Mandiant

AWS GUARDDUTY

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This requires the Cloud Validation license.

The Amazon GuardDuty integration provides events similar to a firewall or endpoint AV tool.

This integration is currently limited since it's behavior based. This means once it identifies a threat & you tell it that it's ok, it will no longer fire on that threat.

Update AWS

You must have an AWS account.

- Create the API credentials and note the Access Key and Secret Access Key.

Update the Validation Platform

Prerequisites

Information to gather before you start:

- Add the AWS account to your Allow list
- Know your Amazon region.
  The following regions are supported:
  - ap-northeast-1
  - ap-northeast-2
  - ap-northeast-3
  - ap-southeast-1
  - ap-southeast-2
  - ap-south1
  - ca-central-1
  - eu-central-1
  - eu-west-1
  - eu-west-2
  - eu-west-3
  - sa-east-1
  - us-east-1
  - us-east-2
  - us-west-1
  - us-west-2
  - us-gov-east-1
  - us-gov-west-1

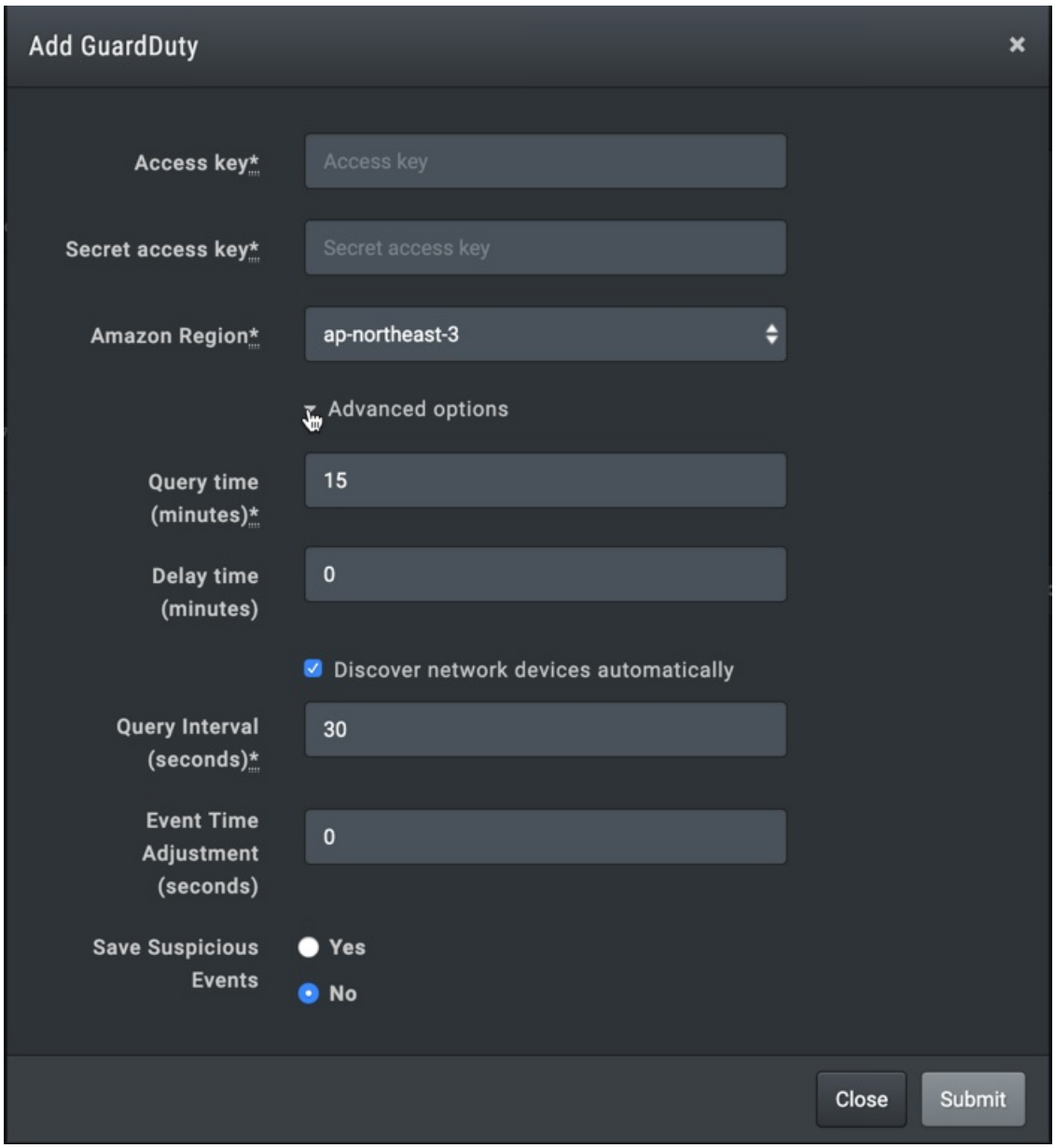
See the **AWS documentation** **(https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)** for information on the different regions and their full names.

- Have the Access key and the Secret access key

Configuration

TO ADD THE AWS CLOUDTRAIL INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **GuardDuty**.



Add AWS GuardDuty

3. Enter the **Access key Id** and the **Secret access key**.
4. Select the **Amazon Region**.
5. Expand **Advanced options**.
6. Update the **Query time** and the **Delay time** information.
7. (Optional) Select **Discover network devices automatically**.
8. Specify the **Query interval**.
9. (Optional) Set the **Event Time Adjustment**.
10. Assing a **Name**.
11. (Optional) Choose whether to save suspicious events.
12. Click **Submit**.

Verify connectivity

TO VERIFY CONNECTIVITY TO AWS GUARDDUTY

- Click **Test** to verify that the keys and region information is correct.