

Gigamon Metadata Application for Splunk Deployment Guide

#### COPYRIGHT

Copyright © 2018 Gigamon. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without Gigamon's written permission.

#### TRADEMARK A TT RIBUTIONS

Copyright © 2018 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 foundat www.gigamon.com/legal-trademarks. All other trademarks are the trademarks of their respective owners.

This page is intentionally left blank

# Table of Contents

Overview	5
Gigamon Metadata Application for Splunk	6
Audience	6
Notes	6
Setting up Splunk	7
Downloading the Splunk SIEM	7
Installing the Splunk SIEM	9
Downloading and installing the Gigamon Metadata Application for Splunk	11
Configuring IPFIX Generation on GigaVUE node	15
Configuration to generate IPFIX Summary of below config: Tips for below config:	
Verifying the configuration On Gigamon Device: On the Machine(or VM) which has a Splunk instance:	
Setting up Splunk to ingest IPFIX – Part 1 (file level changes)	23
Setting up Splunk to ingest IPFIX- Part 2(within Splunk)	24
Verifying the Setup	27
Configuring CEF Generation on GigaVUE node	28
Summary of below config:	28
Tips for below config:	28
Configuration to generate	29
Verifying the configuration On Gigamon Device: On the Machine(or VM) which has a Splunk instance:	
Setting up Splunk to ingest CEF	
Verifying the Setup	
Summary	
Appendix	
Use cases available with Gigamon's custom metadata elements	

### Overview

IPFIX and CEF are powerful standards-based technology that are gaining momentum in the network security space for forensics, trend analysis, and anomaly detection. They looks at raw network packets and derives sophisticated flow-based metadata such as records of conversations between endpoints, duration of conversations, and channels of communications.

Gigamon centralizes the function of generating these flow records so that this can be done consistently across heterogeneous and disparate infrastructure. The flow records can be served up to a variety of security solutions that analyze flow metadata. Gigamon has also extended the metadata to include URL information, providing insight into HTTP and SIP traffic. Other enterprise extensions for metadata are HTTP, DNS, and SSL certificates, which provide metadata that can be used for security analysis.

The Gigamon Security Delivery Platform with metadata Generation:

- provides unsampled metadata record generation to detect "low-and-slow" attacks
- filters records based on configurable parameters to predetermined tools
- offloads metadata record generation from the overloaded network infrastructure
- enables end-to-end security enforcement with visibility into every flow
- provides advanced information elements



Figure 1: IPFIX/CEF Generation using Gigamon Visibility Platform

Incoming packets from network(s) enter the Gigamon Visibility Platform and are directed by maps to GigaSMART engine for metadata generation. Metadata generation process examines the incoming packets and converts the packets of choice into flow records. Specific flows are then forwarded to specific tools, such as Security, Application Performance, and Customer Experience Management (CEM) tools.

# Gigamon Metadata Application for Splunk

The Gigamon Metadata Application for Splunk allows customers to extract, index and display network metadata generated by the GigaSECURE Security Delivery Platform. The application comes packaged with dashboards, demo views, and tutorial to make deployment simple and intuitive.

The Gigamon GigaSECURE Security Delivery Platform allows users to extract and consolidate metadata from monitored network traffic flows, package them into NetFlow IPFIX/CEF records, then send them to collectors like Splunk SIEM for indexing and analysis. Gigamon has enriched the IPFIX/CEF records with information like URL information, HTTP/HTTPS return codes, and DNS query/response information, all of which can provide the ability to rapidly diagnose security events for use cases such as, identifying rogue DNS services, spotting potential Command and Control server communications using high entropy domains and detecting use of non-trusted or self-signed certificates for SSL-decrypted traffic that could indicate nefarious activity.

See Appendix for Use cases available with Gigamon's custom metadata elements For more information on Gigamon's NetFlow and Metadata Generation see:

https://www.gigamon.com/products/traffic-intelligence/gigasmart/metadata-generation.html

### Audience

This guide is intended for users who have basic understanding of Splunk. This document expects users to be familiar with Splunk administration, installation of additional Splunk components, administrative permissions to restart services and edit configuration files.

This deployment guide covers installation and configuration of a single-instance deployment, where one Splunk instance serves as both the search head and indexer running on Linux- based servers.

#### Notes

The below notes apply to GigaVUE visibility node running GigaVUE-OS 5.0.

- Maximum of five records can be added to single monitor with all the records having same match fields but can differ in collect fields
- Only one monitor can be configured per GigaSMART Group
- GigaSMART Operation can only be assigned to GigaSMART Group consisting of single engine port.
- For more than one monitors, multiple engine ports must be bound to separate GigaSMART Groups and different monitors can be assigned to each of them.
- Maximum number of exporters supported by a tunnel is six

# Setting up Splunk

# Downloading the Splunk SIEM

Go to <a href="https://www.splunk.com/">https://www.splunk.com/</a>

🛡 🔍 🔰 SIEM.					
← → C 🔒 Sec	cure https://www.splunk.com			<b>\$</b>	6 8 2 0 1
				Training Support Pricing III Splunk	: Sites 🜐 🗟 utkarsh
splunk>	PRODUCTS SOLUTIONS CUSTOMERS	PARTNERS RESOURCES ABOUT	JS	Q	Free Splunk
	SPLUNK PLATFORM	SPLUNK FOR IT OPERATIONS	SPLUNK FOR SECURITY	MORE SPLUNK	
	Splunk Enterprise	Splunk IT Service Intelligence	Splunk Enterprise Security	Products Overview	
	Splunk Cloud	Splunk Insights for Infrastructure	Splunk User Behavior Analytics	Pricing	
	Splunk Light	Splunk Insights for AWS Cloud	Splunk Insights for Ransomware	Apps & Add-Ons	
		Monitoring	Phantom	Free Trials & Downloads	

#### Click the free trial option



Sign-in or Login into your Splunk account to download Splunk.



Now, download the Splunk Enterprise as per your OS. For Ubuntu machines, download .deb as shown below:

● ● ● <b>●</b> Dow	nload Splunk Enterprise fc ×					Utkarsh
← → C 🔒 Se	cure https://www.splunk.com	/en_us/download/get-started-with-your-free-tria	al.html#tabs/linux		\$	G 🗉 🖸 🗿 🗄
					Training Support Pricing 🏭 Splund	i Sites 🍈 🔒 utkarsh
splunk>	PRODUCTS SOLUTIONS	CUSTOMERS PARTNERS RESOURCES	ABOUT US		Q	Free Splunk
	Splunk Er	nterprise 7.1.0				
	Index 500 MB/Day. Enterprise license to	Sign up and download now. After 60 continue using the expanded function	0 days you can co ionality designed	nvert to a perpetual free licer for enterprise-scale deployme	nse or purchase a Splunk ents.	
	Choose Your Installa	tion Package				
	Windows	🗴 Linux 🗯 Mac OS				
	64-bit	2.6+ kernel Linux distributions	.rpm	251.87 MB	± Download Now	
			.deb	251.1 MB	🛓 Download Now	
			.tgz	252.69 MB	± Download Now	
			Release Notes	I System Requirements I Older F	Releases I All Other Downloads	

## Installing the Splunk SIEM

Splunk setup would be downloaded in the "Downloads" directory

Files			tų En	<b>∢</b> )))	2:26 PM 🔱
0	utkarsh@utkarsh-virtual-machine:-/Downloads\$ ll total 257144 drwkr-xr-x 2 utkarsh utkarsh 4096 May 21 08:05 ./ drwkr-xr-x 18 utkarsh utkarsh 4096 May 30 16:56 .// .rw-rw-r-1 utkarsh utkarsh 263300382 May 21 08:05 splu utkarsh@utkarsh-virtual-machine:-/Downloads\$ ]	-			
: <u>-</u>	ලෙ⊜ා Downloads < > බthome Downloads	 ۹ 🗉			ľ
<b>2</b>	<ul> <li>⊘ Recent</li> <li>☆ Home</li> <li>⇒ Desktop</li> <li>⇒ Documents</li> <li>&gt; Documents</li> <li>&gt; Downloads</li> <li>&gt; Music</li> <li>&gt; Pictures</li> <li>&gt; Videos</li> </ul>				

You might need superuser permissions to perform the below commands. You can use:

\$ sudo -i

Use the below command to install splunk on ubuntu:

\$ dpkg -I <package\_name>



Splunk is installed in the '/opt' directory: To start Splunk use the below command

\$ cd /opt/splunk/bin
\$ ./splunk start

When you set up Splunk for the first time, it takes you over the license agreement, hit yes and create a password.



🛛 🔍 > Login   Splunk 🛛 🔹 🔛				ŧ
C O Not Secure   10.115.94.45:8000/en-l	JS/account/login?return_to=%2Fen-US	%2F		\$
	<b>splunk</b> >e	nterprise		
	admin		Sign In	
	First time sig If you've forgette Splunk administre			

Now you can access Splunk by opening the browser and hitting 127.0.0.1:8000 or the machine's IP.

# Downloading and installing the Gigamon Metadata Application for Splunk







Similarly download "Splunk Stream" and "URL Toolbox" apps. \*Splunk Stream is only required for IPFIX. If you just want CEF, you can skip installing Splunk Stream

Now in Splunk, follow the steps to install these apps: Click the wheel button near Apps.

• • • • Home   Splunk 7.1.0	×				100
← → C ① Not Secure 10.115.94.	.45:8000/en-US/app/launcher/home				☆ 💿
splunk>enterprise		🖪 Admin	istrator 👻 😑 Messages 👻 Settings 💌	Activity - Help - Find	٩
Apps 🌣	Expore optionk Enterprise				×
Search & Reporting	·····································				
+ Find More Apps	Product Tours	Add Data	Explore Data	Splunk Apps 🗗	
	New to Splunk? Take a tour to help you on your way.	Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.	Explore data and define how Hunk parses that data.	Apps and add-ons extend the capabilities of Splunk Enterprise.	
					Close
		Choose a hor			
	ł				
10.115.94.45:8000/en-US/manager/launcher/apps/	s/local				

#### Click "install from file"

O Not Secure 10.115	5.94.45:8000/en-US/manager/laur	icher/apps/lo	cal				<u> </u>
plunk>enterprise Apps <del>-</del>					Administ	rator 🔻 🧿 Messag	ges • Settings • Activity • Help • Find
Apps							Browse more apps Install app from file Create ap
nowing 1-17 of 17 Items							
liter Q							25 per page
Name =	Folder name •	Version \$	Update checking •	Visible •	Sharing ¢	Status #	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App   Permissions	Disabled   Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App   Permissions	Disabled   Enable	
og Event Alert Action	alert_logevent	7.1.0	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
Vebhook Alert Action	alert_webhook	7.1.0	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
Apps Browser	appsbrowser	7.1.0	Yes	No	App   Permissions	Enabled	Edit properties 1 View objects
ramework	framework		Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
Setting started	gettingstarted	1.0	Yes	Yes	App   Permissions	Disabled   Enable	
ntrospection_generator_addon	introspection_generator_addon	7.1.0	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
lome	launcher		Yes	Yes	App   Permissions	Enabled	Launch app   Edit properties   View objects
amed	learned		Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
agacy	legacy		Yes	No	App   Permissions	Disabled   Enable	
ample data	sample_app		Yes	No	App   Permissions	Disabled   Enable	
Search & Reporting	search	7.1.0	Yes	Yes	App   Permissions	Enabled	Launch app 1 Edit properties 1 View objects
plunk Archiver App	splunk_archiver	1.0	Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects   👩 View details on Splunkbe
plunk_httpinput	splunk_httpinput		Yes	No	App   Permissions	Enabled   Disable	Edit properties   View objects
nstrumentation	splunk_instrumentation	4.1.5	Yes	Yes	App   Permissions	Enabled	Launch app   Edit properties   View objects
fonitoring Console	splunk_monitoring_console	7.1.0	Yes	Yes	App   Permissions	Enabled   Disable	Launch app   Edit properties   View objects

Choose the downloaded file to be installed

Settings   Splunk ×	nonariannastalli unland?brandarumba-Rattinge# 70# /Emonanad/ / Elisung	100 100 100 100 100 100 100 100 100 100	managadi 2Elaunaha	19/2500019/251000	ة م م
splunk>enterprise Apps -	nagerjappinstalij_pploauroreadorumos=settings xx C xz manager xz hadiito	ator • 3 Messages •	Settings  Activ	vity • Help •	Find Q
Upload app Apps > Upload app					
$\rightarrow$	Upload an app If you have a .spl or .targz app file to install, you can upload it using this form You can replace an existing app via the Splunk CLL. L2 Learn more. File Choose File gigamon-metadat_unk_120 (6).tgz Upgrade app. Checking this will overwrite the app If it already exists.	L			
	Cancel	Upload			

Restart Splunk to complete installation

Settings   Splunk ×								÷
← → C O Not Secure 10.115.94.45:8000/en-US/ma	nager/appinstall/_upload		<b>A</b> 14	C	1-10-00-0-	11-1	Q.	
splunk>enterprise Apps +		H Administrator •	Messages •	Settings •	Activity •	нер▼	Find	4
Apps > Upload app								
	Restart Required							
	You must restart Splunk Enterprise to complete the update.							
	Restart Now		Restart Later					

Similarly, install the "Splunk Stream" and "URL Toolbox" apps. \*Splunk Stream is only required for IPFIX. If you just want CEF, you can skip installing Splunk Stream

### Configuring IPFIX Generation on GigaVUE node

This section details the configuration required for IPFIX solution to work with Splunk. Configuration presented in this document are for representational purposes to get the deployment working. It can be completely customized as per your requirement. Detailed information about each individual element and how to configure NetFlow generation can be found in the GigaVUE-OS CLI User's Guide. Refer to the GigaVUE-OS CLI User's Guide on the Gigamon Customer Portal.

Configuration of IPFIX generation on a GigaVUE node is a simple and straight forward process involving three major steps.

Step 1: Setup the Tunnel Tool port that would be used to export the IPFIX records to the collectorStep 2: Define the NetFlow components – Records, Monitor and ExporterStep 3: Setup the GigaSMART operation for NetFlow

For NetFlow/IPFIX generation on GigaVUE nodes, it should be noted that all the elements mentioned above should be bound to the same GigaSMART Engine Group.

The below picture illustrates the packet flow across various components inside GigaVUE node for IPFIX record generation.



This guide uses GigaVUE FM Workflow to configure IPFIX generation on GigaVUE node. Steps detailed in this guide can also be performed using the H-VUE web interface, as well as outside Workflows within Fabric Manager by selecting GigaSMART<sup>®</sup> from the left menu on the web interface. CLI configuration has also been presented in the Annexure for reference purposes.

# Configuration to generate IPFIX

### Summary of below config:

- Input traffic feed is connected to port 1/1/x1
- Tunnel is created on port 1/1/g1 which is connected to the machine(or VM) running Splunk and has the interface ip configured to 10.2.0.41
- Here, we use the destination IP 10.2.0.41 netmask 255.255.255.0 and destination port 2055

#### Tips for below config:

• SSH into the H series device to use the below config

ssh <UserName>@<IP> i.e. ssh admin@10.115.90.1

- Use the commands: "enable" and "config terminal" before you start using the below config
- Do not copy paste the entire config at once. This might cause the device to be unresponsive. Copy paste the commands in one paragraph together.

port 1/1/x1 params admin enable port 1/1/x2 type network port 1/1/g1 type tool port 1/1/g1 params admin enable

apps netflow exporter alias metadata\_exporter destination ip4addr 10.2.0.41 dscp 10 format netflow version ipfix transport udp 2055 template-refresh-interval 50 ttl 64 exit

## Gsgroup configurations apps netflow record alias dns-1 netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon dns additional-class collect add private pen gigamon dns authority-type-text collect add private pen gigamon dns bits collect add private pen gigamon dns additional-class-text collect add private pen gigamon dns identifier collect add ipv4 protocol collect add ipv4 source address collect add ipv4 destination address collect add transport tcp source-port collect add transport tcp destination-port collect add transport udp source-port collect add private pen gigamon dns ar-count collect add transport udp destination-port collect add private pen gigamon dns additional-name collect add private pen gigamon dns additional-rd-length collect add private pen gigamon dns additional-rdata collect add private pen gigamon dns additional-ttl collect add private pen gigamon dns additional-type collect add private pen gigamon dns additional-type-text collect add private pen gigamon dns an-count collect add private pen gigamon dns authority-class collect add private pen gigamon dns authority-class-text collect add private pen gigamon dns authority-name collect add private pen gigamon dns authority-rd-length collect add private pen gigamon dns authority-rdata collect add private pen gigamon dns authority-ttl collect add private pen gigamon dns authority-type match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port match add ipv4 protocol exit

apps netflow record alias dns-2 netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon dns ns-count collect add private pen gigamon dns response-rdata collect add private pen gigamon dns response-ttl collect add private pen gigamon dns op-code collect add private pen gigamon dns response-type collect add private pen gigamon dns response-type-text collect add ipv4 source address collect add ipv4 destination address collect add transport tcp source-port collect add transport tcp destination-port collect add transport udp source-port collect add private pen gigamon dns response-class-text collect add transport udp destination-port collect add ipv4 protocol collect add private pen gigamon dns qd-count collect add private pen gigamon dns query-class collect add private pen gigamon dns query-class-text collect add private pen gigamon dns query-name collect add private pen gigamon dns query-type collect add private pen gigamon dns query-type-text collect add private pen gigamon dns response-class collect add private pen gigamon dns response-code collect add private pen gigamon dns response-ipv4-addr collect add private pen gigamon dns response-ipv4-addr-text collect add private pen gigamon dns response-ipv6-addr collect add private pen gigamon dns response-ipv6-addr-text collect add private pen gigamon dns response-name collect add private pen gigamon dns response-rd-length match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port match add ipv4 protocol exit

apps netflow record alias http netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon http response-code collect add private pen gigamon http url width 249 collect add private pen gigamon http user-agent width 240 collect add transport tcp destination-port collect add transport tcp source-port collect add ipv4 destination address collect add ipv4 source address match add ipv4 destination address match add ipv4 destination address match add transport source-port match add transport destination-port

match add ipv4 protocol exit apps netflow record alias ssl netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon ssl certificate issuer collect add private pen gigamon ssl server cipher-text collect add private pen gigamon ssl server compressionMethod collect add private pen gigamon ssl certificate issuerCommonName collect add private pen gigamon ssl server nameIndication collect add private pen gigamon ssl server sessionId collect add private pen gigamon ssl server version collect add private pen gigamon ssl server version-text collect add ipv4 destination address collect add ipv4 source address collect add transport tcp source-port collect add private pen gigamon ssl certificate subjectAltName collect add transport tcp destination-port collect add private pen gigamon ssl certificate serialNumber collect add private pen gigamon ssl certificate serialNumber-text collect add private pen gigamon ssl certificate signatureAlgorithm collect add private pen gigamon ssl certificate signatureAlgorithm-text collect add private pen gigamon ssl certificate subject collect add private pen gigamon ssl certificate subjectAlgorithm collect add private pen gigamon ssl certificate subjectAlgorithm-text collect add private pen gigamon ssl certificate subjectCommonName collect add private pen gigamon ssl certificate subjectKeySize collect add private pen gigamon ssl certificate validNotAfter collect add private pen gigamon ssl certificate validNotAfter-text collect add private pen gigamon ssl certificate validNotBefore collect add private pen gigamon ssl certificate validNotBefore-text collect add private pen gigamon ssl server cipher match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port match add ipv4 protocol exit

gsgroup alias gsgrp\_netflow port-list 1/1/e1

#### ##

## Tunnel configurations
##
apps netflow monitor alias metadata\_monitor
cache timeout active 60
cache timeout inactive 15
cache timeout event transaction-end
sampling set no-sampling
port-list all

record add dns-1 record add dns-2 record add ssl record add http exit

tunneled-port 1/1/g1 ip 10.2.0.40 255.255.255.0 gateway 10.2.0.41 mtu 1500 port-list gsgrp\_netflow

## Tunnel netflow exporter configurations

tunneled-port 1/1/g1 netflow-exporter add metadata\_exporter

## Gs params configurations gsparams gsgroup gsgrp\_netflow cpu utilization type total rising 80 dedup-action drop dedup-ip-tclass include dedup-ip-tos include dedup-tcp-seq include dedup-timer 50000 dedup-vlan ignore eng-watchdog-timer 60 erspan3-timestamp format none flow-mask disable flow-sampling-rate 5 flow-sampling-timeout 1 flow-sampling-type device-ip generic-session-timeout 5 gtp-control-sample enable gtp-flow timeout 48 gtp-persistence disable gtp-persistence file-age-timeout 30 gtp-persistence interval 10 gtp-persistence restart-age-time 30 ip-frag forward enable ip-frag frag-timeout 10 ip-frag head-session-timeout 30 lb failover disable Ib failover-thres It-bw 80 lb failover-thres lt-pkt-rate 1000 lb replicate-gtp-c disable lb use-link-spd-wt disable netflow-monitor add metadata monitor resource buffer-asf disable resource cpu overload-threshold 90 resource hsm-ssl buffer disable resource hsm-ssl packet-buffer 1000 resource hsm-ssl session-count 1 sip-media timeout 30 sip-session timeout 30 sip-tcp-idle-timeout 20 ssl-decrypt decrypt-fail-action drop ssl-decrypt enable

ssl-decrypt hsm-pkcs11 dynamic-object enable ssl-decrypt hsm-pkcs11 load-sharing enable ssl-decrypt hsm-timeout 1000 ssl-decrypt key-cache-timeout 10800 ssl-decrypt non-ssl-traffic drop ssl-decrypt pending-session-timeout 60 ssl-decrypt session-timeout 300 ssl-decrypt tcp-syn-timeout 20 ssl-decrypt ticket-cache-timeout 10800 tunnel-arp-timeout 600 tunnel-health-check action pass tunnel-health-check disable tunnel-health-check dstport 54321 tunnel-health-check interval 600 tunnel-health-check protocol icmp tunnel-health-check rcvport 54321 tunnel-health-check retries 5 tunnel-health-check roundtriptime 1 tunnel-health-check srcport 54321 tunnel-ndp-timeout 600 exit

#### ##

## Gsop configurations
##
gsop alias gsop\_netflow flow-ops netflow port-list gsgrp\_netflow

## ## Traffic map connection configurations

#### ## map alias Ipfix\_Metadata\_to\_Splunk type regular byRule

type regular byRule roles replace admin to owner\_roles comment "export DNS,SSL,URL,HTTP metadata to SIEM tools like SPLUNK for analysis" use gsop gsop\_netflow rule add pass ipver 4 to 1/1/g1 from 1/1/x1 exit

# Verifying the configuration

# On Gigamon Device:

Utk-HC1	(config)	#	show	tunneled-port

Port	mac address	ip address	mask	gw	mtu	gsgroup gw status	aging time
1/1/g1 Exporte Utk-HC: % Unred Type "s Utk-HC: brief Utk-HC:	00:1D:AC:2F:27:AF er[1]:metadata_exporter L (config) # show tunne cognized command "tunne show ?" for help. L (config) # show tunne ipv4 ipv6 port s L (config) # show tunne	10.2.0.40 1-po 1-po". led-port tats led-port stats	255.255.255.0	10.2.0.41	1500	gsgrp_netflow Arp Resolved	05:55
Tunnel	port: 1/1/g1 Type :	ipv4					
	TY packata	. 501					
	IX_packets	. 370045					
	tx packate	. 270003					
	ty octets	• 998265998					
	nkts dron	· A					
	nkts drop no arn	: 0					
	okts drop wrong addr	: 0					
ARP	pres_orop_arong_oour						
	okts aro in	: 28					
	pkts arp reg in	: 15					
	pkts_arp_rep_in	: 13					
	pkts_arp_req_out	: 5360					
	pkts_arp_rep_out	: 15					
	pkts_arp_drop	: 0					
ICMP							
	pkts_icmp_in	: 473					
	pkts_ping_req_in	: 0					
	pkts_ping_resp_out	: 0					
	pkts_icmp_drop	: 0					
healt	th-check						
	pkt_health_chk_req_in	: 0					
	pkt_health_chk_req_ou	t :0					
	pkt_health_chk_rep_in	: 473					
	pkt health chk rep ou	t :0					

### On the Machine(or VM) which has a Splunk instance:

root@utkarsh-virtual-machine: /opt/splunk/bin	14	En	<b>4</b> )))	3:04 PM	1 43
root@utkarsh-virtual-machine:/opt/splunk/bin#ifconfig ens30 Link encap:Ethernet MHadd MoBioC:292:27b:25 Linet addr:10.2.0.41 Bcsst:10.2.0.235 Mask:25Link UP BROACCAF RUNNIK MULTICAST MILISIOG Metric:1 RX packets:13560807 errors:0 dropped:0 overruns:0 frame:0 TX packets:2080 errors:0 dropped:0 overruns:0 frame:0 Collisions:0 txqueuelen:1000 RX bytes:17472922351 (1.4 Gu) TX bytes:711149 (711.1 K8)					
ensio0 Link encapiEthernet HWaddr 00:00:29:23:7b:1b Inet addr:10:13:04.5 Bcc23:25.25 Maki255.255.248.0 Inet6 addr:10:13:08:194(13):288:04.25 Maki255.255.248.0 Inet6 addr:10:13:08:194(13):288 Webster addr:10:13:08:194(13):288 Webster addr:10:13:08:194(13):288 Webster addr:10:13:08:194(13):288 Webster addr:10:13:08:194(13):288 Webster addr:10:13:08 Webster a					
lo Link encaptical Loopback Inet addr:127.0.0.1 Mask:255.0.0.0 inet6 addr: ::1/128 Scope:Host UP LOOPBACK RUMNIKG MILOSS36 Metric:1 RX packets:23009800 errors:0 dropped:0 overruns:0 frame:0 TX packets:23009800 errors:0 dropped:0 overruns:0 carrier:0 Chickets:23009800 errors:0 dropped:0 overruns:0 carrier:0 RX bytes:818601064 (8.1 GB) TX bytes:8184631404 (8.1 GB)					
rootgutkarsh-virtuul-machine:/opt/splumk/bin# tcpdump -l ens36 tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on ens30, link-type EMIOMB (Ethernet), capture size 202144 bytes 15:03147.177753 IP 10.2.0.40.23304 - bio.2.0.41.20551 UDP, length 1351 15:03147.177970 IP 10.2.0.40.23304 - 10.2.0.41.20551 UDP, length 1310 unreachable, length 556 15:03147.177970 IP 10.2.0.40.23304 - 10.2.0.41.20551 UDP, length 1108					
15:03:47.178396 1P 10.2.0.40.23384 > 10.2.0.41.255: UDP, length 1296 15:03:47.178305 1P 10.2.0.40.23384 > 10.2.0.41.255: UDP, length 1141 13:03:47.380134 P1 02.2.0.40.23384 > 10.2.0.41.255: UDP, length 1212 13:03:47.380134 P1 02.2.0.40.23384 > 10.2.0.41.255: UDP, length 126 15:03:47.985149 P1 02.2.0.40.23384 > 10.2.0.41.2055: UDP, length 136 15:03:47.985133 P1 02.2.0.40.23384 > 10.2.0.41.2055: UDP, length 1376 15:03:47.985133 P1 02.2.0.40.23384 > 10.2.0.41.2055: UDP, length 1376	ets				

NOTE: the interface receiving IPFIX traffic should not be in promiscuous mode

# Setting up Splunk to ingest IPFIX – Part 1 (file level changes)

The base location of the Gigamon-specific configuration is SPLUNK\_HOME/etc/apps/GigamonMetadaForSplunk/appserver/static/library

When in the base directory, edit gigamon\_streamfwd.conf to change the reciever IP and Port to your local settings (replace @@IP and @@PORT).

tkarsh-virtual-machine: /opt/splunk/etc/apps/GigamonMetadataForSplunk/appserver/static/library
[streamfwd]
netflowReceiver.0.ip = 10.2.0.41
netflowReceiver.0.decoder = netflow
# Gigamon HTP
netflowLlement.0.enterpriseld = 20800
net low Element $\theta$ termid _ diamon bttoPeoUrl
netitowElement.o.termitu = gigamon.nttprequit
netflowElement 1 id - 2
netflowFlement 1 termid = gigamon https://tais
netflowFlement.61.enterpriseid = 26866
netflowFlement.61.id = 3
netflowElement.61.termid = gigamon.httpUserAgent
# Gigamon SSL
netflowElement.10.enterpriseid = 26866
netflowElement.10.id = 101
netflowElement.10.termid = gigamon.sslCertificateIssuerCommonName
netflowElement.11.enterpriseid = 26866
netflowElement.11.id = 102
netflowElement.11.termid = gigamon.sslCertificateSubjectCommonName
netflowElement.12.enterpriseid = 26866
netflowElement.12.id = 103
netflowElement.12.termid = gigamon.sslCertificateIssuer
netflowElement.13.enterpriseid = 26866
netflowElement.13.id = 104
netflowElement.13.termid = gigamon.sslCertificateSubject
netflowElement.14.enterpriseid = 26866
netflowElement.14.id = 105
netflowElement.14.termid = gigamon.ssiCertificateValidNotBefore
netflowElement.15.enterpriseid = 26866
netflowLlement.15.1d = 100
netflowLiement.15.termid = gigamon.ssilertificatevalidNotAfter
netflowElement.16.enterpriseta = 20800
netflowElement 16 termid - gigamon sslCertificateSerialNumber
netflowElement 17 enterpriseid - 26866
netflowFlement 17 id = 108
netflowFlement, 17. termid = gigamon, sslCertificateSignatureAlgorithm
netflowElement.18.enterpriseid = 26866
INSERT

Now the simplest approach is to just use the below commands to copy the files from base directory to Splunk's internal directories: (just copy paste the below commands on terminal when in base directory, no need to modify any file manually thereafter) \*these commands work only for ubuntu, for windows use appropriate commands to copy paste

cp gigamon\_streamfwd.conf /opt/splunk/etc/apps/splunk\_app\_stream/local/streamfwd.conf

cp gigamon\_streamfwd.conf /opt/splunk/etc/apps/Splunk\_TA\_stream/local/streamfwd.conf

cp gigamon\_vocabulary\_7.1.1.xml /opt/splunk/etc/apps/splunk\_app\_stream/default/vocabularies/gigamon.xml

cp gigamon\_vocabulary\_7.1.1.xml /opt/splunk/etc/apps/Splunk\_TA\_stream/default/vocabularies/gigamon.xml

cp gigamon\_stream.json /opt/splunk/etc/apps/splunk\_app\_stream/default/streams/netflow

### Setting up Splunk to ingest IPFIX- Part 2(within Splunk)

Now we need to Configure Stream via the steps at Stream Configuration

- 1. On the Splunk Home page, click on the app "Splunk Stream"
- 2. Use the navigation bar: **Configuration -> Configure Streams**

😑 🗣 🔹 🕞 Analytics Overview   Splank 🔹 📃 👼										
← → C O Not Secure 10.115.94.45:8000/en-US/app/sp	🗢 C 🕜 Not Secure   10.115.94.45:8000/en-US/app/splunk_app_stream/info_overview?earliest=-241%40h&latest=-now 🔄 🔹									
splunk>enterprise App: Splunk Stream -	🕒 Administrator 🕶	3 Messages •	Settings -	Activity -	Help 🔻 🛛 Find	Q				
Informational Dashboards - Admin Dashboards - Stream	m Estimate Configuration - Product Tour					STM Splu	unk Stream			
Setup Stream Run stream for the first time Collect data from this machine using Wire Data input (Splunk, Tr. Proper permissions for Splunk, TA.stream have been set. Le Collect data from other machines. Let's get started	Configure Streams Global IP Filters Distributed Forwarder Management File Server Mount Points									

3. In the top right of the dashboard, click  $\ensuremath{\textit{New Stream}}$  ->  $\ensuremath{\textit{Metadata Stream}}$ 

1.	(Full	Documentation	here)	
----	-------	---------------	-------	--

•	Configure Streams x												
÷	→ G ③ Not Secure   10.115.	94.45:800	0/en-US/	app/splur	nk_app_stre	am/streams#	#metadata						<b>☆</b> ●
s	plunk>enterprise App: Splu	Juniko-enterprise App: Splunk Stream * 😢 Administrator * 💽 Messages * Settings * Activity * Heip * Find q											
	formational Dashboards - Adn	nin Dashbo	ards <del>v</del>	Stream E	stimate	Configurati	on  Product Tour					STM Splunk	Stream
	Configure Streams												
	Create and configure streams for a variet	v of network	data protoc	cols.								new ource	
	Provide Stream												
	Metadata Streams:52	acket Strea	ams:0	Ephem	eral Strean	ns:0						- uoket obeam	_
									Avg. Traffic(	15m)			
									~ 0 B/s	5			
						Search	8						
	Name *	Actions	Mode ?			Protocol 0	Description 0			App o	Created By ©	Recent Traffic(15m)	
	amqp	Edit 🛩	Enabled	Estimate	Disabled	AMQP	AMQP Protocol Events			Stream		Disabled	
	arp	Edit 🛩	Enabled	Estimate	Disabled	ARP	ARP protocol events			Stream		Disabled	
	dhcp	Edit 🛩	Enabled	Estimate	Disabled	DHCP	DHCP Protocol Events			Stream		Disabled	
	diameter	Edit 🛩	Enabled	Estimate	Disabled	Diameter	Diameter Protocol Events			Stream		Disabled	
	dns	Edit 🛩	Enabled	Estimate	Disabled	DNS	DNS Protocol Events			Stream		Disabled	
	ftp	Edit 🛩	Enabled	Estimate	Disabled	FTP	FTP Protocol Events			Stream		Disabled	
	http	Edit 🛩	Enabled	Estimate	Disabled	HTTP	HTTP Protocol Events			Stream		Disabled	
	icmp	Edit 🛩	Enabled	Estimate	Disabled	ICMP	ICMP Protocol Events			Stream		Disabled	
	igmp	Edit 🛩	Enabled	Estimate	Disabled	IGMP	IGMP Protocol Events			Stream		Disabled	
	imap	Edit 🛩	Enabled	Estimate	Disabled	IMAP	IMAP Protocol Events			Stream		Disabled	
	ip	Edit 🗸	Enabled	Estimate	Disabled	IP	IP Flow Events			Stream		Disabled	
	irc	Edit 🛩	Enabled	Estimate	Disabled	IRC	IRC Protocol Events			Stream		Disabled	
	Idap	Edit 🛩	Enabled	Estimate	Disabled	LDAP	LDAP Protocol Events			Stream		Disabled	
	mapi	Edit 🛩	Enabled	Estimate	Disabled	MAPI	MAPI Protocol Events			Stream		Disabled	
	mysql	Edit 🛩	Enabled	Estimate	Disabled	MySQL	MySQL Database Events			Stream		Disabled	

Gigamon Metadata Application for Splunk SIEM Deployment Guide

- 4. Basic Info
  - 1. Protocol: Netflow
  - 2. Name: your source name
- 3. Click Next

Ba: Pick	sic Info a protocol and	d create your own strear	n.
Proto	ocol	HTTP ~	
Na	IGMP		
	IMAP		used as the source of the
	IP		used as the source of the
De	IRC		
	LDAP		
	MAPI		
	MySQL		
	Netflow		
	NFS		
	POP3		

#### **Basic Info**

Pick a protocol and create your own stream.

Protocol	Netflow ~
Name	Ipfix_stream The name of a stream will be used as the source of the events. It cannot be changed afterwards.
Description	

- 5. Aggregation (Full documentation here)
  - 1. Click Next to accept the default of No
- 6. Fields (Full documentation here)
  - 1. Deselect the fields that you do not want to collect
  - 2. Click Next
- 7. Filters (Full documentation here)
  - 1. Create a filter to limit the data that is collected
  - 2. Click Next

#### 8. Settings

- 1. Select an index to collect data to
- 2. Select the status
- 3. Click Next

New Metada	ata Stream	Basic Info	Aggregation	Fields	Filters	Settings	Groups	-O Done	< Next >	Cancel		
Settings Optionally, adjust Sp	olunk App for Stree	am settings.										
Index	default ~											
Status	Enabled	Disabled	Estimate									
	The 'Limate' r These tats sho	node collects ow you the an	s index volume stat mount of data that	s on stream o your Stream o	data, withou deployment	t sending the s is processing	stream data to for each prot	o your inde ocol, which	xers. I can help you configur	e stream capture and	determine your indexe	r requirements.

- 9. Groups
  - 1. Select a forwarder group (if applicable)
  - 2. Click Create Stream
- 10. Done
  - 1. Click Done

# Verifying the Setup

Search	i   Splunk 7.1.0 ×				<b>.</b>				
← → C O Not	Secure 10.115.94.45:8000/en-US/app/search/search				☆ 🕚				
splunk>enterprise App: Search & Reporting * ( Administrator * 🧕 Messages * Settings * Activity * Help * F									
Search Datase	✓ Search & Reporting >			> Search	& Reporting				
Search	Gigamon Metadata Application 🔽 For Splunk								
enter search her	Splunk Stream			Last 24 ho	urs • Q				
	Manage Apps								
No Event Sampling	Find More Apps			🕈 Sr	nart Mode 🔻				
How to Search		What to Search							
If you are not fam	lilar with the search features, or want to learn more, see one of the following resources.	10,633 Events	a few seconds ago EARLIEST EVENT	a few seconds ago					
Documentation	12 Tutorial 12	Data Summary							
> Search Histo	ry								
10.115.94.45:8000/en-US/a	pp/search								



# Configuring CEF Generation on GigaVUE node

#### Summary of below config:

- input traffic feed is connected to port 1/1/x1
- tunnel is created on port 1/1/g1 which is connected to the machine(or VM) running Splunk and has the interface IP configured to 10.2.0.41
- Here, we use the destination IP 10.2.0.41 netmask 255.255.255.0 and destination port 2055

#### Tips for below config:

• SSH into the H series device to use the below config

ssh <UserName>@<IP> i.e. ssh admin@10.115.90.1

- Use the commands: "enable" and "config terminal" before you start using the below config
- Do not copy paste the entire config at once. This might cause the device to be unresponsive. Best practice is to copy paste the commands in one paragraph together.

### Configuration to generate

port 1/1/x1 params admin enable port 1/1/x2 type network port 1/1/g1 type tool port 1/1/g1 params admin enable

apps netflow exporter alias metadata\_exporter destination ip4addr 10.2.0.41 dscp 0 format cef version 23 transport udp 514 template-refresh-interval 1800 ttl 64 exit

## Gsgroup configurations apps netflow record alias dns-1 netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon dns additional-class collect add private pen gigamon dns authority-type-text collect add private pen gigamon dns bits collect add private pen gigamon dns additional-class-text collect add private pen gigamon dns identifier collect add ipv4 protocol collect add ipv4 source address collect add ipv4 destination address collect add transport tcp source-port collect add transport tcp destination-port collect add transport udp source-port collect add private pen gigamon dns ar-count collect add transport udp destination-port collect add private pen gigamon dns additional-name collect add private pen gigamon dns additional-rd-length collect add private pen gigamon dns additional-rdata collect add private pen gigamon dns additional-ttl collect add private pen gigamon dns additional-type collect add private pen gigamon dns additional-type-text collect add private pen gigamon dns an-count collect add private pen gigamon dns authority-class collect add private pen gigamon dns authority-class-text collect add private pen gigamon dns authority-name collect add private pen gigamon dns authority-rd-length collect add private pen gigamon dns authority-rdata collect add private pen gigamon dns authority-ttl collect add private pen gigamon dns authority-type match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port

match add ipv4 protocol exit apps netflow record alias dns-2 netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon dns ns-count collect add private pen gigamon dns response-rdata collect add private pen gigamon dns response-ttl collect add private pen gigamon dns op-code collect add private pen gigamon dns response-type collect add private pen gigamon dns response-type-text collect add ipv4 source address collect add ipv4 destination address collect add transport tcp source-port collect add transport tcp destination-port collect add transport udp source-port collect add private pen gigamon dns response-class-text collect add transport udp destination-port collect add ipv4 protocol collect add private pen gigamon dns qd-count collect add private pen gigamon dns query-class collect add private pen gigamon dns query-class-text collect add private pen gigamon dns query-name collect add private pen gigamon dns query-type collect add private pen gigamon dns query-type-text collect add private pen gigamon dns response-class collect add private pen gigamon dns response-code collect add private pen gigamon dns response-ipv4-addr collect add private pen gigamon dns response-ipv4-addr-text collect add private pen gigamon dns response-ipv6-addr collect add private pen gigamon dns response-ipv6-addr-text collect add private pen gigamon dns response-name collect add private pen gigamon dns response-rd-length match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port match add ipv4 protocol exit

apps netflow record alias http netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon http response-code collect add private pen gigamon http url width 249 collect add private pen gigamon http user-agent width 240 collect add transport tcp destination-port collect add transport tcp source-port collect add ipv4 destination address collect add ipv4 source address match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port match add ipv4 protocol exit

apps netflow record alias ssl netflow-version ipfix export-blank-pen no sampling set 1 in 1 collect add private pen gigamon ssl certificate issuer collect add private pen gigamon ssl server cipher-text collect add private pen gigamon ssl server compressionMethod collect add private pen gigamon ssl certificate issuerCommonName collect add private pen gigamon ssl server nameIndication collect add private pen gigamon ssl server sessionId collect add private pen gigamon ssl server version collect add private pen gigamon ssl server version-text collect add ipv4 destination address collect add ipv4 source address collect add transport tcp source-port collect add private pen gigamon ssl certificate subjectAltName collect add transport tcp destination-port collect add private pen gigamon ssl certificate serialNumber collect add private pen gigamon ssl certificate serialNumber-text collect add private pen gigamon ssl certificate signatureAlgorithm collect add private pen gigamon ssl certificate signatureAlgorithm-text collect add private pen gigamon ssl certificate subject collect add private pen gigamon ssl certificate subjectAlgorithm collect add private pen gigamon ssl certificate subjectAlgorithm-text collect add private pen gigamon ssl certificate subjectCommonName collect add private pen gigamon ssl certificate subjectKeySize collect add private pen gigamon ssl certificate validNotAfter collect add private pen gigamon ssl certificate validNotAfter-text collect add private pen gigamon ssl certificate validNotBefore collect add private pen gigamon ssl certificate validNotBefore-text collect add private pen gigamon ssl server cipher match add ipv4 source address match add ipv4 destination address match add transport source-port match add transport destination-port match add ipv4 protocol exit

gsgroup alias gsgrp\_netflow port-list 1/1/e1

#### ##

## Tunnel configurations
##
apps netflow monitor alias metadata\_monitor
cache timeout active 60
cache timeout inactive 15
cache timeout event transaction-end

sampling set no-sampling port-list all record add dns-1 record add dns-2 record add ssl record add http exit

tunneled-port 1/1/g1 ip 10.2.0.40 255.255.255.0 gateway 10.2.0.41 mtu 1500 port-list gsgrp\_netflow

## Tunnel netflow exporter configurations

tunneled-port 1/1/g1 netflow-exporter add metadata\_exporter

## Gs params configurations gsparams gsgroup gsgrp\_netflow cpu utilization type total rising 80 dedup-action drop dedup-ip-tclass include dedup-ip-tos include dedup-tcp-seq include dedup-timer 50000 dedup-vlan ignore eng-watchdog-timer 60 erspan3-timestamp format none flow-mask disable flow-sampling-rate 5 flow-sampling-timeout 1 flow-sampling-type device-ip generic-session-timeout 5 gtp-control-sample enable gtp-flow timeout 48 gtp-persistence disable gtp-persistence file-age-timeout 30 gtp-persistence interval 10 gtp-persistence restart-age-time 30 ip-frag forward enable ip-frag frag-timeout 10 ip-frag head-session-timeout 30 lb failover disable Ib failover-thres It-bw 80 lb failover-thres lt-pkt-rate 1000 lb replicate-gtp-c disable lb use-link-spd-wt disable netflow-monitor add metadata monitor resource buffer-asf disable resource cpu overload-threshold 90 resource hsm-ssl buffer disable resource hsm-ssl packet-buffer 1000 resource hsm-ssl session-count 1 sip-media timeout 30 sip-session timeout 30 sip-tcp-idle-timeout 20

ssl-decrypt decrypt-fail-action drop ssl-decrypt enable ssl-decrypt hsm-pkcs11 dynamic-object enable ssl-decrypt hsm-pkcs11 load-sharing enable ssl-decrypt hsm-timeout 1000 ssl-decrypt key-cache-timeout 10800 ssl-decrypt non-ssl-traffic drop ssl-decrypt pending-session-timeout 60 ssl-decrypt session-timeout 300 ssl-decrypt tcp-syn-timeout 20 ssl-decrypt ticket-cache-timeout 10800 tunnel-arp-timeout 600 tunnel-health-check action pass tunnel-health-check disable tunnel-health-check dstport 54321 tunnel-health-check interval 600 tunnel-health-check protocol icmp tunnel-health-check rcvport 54321 tunnel-health-check retries 5 tunnel-health-check roundtriptime 1 tunnel-health-check srcport 54321 tunnel-ndp-timeout 600 exit

#### ##

## Gsop configurations ## gsop alias gsop\_netflow flow-ops netflow port-list gsgrp\_netflow

#### ##

## Traffic map connection configurations
##
map alias cef\_Metadata\_to\_Splunk
type regular byRule
roles replace admin to owner\_roles
comment "export DNS,SSL,URL,HTTP metadata to SIEM tools like SPLUNK for analysis"
use gsop gsop\_netflow
rule add pass ipver 4
to 1/1/g1
from 1/1/x1
exit

# Verifying the configuration

### On Gigamon Device:

Utk-HC1 (config) # show tunneled-port

Port	mac address	ip address	mask	gw	mtu	gsgroup gw status	aging time
<pre>1/1/g1 00:1D:AC:2F:27:AF 10.2.0.40 Exporter[1]:metadata_exporter Utk-HC1 (config) # show tunnel-po % Unrecognized command "tunnel-po". Type "show ?" for help. Utk-HC1 (config) # show tunneled-port brief ipv4 ipv6 port stats Utk-HC1 (config) # show tunneled-port stats</pre>			255.255.255.0	10.2.0.41	1500	gsgrp_netflow Arp Resolved	05:55
Tunnel	port: 1/1/g1 Type : :	ipv4					
	porer ryrygr Type r						
	rx_packets	: 501					
	rx_octets	: 278065					
	tx_packets	: 754869					
	tx_octets	: 990265998					
	pkts_drop	: 0					
	pkts_drop_no_arp	: 0					
	pkts_drop_wrong_addr	: 0					
ARP	10 Theory Articles, All Market, Sciences, And Sciences, Sciences, 1997, 1997.						
	pkts_arp_in	: 28					
	pkts_arp_req_in	: 15					
	pkts_arp_rep_in	: 13					
	pkts_arp_req_out	: 5360					
	pkts_arp_rep_out	: 15					
12260-02	pkts_arp_drop	: 0					
ICMP	Crazili por Compositivity de la compositivity	0.00000					
	pkts_icmp_in	: 473					
	pkts_ping_req_in	: 0					
	pkts_ping_resp_out	: 0					
0.0707022	pkts_icmp_drop	: 0					
heal	th-check						
	pkt_health_chk_req_in	: 0					
	pkt_health_chk_req_out	t :0					
	pkt_health_chk_rep_in	: 473					
	pkt_health_chk_rep_out	t :0					

# On the Machine(or VM) which has a Splunk instance:



# Setting up Splunk to ingest CEF

On Splunk web interface, click on the settings button: Under "Data" find the option "Data inputs" and select it

Home   Splunk 7.1.0	× 📼					
← ○ C ① Not Secure 10.115.94.4	45:8000/en-US/app/launcher/home					☆ 💿
splunk>enterprise		e	Administrator 🕶	3 Messages • Settings •	Activity • Help • Find	٩
Apps     C       Apps     C       Search & Reporting     G       Gigamon Metadata     Application For Splunk       STM     Splunk Stream       + Find More Apps     H	Explore Splunk Enterprise Product Tours New to Splunk? Takes a tour to help you on your way.	Add Data Add Data Add or forward data to S Enterprise. Afterwards, yo extract fields.	Add Data	XNOWLEDGE Searches, reports, and alerts Data models Event types Tags Fields Lookups User Interface Alert actions Advanced search All configurations Server settings Server controls Instrumentation Licensing	DATA Data Data Data Forwarding and receiving Indexes Report acceleration summaries Virtual indexes Source types Distributed Environment Indexer clustering Forwarder management Distributed search USERS AND AUTHENTICATION Access controls	×

Add a new UDP input under Local inputs

🛡 🔍 🥟 Data inputs - Settings   Splunk × 🛌									
← → C ① Not Secure 10.115.	94.45:8000/en-US/manager/launcher/datainputstats						☆ 💿		
splunk>enterprise Apps -		🕕 Administrator 🕶	3 Messages ▼	Settings   Activ	ity 🕶 Help 🕶	Find	Q,		
Data inputs Set up data inputs from files and direct	tories, network ports, and scripted inputs. If you want to set up forwarding and receiv	ing between two Splunk ins	stances, go to For	warding and receiving.					
L	ocal inputs								
	Туре	In	nputs	Actions					
	Files & Directories Index a local file or monitor an entire directory.	6		+ Add new					
	HTTP Event Collector Receive data over HTTP or HTTPS.	1		+ Add new					
	TCP Listen on a TCP port for incoming data, e.g. syslog.	0		+ Add new					
	UDP Listen on a UDP port for incoming data, e.g. syslog.	0		+ Add new	<b>(</b>				
	Scripts Run custom scripts to collect or generate more data.	7		+ Add new					
	Wire data Passively capture wire data from network traffic.	1		+ Add new					
	PCAP Files Upload pcap data for indexing.	0		+ Add new					
F	orwarded inputs								
10.115.94.45:8000/en-US/manager/launcher/ad	Turnen Iddata/selectsource?input_type=udp&input_mode=1	In	nputs	Actions					

514 is the port number used. Change it to whatever the port number desired. Make sure that it matches with port number configuration on GigaSMART device.

▲ ● ● ● ▲ > Add Data - Select Source   So × ● <ul> <li></li></ul>										
splunk>enterprise A	spps ▼		🕕 Admini	strator 👻 🧿 🛚	Messages 🕶 Settings 🕶 A	Activity - Help - Fir	id Q,			
	Add Data Select Sou	ce Input Settings Revie	w Done	< Back	Next >					
	Files & Directories Upload a file, index a local file, or monitor an entire directory.	Configure this instance to (such as syslog). Learn Mo	Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as sysiog). Learn More 12							
	HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.			TCP	UDP					
	TCP / UDP >	Por	t ? 514 Example: 5	14						
	Scripts Get data from any API, service, or database with a script.	Source name override	cef							
	Wire data Passively capture wire data from network traffic.	Only accept connecti from	on optional example: 10	).1.2.3, Ibadhost.splu						
	PCAP Files Uploed pcap data for Indexing.	FAQ								
		> How should I configure	Splunk for sy	slog traffic?						
		> What's the difference b	etween receiv	ving data over TC	P versus UDP?					
		<ul> <li>&gt; Can I collect syslog dat</li> <li>&gt; What is a source type?</li> </ul>	a from Windo	ws systems?						
10.115.94.45:8000/en-US/manager/la	suncher/adddata/selectsource?input_type=udp&input_mode=1#	_		_	_	_	-			
← C ① Not Secure	10.115.94.45:8000/en-US/manager/launcher/adddata/inputset	lings					☆ ⊙			
splunk>enterprise A	pps ▼		Administ	trator 👻 🧿 M	essages 🕶 Settings 🕶 Act	tivity 🕶 Help 🕶 Find	Q			
	Add Data	Input Settings Review	-O	< Back Rev	view >					
	Input Settings									
	Optionally set additional input parameters for this data input	as follows:								
	Source type									
	all incoming data. It tells blunk what kind of data you've go	t, so	Select	New						
	it's a way to categorize your data, so that you can search it e	Nasily.	cefev	ents •						
				_						
	App context	piter			q					
	Application contexts are folders within a Splunk instance the contain configurations for a specific use case or domain of o	it Appli lata. A Data	base		on For Splunk (Gigam •					
	App contexts improve manageability of input and source typ definitions. Splunk loads all app contexts based on precede	nce Emai	1		E					
	rules. Learn More 12	Metri	ics		E					
	Host	Misc	ellaneous		E.					
	When Splunk indexes data, each event receives a "host" val	ue. Netw	rork & Security	1	E.					
	the event originates. The type of input you choose determine	les Struc	tured		F					
	the available configuration options. Learn More 12	Unca	tegorized		✓ cefevents	🦕				
	Index	Web			).					
	Splunk stores incoming data as events in the selected index Consider using a "sandbox" index as a destination if you har problems determining a source type for your data. A sandb index lets you troubleshoot your configuration without impa production indexes. You can always chance this settina late	r. ve Ind ox cting r.	ex Defau	ult • Create a	new index					
10.115.94.45:8000/en-US/manager/la	uncher/adddata/inputsettings#									

🗧 🔍 💿 Add Data - Input Settings   Sin X					
splunk>enterprise Apps	11594.45/30/00/en-US/manager/iauncher/adddata/mputsettings 🛠 👔				
	Add Data O (Back Review >				
	Input Settings Optionally set additional input parameters for this data input as follows:				
	Source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And It's a way to categorize your data, so that you can search it easily.				
	App context Application configurations for a specific use case or domain of data. App Context App contexts improve manageability of input and source type definitions. Splunk loads all app contexts based on precedence rules. Learn More 12				
	Host When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More 12				
	Index Splunk stores incoming data as events in the selected index. Consider using a "sandbac" index as a destination if you have Index Index Index To Default  Create a new index Index Ites you roubleshoot your configuration without impacting production indexes. You can always change this setting later.				



# Verifying the Setup

🗟 🗣 🔊 > Search   Splunk 7.10 🛛 🛪 💼						
← C () Not Secure 10.115.94.45.8000/en-US/app/search/search (************************************						
splunk>enterprise App: Search & Reporting •	🕒 Administrator 🕶 📀 Messages 🕶 Settings 💌 Activity 👻 Help 💌 Find 🔍					
Search Datase 🗸 Search & Reporting >	Search & Reporting					
Gigamon Metadata Application 🖸 For Splunk						
enter search her	Last 24 hours 👻 📿					
Manage Apps						
No Event Sampling Find More Apps	¥ Smart Mode ♥					
How to Search	What to Search					
If you are not familiar with the search features, or want to learn more, see one of the following resources.	10,633 Events a few seconds ago a few seconds ago INDEXED EARLEST EVENT LATEST EVENT					
Documentation (2) Tutorial (2)	Data Summary					
> Search History						
10.115.94.45:8000/en-US/app/search						

🛎 🗣 🖉 🔊 Metsdata Overview   Splant 💿 📩							
🗧 🔗 C 🕐 Not Secure   10.115.94.45-8000/en-US/app/GigamonMetadataForSplunk/Overview?form.time_restriction.earliest=-1d%40d&form.time_restriction.latest=now 🔅						ጵ 💿	
splunk>enterprise App: Gigamon Metadata Application For Splu	•	🕒 Administrator 🕶	2 Messages 🕶	Settings -	Activity 👻 H	elp 🕶 🛛 Find	Q
Metadata Overview Metadata Dashboards - About Administ	ation - Splunk -					Gigan	non®
Metadata Overview Time Window Last 1 day • Hide Filters		load up			Edit	Export •	
SSL Versions Seen	1542	Top HTTP Error Codes Switching Service Un Moved Per Request No	lee Other Protocols Modified available Timeout of Content		Found		
Top DNS Error Responses Server refused to answer for the query Server function consisted and DNS request		List of DNS Servers Seen Domain Resolvers \$		State ¢			count ¢
	Domán name does not exit	1.1.1.1		Unknown			10
		10.10.1.19		Unknown			8
		10.10.1.20		Trusted			13296
		10.10.1.34		Unknown			10
		10.12.8.156		Unknown			2
		182.19.95.67		Unknown			6
		182.19.95.95		Unknown			8

### Summary

This document described the integration between Splunk SIEM and Gigamon's GigaSECURE Security Delivery Platform. By leveraging metadata, Splunk users can benefit by gaining increased non-intrusive visibility into their infrastructure while minimizing the amount of data that has to be searched through which, in turn, reduces the time to detect suspicious threats and anomalous behavior.

### Appendix

## Use cases available with Gigamon's custom metadata elements

SSL Widgets				
Widget	What YouSee	What You Infer		
SSL Versions Seen	Shows different SSL versions seen in the network and their percentage. Current valid versions are TLSv1, TLSv1.1, TLSv1.2 & SSLv3.	<ul> <li>Percentage of connections (if any) running obsolete SSL versions (SSLv2, SSLv3).</li> <li>Security compliance posture of the organization.</li> <li>List of servers hosted on non-compliant version.</li> </ul>		
SSL Domains Accessed on Non- Standard Ports	Default port for SSL transaction is 443 but SSL transaction is seen on ports other than configured/allowed port list.	<ul> <li>Server misconfiguration.</li> <li>Non-compliance.</li> <li>Server/resources are compromised.</li> </ul>		
Top SSL Certificate Issuers	Shows the top Certificate issuers for a given time range.	<ul> <li>Are those certificates known &amp; trusted</li> <li>Drill down to see source IPs using unknown certificates.</li> </ul>		
Top SSL Cipher	Shows the top Ciphers seen in the network for a given time range.	<ul> <li>Only configured Ciphers should be seen.</li> <li>Drill down to see source IPs using non- complaint ciphers.</li> </ul>		
SSL Self Signed Certificates	Lists all the self-signed certificates seen in the network.	• Determine whether the self-signed certificates are expected or not.		
SSL Certificate Distribution	Shows the heat map of SSL certificates geographic location.	<ul> <li>Geographic location of SSL certificate origin.</li> </ul>		

DNS Widgets			
Widget	What YouSee	What You Infer	
List of DNS Servers Seen	List of DNS servers seen in the network.	<ul> <li>List of DNS servers matches with expected configured list.</li> <li>Unknown DNS servers could be due to misconfiguration or Rouge DNS server.</li> </ul>	
Top DNS Error Responses	Lists the top DNS error responses seen and their percentage.	<ul> <li>Status code seen are expected or not.</li> <li>Timeline of the status code.</li> </ul>	
Top 10 DNS Queries	Liststop DNS Queries seen in the network for a given time period.	• Lists shows DNS query name, source and destination IP addresses, whether the query was successful or not and average TTL values.	
DNS Traffic on Non- Standard Ports	DNS Query traffic seen on non-standard port. Standard port for DNS Query is 53.	<ul> <li>DNS service ran on non-standard ports.</li> <li>Some other service (ex. LDAP) ran on DNS port.</li> </ul>	
Non-DNS Traffic on DNS Port (53)	This widget should be empty.	<ul> <li>One should not see non-DNS traffic on the standard DNS port 53.</li> <li>There should not be any entries in this widget. If you see any entries in this widget then there is misconfiguration.</li> </ul>	
DNS Query Name Entropy	List of DNS domain names with Shannon Entropy values sorted from higher to lower value.	• The higher the entropy value, the higher the chance that the domain name is not valid. By using the entropy values, admins can determine whether a botnet or some kind of command-and-control is making random domain name queries.	
Number of DNS Requests Over the Time	Line graph of DNS requests over a period of time.	One can determine whether requests are sent to primary or secondary DNS server and time when the switchover has happened from primary to secondary or vice-versa.	

URL Widgets					
Widget	What YouSee		What You Infer		
Top HTTP Error Responses	HTTP/HTTPS status codes for the whole network and their percentage.	•	Status code seen are expected. Timeline of the status code.		
TOP URL Domains Visited	PiecharttopURLdomains seen for a given time range.	•	Top URL domains are valid and expected.		
Top URL Domains Visited by Client IP	Lists top URL domains visited by client IP addresses.	•	Top URL domains are valid and expected Drill down to see src & destination IP addresses.		
URL Domain Entropy (Shannon Entropy)	List of URL domain names with Shannon Entropy values sorted from higher to lower value.	•	The higher the entropy value, the higher the chance that the URL domain name is not valid. By using the entropy values, admins can determine whether a botnet or some kind of command-and-control is making random domain name queries.		
Top Domains Visited on Non- Standard Ports	Lists URL domains visited using ports other than port 80(for GTTP) and 443 (for HTTPS).	•	HTTP and HTTPS servers running on non- standard ports. How many HTTP/HTTPS servers running on same servers using different port numbers. Compliance of the servers.		
Count of URLs Accessed using Domain Name vs IP Address	Lists count of URLs accessed using Domain name vs using direct IP addresses.	•	Lists count of URLs accessed using Domain name vs using direct IP addresses.		