Monitoring user activity spikes in AWS

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Monitoring
- Technology: Splunk App for AWS and Splunk Add-on for AWS
- Data: Amazon Web Services: CloudTrail and CloudWatch

Scenario

You are an Amazon Web Services (AWS) admin who manages access to AWS resources and services across your organization. You need to detect and investigate dormant user accounts for your AWS environment that have become active again.

Because inactive and ad-hoc accounts are common attack targets, it's critical to enable governance within your environment. In addition to compromising the security of your data, bad actors leveraging your compute resources can incur monumental costs because you will be billed for any new Elastic Compute Cloud (EC2) instances and increased bandwidth usage.

You can leverage Amazon Web Services (AWS) CloudTrail to give you increased visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

- 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, 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.

Support searches

► Baseline of API calls per user ARN

This search establishes, on a per-hour basis, the average and the standard deviation of the number of API calls made 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.
Baseline of security group activity by ARN

This search establishes, on a per-hour basis, the average and the standard deviation for the number of API calls related to security groups made by each user. It also records the number of data points for each user. This table is then outputted to a lookup file to allow the detection search to operate quickly.

Previously seen API call per user roles in CloudTrail

This search looks for successful API calls made by different user roles, then creates a baseline of the earliest and latest times you have encountered this user role. It also returns the name of the API call in your dataset that occurred within the last 30 days, grouped by user role and name of the API call. In this search, you are only looking for events where the user identity is Assumed Role.

You will need to validate the user role entries in `previously_seen_api_calls_from_user_roles.csv`, which is the lookup file created as a result of running this support search.
Detection Searches

► AWS excessive security scanning

This search looks for CloudTrail events and analyse the amount of eventNames which starts with Describe by a single user. This indicates that this user scans the configuration of your AWS cloud environment.

| search (sourcetype=aws:cloudtrail (eventName=Describe* OR eventName=Get* OR eventName=List*)) | stats dc(eventName) AS dc_events min(_time) AS firstTime max(_time) AS lastTime values(eventName) AS eventName values(src) AS src values(userAgent) AS userAgent BY user userIdentity.arn | where (dc_events > 50) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |

► Detect API activity from users without MFA

This search looks for CloudTrail events where a user logged into the AWS account, is making API calls and has not enabled Multi Factor authentication. Multi factor authentication adds a layer of security by forcing the users to type a unique authentication code from an approved authentication device when they access AWS websites or services. AWS Best Practices recommend that you enable MFA for privileged IAM users.

| search (sourcetype=aws:cloudtrail (eventName=Describe* OR eventName=Get* OR eventName=List*)) | stats dc(eventName) AS dc_events min(_time) AS firstTime max(_time) AS lastTime values(eventName) AS eventName values(src) AS src values(userAgent) AS userAgent BY user userIdentity.arn | where (dc_events > 50) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime) |

► Detect new API calls from user roles

This search works best when you run the Previously seen API call per user roles in CloudTrail support search once to create a history of previously seen user roles.

This search detects new API calls that have either never been seen before or that have not been seen in the previous hour, where the identity type is AssumedRole.

The subsearch executes first and returns the user roles and names of the API calls completed within the last hour, where the type of user identity is AssumedRole. It then adds the historical data to those results in the lookup file. Next, it recalculates the earliest and latest fields for each user role, as well as the name of the API call, and returns only those roles and API calls that have first been seen in the past hour. This is combined with the main search to return the values of API calls, name of the user role, and the earliest and latest time of this activity. The name of the role of a particular user is parsed as userName in the CloudTrail logs.

False positives can occur from this search since there may be legitimate user roles making new or infrequently used API calls in your infrastructure.
Detect spike in AWS API activity

This search detects users who create spikes of API activity in your AWS environment. It also updates 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.
Detect spike in security group activity

This search works best when you run the **Baseline of security group activity by ARN** support search once to create a history of previously seen Security Group Activity.

This search detects users who create spikes in API activity related to security groups in your AWS environment. It also updates 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.

```splunk
search sourcetype=aws:cloudtrail (eventName=AuthorizeSecurityGroupIngress OR eventName=CreateSecurityGroup OR eventName=DeleteSecurityGroup OR eventName=DescribeClusterSecurityGroups OR eventName=DescribeDBSecurityGroups OR eventName=DescribeSecurityGroupReferences OR eventName=DescribeSecurityGroups OR eventName=DescribeStaleSecurityGroups OR eventName=RevokeSecurityGroupIngress OR eventName=UpdateSecurityGroupRuleDescriptionsIngress) [search sourcetype=aws:cloudtrail (eventName=AuthorizeSecurityGroupIngress OR eventName=CreateSecurityGroup OR eventName=DeleteSecurityGroup OR eventName=DescribeClusterSecurityGroups OR eventName=DescribeDBSecurityGroups OR eventName=DescribeSecurityGroupReferences OR eventName=DescribeSecurityGroups OR eventName=DescribeStaleSecurityGroups OR eventName=RevokeSecurityGroupIngress OR eventName=UpdateSecurityGroupRuleDescriptionsIngress)] | spath output=arn path=userIdentity.arn | stats count AS apiCalls BY arn | inputlookup security_group_activity_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 security_group_activity_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
```

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

► Investigate AWS user activities by user field

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

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

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 AWS EC2 for suspicious login activities
- Monitoring AWS S3 for suspicious 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.