Monitoring AWS Elastic Compute Cloud (EC2) for unusual modifications

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. As part of your role, you need to identify unusual changes to your AWS Elastic Compute Cloud (EC2) instances that may indicate malicious activity, for example, by looking for modifications to your EC2 instances by previously unseen users. Adversaries commonly aim to infiltrate a cloud instance and make modifications, then secure access to your infrastructure and hide their activities. It's important for you to look for changes that may indicate that your environment has been compromised.

These searches can help you detect the presence of a threat by monitoring for EC2 instances that have been created or changed - either by users who have never previously performed these activities or by known users who modify or create instances in a way that has not been done before.

- 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. Some searches also require configuration of description inputs.

Support searches

- Previously seen EC2 modifications by user

This search builds a table of previously seen Amazon Resource Names (ARNs) that have launched a EC2 instance.

```
| search (errorCode=success sourcetype=aws:cloudtrail (eventName=AssociateAddress OR eventName=AssociateIamInstanceProfile OR eventName=AttachClassicLinkVpc OR
```
Detection searches

EC2 instance modified with previously unseen user

This search works best when you run the previously seen EC2 modifications by user support search once to create a history of previously seen ARNs.

This search looks for EC2 instances being modified by users who have not previously modified them.

The subsearch returns the ARNs of all successful EC2 instance modifications within the last hour and then appends the historical data in the lookup file to those results. The search then recalculates the firstTime and lastTime field for each ARN and returns only those ARNs that have first been seen in the past hour. This is combined with the main search to return the time, user, and instance ID of those systems.

False positives can occur from this search since it's possible that a new user will start to modify 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.
Contextual searches

► Get EC2 instance details by instanceId

In order to implement this search, you must configure your AWS description inputs.

This search queries AWS description logs and returns all the information about a specific instance via the instanceId field.

```
| search sourcetype="aws:description" source="*:ec2_instances"
| dedup id sortby -_time
| spath output=tags path=tags
| eval tags=mvzip(key,value," = "), ip_address=if((ip_address == "null"),private_ip_address,ip_address)
| table id, tags.Name, aws_account_id, placement, instance_type, key_name, ip_address, launch_time, state, vpc_id, subnet_id, tags
| rename aws_account_id AS "Account ID", id AS ID, instance_type AS Type, ip_address AS "IP Address", key_name AS "Key Pair", launch_time AS "Launch Time", placement AS "Availability Zone", state AS State, subnet_id AS Subnet, "tags.Name" AS Name, vpc_id AS VPC
```

Investigative searches

► AWS investigate user activities by ARN

This search lists all the logged CloudTrail activities by a specific user ARN and creates a table that contains 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 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 which are reproduced here, 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 S3 for suspicious activities
- Monitoring AWS for suspicious traffic

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.