

Amazon Security Lake Integration

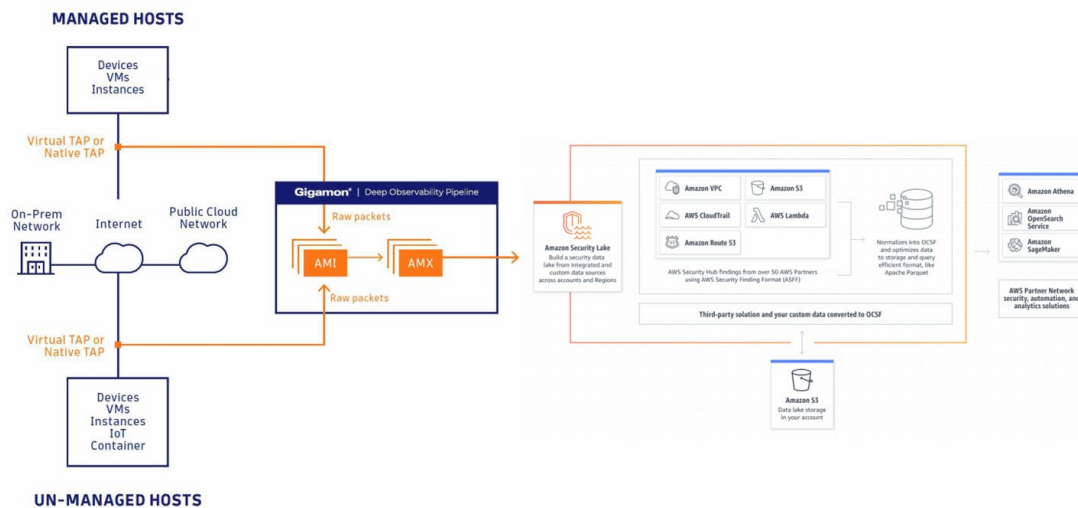
About The Integration

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

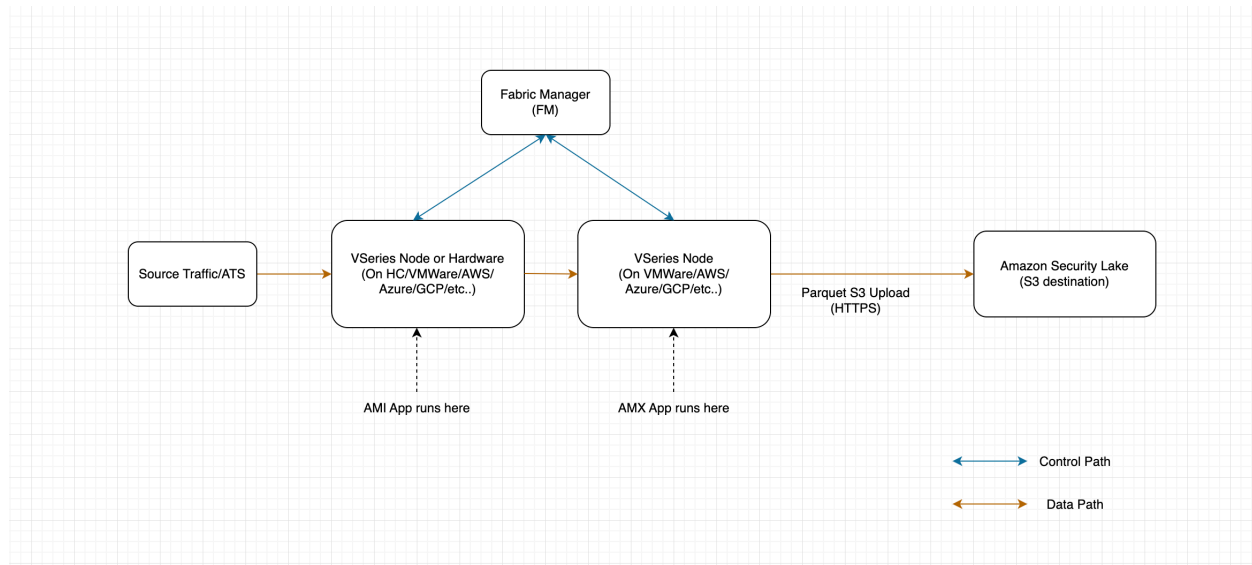
- [Gigamon Application Metadata Intelligence \(AMI\)](#)
- [Amazon Security Lake](#)

Solution Overview



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

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 Application Intelligence Session

Basic Info

Name	Description (optional)	Environment
<input type="text"/>	<input type="text"/>	<input type="text" value="Virtual"/>

0 / 128

Environment Info

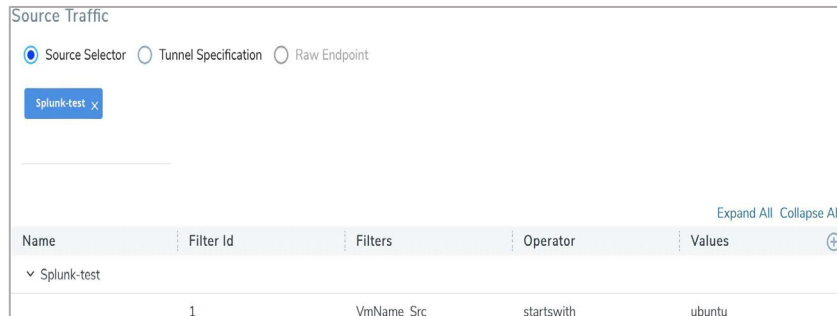
Environment Name	Connection Name
<input type="text"/>	<input type="text"/>

Configurations

Export Interval	<input checked="" type="checkbox"/> Management Interface
<input type="text" value="60"/> secs	

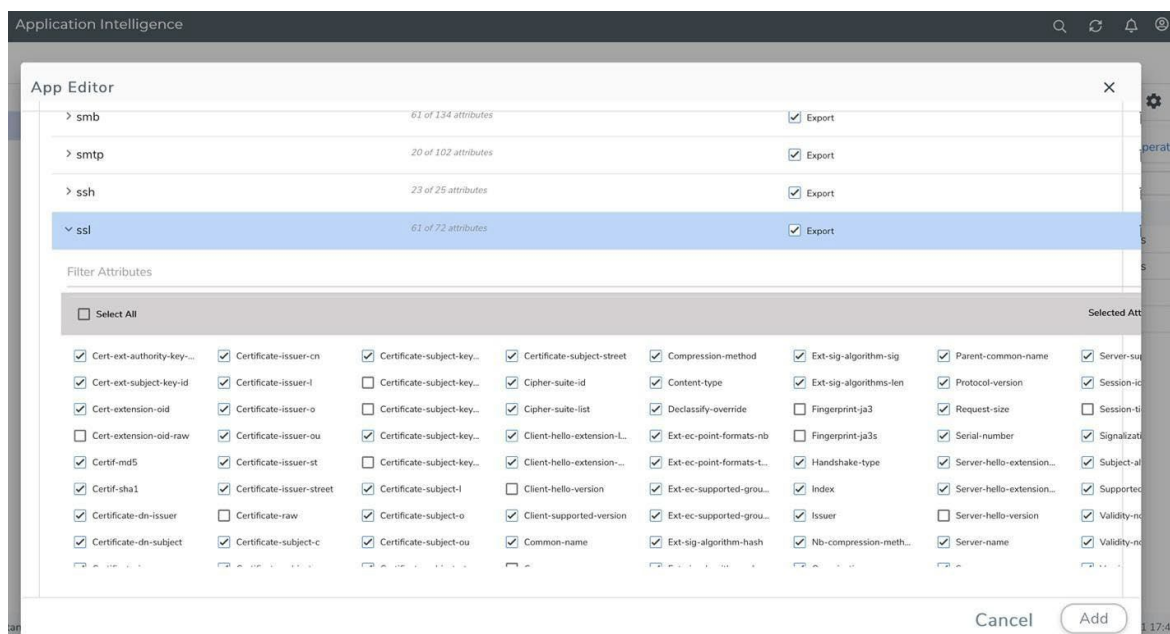
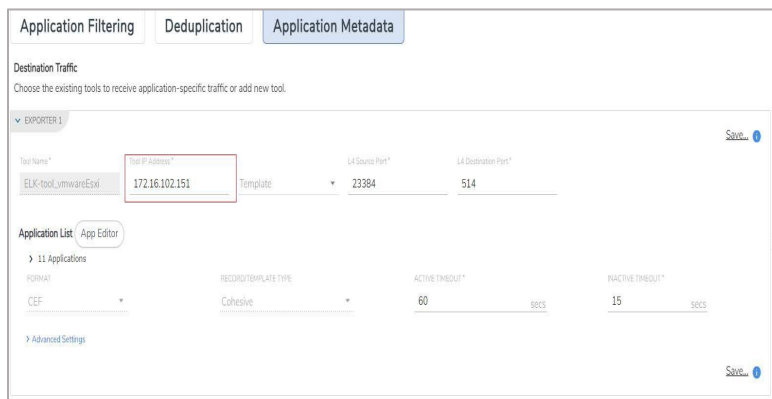
Must be between 60-900

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



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.



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	Type	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.**

The screenshot displays the configuration interface for an AmazonSecurityLake monitoring session. The interface is organized into several sections:

- AmazonSecurityLake** (Section Header)
- Alias***: AmazonSecurityLake
- Cloud Tool***: Other (selected from a dropdown menu)
- Endpoint***: https://s3.us-west-2.amazonaws.com
- Headers***: A list of key-value pairs for headers, each with a red minus icon to its right:
 - amx_exporter_plugin: amazon_sec
 - amx_exporter_format: ocsf
 - aws_source_location: GigamonAM
 - aws_region_name: us-west-2
 - aws_account_id: 3150#####3
 - aws_bucket_name: gigamon.ami.o
 - aws_access_key_id: AKIAU*****
 - aws_secret_access_key: Jsk8NCq7 (with a green plus icon and a red minus icon to its right)
- MORE OPTIONS** (Section Header)
- Enable Export**:
- Format**: JSON
- Zip**:
- Interval (sec)**: 300
- Paraller Writers**: 4
- Export Retries**: 4
- Max Entries**: 5000
- Labels**: Add (button)

- 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*****tecu
```

- Select interval as 5 minutes (300sec) and max entries per export as 5000

4. Deploy the Solution.

raw1 > Interface connecting AMI

raw2 > Interface connecting Amazon Security Lake

Select nodes to deploy the Monitoring Session: AMX

<input type="checkbox"/>	V Series Node Name	Status	
<input checked="" type="checkbox"/>	VSeries.10.115.27.86	OK	⊕

< < Go to page: 1 of 1 > > Total Records: 1

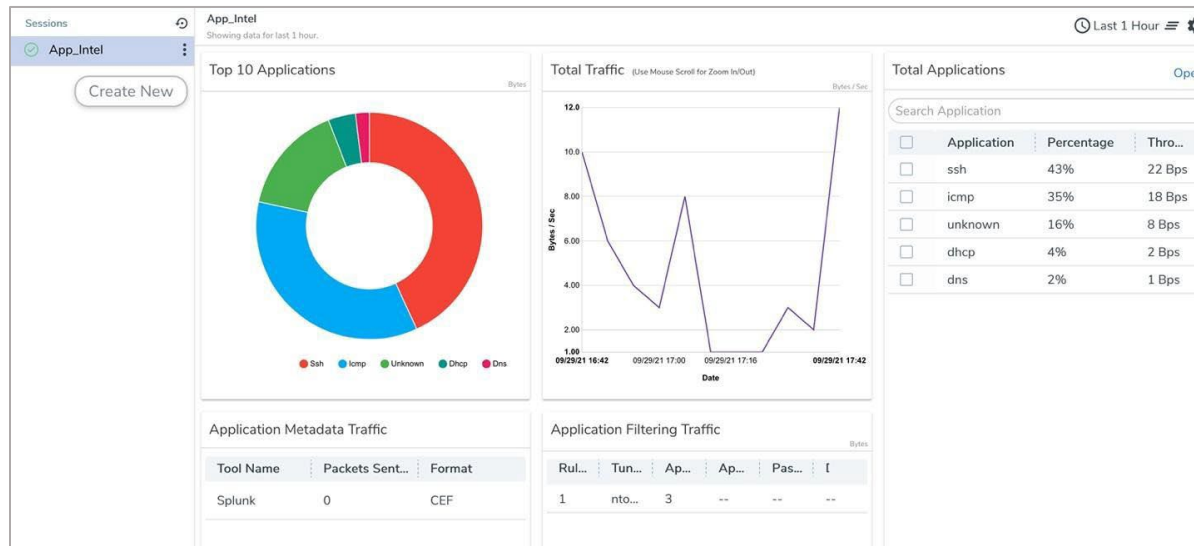
▼ VSeries.10.115.27.86

raw-1 ens6

raw-2 ens7

Deploy Cancel

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.

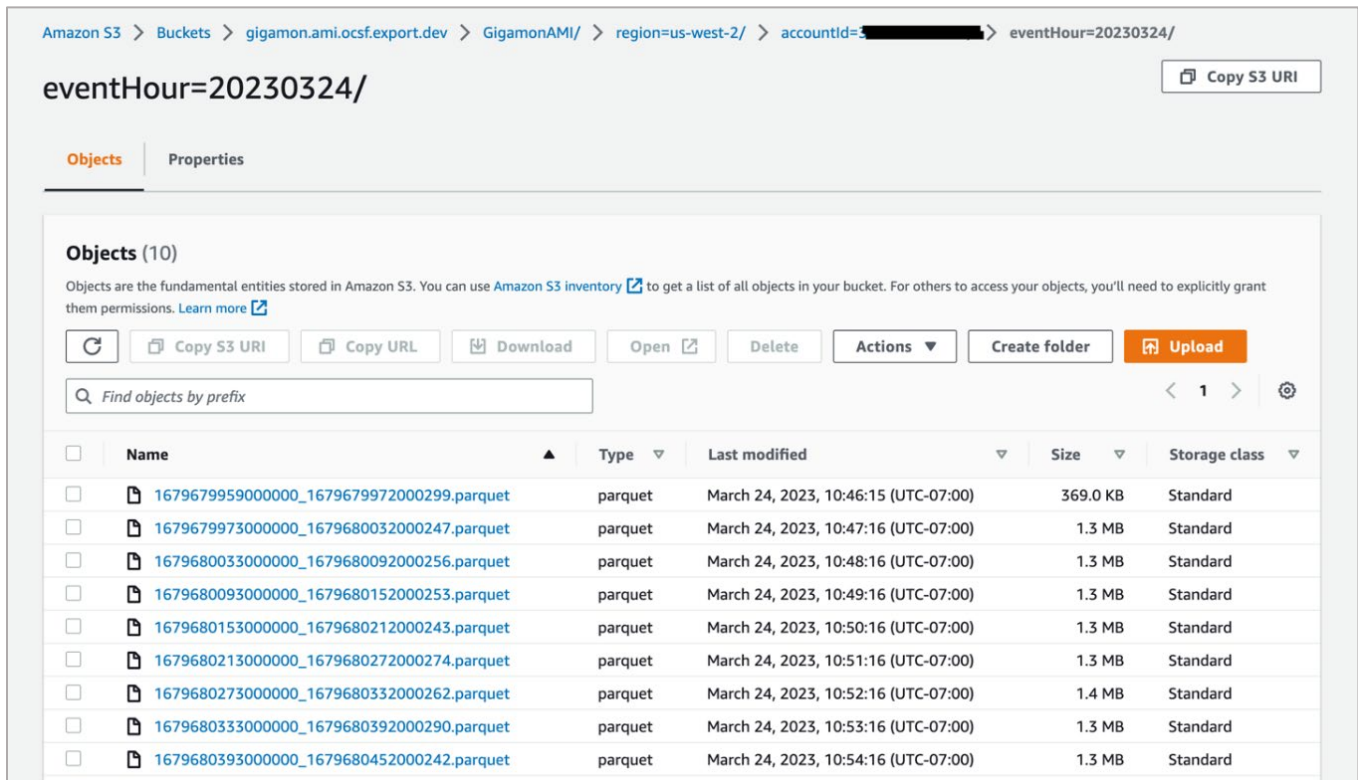


Screenshot of demo data in GigaVUE-FM.

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.



The screenshot shows the Amazon S3 console interface for a bucket named 'eventHour=20230324/'. The breadcrumb navigation path is: Amazon S3 > Buckets > gigamon.ami.ocsf.export.dev > GigamonAMI/ > region=us-west-2/ > accountid=[redacted] > eventHour=20230324/. A 'Copy S3 URI' button is visible in the top right. Below the breadcrumb, there are tabs for 'Objects' (selected) and 'Properties'. The 'Objects' section shows 10 objects, each with a checkbox, a file icon, a name, a type of 'parquet', a last modified date and time (UTC-07:00), a size, and a storage class of 'Standard'. The objects are listed in a table with columns: Name, Type, Last modified, Size, and Storage class.

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	1679679959000000_1679679972000299.parquet	parquet	March 24, 2023, 10:46:15 (UTC-07:00)	369.0 KB	Standard
<input type="checkbox"/>	1679679973000000_1679680032000247.parquet	parquet	March 24, 2023, 10:47:16 (UTC-07:00)	1.3 MB	Standard
<input type="checkbox"/>	1679680033000000_1679680092000256.parquet	parquet	March 24, 2023, 10:48:16 (UTC-07:00)	1.3 MB	Standard
<input type="checkbox"/>	1679680093000000_1679680152000253.parquet	parquet	March 24, 2023, 10:49:16 (UTC-07:00)	1.3 MB	Standard
<input type="checkbox"/>	1679680153000000_1679680212000243.parquet	parquet	March 24, 2023, 10:50:16 (UTC-07:00)	1.3 MB	Standard
<input type="checkbox"/>	1679680213000000_1679680272000274.parquet	parquet	March 24, 2023, 10:51:16 (UTC-07:00)	1.3 MB	Standard
<input type="checkbox"/>	1679680273000000_1679680332000262.parquet	parquet	March 24, 2023, 10:52:16 (UTC-07:00)	1.4 MB	Standard
<input type="checkbox"/>	1679680333000000_1679680392000290.parquet	parquet	March 24, 2023, 10:53:16 (UTC-07:00)	1.3 MB	Standard
<input type="checkbox"/>	1679680393000000_1679680452000242.parquet	parquet	March 24, 2023, 10:54:16 (UTC-07:00)	1.3 MB	Standard

Go to [Amazon Security Lake Getting Started](#) to complete remaining steps to make use of Gigamon Application Metadata Intelligence export.

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