Detecting AWS security hub alerts

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 AWS resources and services across your organization. As part of your role, you need to be able to detect Security Hub alerts generated from AWS.

AWS Security Hub collects and consolidates findings from AWS security services enabled in your environment, such as:

• intrusion detection findings from Amazon GuardDuty
• vulnerability scans from Amazon Inspector
• S3 bucket policy findings from Amazon Macie
• publicly accessible and cross-account resources from IAM Access Analyzer
• resources that lack WAF coverage from AWS Firewall Manager

These searches are designed to uncover these alerts.

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.

Detection searches

► Detect spike in AWS security hub alerts for Elastic Compute Cloud (EC2) instance

To run this search, 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 Security Hub inputs.

This search looks for a spike in number of of AWS security hub alerts for an EC2 instance in 4-hour intervals.

The threshold_value should be tuned to your environment, and you should schedule these searches according to the bucket span interval.
Detect spike in AWS security hub alerts for user

To run this search, 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 Security Hub inputs.

This search looks for a spike in number of AWS security hub alerts for an AWS IAM User in 4-hour intervals.

The threshold_value should be tuned to your environment and you should schedule these searches according to the bucket span interval.

Investigative searches

Investigate user activities by ARN

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

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.
▶ Get EC2 instance details

To run this search, install the Splunk App for AWS (version 5.1.0 or later) and Splunk Add-on for AWS (version 4.4.0 or later), and 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:cloudtrail responseElements.instancesSet.items{}.instanceId={dest} | rename userIdentity.arn AS arn, responseElements.instancesSet.items{}.instanceId AS instanceId, responseElements.instancesSet.items{}.privatelpAddress AS privatelpAddress, responseElements.instancesSet.items{}.imageId AS amiID, responseElements.instancesSet.items{}.architecture AS architecture, responseElements.instancesSet.items{}.keyName AS keyName |
| table arn, awsRegion, instanceId, architecture, privatelpAddress, amiID, keyName |

▶ Get EC2 launch details

To run this search, 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 AWS description inputs.

This search returns key launch details for a EC2 instance.

| search sourcetype=aws:cloudtrail responseElements.instancesSet.items{}.instanceId={dest} | rename userIdentity.arn AS arn, responseElements.instancesSet.items{}.instanceId AS instanceId, responseElements.instancesSet.items{}.privatelpAddress AS privatelpAddress, responseElements.instancesSet.items{}.imageId AS amiID, responseElements.instancesSet.items{}.architecture AS architecture, responseElements.instancesSet.items{}.keyName AS keyName |
| table arn, awsRegion, instanceId, architecture, privatelpAddress, amiID, keyName |

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
- 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