Gigamon Metadata Application for IBM QRadar Deployment Guide

Document Revised: 6/19/2018

Table of Contents

Overview

Today's Security Operations Center (SOC) depends heavily on the ability to collect, correlate and analyze network events to quickly identify and respond to security threats – but getting access to the right traffic data from across the network, and without overloading the system, can be a challenge.

Metadata is data that provides information about other data. In a security context, this is especially useful because security appliances are looking for the "needle in the haystack"; that is, to identify the one single sequence of threat packets or flows from the entire mass of network flows.

A key benefit of metadata is minimizing the amount of data that has to be searched through which, in turn, reduces the time to detect suspicious threats and anomalous behavior. The GigaSECURE Security Delivery Platform is the ideal platform for generating this metadata because it taps the network and extracts the relevant information at high speeds with high fidelity. In doing so, there is no impact to the users, devices, applications, or network appliances. The generated metadata is packaged in IPFIX format and exported to IBM QRadar SIEM for further analysis.

IBM QRadar is a Security Information and Event Management (SIEM) solution that provides insight into machine data generated from a wide variety of sources. Of course, to fully utilize the power of this platform, users need to be able to help ensure that the right data from across their network is available – and can be easily indexed within the IBM QRadar platform.

This document describes how to set up IBM QRadar to ingest custom IPFIX metadata elements generated by the Gigamon GigaSECURE® Security Delivery Platform. Additionally, this document also describes how to install the Gigamon Metadata Application for IBM QRadar.

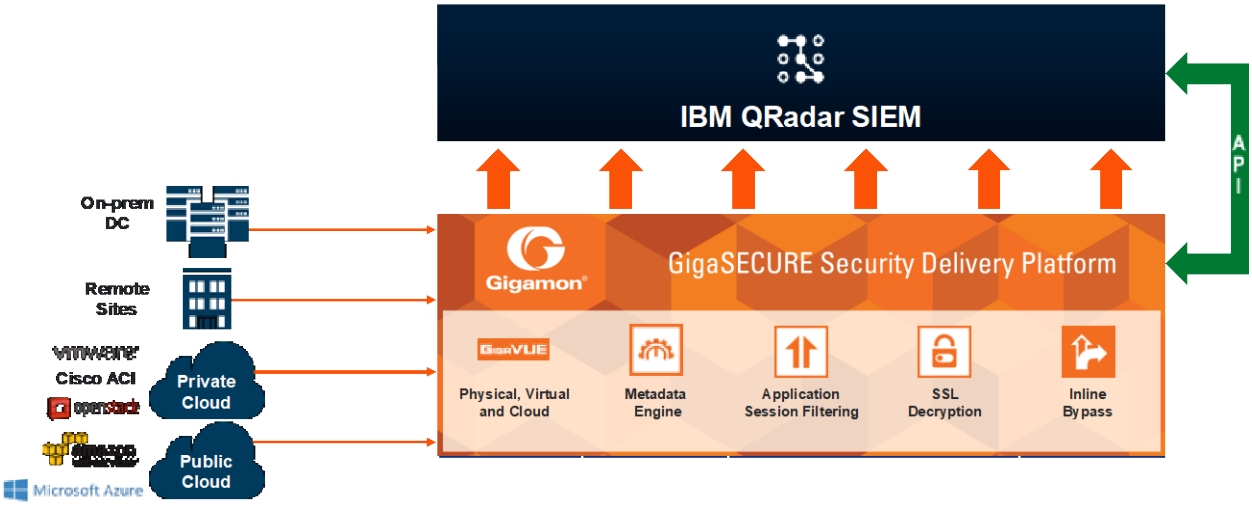


Figure 1: Gigamon GigaSECURE Security Delivery Platform and IBM QRadar SIEM

Gigamon Metadata Application for IBM QRadar

The Gigamon Metadata Application for IBM QRadar allows customers to extract, index and display network metadata generated by the GigaSECURE Security Delivery Platform. The application comes packaged with custom flow properties, saved searches and dashboards that allow integration of Gigamon's IPFIX metadata with IBM QRadar SIEM.

The Gigamon GigaSECURE Security Delivery Platform allows users to extract and consolidate metadata from monitored network traffic flows, package them into NetFlow IPFIX records, then send them to collectors like IBM QRadar SIEM for indexing and analysis. Gigamon has enriched the IPFIX 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 IBM QRadar. This document expects users to be familiar with IBM QRadar administration, installation of additional IBM QRadar components, administrative permissions to restart services and edit configuration files.

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

Requirements

The following are the prerequisites for setting up the IPFIX record generation on GigaVUE nodes:

- GigaVUE node must be running GigaVUE-OS 5.2 or later
- GigaVUE-FM used for managing the GigaVUE node must be running software version 5.2 or later
- GigaVUE node must contain GigaSMART card for NetFlow/IPFIX generation
- Valid NetFlow / IPFIX Generation license must be installed on the GigaVUE node

The solution detailed in this deployment guide has been validated with:

- IBM QRadar SIEM version 7.2.8, updated with latest patch (7.2.8.20180416164940).
- Gigamon IPFIX Metadata Application for QRadar version 1.0, which can be downloaded from the IBM Security App Exchange: https://www.ibm.com/security/community/app-exchange

Notes

Refer to the following notes on GigaVUE nodes running GigaVUE-OS 5.2.

- NetFlow/IPFIX records are exported using IPv4 only. IPv6 is not supported.
- Maximum of five records can be added to a single monitor with all the records having the 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

Operational Flow

The operational flow of the Gigamon Metadata Application for IBM QRadar is as follows:

1) Traffic arrives into a Gigamon node
2) The node is configured to consume the traffic and generate metadata information. This configuration includes *records* for the traffic of interest (DNS, SSL, HTTP, etc.). the node is a NetFlow/metadata exporter.
3) The IBM QRadar instance running the Gigamon Metadata Application for QRadar is setup as a collector, requiring it's IP address and UDP port where the metadata will be sent to.
4) The metadata, contained in IPFIX format, is sent to the QRadar instance where it is ingested by the QRadar Flow Collector.
5) Ingested data is then extracted into Custom Properties by use of Regular Expressions.
6) The Custom Properties are then used to write complex queries and build dashboards that will render the data into meaningful stories.

Figure 2 illustrates the configuration detailed in this guide. Traffic tapped from the various points across the network are fed to the network port of GigaVUE node where IPFIX records are be generated and exported via the tunnel port and sent to the collector.

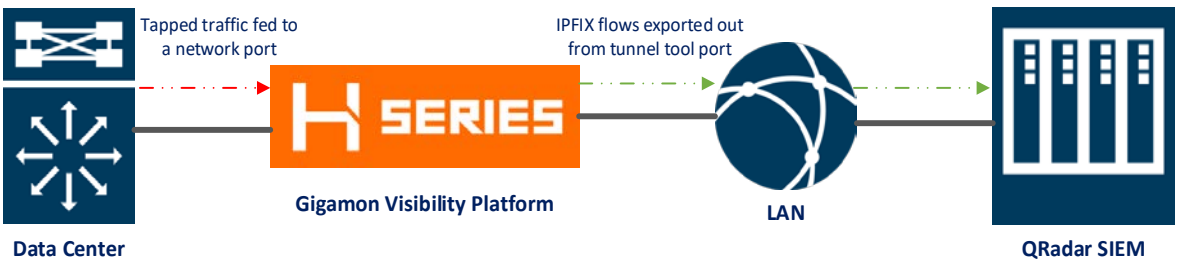


Figure 2: IPFIX Solution Logical Diagram

Configuring IPFIX Generation on GigaVUE node

This section details the configuration required for IPFIX solution to work with IBM QRadar. 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.

Configuring the IPFIX Record

When configuring the IPFIX Record on Gigamon, you must:

1. Ensure the below mentioned collect fields are present in at least one of the records you export.

```
collect add timestamp sys-uptime first
collect add timestamp sys-uptime last
collect add counter bytes long
collect add counter packets long
collect add ipv4 source address
collect add ipv4 destination address
collect add ipv4 protocol
collect add transport source-port
collect add transport destination-port
collect add transport tcp flags ack enable cwr enable ece enable fin enable psh
enable rst enable syn enable urg enable
```

2. Ensure you do not collect the same field in multiple records apart from the first eight mandatory fields mentioned above. Failing to do so would cause QRadar to display the field multiple times or display an aggregated value in case of Byte or Packet count.

   Below is a sample configuration used during solution validation. Records have been split based on the protocols with no overlapping collect fields. DNS meta-data has been split into two records to ensure QRadar places fields in appropriate payloads.

```
apps netflow record alias QRadar_IPFIX_IPV4
  description "IPFIX Record with IPV4 Elements (Base Record)"
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add counter bytes long
  collect add counter packets long
  collect add timestamp sys-uptime first
  collect add timestamp sys-uptime last
  collect add timestamp flow-start-sec
  collect add timestamp flow-end-sec
  collect add timestamp flow-start-msec
```

```
  collect add timestamp flow-end-msec
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add ipv4 protocol
  collect add ipv4 version
  collect add transport source-port
  collect add transport destination-port
  collect add transport tcp flags ack enable cwr enable ece enable fin enable
psh enable rst enable syn enable urg enable
  match add ipv4 source address
  match add ipv4 destination address
  match add ipv4 protocol
  match add ipv4 version
  match add transport tcp source-port
  match add transport tcp destination-port
  match add transport udp source-port
  match add transport udp destination-port
  exit
!
!
apps netflow record alias QRadar_IPFIX_HTTP
  description "IPFIX Record with HTTP Elements"
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add ipv4 protocol
  collect add transport source-port
  collect add transport destination-port
  collect add timestamp sys-uptime first
  collect add timestamp sys-uptime last
  collect add private pen gigamon http url
  collect add private pen gigamon http response-code
  match add ipv4 source address
  match add ipv4 destination address
  match add ipv4 protocol
  match add ipv4 version
  match add transport tcp source-port
  match add transport tcp destination-port
  match add transport udp source-port
```

```
  match add transport udp destination-port
  exit
!
!
apps netflow record alias QRadar_IPFIX_SSL
  description "IPFIX Record with SSL Elements"
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add ipv4 protocol
  collect add transport source-port
  collect add transport destination-port
  collect add timestamp sys-uptime first
  collect add timestamp sys-uptime last
  collect add private pen gigamon ssl certificate serialNumber
  collect add private pen gigamon ssl certificate signatureAlgorithm-text
  collect add private pen gigamon ssl certificate subjectAlgorithm-text
  collect add private pen gigamon ssl certificate subjectKeySize
  collect add private pen gigamon ssl certificate subjectAltName
  collect add private pen gigamon ssl certificate issuerCommonName
  collect add private pen gigamon ssl certificate subjectCommonName
  collect add private pen gigamon ssl certificate issuer
  collect add private pen gigamon ssl certificate subject
  collect add private pen gigamon ssl certificate validNotBefore
  collect add private pen gigamon ssl certificate validNotAfter
  collect add private pen gigamon ssl server nameIndication
  collect add private pen gigamon ssl server version-text
  collect add private pen gigamon ssl server cipher-text
  collect add private pen gigamon ssl server compressionMethod
  collect add private pen gigamon ssl server sessionId
  match add ipv4 source address
  match add ipv4 destination address
  match add ipv4 protocol
  match add ipv4 version
  match add transport tcp source-port
  match add transport tcp destination-port
  match add transport udp source-port
  match add transport udp destination-port
  exit
```

```
!
!
apps netflow record alias QRadar_IPFIX_DNSQuery
  description "IPFIX Record with DNS Query Elements"
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add ipv4 protocol
  collect add transport source-port
  collect add transport destination-port
  collect add timestamp sys-uptime first
  collect add timestamp sys-uptime last
  collect add private pen gigamon dns bits
  collect add private pen gigamon dns identifier
  collect add private pen gigamon dns op-code
  collect add private pen gigamon dns qd-count
  collect add private pen gigamon dns query-name
  collect add private pen gigamon dns query-class-text
  collect add private pen gigamon dns query-type-text
  match add ipv4 source address
  match add ipv4 destination address
  match add ipv4 protocol
  match add ipv4 version
  match add transport tcp source-port
  match add transport tcp destination-port
  match add transport udp source-port
  match add transport udp destination-port
  exit
!
!
apps netflow record alias QRadar_IPFIX_DNSResponse
  description "IPFIX Record with DNS Response Elements"
  netflow-version ipfix
  export-blank-pen no
  sampling set 1 in 1
  collect add ipv4 source address
  collect add ipv4 destination address
  collect add ipv4 protocol
  collect add transport source-port
```

```
collect add transport destination-port
collect add timestamp sys-uptime first
collect add timestamp sys-uptime last
collect add private pen gigamon dns an-count
collect add private pen gigamon dns ar-count
collect add private pen gigamon dns ns-count
collect add private pen gigamon dns response-ipv4-addr
collect add private pen gigamon dns response-ipv6-addr
collect add private pen gigamon dns response-code
collect add private pen gigamon dns response-name
collect add private pen gigamon dns response-type-text
collect add private pen gigamon dns response-class-text
collect add private pen gigamon dns response-ttl
collect add private pen gigamon dns response-rd-length
collect add private pen gigamon dns authority-name
collect add private pen gigamon dns authority-type-text
collect add private pen gigamon dns authority-class-text
collect add private pen gigamon dns authority-ttl
collect add private pen gigamon dns authority-rd-length
collect add private pen gigamon dns additional-name
collect add private pen gigamon dns additional-type-text
collect add private pen gigamon dns additional-class-text
collect add private pen gigamon dns additional-ttl
collect add private pen gigamon dns additional-rd-length
match add ipv4 source address
match add ipv4 destination address
match add ipv4 protocol
match add ipv4 version
match add transport tcp source-port
match add transport tcp destination-port
match add transport udp source-port
match add transport udp destination-port
exit
```

Configuring the IPFIX Exporter

Follow the standard process to define the IPFIX exporter. For IBM QRadar to work properly, it is recommended that you set the Template Refresh Interval to 60.

Setting up IBM QRadar for IPFIX

Installing the IBM QRadar SIEM

Refer to the official IBM QRadar installation guide for installing the IBM QRadar SIEM. Ensure the latest patch is applied on your setup. This information in this deployment guide is presented based on IBM QRadar version 7.2.8 with patch 7.2.8.20180416164940.

Defining the Gigamon Private IPFIX Elements

The Gigamon private elements can be defined on QRadar by appending the below mentioned lines to the conf file "`/opt/qradar/conf/IPFIXFields.conf`". CLI access to the console is required to perform this operation.

```
## GIGAMON Private Enterprise Element Definition
26866,1,HTTP_URL,STRING,1
26866,2,HTTP_RespCode,INT,1
26866,101,CERT_IssuerCname,STRING,1
26866,102,CERT_SubjectCname,STRING,1
26866,103,CERT_Issuer,STRING,1
26866,104,CERT_Subject,STRING,1
26866,105,CERT_ValidFrom,STRING,1
26866,106,CERT_ValidTo,STRING,1
26866,107,CERT_SerialNo,HEX,1
26866,108,CERT_SignatureAlgo,STRING,1
26866,109,CERT_SubjectAlgo,STRING,1
26866,110,CERT_SubjectKeySize,INT,1
26866,111,CERT_SubjectAltName,STRING,1
26866,112,SERVER_SNI,STRING,1
26866,113,SERVER_Version,INT,1
26866,114,SERVER_Cipher,INT,1
26866,115,SERVER_CompressionMethod,INT,1
26866,116,SERVER_SessionId,HEX,1
26866,117,CERT_SignatureAlgoTxt,STRING,1
26866,118,CERT_SubjectAlgoTxt,STRING,1
26866,119,SERVER_CipherTxt,STRING,1
26866,120,SERVER_VersionTxt,STRING,1
26866,201,DNS_ID,HEX,1
26866,202,DNS_OPCODE,INT,1
26866,203,DNS_RespCode,INT,1
26866,204,DNS_QueryName,STRING,1
26866,205,DNS_RespName,STRING,1
26866,206,DNS_RespTTL,INT,1
```

```
26866,207,DNS_RespIPv4,IPV4,1
26866,208,DNS_RespIPv6,IPV6,1
26866,209,DNS_Bits,STRING,1
26866,210,DNS_QdCt,INT,1
26866,211,DNS_AnCt,INT,1
26866,212,DNS_NsCt,INT,1
26866,213,DNS_ArCt,INT,1
26866,214,DNS_QueryType,INT,1
26866,215,DNS_QueryClass,INT,1
26866,216,DNS_RespType,INT,1
26866,217,DNS_RespClass,INT,1
26866,218,DNS_RespRdlen,INT,1
26866,219,DNS_RespRdata,STRING,1
26866,220,DNS_AuthName,STRING,1
26866,221,DNS_AuthType,INT,1
26866,222,DNS_AuthClass,INT,1
26866,223,DNS_AuthTTL,INT,1
26866,224,DNS_AuthRdlen,INT,1
26866,225,DNS_AuthRdata,STRING,1
26866,226,DNS_AddName,STRING,1
26866,227,DNS_AddType,INT,1
26866,228,DNS_AddClass,INT,1
26866,229,DNS_AddTTL,INT,1
26866,230,DNS_AddRdlen,INT,1
26866,231,DNS_AddRdata,STRING,1
26866,232,DNS_QueryTypeTxt,STRING,1
26866,233,DNS_QueryClassTxt,STRING,1
26866,234,DNS_RespTypeTxt,STRING,1
26866,235,DNS_RespClassTxt,STRING,1
26866,236,DNS_AuthTypeTxt,STRING,1
26866,237,DNS_AuthClassTxt,STRING,1
26866,238,DNS_AddTypeTxt,STRING,1
26866,239,DNS_AddClassTxt,STRING,1
```

Updating the Private Enterprise ID Definition

To reduce the length of Gigamon field names and to optimize the storage requirements, it is recommended to update the PEN ID name from "Gigamon Systems LLC" to "Gigamon" in the "`/opt/qradar/conf/iana-pen.conf`" file.

```
[root@sol-qradar conf]# cat iana-pen.conf | grep 26866
26866,Gigamon,Ted Ho,ted.ho&gigamon.com
[root@sol-qradar conf]#
```

Figure 3: Updating the PEN ID

Configuring the Maximum Content Capture Size

Increase the size of Maximum Content Capture to a large value to allow maximum content to be captured from the flows. To update the Maximum Content Capture size:

1. Go to System and License Management in the Admin tab.
2. In the pop-up window, select the host and choose Edit Host option from Deployment Actions.
3. Click on the Component Management setting gear.
4. Edit the Maximum Content Capture value found under the Flow Collector in the pop-up window.

Note: Editing this value has both performance and storage implications. A value of 3000 was set during the validation but this value can be changed based on the environment.

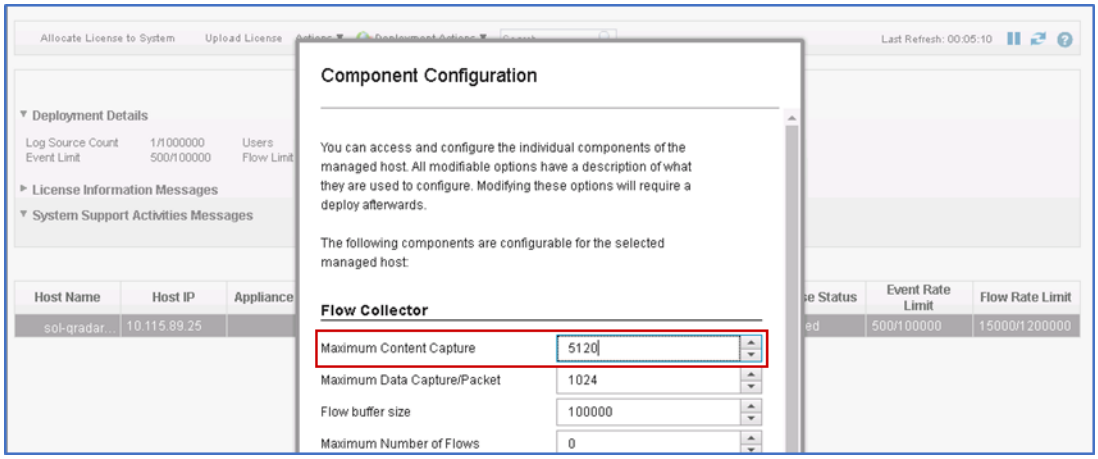


Figure 4: IBM QRadar Component Configuration Window

Configuring the Flow on QRadar

To configure QRadar to accept IPFIX flow traffic, you must add a NetFlow/IPFIX flow source as follows:

1. Login into the QRadar Console via web browser.
2. Click the Admin tab.
3. On the navigation menu, click Data Sources. The Data Sources pane is displayed.
4. On the navigation menu, click Flows. The Flows pane is displayed.

5. Click the Flow Sources icon. The Flow Sources window is displayed.
6. Click Add. The Add Flow Source window is displayed. You may edit the default flow or add a new one using the options presented.
7. Once done, go back to Admin tab and click Deploy Changes.

Note: The monitoring interface should be set to ANY in the flow configuration.

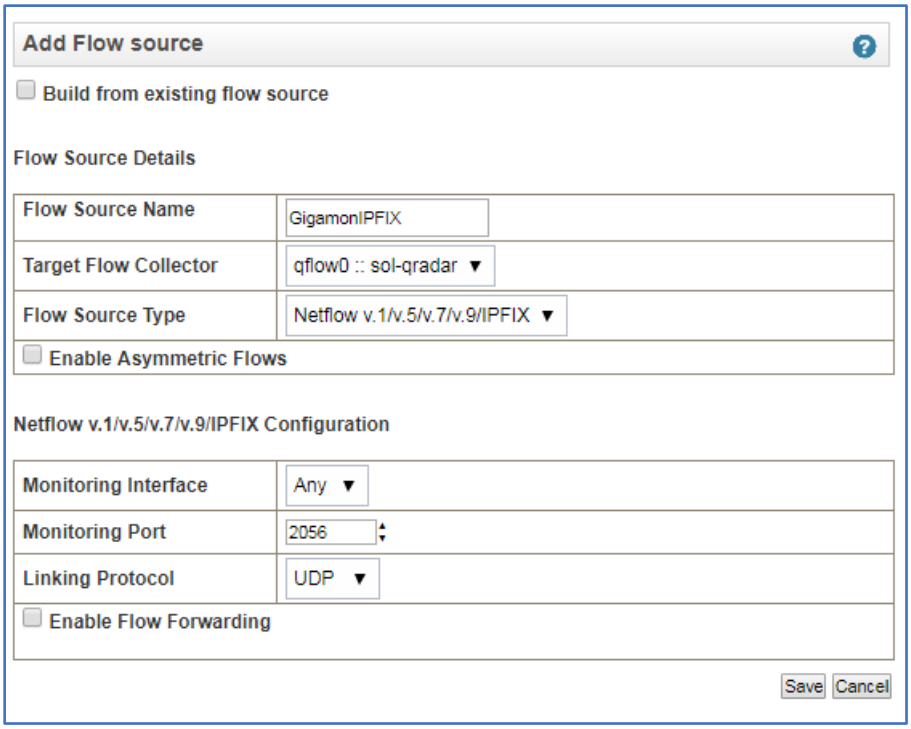


Figure 5: IBM QRadar Add Flow Source Window

Installing the Gigamon Metadata Application for IBM QRadar

The Gigamon Metadata Application for IBM QRadar bundles custom flow properties and dashboard that allows QRadar to extract Gigamon Private meta-data elements from an IPFIX record and transform the data into charts and tables. To install the application:

1. Login into the QRadar Console via web browser.
2. Click the Admin tab.
3. On the navigation menu, click Extensions Management. A pop-up will be displayed.
4. Click on Add on top right corner to add a new extension.
5. Click Browse in the pop-up and select the Gigamon application zip file.
6. Once added, select the application and click Install.

Upon completion of all the above steps, restart the process to let changes take effect. Go to the CLI and issue command "`service hostcontext restart`".

Note: IBM QRadar allows integration with third party tools and feeds to enhance the flow data

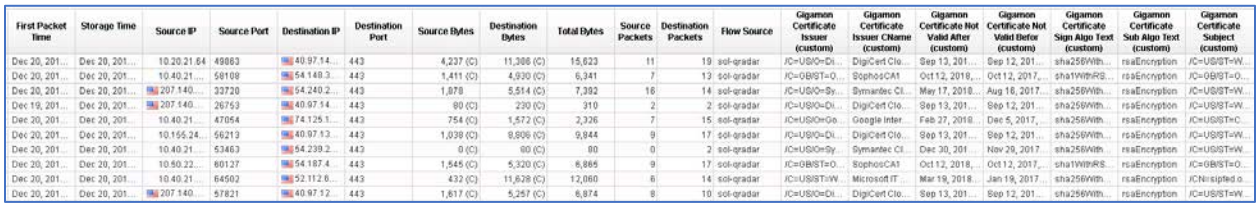
available for analysis. Saved searches as part of this app leverage IBM Threat Intelligence Application to classify and categorize IP addresses and domains. To enable this feature, you may need to download and install the IBM Threat Intelligence Application from IBM APP Exchange. Once installed, enable the Threat Intelligence Application Functions by going to System Settings under the Admin tab and select YES for the Enable X-Force Threat Intelligence Feed. Click Deploy Changes under the Admin tab once done.

Verifying the Setup

To verify the setup, ensure you have IPFIX records being exported from the Gigamon node. On QRadar, use the below commands to verify:

- To verify qflow process is running, use `service qflow0 status`
- To verify port is open and in listening state, use `netstat -an | grep <port-num>`
- To verify traffic is received on the QRadar machine, use `tcpdump -i <iface>`

Once the above is verified, you may login into the web browser and navigate to the Network Activity tab. IPFIX records should keep flowing in this window as shown below. The window has column view customized to show the metadata elements which can be done by creating a new search and selecting the required columns.



First Packet Time	Storage Time	Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Flow Source	Gigamon Certificate Issuer (custom)	Gigamon Certificate Issuer CName (custom)	Gigamon Certificate Not Valid After (custom)	Gigamon Certificate Not Valid Befor (custom)	Gigamon Certificate Sign Algo Text (custom)	Gigamon Certificate Sub Algo Text (custom)	Gigamon Certificate Subject (custom)
Dec 20, 201...	Dec 20, 201...	10.20.21.64	49883	40.97.14...	443	4,237 (C)	11,306 (C)	15,623	11	19	sol-qradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.40.21....	58108	54.148.3...	443	1,411 (C)	4,930 (C)	6,341	7	13	sol-qradar	/C=GB/ST=O...	SophosCA1	Oct 12, 2018,...	Oct 12, 2017,...	sha1WithRS...	rsaEncryption	/C=GB/ST=O...
Dec 20, 201...	Dec 20, 201...	207.140....	33720	54.240.2...	443	1,878	5,514 (C)	7,392	16	14	sol-qradar	/C=US/O=Sy...	Symantec Cl...	May 17, 2018...	Aug 16, 2017...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 19, 201...	Dec 20, 201...	207.140....	26753	40.97.14...	443	80 (C)	230 (C)	310	2	2	sol-qradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.40.21....	47054	74.125.1...	443	754 (C)	1,572 (C)	2,326	7	15	sol-qradar	/C=US/O=Go...	Google Inter...	Feb 27, 2018...	Dec 5, 2017,...	sha256With...	rsaEncryption	/C=US/ST=C...
Dec 20, 201...	Dec 20, 201...	10.155.24...	56213	40.97.13...	443	1,039 (C)	9,805 (C)	9,844	9	17	sol-qradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.40.21....	53463	54.239.2...	443	0 (C)	80 (C)	80	0	2	sol-qradar	/C=US/O=Sy...	Symantec Cl...	Dec 30, 201...	Nov 29, 2017...	sha256With...	rsaEncryption	/C=US/ST=W...
Dec 20, 201...	Dec 20, 201...	10.50.22....	60127	54.187.4...	443	1,545 (C)	5,320 (C)	6,866	9	17	sol-qradar	/C=GB/ST=O...	SophosCA1	Oct 12, 2018,...	Oct 12, 2017,...	sha1WithRS...	rsaEncryption	/C=GB/ST=O...
Dec 20, 201...	Dec 20, 201...	10.40.21....	64502	52.112.6...	443	432 (C)	11,628 (C)	12,060	6	14	sol-qradar	/C=US/ST=W...	Microsoft IT ...	Mar 19, 2018...	Jan 19, 2017...	sha256With...	rsaEncryption	/CN=sipfed.o...
Dec 20, 201...	Dec 20, 201...	207.140....	57821	40.97.12...	443	1,617 (C)	5,257 (C)	6,874	8	10	sol-qradar	/C=US/O=Di...	DigiCert Clo...	Sep 13, 201...	Sep 12, 201...	sha256With...	rsaEncryption	/C=US/ST=W...

Figure 6: Network Metadata Elements

Click on the pause button on top right corner and double click on any record to view the complete record with all the extracted properties and respective source and destination payload.

The application comes with a few pre-defined searches and dashboards that users could leverage. This can be accessed by going to the Dashboard tab and selecting any one of the three Gigamon dashboards. Below are sample screens for each of the dashboards.

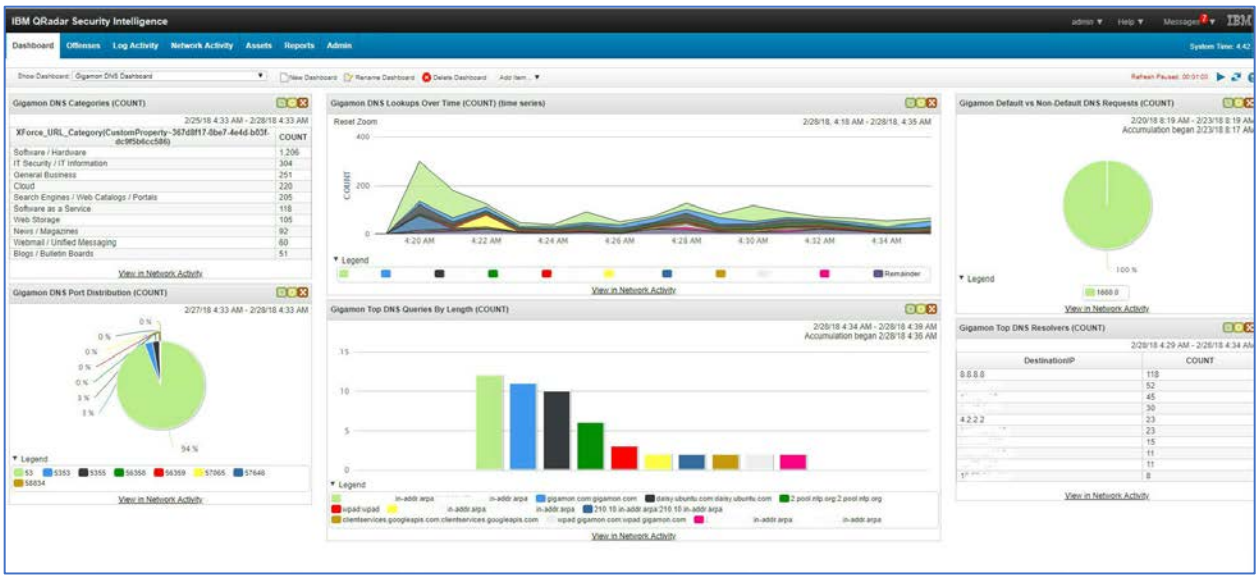


Figure 7: Gigamon DNS Dashboard

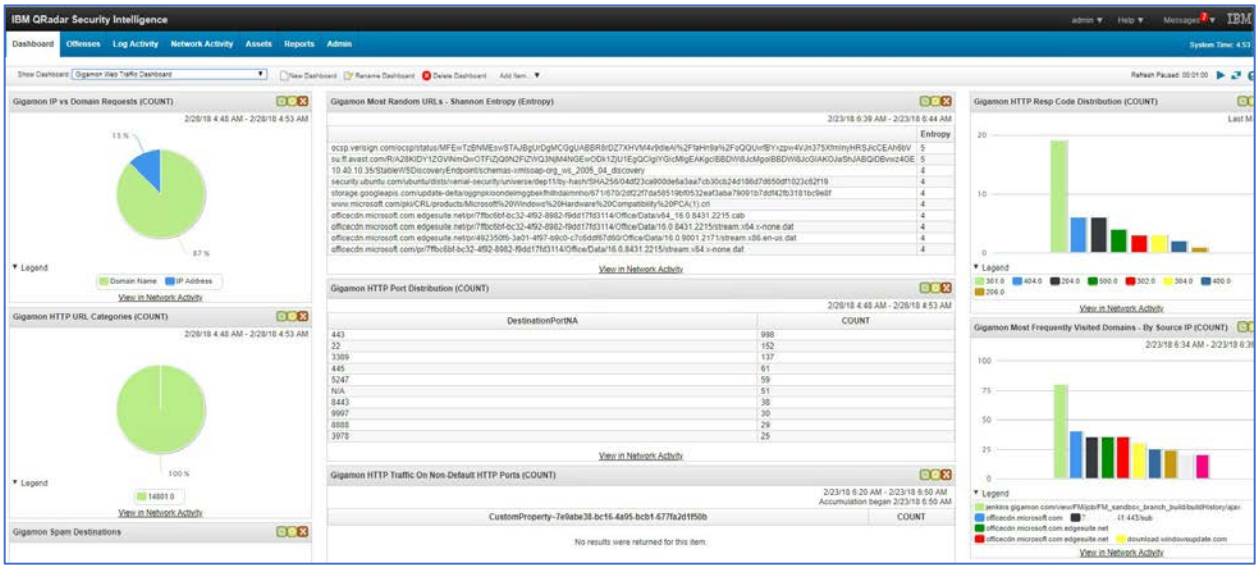


Figure 8: Gigamon Web Traffic Dashboard

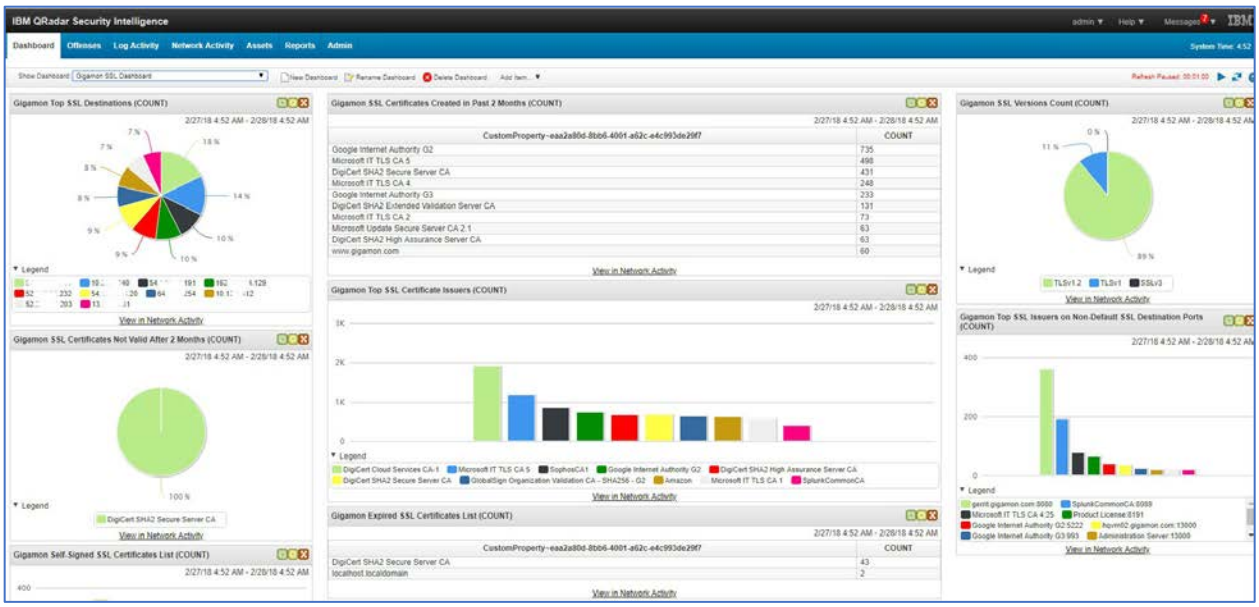


Figure 9: Gigamon SSL Metadata Dashboard

Note: By default, all the graphs are shown for the last minute in these dashboards. To extend the time range, select a graph and click on the settings gear, check the Capture Time Series Data check box and save it. You will need to open the search in Network Activity using the View in Network Activity" option present beneath the chart and click Save Criteria. Choose Recent in the timespan options and click OK. Now navigate back to the dashboards tab and you will see the graph show historical data.

Deployment Caveats

The following are the few known caveats observed in IBM QRadar:

- Record Aggregation—IBM QRadar aggregates flows based on five tuple information for every minute and this applies to IPFIX flows as well. When two distinct transaction happen within a minute with same five tuple information, this will be aggregated, and summarized flow will be presented in QRadar. For instance, if there are 2 DNS resolutions happening within a minute for two different domains but use the same source port, Gigamon would export two IPFIX records but QRadar would aggregate them into one record.
- Multi-collect Resource Record—Gigamon supports exporting data from multiple DNS resource records which as on date is not supported by QRadar. When exporting multiple fields in the IPFIX record, QRadar will process the first value and drop the others.

Summary

This document described the integration between IBM QRadar SIEM and Gigamon's GigaSECURE Security Delivery Platform. By leveraging metadata, QRadar 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 You See**	**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.	• Percentage of connections (if any) running obsolete SSL versions (SSLv2, SSLv3). • Security compliance posture of the organization. • List of servers hosted on non-compliant version.
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.	• Server misconfiguration. • Non-compliance. • Server/resources are compromised.
Top SSL Certificate Issuers	Shows the top Certificate issuers for a given time range.	• Are those certificates known & trusted • Drill down to see source IPs using unknown certificates.
Top SSL Cipher	Shows the top Ciphers seen in the network for a given time range.	• Only configured Ciphers should be seen. • Drill down to see source IPs using non-complaint ciphers.
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.	• Geographic location of SSL certificate origin.

DNS Widgets		
Widget	**What You See**	**What You Infer**
List of DNS Servers Seen	List of DNS servers seen in the network.	• List of DNS servers matches with expected configured list. • Unknown DNS servers could be due to misconfiguration or Rouge DNS server.
Top DNS Error Responses	Lists the top DNS error responses seen and their percentage.	• Status code seen are expected or not. • Timeline of the status code.
Top 10 DNS Queries	Lists top 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.	• DNS service ran on non-standard ports. • Some other service (ex. LDAP) ran on DNS port.
Non-DNS Traffic on DNS Port (53)	This widget should be empty.	• One should not see non-DNS traffic on the standard DNS port 53. • There should not be any entries in this widget**.** If you see any entries in this widget then there is misconfiguration.
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 You See**	**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	Pie chart top URL domains 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.