Detecting AWS suspicious provisioning activities

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Feature: Splunk App for AWS and Splunk Add-on for AWS
- 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. You need to monitor your AWS provisioning activities for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your network.

Because most enterprise AWS activities originate from familiar geographic locations, activity from unknown or unusual regions is an important security measure. This indicator can be especially useful in environments where it is impossible to create allow lists for specific IP addresses because they vary.

These searches are designed to give you flexibility in specifying legitimate geographic regions. You can be as specific as an IP address or a city, or as broad as a region or state or an entire country.

These searches allow you to detect adversaries as they begin to probe your environment. Be aware that there are legitimate reasons for activities from unfamiliar locations, so these searches are not a standalone indicator. However, these searches can still provide you with location information that you may wish to investigate further.

- 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

- Previously seen AWS provisioning activity sources

  This search creates a table of the first and last times seen for every IP address and its physical location associated with cloud-provisioning activity. Provisioning activities are defined as any event that begins with Run or Create.
Detection searches

These searches look for AWS provisioning activities from previously unseen cities, countries, IP addresses or regions. Provisioning activities are defined as any event that begins with Run or Create.

In all of these searches, the subsearch returns all events with event names that start with Run or Create, and then does a GeoIP lookup on the IP address that initiated the action within the last hour. It adds the historical data to those results in the lookup file. Next, it recalculates the `firstTime` and `lastTime` field for each country, region, city, and IP address and outputs this data to the lookup file to update the local cache. It then calculates the `firstTime` and `lastTime` for each city. It returns only those events from cities/countries/IP addresses/regions that have first been seen in the past hour. This is combined with the main search to return the time, user, IP address, city/country/region, event name, and error code from the action.

The searches will return the first occurrence in the time period you're searching within, plus what is stored in the cache feature. While there are no false positives in a traditional sense, there will likely be a lot of noise.

If you typically do all provisioning from tools inside of your city, there should be few false positives. If you are located in a country where the free version of MaxMind GeoIP that ships by default with Splunk software has weak resolution, this search may be much less valuable to you.

► AWS cloud provisioning from previously unseen city

This search works best when you run the Previously seen AWS provisioning activity sources support search to create a history of previously seen locations that have provisioned AWS resources.

This search looks for AWS provisioning activities from previously unseen cities.

```bash
sourcetype=aws:cloudtrail (eventName=Run* OR eventName=Create*) | iplocation sourceIPAddress | stats earliest(_time) AS firstTime, latest(_time) AS lastTime BY sourceIPAddress, City, Region, Country | outputlookup previously_seen_provisioning_activity_src.csv | stats count
```

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.
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.
AWS cloud provisioning from previously unseen region

This search works best when you run the [Previously seen AWS provisioning activity sources](#) support search to create a history of previously seen locations that have provisioned AWS resources.

This search looks for AWS provisioning activities from previously unseen regions. Region in this context is similar to a state in the United States.

```
sourcetype=aws:cloudtrail (eventName=Run* OR eventName=Create*)
| iplocation sourceIPAddress
| search Region=* [search sourcetype=aws:cloudtrail (eventName=Run* OR eventName=Create*)
| iplocation sourceIPAddress
| search Region=*
| stats earliest(_time) AS firstTime, latest(_time) AS lastTime BY sourceIPAddress, City, Region, Country 
| inputlookup append=t previously_seen_provisioning_activity_src.csv
| stats min(firstTime) AS firstTime max(lastTime) AS lastTime BY sourceIPAddress, City, Region, Country 
| outputlookup previously_seen_provisioning_activity_src.csv
| stats min(firstTime) AS firstTime max(lastTime) AS lastTime BY Region
| eval newRegion=if(firstTime >= relative_time(now(), "-1h@h"), 1, 0)
| where newRegion=1
| table Region
| spath output=user userIdentity.arn
| rename sourceIPAddress AS src_ip
| table _time, user, src_ip, Region, eventName, errorCode
```

Investigative searches

Investigate Security Hub alerts by dest

This search retrieves the all the alerts created by AWS Security Hub for a specific dest(instance_id).

```
sourcetype="aws:securityhub:firehose" "findings{}.Resources{}.Type"=AWSEC2Instance
| rex field=findings{}.Resources{}.Id ."instance/(?<instance>.*)."
| rename instance AS dest
| search dest = $dest$
| rename findings{}. AS *
| rename Remediation.Recommendation.Text AS Remediation
| table dest Title ProductArn Description FirstObservedAt RecordState Remediation
```

Investigate user activities by ARN

This search lists all the logged CloudTrail activities by a specific user Amazon Resource Name (ARN) 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 all 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
```

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 city

This search returns all activity from a specific city and creates a table containing the time, city, ARN, username, the type of user, the source 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 City={City}
| 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, City, user, userName, userType, src_ip, awsRegion, eventName, errorCode
```

- Get all AWS activity from country

This search returns all activity from a specific country and creates a table containing the time, country, ARN, username, the type of user, the source 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 Country={Country}
| 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, Country, user, userName, userType, src_ip, awsRegion, eventName, errorCode
```

- Get all AWS activity from IP address

This search returns all 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
```

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 region

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

```plaintext
| search sourcetype=aws:cloudtrail
| iplocation sourceIPAddress
| search Region={Region}
| 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, Region, user, userName, userType, src_ip, awsRegion, eventName, errorCode
```

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
- Monitoring user activity spikes in AWS
- 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.