AWS Security Hub Integrations

Introduction

The AWS Security Hub integration collects and parses data from AWS Security Hub REST APIs.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Compatibility

- This module is tested against AWS Security Hub API version 1.0.

Requirements

To collect data from AWS Security Hub APIs, users must have an Access Key and a Secret Key. To create API token follow below steps:

1. Login to https://console.aws.amazon.com/.
2. Go to https://console.aws.amazon.com/iam/ to access the IAM console.
3. On the navigation menu, choose Users.
4. Choose your IAM user name.
5. Select Create access key from the Security Credentials tab.
6. To see the new access key, choose Show.

Note:

1. For the current integration package, it is recommended to have interval in hours.

2. For the current integration package, it is compulsory to add Secret Access Key and Access Key ID.

Logs:

1. Findings - This is the securityhub_findings data stream.

2. Insights - This is the securityhub_insights data stream.

AWS Security Hub Integration Procedures

Please provide the following information to CyTech:

Collect AWS Security Hub logs via API

1. AWS Region - AWS Region.

Collect AWS Security Hub Insights from AWS

1. AWS Region - AWS Region.

Revision #2
Created 23 April 2024 10:44:47
Updated 19 June 2024 06:54:01