

# CrowdStrike + Gigamon Application Metadata Intelligence Deployment Guide

October, 2024

## Pre-requisite:

Deploying Gigamon Application Metadata Exporter (AMX) VSN:

- Deploy a GigaVUE V series node (for AMX) with traffic acquisition method as Customer Orchestrated Source.
- And create a Monitoring Session (Rep1 (In) --->AMX --->Rep 2 (Out) )

#### CrowdStrike:

- User should have their own http endpoint with API key, to which data has to be ingested.
- How to get create the http endpoint.  $\rightarrow$  Configure the HTTP Event Connector with Datatype as JSON, and give your parser details.
- You will be able to get an endpoint along with the ingestion key, use this as part of the GIGAMON AMX config.

## Configuration:

### How to configure Gigamon Application Metadata Intelligence (AMI)

- Pls refer this public doc link: (Pls choose the release configuration guide corresponding to the running FM/Vseries )
- <u>https://community.gigamon.com/gigamoncp/s/docs</u> **Doc Library**
- Below is the sample for 6.8 AMI
- <u>Application Metadata Intelligence</u>

### Configuring CrowdStrike Details in AMX:

• Please refer to the doc guide for details related to AMX configuration for 6.8: (Switch to corresponding release as required. As of 4th October 2024, 6.8 is the GA Release)

https://docs.gigamon.com/doclib68/Content/GV-Cloud-V-Series-Applications/AMX\_intro.html?Highlight=AMX

- Edit the MS, Click on AMX and give details.
- Go to Cloud Tools Exports :
- Configure Alias as "CRWD or name as desired by the user"
- Cloud Tool as "Other"
- configure the Endpoint as per your HEC config
- Add a header to give the authorization key in this format "Authorization: Bearer 5bb3b51f89a346cf906"
- Type as "AMI"
- Enable Export
- Make sure you provide Label with "Key" as "event" and "value" as "Gigamon"
- Others with default values.
- Below is the snapshot:

~	Cloud Tool Exports		
	Alias* ()	Crowdstrike_Gigamon	
	Cloud Tool* ()	Other ~	
	Endpoint* ()	https://eb087263d7764b3eb37d24d1ba	
	Headers* ()	Authorization: Bearer 5bb3b51f89	⊛⊝
	Туре	ami ~	)

MORE OPTIONS	
Source IP Address ()	Optional
Enable Export ()	
Format ①	JSON
Zip (j)	•
Interval (sec) (j	30
Parallel Writers (i)	4

Export Retries (j)	4
Max Entries (1)	1000
Labels* (j)	Key     event       Value     Gigamon

- Now click save and deploy the monitoring session.
- The configuration part is done, now you can test by sending traffic.

#### Configuring CrowdStrike to Ingest Json data:

- Login to crowd strike NGSIEM
- Go to Homepage --> NG SIEM  $\rightarrow$  Event Search  $\rightarrow$  Check for Vendor as Gigamon in the query, you will be able to see the below content if the ingestion is successful.

Weicome to the new Event Search	experience (Jaars more)							×
New query			Unsaved changes	New	Import	Queries	See	More v
Source Al 🛛 🗸 🖽	Last 1 day						15	Hide adlise
Match Any All of t	Ne following conditions in $AI \sim$ events							
#Vendur	× 8	equal to	v Gipanon					$\odot$
© Add conditional group								
Display query results as Events ~								
Retrointy Actions ~		-						
Ra: 1000   Speed: 4 Gibh   EPS: 50	133306   Work: 11   Completion: 100   Status	a Dune						8 E
Timestump	feet							
0ct. 4, 2804 15:58-40	E Neuroscientes (Normanis) Neuroscientes (Normanis)	80 4800°, 						

#### Below are the sample dashboards

· (heate its 5.0 Ver Hony Bulmate Pulles he Mider Hop			● > ○ ● × ▼ Q ₽ ALADA BETAN
• • • • • • • • • • • • • • • • • • •	E terr + B terr + 1	() then a light part of the last of the light of the ligh	Bine x Xine x when x x
+ + 0 (5, Monus Landolfs and resign/contribution deficiency	dentric later and add	8. hep-0 viewharter search all	<ul> <li>• • •</li> </ul>
E Standarder Instante D	Q.	hear A	
Sarch Darborch Lusiup Re-			
BB. Crystegraphic Details			24 1
V files to file - @ heateles			distribute v 😁 Bandine 🗇 De
7.5 Versions seen in the network	20 mp × -1	Compression Algorithms Detected	Hans - I
		Senter Stage, senting 1 yr 101(11)	
Signature Rigorithm	it nor v 1	Key Exchange Protocols weet on the network Transform sound	may v 1
		EDGA TANK	
0			
	🖸 🛃 🔛 💋 (	3 🗶 💿 📾 📾 📾 🚳 💿	

· Nan Can Stille	Dertoreth Cl					Q family						
nd Selfords	Lang Sa											
spicitus Cannacifiera												/10
Films Authors	· · · · · · · · · · · · · · · · · · ·									-	ilitaria v 🔳	Danitra (
te fuerine Core	ethers.		Name of the	List of Baselin	the Contraction							A 1001
						-			-	-		
								1000.0000.0.00			term in concerning the second	
- Andrew				1000			170.00.00.0	100.00.0.0	10.00		MARKING AND ADDRESS	
				a subsc	100	10	10.0.00.0	100.101.1.14	tella.		Los Arrival Sciences	
mathema in the second	- 10			d'autors.	100	100	170.06.04.2	100.03.1.18	Market.	842	MARCHINE AND ADDRESS	
union in the second				d'ades	25/9	1.000	170.00.08.2	100.00.1.0	Marca.		and the second	
raphen	-			di taglica	100	-	10.0.04.04.2	100.001.0.08	14174	80	100207024140400	
agines.				arrestee.	21/2	1.08	170.00.04.7	102.125.1.18	1474		100.0110010 (MILMO)	
8 2 3 4				8 2 3	1.1.4	29						
urt Speerling Activity						1						
attains by F	Destination, P	Sec. Part	Dest. Part	Front D								
maters \$173.58	10.7 10.101.1.10	THE PARTY		Service Property and the								
adres \$73.14	10.2 10.10.1.10	190704	-	LANGE THE MONTH	6							
uster 173.34	N.J. 143.125.1.18	140704		Level 1 for further	8							
uples \$73.34	W.1.03.101 L.W.	INCOM.	-	INVESTIGATION OF	6							
uter 173.34	N.1. 161.125.1.18	160706		LANGE THE TOTAL OF	6							
uphen \$75.34	W.L.R.L.M. L.W.	160706	40	servicitienceber	6							
uphen EVI.14	W.L.MI.LM. L.W.	34034	10	LINE CONTRACTOR OF THE OWNER	6							
	4 7 14											



Worldwide Headquarters 3300 Olcott Street, Santa Clara, CA 95054 USA +1 (408) 831-4000 | www.gigamon.com

© 2024 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 www.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.