Monitoring AWS S3 for suspicious activities

Applicability

- **Product:** Splunk Cloud Platform or Splunk Enterprise
- **Feature:** [Splunk App for AWS](https://www.splunk.com/app/9805) and [Splunk Add-on for AWS](https://www.splunk.com/extension/3281)
- **Data:** Amazon Web Services: CloudTrail and CloudWatch
- **Function:** Monitoring

Scenario

You are an Amazon Web Services (AWS) admin who manages access to AWS resources and services across your organization. Your organization uses Amazon S3, otherwise known as Amazon Simple Storage Service. You use Amazon's "shared responsibility" S3 model, which states that Amazon has responsibility for the environment outside of the VM but your company is responsible for the security inside of the S3 container. Because of this, it's important for you important to stay vigilant for activities that may indicate suspicious behavior inside of your environment.

These searches allow you to monitor your AWS S3 buckets for evidence of anomalous activity and suspicious behaviors, such as detecting open S3 buckets and buckets being accessed from a new IP.

- Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.
- To run these searches, you must install the AWS App for Splunk (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later), and configure your [CloudTrail inputs](https://www.splunk.com/app/9805). Some searches also require configuration of [S3 access log inputs](https://www.splunk.com/app/3281).

Support searches

**Baseline of S3 bucket deletion activity by ARN**

This search establishes, on a per-hour basis, the average and standard deviation for the number of API calls related to deleting an S3 bucket by each user. The number of data points for each user is also recorded. This table is then outputted to a lookup file to allow the detection search to operate quickly.

```
sourcetype=aws:cloudtrail eventName=DeleteBucket | spath output=arn path=userIdentity.arn | bucket _time span=1h
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
| stats count AS apiCalls BY _time, arn |
| stats count(apiCalls) AS numDataPoints, latest(apiCalls) AS latestCount, avg(apiCalls) AS avgApiCalls, stdev(apiCalls) AS stdevApiCalls BY arn |
| table arn, latestCount, numDataPoints, avgApiCalls, stdevApiCalls |
| outputlookup s3_deletion_baseline |
| stats count |

**Previously seen S3 bucket access by remote IP**

This search looks for successful access to S3 buckets from remote IP addresses, then creates a baseline of the earliest and latest times you have encountered this remote IP within the last 30 days. In this support search, you are only looking for S3 access events where the HTTP response code from AWS is 200, indicating success.

You must validate the remote IP and bucket name entries in *previously_seen_S3_access_from_remote_ip.csv*, which is a lookup file created as a result of running this support search.

```
| sourcetype=aws:s3:accesslogs http_status=200 |
| stats earliest(_time) AS earliest latest(_time) AS latest BY bucket_name remote_ip |
| outputlookup previously_seen_S3_access_from_remote_ip |
| stats count |
```

**Detection searches**

**Detect new open S3 buckets**

This search looks for CloudTrail events where a user has created an open/public S3 bucket. It queries CloudTrail logs for events with S3 bucket access controls given to the "All Users" group, which allows anyone in the world access to the resource. The search then generates a table displaying the time when the bucket was made public, the permission of the S3 bucket, the bucket name, and the ARN of the user who created the bucket.

While this search has no known false positives, it is possible that an AWS admin has legitimately created a public bucket for a specific purpose. AWS strongly advises against granting full control to the "All Users" group.

```
| sourcetype=aws:cloudtrail AllUsers eventName=PutBucketAcl |
| spath output=userIdentityArn path=userIdentity.arn |
| spath output=bucketName path=requestParameters.bucketName |
| spath output=aclControlList path=requestParameters.AccessControlPolicy.AccessControlList |
| spath input=aclControlList output=grantee path=Grant{} |
| mvexpand grantee |
| spath input=grantee |
| search Grantee.URI=*AllUsers |
| rename userIdentityArn AS user |
| table _time, src,awsRegion Permission, Grantee.URI, bucketName, user |
```
► Detect new open S3 buckets over AWS CLI

This search looks for CloudTrail events where a user has created an open/public S3 bucket over the AWS CLI.

While this search has no known false positives, it is possible that an AWS admin has legitimately created a public bucket for a specific purpose. AWS strongly advises against granting full control to the "All Users" group.

```
search (eventSource="s3.amazonaws.com" sourcetype=aws:cloudtrail (eventName=PutBucketAcl OR "requestParameters.accessControlList.x-amz-grant-full-control"="*AllUsers" OR "requestParameters.accessControlList.x-amz-grant-full-control"="*AuthenticatedUsers" OR "requestParameters.accessControlList.x-amz-grant-read-acp"="*AllUsers" OR "requestParameters.accessControlList.x-amz-grant-read-acp"="*AuthenticatedUsers" OR "requestParameters.accessControlList.x-amz-grant-write"="*AllUsers" OR "requestParameters.accessControlList.x-amz-grant-write"="*AuthenticatedUsers" OR "requestParameters.accessControlList.x-amz-grant-read-acp"="*AllUsers" OR "requestParameters.accessControlList.x-amz-grant-read-acp"="*AuthenticatedUsers", OR "requestParameters.accessControlList.x-amz-grant-write"="*AllUsers" OR "requestParameters.accessControlList.x-amz-grant-write"="*AuthenticatedUsers" OR "requestParameters.accessControlList.x-amz-grant-read-acp"="*AllUsers" OR "requestParameters.accessControlList.x-amz-grant-read-acp"="*AuthenticatedUsers") | rename "requestParameters.bucketName" as bucketName | fillnull
```

► Detect S3 access from a new IP

In order to run this search you'll need to configure your S3 access log inputs. This search works best when you run the Previously seen S3 bucket access by remote IP support search once to create a history of previously seen remote IPs and bucket names.

This search looks at S3 bucket-access logs and detects new or previously unseen remote IP addresses that have successfully accessed an S3 bucket.

The subsearch executes first and returns all successful S3 bucket-access attempts (HTTP code 200) within the last hour. It groups the results by the earliest and latest times it has seen a remote IP accessing a particular bucket. It appends this information to the historical data from the lookup file and then recalculates the `firstTime` and `lastTime` field for each remote IP accessing an S3 bucket. Next, it returns only those remote IP addresses that have first been seen accessing a specific bucket within the past hour. This is combined with the main search to return the time, bucket name, source IP, city, and country operations performed, as well as the requested URI of the resource.

S3 buckets can be accessed from any IP, as long as it can make a successful connection. This will be a false positive because the search is looking for a new IP within the past hour.

```
sourcetype=aws:s3:accesslogs http_status=200  
| search sourcetype=aws:s3:accesslogs http_status=200  
| stats earliest(_time) AS firstTime latest(_time) AS lastTime BY bucket_name remote_ip  
| inputlookup append= previously_seen_S3_access_from_remote_ip.csv  
| stats min(firstTime) AS firstTime, max(lastTime) AS lastTime BY bucket_name remote_ip  
| outputlookup previously_seen_S3_access_from_remote_ip.csv  
| eval newIP=if(firstTime >= relative_time(now(), "-1h@h"), 1, 0)  
| where newIP=1
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Detect spike in S3 bucket deletion

This search works best when you run the [Baseline of S3 bucket deletion activity by ARN](#) support search once to create a baseline of previously seen IAM users within the last 30 days.

This search detects users creating spikes in API activity related to deletion of S3 buckets in your AWS environment. It will also update the cache file that factors in the latest data.

You can modify `dataPointThreshold` and `deviationThreshold` to better fit your environment. The `dataPointThreshold` variable is the minimum number of data points required to have a statistically significant amount of data to determine. The `deviationThreshold` variable is the number of standard deviations away from the mean that the value must be to be considered a spike.

[Click here](#) to read a detailed breakdown of how this search works.

```
| sourcetype=aws:cloudtrail eventName=DeleteBucket [search sourcetype=aws:cloudtrail eventName=DeleteBucket
|   | spath output=arn path=userIdentity.arn
|   | stats count AS apiCalls BY arn
|   | inputlookup s3_deletion_baseline append=t
|   | fields - latestCount
|   | stats values(*) AS * BY arn
|   | rename apiCalls AS latestCount
|   | eval newAvgApiCalls=avgApiCalls + (latestCount-avgApiCalls)/720
|   | eval newStdevApiCalls=sqrt(((pow(stdevApiCalls, 2)*719 + (latestCount-newAvgApiCalls)*(latestCount-
|   |   |   | avgApiCalls))/720))
|   | eval avgApiCalls=coalesce(newAvgApiCalls, avgApiCalls), stdevApiCalls=coalesce(newStdevApiCalls,
|   |   |   | stdevApiCalls), numDataPoints=if(isnull(latestCount), numDataPoints, numDataPoints+1)
|   | table arn, latestCount, numDataPoints, avgApiCalls, stdevApiCalls
|   | outputlookup s3_deletion_baseline
|   | eval dataPointThreshold = 15, deviationThreshold = 3
|   | eval isSpike=if((latestCount > avgApiCalls+deviationThreshold*stdevApiCalls) AND numDataPoints >
|   |   |   | dataPointThreshold, 1, 0)
|   | where isSpike=1
|   | rename arn AS userIdentity.arn
|   | table userIdentity.arn]
|   | spath output=user userIdentity.arn
|   | spath output=bucketName path=requestParameters.bucketName
|   | stats _time values(bucketName) AS bucketName, count AS numberOfApiCalls, dc(eventName) AS
|   | uniqueApisCalled BY user
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Investigative searches

► **AWS investigate user activities by ARN**

This search lists all the logged CloudTrail activities by a specific user ARN and will create a table containing the source of the user, the region of the activity, the name and type of the event, the action taken, and all of the user's identity information.

```
| search sourcetype=aws:cloudtrail userIdentity.arn={arn}
| table _time userIdentity.type userIdentity.userName userIdentity.arn aws_account_id src awsRegion eventName eventType
```

► **AWS network ACL details from ID**

This search queries AWS description logs and returns all the information about a specific network ACL via network ACL ID.

```
| search sourcetype=aws:description
| rename id AS networkAclId
| search networkAclId=$networkAclId$
| table id account_id vpc_id network_acl_entries{}.*
```

► **AWS network interface details via resourceId**

This search queries AWS configuration logs and returns the information about a specific network interface via network interface ID. The information will include the ARN of the network interface, its relationships with other AWS resources, the public and the private IP associated with the network interface.

```
| search sourcetype=aws:config resourceId=$resourceId$
| table _time ARN relationships{}.resourceType relationships{}.name relationships{}.resourceId configuration.privateIpAddresses{}.privateIpAddress configuration.privateIpAddresses{}.association.publicIp
```

► **AWS S3 bucket details via bucketname**

This search queries AWS configuration logs and returns the information about a specific S3 bucket. The information returned includes the time the S3 bucket was created, the resource ID, the region it belongs to, the value of action performed, AWS account ID, and configuration values of the access-control lists associated with the bucket.

```
| search sourcetype=aws:config
| rename resourceId AS bucketName
| search bucketName=$bucketName$
| table resourceCreationTime bucketName vendor_region action aws_account_id supplementaryConfiguration.AccessControlList
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Get all AWS activity from IP address

This search retrieves all the activity from a specific IP address and creates a table containing the time, ARN, username, the type of user, the IP address, the AWS region the activity was in, the API called, and whether or not the API call was successful.

```
| search sourcetype=aws:cloudtrail
| iplocation sourceIPAddress
| search sourceIPAddress={src_ip}
| spath output=user path=userIdentity.arn
| spath output=awsUserName path=userIdentity.userName
| spath output=userType path=userIdentity.type
| rename sourceIPAddress AS src_ip
| table _time, user, userName, userType, src_ip, awsRegion, eventName, errorCode
```

Investigate AWS activities via region name

This search lists all the user activities logged by CloudTrail for a specific region in question and creates a table of the values of parameters requested, the type of the event, and the response from the AWS API by each user.

```
| search sourcetype=aws:cloudtrail awsRegion={awsRegion}
| rename requestParameters.instancesSet.items{}.instanceId AS instanceId
| stats values(eventName) BY userName instanceId
```

Additional resources

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help reinforce your Cloud Security posture, including:

- Detecting AWS cross-account activity
- Detect suspicious new instances in your EC2 environment
- Detecting AWS network ACL activity
- Detecting AWS suspicious provisioning activities
- Monitoring user activity spikes in AWS
- Monitoring AWS EC2 for suspicious login activities
- Monitoring AWS for suspicious traffic
- Monitoring AWS EC2 for unusual modifications

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.