# **Amazon Security Lake Integration**

### **About The Integration**

Gigamon leverages deep packet inspection (DPI) to extract over 7500+ app related metadata attributes from the raw packets in the network. With Amazon Security Lake integration, users can centralize security data to get a complete understanding of the security data across the entire organization.

#### **Components Involved**

- Gigamon Application Metadata Intelligence (AMI)
- Amazon Security Lake

### **Solution Overview**



Gigamon accesses network traffic from all sources, extracts network-derived attributes, and sends Amazon Security Lake for further analysis, exploration, and enrichments.

## Gigamon®

### **Deployment Model**



- Whole pipeline (packet capture, AMI, AMX) could be running in AWS or on-prem or other environments
- Customers own their own nodes/VPC/IAM

## **Gigamon Setup:**

Configure Application Metadata Intelligence (AMI)

- 1. Go to Traffic > Solutions > Application Intelligence
- 2. Click on Create New > Select the Environment

Create Applic	ation Inte	lligence Se	ession	
Basic Info				
			Environment	
Name	0/128 Descrip	tion (optional)	Virtual	
Environment Info				
Environment Name	Connec	tion Name		
Configurations				
Export Interval				
60	secs	Manager	ent interface	

2. Select the source from where the traffic has to be tapped.

Source Traffic					
Source Selector	O Tunnel Specification	) Raw Endpoint			
Splunk-test $\times$					
				Expand All	Collapse All
Name	Filter Id	Filters	Operator	Values	$\oplus$
✓ Splunk-test					
	1	VmName_Src	startswith	ubuntu	

- 3. Select Application Metadata
  - Tool IP Address should be AMX ingress IP Address.
  - L4 Src & Dest port.
  - Using Advanced settings, you can also select any specific applications and its attribute to be exported.

ing Dedup	lication App	lication Metadata						
ceive application-specifi	traffic or add new tool.							
							Save., 6	
Tool IP Address *		L4 Source Part*	14 Destination Pe					
172.16.102.151	Template	* 23384	514					
	RECORD/TEMPLATE TYPE		ACTIVE TIMEOUT*		INACTIVE TIMEOUT*			
	Cohesive		60	secs	15	secs		
							Sawe	
	Dedup     Dedup     telve application-specific     T7216102.151	ing         Deduplication         App           scelve application-specific traffic or add new tool.	Image         Deduplication         Application Metadata           vetwe application-specific traffic or add new tool.         .           Image:	Image     Deduplication     Application Metadata       verve application-specific traffic or add new tool.	Image: Marging and Margina Application Metadata       Serve application -specific traffic or add new tool.       Image: Margina Application Metadata       Image: Margina A	ing Deduplication Application Metadata  Exerve application -specific traffic or add new tool.        Image: traffic or add new tool.       Image: traffic	Image: Deduplication     Application Metadata       ceve application-specific traffic or add new tool.       Image: Deduplication for add new tool. <tr< td=""><td>ing Deduplication Application Metadata  tele application - specific traffic or add new tool.  The filenese:  tele application Metadata  tele application - specific traffic or add new tool.  Save.   tele application - specific traffic or add new tool.  Save.  tele application -</td></tr<>	ing Deduplication Application Metadata  tele application - specific traffic or add new tool.  The filenese:  tele application Metadata  tele application - specific traffic or add new tool.  Save.   tele application - specific traffic or add new tool.  Save.  tele application -

							、 ~~	
Editor							×	
> smb		61 of 134 attributes	5		Z Export			
> smtp		20 of 102 attributes	5		Z Export			
> ssh		23 of 25 attributes			Export			
∽ ssl		61 of 72 attributes			Export			
Filter Attributes								
Select All							Select	ed /
Cert-ext-authority-key	Certificate-issuer-cn	Certificate-subject-key	Certificate-subject-street	Compression-method	Z Ext-sig-algorithm-sig	Parent-common-name	Serv	ver-
Cert-ext-subject-key-id	Certificate-issuer-I	Certificate-subject-key	Cipher-suite-id	Content-type	Ext-sig-algorithms-len	Protocol-version	Ses:	sion
Cert-extension-oid	Certificate-issuer-o	Certificate-subject-key	Cipher-suite-list	Declassify-override	Fingerprint-ja3	Request-size	Ses:	sion
Cert-extension-oid-raw	Certificate-issuer-ou	Certificate-subject-key	Client-hello-extension-L	Ext-ec-point-formats-nb	Fingerprint-ja3s	Serial-number	Sigr	aliz
Certif-md5	Certificate-issuer-st	Certificate-subject-key	Client-hello-extension	Ext-ec-point-formats-t	Handshake-type	Server-hello-extension	Sub	ject-
Certif-sha1	Certificate-issuer-street	Certificate-subject-l	Client-hello-version	Ext-ec-supported-grou	Index	Server-hello-extension	Sup	port
	Certificate-raw	Certificate-subject-o	Client-supported-version	Ext-ec-supported-grou	Sissuer	Server-hello-version	Vali	dity-
Certificate-dn-issuer								
Certificate-dn-issuer	Certificate-subject-c	Certificate-subject-ou	Common-name	<ul> <li>Ext-sig-algorithm-hash</li> </ul>	Nb-compression-meth	Server-name	Valie Valie	dity-

The example above shows SSL attributes available to be exported.

4. Click Save and then Deploy

How to configure Gigamon Application Metadata Exporter (AMX) to integrate with Amazon Security Lake

How to Bring up AMX from GigaVUE-FM (fabric manager)

1. Create Monitoring Domain:

Inventory > Virtual > Select the Environment > Create Monitoring Domain

Monitoring Domain	Connections	Name	Management IP	Туре	Version	¢
ELK-Test						
	ELKTest					
		VSeries-OGW10-115-81-	10.115.86.55	V Series Node	6.2.00	

2. Create Monitoring Session:

Traffic > Orchestrated Flows (select the right environment) > Create Monitoring Session

- Create REP from AMI to AMX to Amazon Security Lake (REP-Raw End Point which is an IP Address)
- Ingress to AMX will be from AMI
- Egress from AMX should be pointing to AWS S3 bucket which is designated for Amazon Security Lake
- As shown in the snapshot below, select "Other" from cloud tool drop down. Tip: entries are

3. Create Monitoring Session:

Traffic > Orchestrated Flows (select the right environment) > Create Monitoring Session

- Create REP from AMI to AMX to Amazon Security Lake (REP-Raw End Point which is an IP Address)
- Ingress to AMX will be from AMI
- Egress from AMX should be pointing to AWS S3 bucket which is designated for Amazon Security Lake
- As shown in the snapshot below, select "Other" from cloud tool drop down. Tip: entries are given below the screenshot for copy paste.

✓ AmazonSecurityLake		
Alias*	AmazonSecurityLake	
Cloud Tool*	Other	*
Endpoint*	https://s3.us-west-2.amazonaws.com	
Headers*	amx_exporter_plugin: amazon_sec	Θ
	amx_exporter_format: ocsf	Θ
	aws_source_location: GigamonAM	Θ
	aws_region_name: us-west-2	Θ
	aws_account_id: 3150#######3	Θ
	aws_bucket_name: gigamon.ami.or	Θ
	aws_access_key_id: AKIAU******	Θ
	aws_secret_access_key: Jsk8NCq7	⊕ <del>⊝</del>
MORE OPTIONS		
Enable Export		
Format	NOR	
Zip		
Interval (sec) 🕄	300	
Paraller Writers	4	
Export Retries	4	
Max Entries	5000	
Labels	Add	

• Enter following info in the endpoint section

https://s3.us-west-2.amazonaws.com

• Enter following info in the headers section

amx\_exporter\_plugin: amazon\_security\_lake amx\_exporter\_format: ocsf aws\_bucket\_name: gigamon.ami.ocsf.export aws\_source\_location: GigamonAMI aws\_region\_name: us-west-2 aws\_account\_id: 3150#######3 aws\_access\_key\_id: AKIAU\*\*\*\*\*\*\*\*\*\*\*ZII7 aws\_secret\_access\_key: Jsk8N\*\*\*\*\*\*\*\*\*\*\*\*\*\*

- Select interval as 5 minutes (300sec) and max entries per export as 5000
- 4. Deploy the Solution.

rawl > Interface connecting AMI raw2 > Interface connecting Amazon Security Lake

Select nod	les to deploy the Monitorin	g Sessio	n: AMX	(			
	V Series Node Name				Status		$\oplus$
	VSeries.10.115.27.86				ОК		
K	Go to page: 1	•	of <b>1</b>	>	) >I	Total Records: 1	
✓ VSeri	es.10.115.27.86						
raw-1		ens6				X Y	
raw-2		ens7				×	
						Deploy	ancel

## Gigamon®

Once GigaVUE Cloud Suite is deployed in the environment it provides Amazon Security Lake the ability to see all available applications communicating across the environment and collect metadata from that traffic.



Screenshot of demo data in GigaVUE-FM. Note: Production environments will display hundreds of applications.

### Verify data is being sent to Amazon Security Lake/S3

1. Go to AWS S3 bucket that is configured for export and follow the hierarchy of folders which Amazon Security Lake expects.

nazon S3 > Buckets > gigamon.ami.ocsf.export.dev > GigamonAM	11/ > region=us	-west-2/ > accountId=3	> eventHour=2023	0324/
ventHour=20230324/				🗇 Copy S3 URI
Objects Properties				
Objects (10)				
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 them permissions. Learn more	inventory 🗹 to get	a list of all objects in your bucket. For others to ac	cess your objects, you'll	need to explicitly grant
C Copy S3 URI Copy URL 🕑 Downloa	d Open [	Z Delete Actions ▼	Create folder	🕅 Upload
Q Find objects by prefix				< 1 > 💿
Name A	Type ⊽	Last modified	⊽ Size ⊽	Storage class 🛛 🗸
□ 167967995900000_1679679972000299.parquet	parquet	March 24, 2023, 10:46:15 (UTC-07:00)	369.0 KB	Standard
I679679973000000_1679680032000247.parquet	parquet	March 24, 2023, 10:47:16 (UTC-07:00)	1.3 MB	Standard
1679680033000000_1679680092000256.parquet	parquet	March 24, 2023, 10:48:16 (UTC-07:00)	1.3 MB	Standard
1679680093000000_1679680152000253.parquet	parquet	March 24, 2023, 10:49:16 (UTC-07:00)	1.3 MB	Standard
1679680153000000_1679680212000243.parquet	parquet	March 24, 2023, 10:50:16 (UTC-07:00)	1.3 MB	Standard
1679680213000000_1679680272000274.parquet	parquet	March 24, 2023, 10:51:16 (UTC-07:00)	1.3 MB	Standard
1679680273000000_1679680332000262.parquet	parquet	March 24, 2023, 10:52:16 (UTC-07:00)	1.4 MB	Standard
1679680333000000_1679680392000290.parquet	parquet	March 24, 2023, 10:53:16 (UTC-07:00)	1.3 MB	Standard

Go to <u>Amazon Security Lake Getting Started</u> to complete remaining steps to make use of Gigamon Application Metadata Intelligence export.

To try this integration in your environment please reach out to <u>tme@gigamon.com</u>. If you would like to learn more about GigaVUE Cloud Suite, contact us at <u>gigamon.com/contact-sales</u>.

Worldwide Headquarters 3300 Olcott Street, Santa Clara, CA 95054 USA +1 (408) 831-4000 | <u>www.gigamon.com</u> © 2023 Gigamon. All rights reserved. Gigamon and the Gigamon logo are trademarks of Gigamon in the United States and/or other countries. Gigamon trademarks can be found at gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners. Gigamon reserves the right to change, modify, transfer, or otherwise revise this publication without notice.