FIREEYE™ HELIX CONNECT

AWS CloudTrail

Amazon, Inc.

Installation

1 - Locate CloudTrail bucket location

- This integration will forward AWS CloudTrail logs from the desginated bucket into FireEye Helix for audit and detection capabilities. To get started:
- 1. Ensure that the correct Helix instance is selected in the drop-down.
- Log into your AWS account (https://console.aws.amazon.com).
- Go to the CloudTrail console, click on "Trails" and locate the "S3 bucket" entry and "Log file prefix" for the CloudTrail you want to send into Helix.
- Note the AWS region this bucket is in and the bucket name, and record it below.
- Click **Submit and Verify**, which will generate a Cloudformation template for you.
- **IMPORTANT!!!** If there is an existing notification configuration on the bucket, the template will fail unless you set OverwriteExistingConfig to 1. This will remove the existing configuration, so ensure that is acceptable first.

Inputs

- AWS region name *AWS region name containing the CloudTrail bucket, e.g. us-west-2*
- AWS bucket to monitor *AWS bucket name containing the CloudTrail bucket, e.g. mybucket-cloudtrail*
- (Optional) Override prefix for files *Prefix, ending with a slash, in which files extracted from network are stored in the bucket, defaults to "files/"*
- (Optional) KMS key *ARN of any KMS key used to encrypt the objects.*
- (Optional) Existing SNS topic *ARN of an existing SNS topic to use instead of creating one (default)*
- (Optional) Override existing bucket notification configuration *Set to "1" to overwrite any existing notification configuration on the source bucket*

2 - Verify Integration