

IBM® QRadar® Security Information and Event Management (SIEM) helps security teams accurately detect and prioritize threats across the enterprise, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents. By consolidating log events and network flow data from thousands of devices, endpoints and applications distributed throughout your network, QRadar correlates all this different information and aggregates related events into single alerts to accelerates incident analysis and remediation. QRadar SIEM is available on premises and in a cloud environment.

NeuVector is a full lifecycle container security platform which fully supports QRadar integration. This integration enables QRadar to be able to collect events, logs and incident information for container and Kubernetes environment. By using NeuVector's DSM for QRadar, customers will be able to normalize the NeuVector security log data in QRadar, then analyze, report or remediate container security events.

### **How to Integrate NeuVector with QRadar**

Before importing the NeuVector DSM into QRadar, we recommend you check/modify these QRadar configurations to make sure everything will work as expected:

- IBM QRadar version 7.3.1 and later:

# IBM QRadar

v7.3.1 Build 20171206222136

Tuning template is Enterprise

[Additional Release Information...](#)

- Configure QRadar “System Settings” to make sure the Syslog Payload Length is big enough for example:

**System Settings** ⚠ No changes have been made.

System Settings

Administrative Email Address	root@localhost
Alert Email From Address	QRADAR@localhost.localdomain
Email Locale	English
Max Email Attachment Size (KB)	15,360
Delete Root Mail	Yes
Temporary Files Retention Period	6 hours
Asset Profile Query Period	1 day (default)
Coalescing Events	Yes
Store Event Payload	Yes
Global Iptables Access (comma separated)	
Syslog Event Timeout (minutes)	720
Partition Testers Timeout (seconds)	30
Max UDP Syslog Payload Length	8,192
Max TCP Syslog Payload Length	16,384
Max Number of TCP Syslog Connections	2,500
Max TCP Syslog Connections Per Host	10
Timeout for Idle TCP Syslog Connections (seconds)	900
Log and Network Activity Data Export Temporary Directory	/store/exports
Display Country/Region Flags	Yes
Display Embedded Maps in IP Address Tooltips	Yes
Enable X-Force Threat Intelligence Feed	No

Switch to: **Basic**

Database Settings

User Data Files	/store/users/
Accumulator Retention - Minute-hv-Minute	1 week (default)

## Configure NeuVector to Send Syslog to QRadar

Enable Syslog configuration in Settings -> Configuration. The Server IP/URL and port should be pointing to the QRadar service IP and Port, and the default Syslog port will be 514. Use the UDP protocol and “In Json” log format. Select the log level and categories to report. In a multi-cluster NeuVector environment, to collect all clusters logs, this setting needs to be enabled in every cluster. You can configure the cluster name on this page to distinguish cluster events from each other.

**Syslog** ON

Server \* 192.168.86.243

Protocol UDP

Port \* 514

Level Info

Categories: ☒ Event ☒ Security event ☒ Risk reports

In Json: ☒

## Configure QRadar to Analyze NeuVector Logs

- Enable or Import the NeuVector DSM to QRadar

When adding a new QRadar log source, if “NeuVector” appears in the QRadar log source type, then please ignore the log source importing instructions below and take the next step “Add and enable log sources for NeuVector”.

**Add a log source**

Log Source Name

Log Source Description

Log Source Type

Protocol Configuration

Log Source Identifier

Enabled ☒

If the “NeuVector” log source type was not found in QRadar, please refer to QRadar user manual to install NeuVector DSM via Admin > Extension Management.

**Extensions Management**

Search by extension name

**ALL ITEMS** | **INSTALLED** | **NOT INSTALLED**

Name	Status
IBM QRadar Pre-v	Installed
App Authorization	Installed
QRadar Assistant	Installed
QRadar Log Source Management	Installed

**Add a New Extension**

From local storage:

☐ Install immediately

- Add and enable log sources for NeuVector

Now we can add a new log source for NeuVector logs:

Log Sources - Google Chrome

Not secure | 192.168.86.243/console/do/sem/maintainSensorDevice?dispatch=edit&appName=eventviewer&p

### Edit a log source

Log Source Name	NeuVector Log Source
Log Source Description	NeuVector Logs
Log Source Type	NeuVector
Protocol Configuration	Syslog
Log Source Identifier	neuvector-allinone-pod-ky
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: qradar3
Coalescing Events	<input checked="" type="checkbox"/>
Incoming Payload Encoding	UTF-8
Store Event Payload	<input checked="" type="checkbox"/>
Log Source Language	
Log Source Extension	NeuVectorCustom_ext

Please select any groups you would like this log source to be a member of:

Save Cancel

“Log Source Identifier” should be the lead controller’s pod name. NeuVector’s lead controller’s pod name can be found in the raw log data of QRadar or from NeuVector’s management console “Assets\Controllers” as below:

Dashboard

Network activity

Assets

- Platforms
- Nodes
- Containers
- Registries
- Controllers

### Controllers

3 controllers found

Filter...

Name	IP	Status	Version	Le...
neuvector-controller-pod-5b6c45fb59-g49b2	10.24.1.4	Connected	v3.2.2	
neuvector-controller-pod-5b6c45fb59-j7a2d	10.24.5.5	Connected	v3.2.2	
neuvector-controller-pod-5b6c45fb59-pwxf	10.24.6.4	Connected	v3.2.2	

Multiple log sources should be added if there are multiple NeuVector clusters running.

NeuVector log source is added and enabled:

Log Sources - Google Chrome											
Not secure   192.168.86.243/console/do/core/genericsearchlist?appName=eventviewer&pagel=SensorDeviceList&columnSorting=true&orderBy=deviceName&sorting=asc&hasSearched=false&searchcondition=&searchvalue=&pageNumber=1&queryId=											
Search For: Group All Log Source Groups Go Add Edit Enable/Disable Delete Bulk Actions Extensions Planning Order Assign											
Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Destination	Credibility	Autodiscovered	Last Event Time
NeuVector Log Source	NeuVector Logs	Success	Syslog		NeuVector	True	enabled	eventcollector...	5	False	Feb 2, 2009, 1...
Creation Date	Modification Date	Average EPS (Last Minute)									
Jan 22, 2009, 1...	Feb 2, 2009, 1...	N/A									

Verify the Log Activities

Generate some NeuVector logs, for example Network Policy Violations, Configuration change events or do some Vulnerability Scans on containers/nodes. These incident or event logs will be sent to QRadar in seconds. And the NeuVector logs should be normalized in QRadar console. It can also be verified through QRadar’s DSM editor:

Log Source Type

NeuVector

Change

Properties

Event Mappings

Configuration

Filter

+

Action

Text Custom

aggregation\_from

Text Custom

Applications

Text Custom

applications0

Text Custom

client\_domain

Text Custom

client\_id

Text Custom

client\_image

Text Custom

Workspace

Use sample event payloads to help fine tune the behavior of this Log Source Type. Matches in the payload are highlighted when a property is selected. Note: System properties that have not been overridden cannot be highlighted in the workspace.

☒ Wrap Content

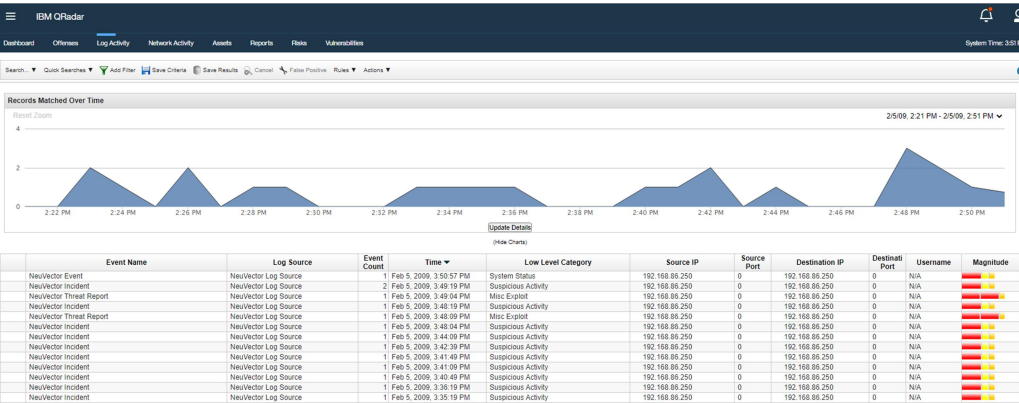
<132>1 2020-08-18T17:10:26Z neuvector-allinnone-pod-kwldf /usr/local/bin/controller 6793 neuvector - {"notification": "incident", "name": "Process.Profile.Violation", "level": "Warning", "reported\_timestamp": 1597770622, "reported\_at": "2020-08-18T17:10:22Z", "cluster\_name": "cluster.master.allinnone", "host\_id": "servv-ubt18-3015640788C-E648-BE65-72B8-e16735940AB6", "host\_name": "servv-ubt18-30", "enforcer\_id": "a2997f2299a72a87059796dcb154bb672154669143e31c2ad62855a8dad273a", "enforcer\_name": "neuvector-allinnone-pod-kwldf", "id": "c5f2f4a7-995b-4cff-bc58-1cea42483020", "workload\_id": "830d4e9fa0effba2ff27c08db4feea1aa5c507c6c0da2fe6d0ab8659897ff", "workload\_name": "calico-node-rqbs-c", "workload\_domain": "k8s-gcr.io/pause:3.14.0", "workload\_service": "calico-node.kube-system", "proc\_name": "iptables-legacy", "proc\_path": "/usr/sbin/iptables-legacy-multi", "proc\_cmd": "iptables-legacy-save -t nat", "proc\_effective\_user": "root", "client\_ip": "", "server\_ip": "", "client\_port": 0, "server\_port": 0}

Log Activity Preview

A preview of the payloads in the Workspace as they would appear in the Log Activity viewer using the current configuration.

Action (custom)	aggregation_from (custom)	Applications (custom)	applications0 (custom)	Client Name (custom)	client_domain (custom)	client_id (custom)	client_image (custom)	cli
violate	1597770622							
		[DNS]	DNS	node-pod-6c0550b445-9yb9	demo	7d052e3ba01a964c	k8s gcr.io/pause:3.1	17:
		[DNS]	DNS	node-pod-6c0550b445-9yb9	demo	7d052e3ba01a964c	k8s gcr.io/pause:3.1	17:

Save Close



Integration Summary

With the completed integration, NeuVector security and management events can be managed through QRadar together with event data from other sources. QRadar serves as the permanent event storage for NeuVector events, while the NeuVector controller performs real-time security

responses and short-term cluster storage for events. QRadar can perform advanced correlation and alerting for critical container and Kubernetes security events.