 Resource	4
Boto3/1.17.48 Python/3.7.1 Linux/5.4.0-1032-gke Botocore/1.20.48 Resource	4
Boto3/1.18.18 Python/3.9.4 Linux/5.4.0-1044-gke Botocore/1.21.18 Resource	4
Boto3/1.20.12 Python/3.9.9 Linux/5.4.0-1051-gke Botocore/1.23.12 Resource	4
Boto3/1.20.24 Python/3.9.10 Linux/5.4.0-1054-gke Botocore/1.23.24 Resource	4
Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36	4
aws-sdk-go/1.34.2 (go1.10.4; linux; amd64)	4
aws-sdk-go/1.35.1 (go1.14.4; linux; amd64)	4
Apache-HttpClient/4.5.2 (Java/1.8.0_121)	2
Boto3/1.14.52 Python/3.8.3 Windows/10 Botocore/1.17.52	2
Boto3/1.16.39 Python/3.8.5 Linux/5.4.0-1029-aws Botocore/1.19.39	2
Boto3/1.17.49 Python/3.7.1 Linux/5.4.0-1032-gke Botocore/1.20.49 Resource	2
Boto3/1.17.76 Python/3.7.3 Linux/4.19.0-16-amd64 Botocore/1.20.105 Resource	2
Java/11.0.8	2
Java/11.0.9.1	2
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36 Edg/89.0.774.57	2
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36	2
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0	2
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:25.0) Gecko/20100101 Firefox/25.0	2
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36	2
Repeated Attempts:1	2
aws-sdk-go/1.35.1 (go1.13; linux; amd64)	2
aws-sdk-go/1.35.1 (go1.15.3; linux; amd64)	2
aws-sdk-go/1.35.1 (go1.15.6; linux; amd64)	2
aws-sdk-go/1.40.9 (go1.13.8; linux; amd64)	2

Request User Agent	count
aws-sdk-go/1.40.9 (go1.16.3; linux; amd64)	2

Analysis of Request Parameters

Panel Purpose: To observe common request parameters, particularly useful for spotting unusual or suspicious parameters that could indicate probing.

Request Parameters	count
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.amazonaws.com'}	368
{'list-type': '2', 'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.amazonaws.com', 'encoding-type': 'url'}	110
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.amazonaws.com', 'encoding-type': 'url'}	56
{'list-type': '2', 'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com'}	26
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com', 'key': 'writeable_bucket.txt'}	6
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com'}	6
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com', 'encoding-type': 'url', 'prefix': '*'}	4
{'list-type': '2', 'bucketName': 'microsoft-devtest', 'encoding-type': 'url', 'prefix': '', 'delimiter': '/', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com'}	4
{'list-type': '2', 'bucketName': 'microsoft-devtest', 'max-keys': '0', 'encoding-type': 'url', 'x-amz-request-payer': ' requester', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com'}	4
{'bucketName': 'microsoft-devtest', 'Host': 'Microsoft-devtest.s3.amazonaws.com'}	2
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3-eu-west-1.amazonaws.com'}	2
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.amazonaws.com', 'max-keys': '1000', 'prefix': 'a'}	2
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.amazonaws.com', 'max-keys': '1000', 'prefix': 'd'}	2
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com', 'encoding-type': 'url'}	2
{'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com', 'key': 'hello.txt'}	2
{'bucketName': 'microsoft-devtest', 'Host': 's3.eu-west-1.amazonaws.com'}	2
{'list-type': '2', 'bucketName': 'microsoft-devtest', 'Host': 'microsoft-devtest.s3.amazonaws.com'}	2
{'list-type': '2', 'bucketName': 'microsoft-devtest', 'max-keys': '500', 'encoding-type': 'url', 'x-amz-request-payer': 'requester', 'Host': 'microsoft-devtest.s3.eu-west-1.amazonaws.com'}	2

Temporal Trends

Panel Purpose: To track when most requests are made, helping to identify peak times or unusual spikes in activity.