USER GUIDE

--////

---/, --//

---///

--////

--/////

--////

-~///

-///

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		
/	80	OCSF Maintenance		
/	80	Basic Troubleshooting		
/	80	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 of 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 seamless 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:

- 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

Trellix CLOUD CONNECT	
O Back to Installed Connections	
Add Connection (2 Available)	
security lake Q	
Jump to Category: Cloud Security (1)	
Cloud Security	
Amazon Security Lake	

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.
- 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.
- 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.
- 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.
- 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

- 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



You will see Helix authentication configuration screen.

Trelix CLOUD CONNECT		٢
Your Integration Instructions 	2 Choisse Bucket	3 Verify Integration
Step 1: Create Helix API Key		Select a Helix Instance v Previous Step Next Step Please select are Helix Postance
4 200 Torda	This plagen will call Helix search API and pull alert data to send the alerts into Amazon Security Lake. You can restrict which events are sent by search region. Clearte a Helix API key in the MAI console, assign these following entitlements to your account: tap search region, tap search browse. Helix API key the lake the following terms below and click enter: O input: Required For Herite in the MAI console, assign these following entitlements to your account: tap search region. Base achieves the MAI well and the enter: O input: Required Herite Herite in the MAI console, assign these following terms the magnetise in the MAI and the enter in the intervent of the MAI and the enter intervent of the MAI and the enter intervent of the MAI and the enter intervent of the MAI and the entervent of the MAI and the entervent of the MAI and the entervent of the main and the e	

5. Configure Amazon Security Bucket Lake S3 bucket location

Trellix CLOUD CONNECT					
Your Integration Instructions					
Create Helix API Key	Choose Bucket				
Step 2: Choose Bucket	Helix Instance: hexzsp68	9~			
	 Log into your AWS account (https://console.aws.amazon.com). Go to the Amazon Security Lake console and enable Security Lake for the given region. In the Amazon Security Lake console, go to Custom Sources and: Create a new source named "Trellix" Use Event Class SECURITY_FINDING. Cuse account ID 264756907367 Select Create and use a new service role Go to the S3 console and look for the Amazon Security Lake bucket name for this region. Note the AWS region this bucket is in and the Amazon Security Lake bucket name and record it below. It should look sort the Amazon Security Lake bucket for the claugf." Note the AWS region this bucket is in) and record it below. So to the AWS IAM console and search for the role created by searching roles for "trellix" and record this full ARN below. Click Submit and Verify 				
	Program Range ANS region name Anse of security Lake bucket, e.g. us west 2 Anse of Security Lake bucket ANS decount 20 of the account coming the Amazon Security Lake bucket ANS decount 20 ANS decount 20 ANS decount 20 Anse of the ANS MM relic created by Security Lake for the bucket region Like are are and off 202405/PBP viele/AmagenSecurityLake for the bucket region Like are are and and; dt22405/PBP viele/AmagenSecurityLake Averdeder TorEllice on exail-1 Coptionally Prefix in Security Lake. Defination to ext/Trellix Herefix in the bucket				

USER GUIDE

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

Amazon Security Lake $~~ imes$	Amazon Security Lake > Custom sources > Create custom source
Summary Sources Subscribers	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 beha source.
Regions Custom sources	Custom source details
r Settings General Rollup region	Data source name This must be globally unique. Trelluk Event class SECURITY_FINDING Vou can only create a custom data source in your current Region. US East (N. Virginia)
	AWS account with permission to write data Provide an account that is authorized to write data to your data lake.
	Account Id 264756907367

8. 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

9. Find AWS IAM role created by the Amazon Security Lake console

Identity and Access Management (IAM)	Identity and Access X IAM > Roles > AmazonSecurityLake-Provider-Trellix-us-east-1					
Final agement (Pri-1)	AmazonS	AmazonSecurityLake-Provider-Trellix-us-east-1				
	Trusts a Security La	ake Log Provider to access the Security Lake.				
Q, Search IAM						
Dashboard	Summary					
 Access management 	Creation date		O A	RN Copied		
User groups	March 23, 2023, 16	:23 (UTC-05:00)		௴ arn:aws	am::608431750586:role/AmazonSecurityLake-Provider-Trellix-u	
Users				s-east-1		
Roles	Last activity			Maximum s	ession duration	
Policies	None			1 hour		
Identity providers						
Account settings	Permissions	Trust relationships Tags Acce	ss Advisor	Revoke	e sessions	
 Access reports 		-				

USER GUIDE

Events in Security Lake

Amazon S3 ×	Amazon 53 > Buckets > aws-security-Gata-lake-us-east-1-udz1yoxx0yfsfft/sev09pf1ettzugf > ext/ > Trellix/ > region=us-east-1/ > accountid=508x51750585/ > eventhou=2023032322/
Buckets Access Points Object Lambda Access Points	eventHour=2023032322/ C copy s3 URI
Mutti-Hegion Access Points Batch Operations IAM Access Analyzer for 53	Objects (1) Objects are the fundamental and in Armann 55. You can use Amazon 55 monetary 🔀 in get a list of all objects in your backet. For others to access your objects, you'll need to exploitly genet them permissions. Lawr more 🕃
Block Public Access settings for this account	• Copy S3 URI • Copy URL • Copy URL • Copy URL • Copy URL • Copy S3 URI • Copy S4 URI
 Storage Lens Dashboards AWS Organizations settings 	Name ▼ Type ♥ Last modified ♥ Size ♥ Storage class ♥ Intellix-xit-bd70e1ice-6432-4616-858e-89074fd61af0.parquet parquet March 23, 2023, 17:15:12 (UTC-65:00) 38.5.48 Standard

Example fields from a Trellix finding:

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

Example objects saved to S3:

Amazon S3 ×	Amazon 53 > Buckers > aws-security-data-lake-us-east-1-udz1ygxxbyfsfft6ev09pf1et/zugf > ext/ > Trellx/ > region=us-east-1/ > accountd=608451750586/ > eventHour=2023032322/
Buckets Access Points Object Lambda Access Points Multi-Region Access Points	eventHour=2023032322/
Batch Operations IAM Access Analyzer for S3	Objects (1) Objects are the fundamental and ten stand in Amazen 53. You can use Amazen 53 inventory 🕑 to get a list of all objects in your bucket. For others to accese your objects, you'll need to excitaitly great them permissions. Learn mov 🖉
Block Public Access settings for this account	C Copy S3 URI Copy URL E Download Open C Delete Actions V Create folder IT Upload Q. Find objects by prefix
 Storage Lens Dashboards 	Name ▲ Type ▼ Last modified ▼ Size ▼ Storage class ▼
AWS Organizations settings	D trellis-xd-bd70c1ce-6432-6618-8509-69074f0614/0 parquet parquet March 25, 2023, 17:15:12 (JTC-05:00) 38.5 KB Standard

OCSF Maintenance

Trellix will handle the OSCF 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 topright 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 <u>Trellix.com</u> 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.