Detecting suspicious activities within cloud instances

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 need to monitor your cloud instances for behaviors originating from unfamiliar or unusual locations. These behaviors may indicate that malicious activities are occurring somewhere within your cloud environment.

Monitoring your cloud infrastructure logs allows you to enable governance, compliance, and risk auditing. It is crucial for a company to monitor events and actions taken in their cloud environments to ensure that your instances are not vulnerable to attacks.

These searches help you identify, respond to, and investigate suspicious activities in your cloud compute instances.

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.

Support searches

- Previously seen cloud instance modifications by user - initial
  - To run this search, your deployment must be ingesting cloud infrastructure logs.
  - Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Change data model. For information on installing and using the CIM, see the Common Information Model documentation.

This search builds a table of previously seen users that have modified a cloud instance.

```
| tstats earliest(_time) AS firstTimeSeen, latest(_time) AS lastTimeSeen FROM datamodel=Change WHERE All_Changes.action=modified All_Changes.change_type=EC2 All_Changes.status=succ AS user
| rename "All_Changes.*" AS "***"
| eventstats min(firstTimeSeen) AS globalFirstTime
```

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.
Previously seen cloud instance modifications by user - update

To run this search, you must install the Splunk App for AWS (version 5.1.0 or later) and Splunk Add-on for AWS version (4.4.0 or later), then configure your CloudTrail inputs.

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Change data model. For information on installing and using the CIM, see the Common Information Model documentation.

This search updates a table of previously seen cloud instance modifications that have been made by a user.

Detection searches

Cloud instance modified by previously unseen user

This search relies on the output lookup table created and updated through the Support searches Previously seen cloud instance modifications by user - initial and Previously Seen Cloud Instance Modifications By User - Update.

To run this search, 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), then configure your CloudTrail inputs.

Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Change data model. For information on installing and using the CIM, see the Common Information Model documentation.

This search looks for cloud instances being modified by users who have not previously modified them.

False positives from this search may occur since it's possible that a new user will start to modify Elastic Compute Cloud (EC2) instances when they haven't before for any number of reasons. Verify with the user that is modifying instances that this is the intended behavior.
Changes.status"=success) BY "All_Changes.user"
| rename "All_Changes.*" AS "*"
| lookup previously_seen_cloud_instance_modifications_by_user user AS user OUTPUTNEW
firstTimeSeen, enough_data
| eventstats max(enough_data) AS enough_data
| where (enough_data == 1)
| eval firstTimeSeenUser=min(firstTimeSeen)
| where ((firstTimeSeenUser > relative_time(now(),"-24h@h")) OR isnull(firstTimeSeenUser))
| table firstTime, user, command, object_id, count
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)

---

**Investigative searches**

► **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.

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

► **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.

```splunk
| 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
```

---

**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:

---

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.
- Detecting AWS cross-account activity
- 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 S3 for suspicious activities
- Monitoring AWS for suspicious traffic
- Monitoring AWS EC2 for unusual modifications