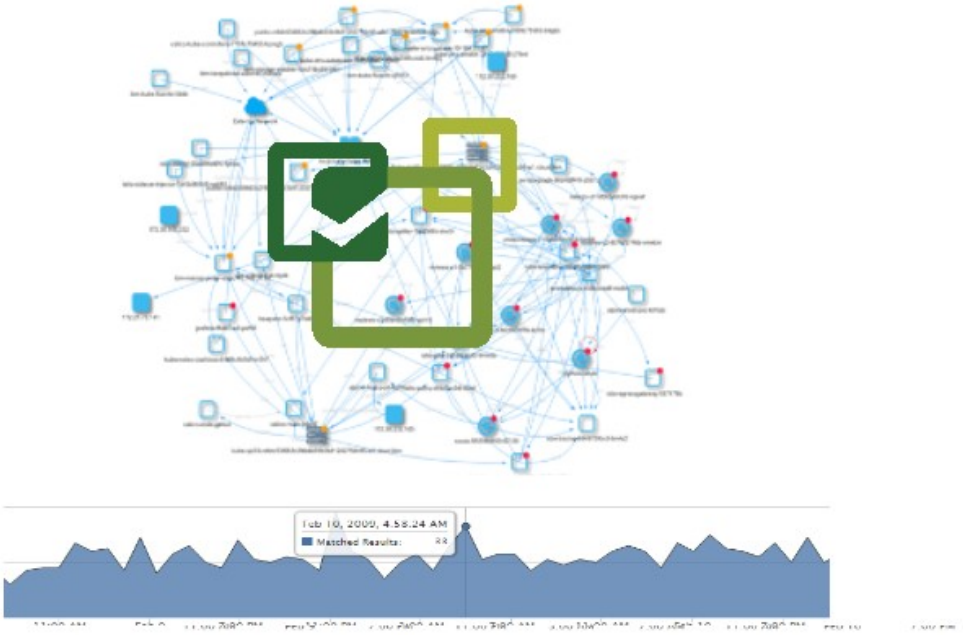


IBM® QRadar® Security Information and Event Management (SIEM) helps security teams accurately detect and prioritize threats across the enterprise, and it provides intelligent insights that enable teams to respond quickly to reduce the impact of incidents. By consolidating log events and network flow 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.

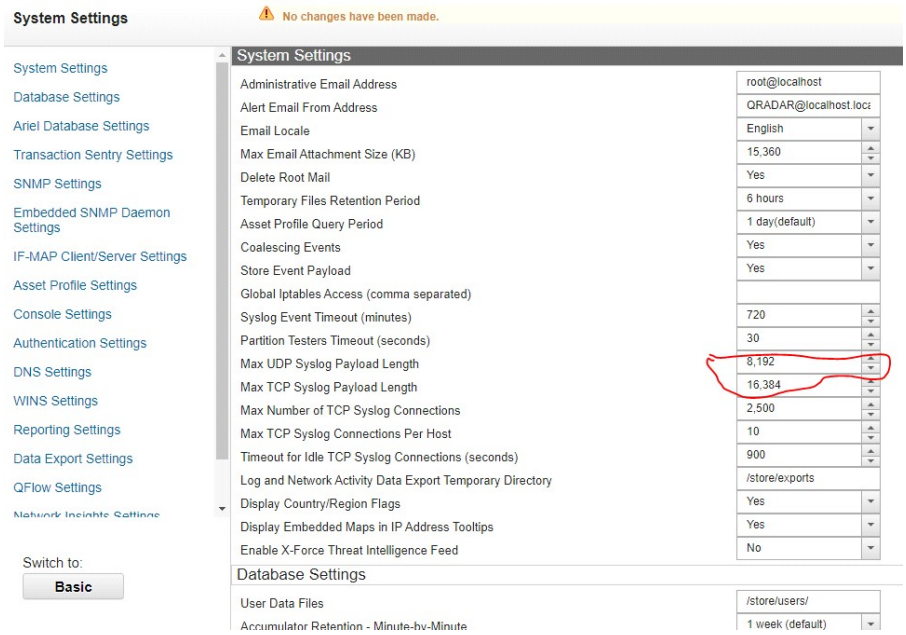
NeuVector is a full lifecycle container security platform which fully supports QRadar integration. This integration enables QRadar to be able to collect events, logs and incident information for container and Kubernetes environment. By using NeuVector's DSM for QRadar, customers will be able to normalize 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:

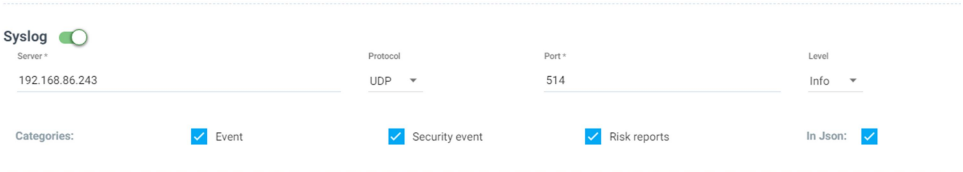
- IBM QRadar version 7.3.1 and later:

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



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.

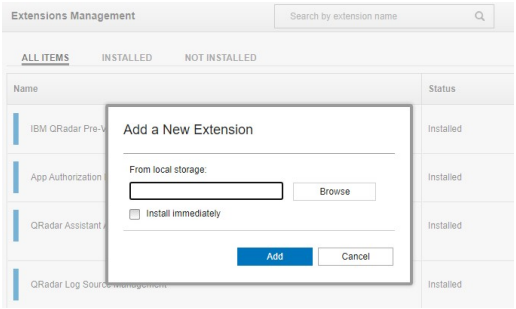


Configure QRadar to Analyze NeuVector Logs

- Enable or Import the NeuVector DSM to QRadar

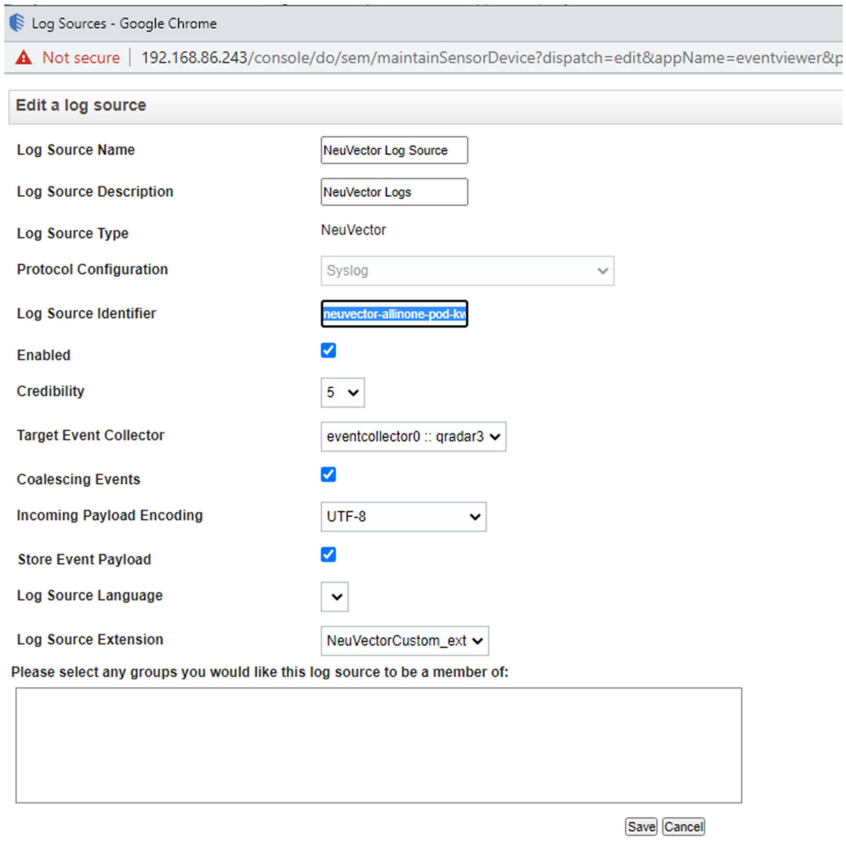
  When adding a new QRadar log source, if “NeuVector” appears in the QRadar log source type, then please ignore the log source importing instructions below and take the next step “Add and enable log sources for NeuVector”.

  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.



- Add and enable log sources for NeuVector

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



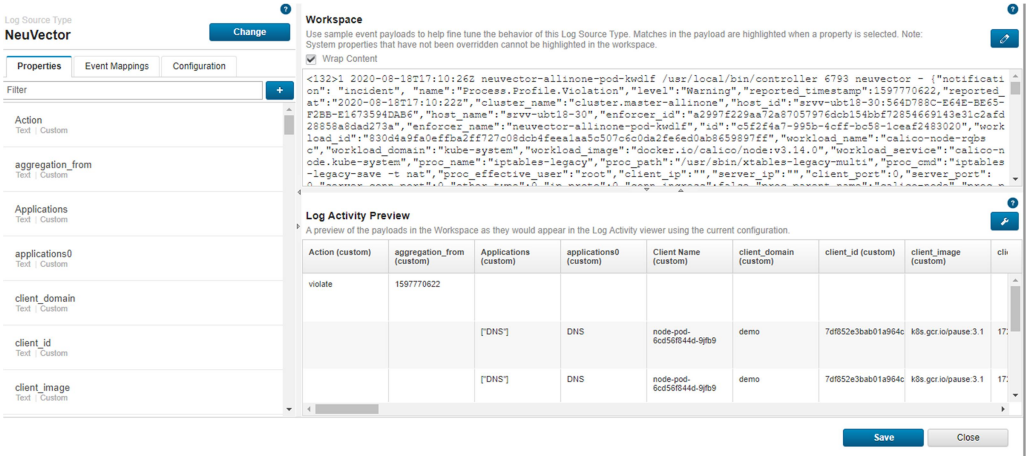
"Log Source Identifier" should be the lead controller's pod name. NeuVector's lead controller's pod name can be found in the raw log data of QRadar or from NeuVector's management console "Assets\Controllers" as below:

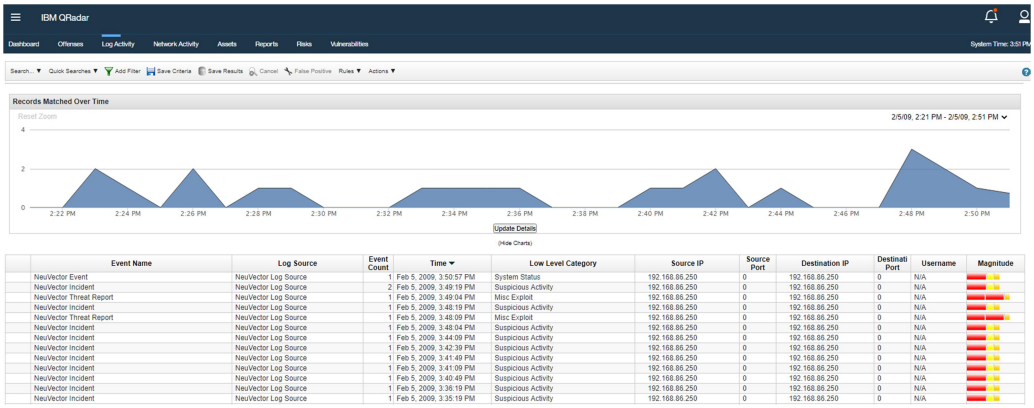
Multiple log sources should be added if there are multiple NeuVector clusters running.

NeuVector log source is added and enabled:

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:





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.