Mandiant

AWS GUARDDUTY INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by AWS GuardDuty to test the efficacy and configuration of the security control using Security Validation jobs. The AWS GuardDuty integration provides events similar to a firewall or endpoint AV tool.

This requires the Cloud Validation license.

Use this document to configure the integration using one of the following methods:

- MSI (Supported and recommended for new integration configurations)
- Legacy (Supported for existing integration configurations)

Configure MSI Integration

This method is the recommended approach for configuring new integrations in Security Validation.

To configure an integration, this document walks you through the following high-level steps:

1. Configure the third-party technology
2. Configure Security Validation
3. Verify connectivity

Configure AWS GuardDuty

API Calls

The integration uses the AWS Python client

Supported Versions

AWS Python client (boto3 version 1.16.63)

Information to gather before you start:

- Add the AWS account to your Allow list.
- Know he AWS region of your GuardDuty service
- 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.

- An AWS Access Key ID and Secret Access Key

Create an Access Key for another IAM user

1. Log in to the AWS Management Console and open the IAM console at **https://console.aws.amazon.com/iam/**.
2. In the navigation pane, click **Users**.
3. Select the name of the user whose access keys you want to manage, and then click the **Security credentials** tab.
4. In the Access keys section:
   a. Click **Create access key**.
   b. Click **Download .csv file** to save the access key ID and secret access key to your computer. You will use these values in the integration configuration.
   c. Store the file in a secure location. **Note:** you will not have access to the secret access key again after closing this dialog box.
   d. Click **Close.**
5. Ensure that the IAM user associated with this key has sufficient permission to read GuardDuty events.

Configure Security Validation

1. Go to **Settings > Integrations**.
2. From the Integrations table, click **Add Integration > AWS GuardDuty**.

   > You can add this as either a Direct or Remote Integration.

3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule (https://docs.mandiant.com/home/msv-proxy-rules)**.
5. From the **AwsRegions** dropdown, choose the AWS DataCenter Region for your AWS deployment.
6. Enter the **Access Key Id** and **Secret Access Key**.
7. Optional: Enter the **AWS Session Token**.
8. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
9. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
10. Optional: Change the values for **Page Size** (default **100**) or **Max Page** (default **5**), if needed.
11. Optional: Enter **Event Sensor Uuids** and **Alarm Sensor Uuids** if you want to filter events and alarms to specific sensors.
12. Optional: Modify the **Field Map** values, as necessary.

- Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
- When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

13. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

    The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

    If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

    b. Update **Query Interval** (seconds).
    c. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    d. Modify the **Correlation Query Interval**, if necessary (minutes).
    e. Select **Discover network devices automatically**, the default and recommended option.

    If unselected, reported events won't include product information for any matching network security technology.

    f. Select **Save Suspicious Events**.
    g. Modify the **Event Time Adjustment** (seconds). The default is **0**.
    h. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

14. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
   - The Director can communicate with the integration host on the port and protocol specified.
   - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-

integrations).

Configure Legacy Integration

> 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

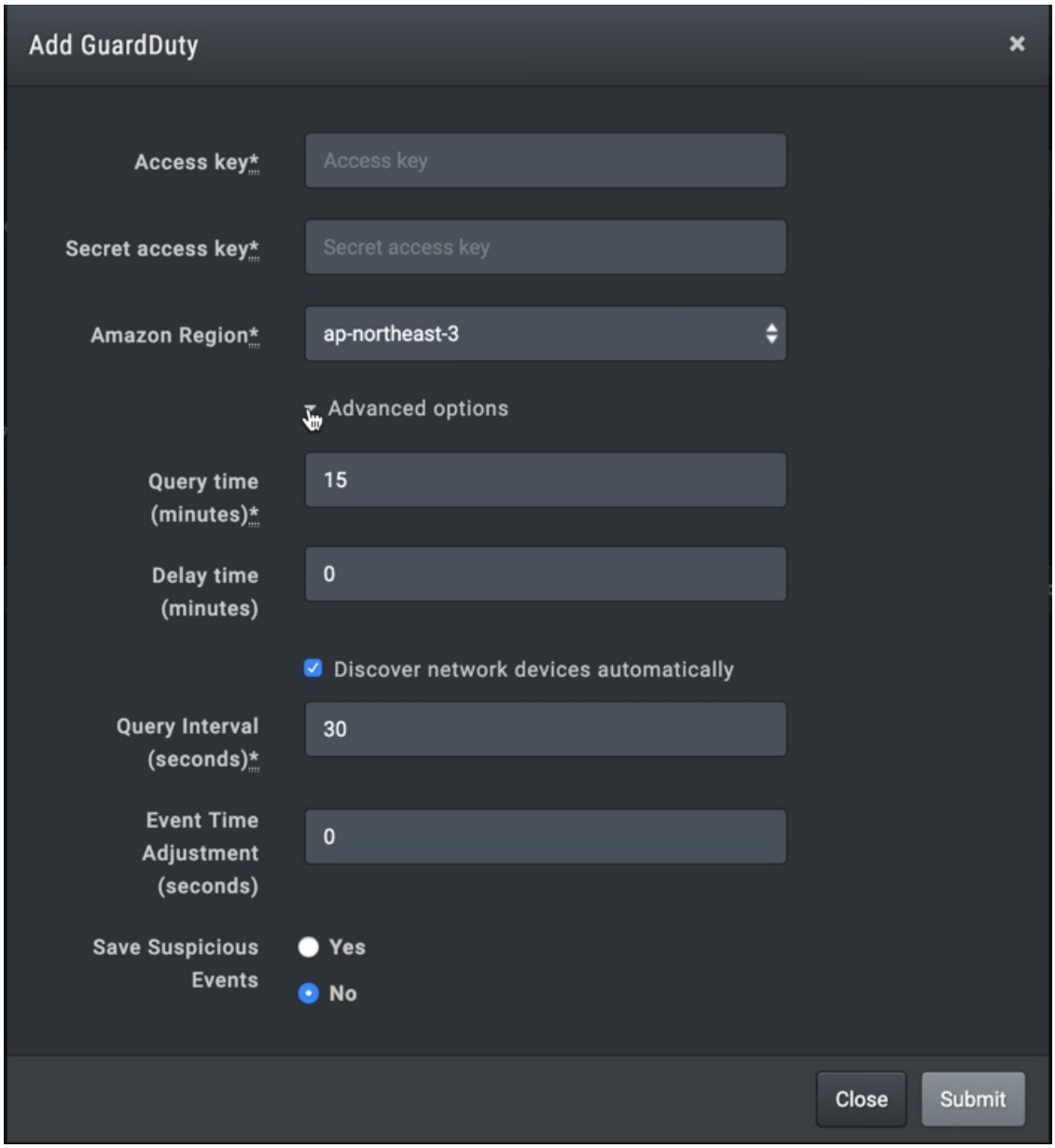
See the **AWS documentation (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)** for information on the different regions and their full names.

- 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.