

Getting Started with Trellix and Amazon Security Lake

Table of Contents

/ 03	Introduction
03	Amazon Security Lake
03	How the integration works using Trellix XDR
/ 03	Trellix Helix Integration with Amazon Security Lake
03	How to enable Trellix Helix Integration with Amazon Security Lake in Minutes
04	Troubleshooting
/ 04	How to use Trellix as a Source
/ 08	OCSF Maintenance
/ 08	Basic Troubleshooting
/ 08	Trellix Customer Support Process
/ 08	Trellix Product Documentation

Introduction

Amazon Security Lake

Amazon Security Lake is a data lake for security logs, built in the customer's account. It's backed by an Amazon S3 bucket and organizes data as a set of Lake Formation tables. Amazon Security Lake is designed to optimize the cost of storing and querying massive security log sources, while maintaining good query performance and compatibility with a wide variety of analytic infrastructure. Amazon Security Lake customers retain low-level ownership of their data. Amazon Security Lake also delivers a set of core AWS-native security logs, minimizing costs and maximizing performance.

How the integration works using Trellix XDR

As an open platform that seamlessly integrates across hundreds of solutions, the Trellix integration with Amazon Security Lake allows customers to easily connect data across their organization and share insights across differing vendor products more cost effectively.

Customers can augment their Amazon Security Lake with the 1000+ sources of security events in Trellix XDR, getting complete detection and response capabilities for their AWS environments by correlating the risks and providing customers with the necessary playbooks to respond to a risk in a timely manner.

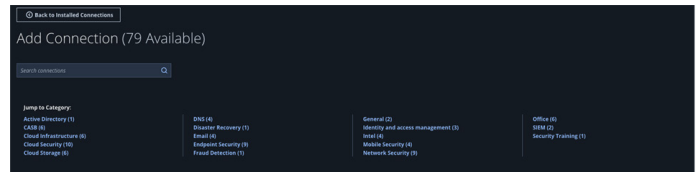
Trellix Helix Integration with Amazon Security Lake

How to Enable Trellix Helix Integration with Amazon Security Lake in Minutes

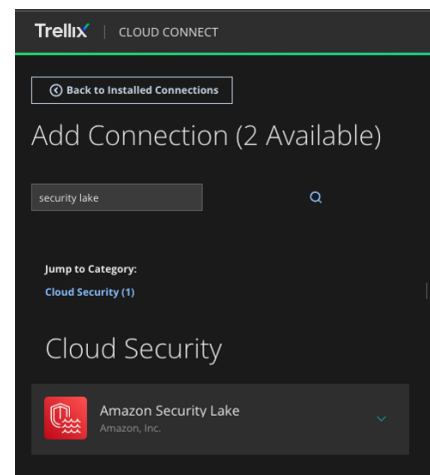
Navigate to the Trellix Helix Cloud Connect portal:

1. Select **Configure > Cloud Connect** to open the Cloud Connect page.
2. Click **Add Connection**.

3. Locate the connection under Cloud Security



- **As a subscriber:** Select **Amazon Security Lake Tile** under **Cloud Security**



This Trellix integration will forward any files found in a given (Amazon Security Lake) S3 bucket to Trellix Helix. You can restrict which files are sent by setting the optional prefix filter below. To install:

1. Ensure that the correct Helix instance is selected in the drop-down.
2. Log into your AWS account (<https://console.aws.amazon.com>) in a different browser tab.
3. In the region you want to subscribe to Trellix XDR, go to the AWS SNS Console and create a topic named "trellix-xdr". The topic can be standard (not FIFO).
4. Click the "Create topic" button and copy the ARN of this topic and paste it in the form below in Cloud Connect under the "SNS topic" field.
5. In Trellix Helix Cloud Connect portal, enter "Amazon Security Lake" in the search bar and choose the entry under the "Cloud Security" category.

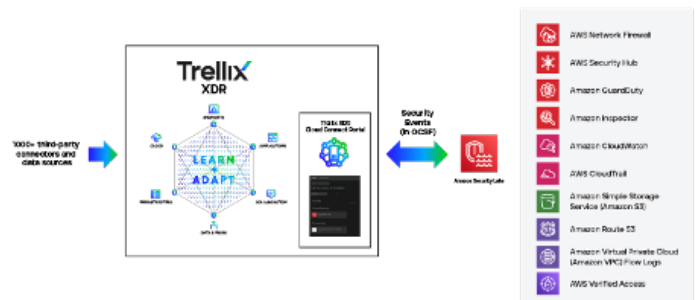
6. In the other browser tab, go to the Amazon Security Lake console and click the "Regions" menu item.
7. For each region listed, you will need to create this Trellix integration in Cloud Connect. You may choose to create a rollup region and use just that region.
8. In the Amazon Security Lake console for this region, find the corresponding bucket name and enter it in the "AWS bucket to monitor" field in Cloud Connect, along with the region in the "AWS region name" field.
9. In the Amazon Security Lake console, click on "Subscribers," then click the "Create subscriber" button.
10. Enter "Trellix" as the Subscriber name.
11. Enter "Trellix XDR" as the description.
12. Choose all or specific log sources.
13. Choose "S3" as the data access method.
14. Under "Subscriber credentials" enter 264756907367 as the Account ID. Enter the unique external ID generated in the instructions in the form below for the external ID in the Amazon Security Lake Console.
15. Under "Notification details" choose "Subscription endpoint" and enter the SNS topic ARN you created earlier as the Subscription endpoint.
16. Click "Create" in the Amazon Security Lake Console.
17. In the Amazon Security Lake console list of subscribers, click on the newly-created subscriber. Copy the AWS role ID and paste it in the Cloud Connect field for "S3 Access Role."
18. Click "Submit" in Cloud Connect below, and the integration setup will generate a CloudFormation template. The CloudFormation template adds necessary permissions for Trellix to subscribe to the SNS topic and for AWS EventBridge to publish to the SNS topic. Run that template in the same AWS account and region, and the setup will be complete.

Troubleshooting

Ensure the CloudFormation template executes successfully. It is valid for 24 hours after being created.

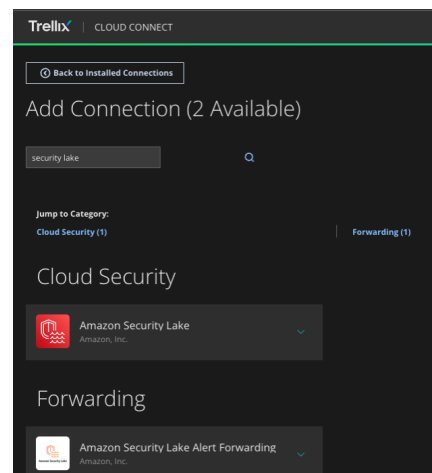
You can use the Helix Cloud Connect console to view integration status, including latest event times.

How to use Trellix as a Source



As a Source (to send security events from Trellix XDR into Amazon Security Lake): Select Amazon Security Lake Alert Forwarding

1. Select **Configure > Cloud Connect** to open the Cloud Connect page.
2. Click **Add Connection**.
3. Locate the connection under **Cloud Security**
4. Click on the **Amazon Security Lake Alert Forwarding** Tile



USER GUIDE

You will see Helix authentication configuration screen.

The screenshot shows the 'Your Integration Instructions' page for Trellix Cloud Connect. The progress bar indicates Step 1 of 3: 'Create Helix API Key'. The page title is 'Step 1: Create Helix API Key'. A button 'Select a Helix Instance' is visible, with a dropdown arrow and a red error message 'Please select one Helix instance'. The main content area explains that the plugin will call the Helix search API and pull alert data to send to Amazon Security Lake. It instructs the user to create a Helix API key in the IAM console with specific entitlements: `tap:search:regex`, `tap:search:browse`, and `Helix APIKEY`. Below this, an 'Input Required' form is shown with fields for 'API Key', 'Optional: EU or AP Instance of Helix', and 'Optional: Custom Helix query'. A warning note states: 'Query is executed in Helix. Defaults to cluster alerts. Warning: Queries returning high numbers (> 100k per minute) of events are not supported.'

5. Configure Amazon Security Bucket Lake S3 bucket location

The screenshot shows the 'Your Integration Instructions' page for Trellix Cloud Connect, Step 2 of 3: 'Choose Bucket'. The progress bar indicates Step 2 of 3. The page title is 'Step 2: Choose Bucket'. A dropdown menu shows 'Helix Instance: hexzsq89'. The main content area lists 8 steps for configuring the Amazon Security Lake bucket location. Below the instructions, an 'Input Required' form is shown with fields for: 'AWS region name', 'AWS region name containing the bucket, e.g. us-west-2', 'Amazon Security Lake bucket', 'AWS Bucket name, e.g. mybucket', 'AWS account ID of the account owning the Amazon Security Lake bucket', 'AWS account ID', 'ARN of the AWS IAM role created by Security Lake for the bucket region', 'Prefix in Security Lake. Defaults to ext/Trellix', and 'Prefix in the bucket'.

USER GUIDE

- Go to Amazon Security Lake console and Create custom source
- Add Trellix info and set event class to SECURITY_FINDING

Amazon Security Lake ×

Amazon Security Lake > Custom sources > Create custom source

Create custom data source

To create a custom data source, first tell Amazon Security Lake which role can write data to your data lake and which role Amazon Security Lake can use to invoke AWS Glue on your behalf.

Custom source details

Data source name
This must be globally unique.

Event class

Region
You can only create a custom data source in your current Region.

AWS account with permission to write data
Provide an account that is authorized to write data to your data lake.

Account Id

- Create and use a new service role

Service Access

Security Lake requires permission to invoke AWS Glue on your behalf. [Learn more](#)

- ☒ Create and use a new service role
- ☐ Use an existing service role

Service Role Name

AmazonSecurityLakeCustomDataGlueCrawler-Trellix

- Find AWS IAM role created by the Amazon Security Lake console

Identity and Access Management (IAM) ×

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

▼ Access reports

IAM > Roles > AmazonSecurityLake-Provider-Trellix-us-east-1

AmazonSecurityLake-Provider-Trellix-us-east-1

Trusts a Security Lake Log Provider to access the Security Lake.

Summary

Creation date
March 23, 2023, 16:23 (UTC-05:00)

Last activity
None

ARN Copied

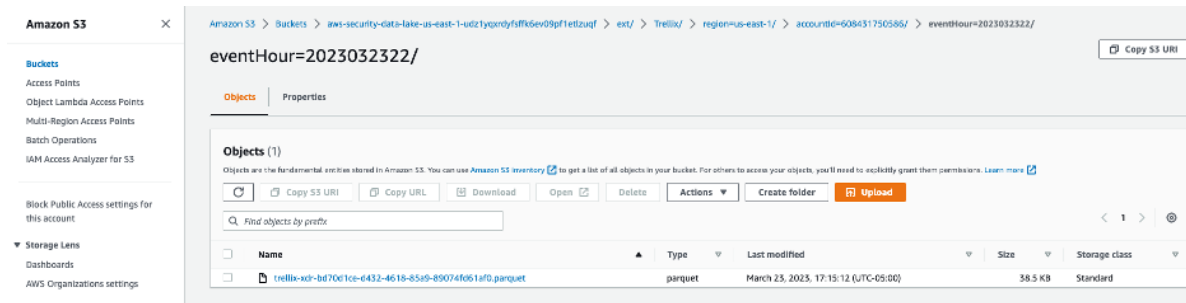
am:aws:iam::608431750586:role/AmazonSecurityLake-Provider-Trellix-us-east-1

Maximum session duration
1 hour

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

USER GUIDE

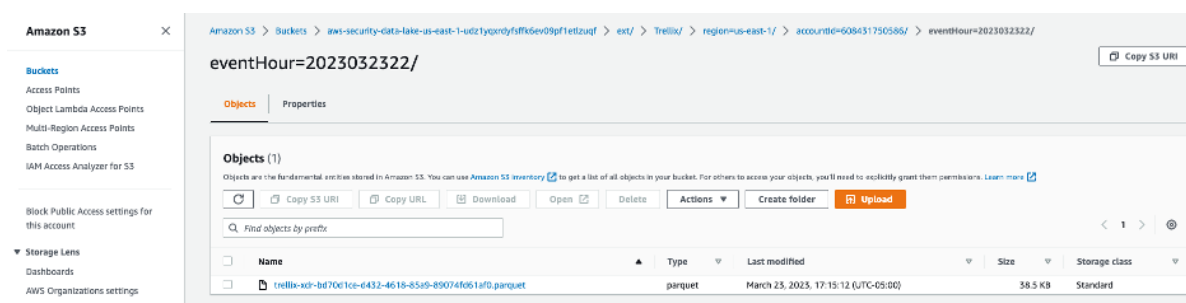
Events in Security Lake



Example fields from a Trellix finding:

```
{
  "activity_id": 1,
  "activity_name": "Generate",
  "category_name": "Findings",
  "category_uid": 2,
  "class_name": "Security Finding",
  "class_uid": 2001,
  "confidence": 100,
  "data": {"__metadata__": {"customer_id": "foo"}},
  "message": null,
  "severity": null,
  "severity_id": null,
  "status": null,
  "status_id": -1,
  "state": null,
  "state_id": 1,
  "time": null,
  "timezone_offset": 0,
  "type_name": "Security Finding: Generate",
  "type_uid": 200101,
  "metadata": {
    "logged_time": -2208988800.0,
    "original_time": null,
    "labels": [],
    "product": {
      "lang": "en",
      "name": "Trellix XDR",
      "uid": "trellix_xdr",
      "feature": {
        "uid": null,
        "name": "XDR"
      },
      "vendor_name": "Trellix",
      "version": "1.0.0"
    },
    "profiles": []
  },
  "finding": {
    "title": null,
    "uid": "26c7c83d-0aad-411b-88ee-52343ff22064",
    "types": [],
    "src_url": "https://apps.fireeye.com/helix/id/foo/alerts/None",
    "remediation": {
      "desc": "If this IP address is tied to your network via any observables attached to this event, take immediate steps to find the related device on your network and remove the infection seen from external threat intelligence",
      "kb_articles": null
    },
    "product_uid": "ssc_malware_dns_sinkhole",
    "last_seen_time": 1668535199948,
    "desc": null
  },
  "resources": [],
  "observables": []
}
```

Example objects saved to S3:



OCSF Maintenance

Trellix will handle the OCSF maintenance on behalf of the customer.

Basic Troubleshooting

Ensure the CloudFormation template executes successfully. It is valid for 24 hours after being created.

You can use the Helix Cloud Connect console to view integration status, including latest event times.

Trellix Customer Support Process

You can request assistance from Trellix Customer Support directly from Trellix Helix. To use this feature, you can click the Chat icon at the top-right of any Helix page and select **Customer Support**. A chat window will open and connect you directly to a Trellix customer support engineer.

[Trellix Support](#)

Trellix Product Documentation

[Trellix Product Documentation](#)



Visit [Trellix.com](https://trellix.com) to learn more.

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at <https://trellix.com>.

Copyright © 2023 Musarubra US LLC

052023-22