QRadar Searches

Jack Radigan
Principal Security Sales Specialist

IBM **Security**

Agenda

Quick Filter Searches	5
Basic Searches	9
Indexed Properties	12
Advanced Searches	17
Resources	22

Types of Searches

Quick Filter

- Full text search of event or flow payloads using the Lucene index engine
- Fastest search and easy to learn

Basic Search

- Uses event or flow properties
- Very easy to use, and to get into trouble (painfully slow search execution)

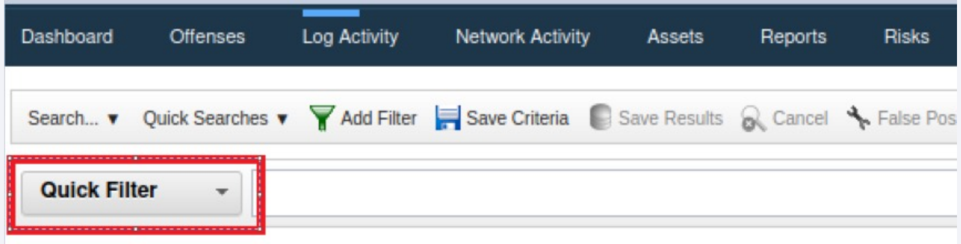
Advanced Search

- Uses Ariel Query Language (AQL)
- Most powerful, but takes time to learn and use effectively

QRadar Searches

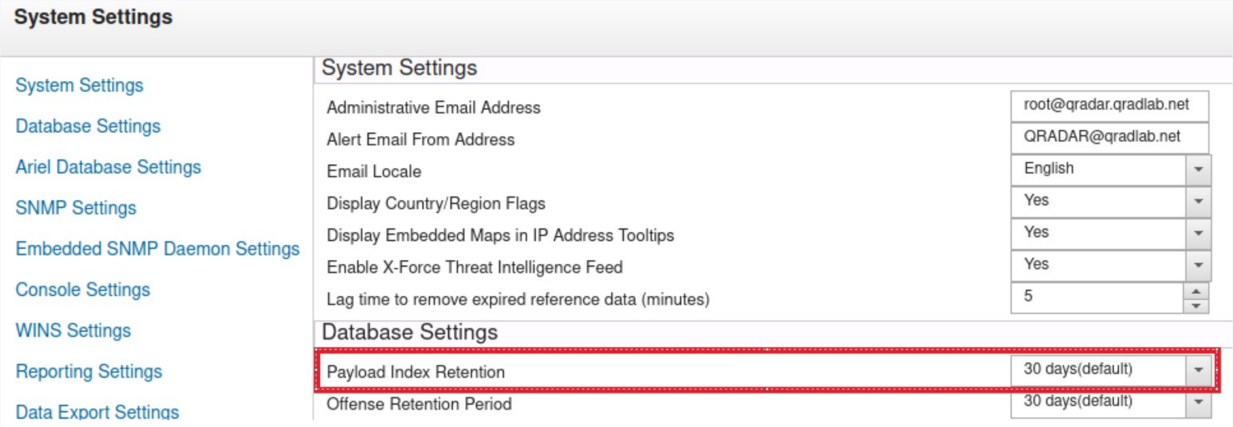
Quick Filter Searches

Quick Filter



The Quick Filter is one of the fastest methods to search event and flow information that contains specific data by using a full-text index of payloads. Use Quick Filter in combination with other filers to accelerate searches.

Payload Retention Index Settings



System Settings

- System Settings
- Database Settings
- Ariel Database Settings
- SNMP Settings
- Embedded SNMP Daemon Settings
- Console Settings
- WINS Settings
- Reporting Settings
- Data Export Settings

System Settings

Administrative Email Address	root@qradar.qradlab.net
Alert Email From Address	QRADAR@qradlab.net
Email Locale	English
Display Country/Region Flags	Yes
Display Embedded Maps in IP Address Tooltips	Yes
Enable X-Force Threat Intelligence Feed	Yes
Lag time to remove expired reference data (minutes)	5

Database Settings

Payload Index Retention	30 days(default)
Offense Retention Period	30 days(default)

The minimum retention period is 1 day, and the maximum period is 2 years.

Quick Filter Examples

`Session* AND NOT SessionToken`

- Boolean operators; AND, OR, NOT must be uppercase
- Alternate: `Session* -SessionToken`

`“firewall accept” AND (admin OR nobody)`

- Terms with spaces must be enclosed in double-quotes

`/.*.pdf/ OR /.*.exe/`

- Regular expressions are defined within a pair of forward slashes

`/.*\^.*\..*/ OR \*END\*`

- Special characters must be escaped with a backslash

`+ - && || ! ( ) { } [ ] ^ " ~ * ? : \ .`

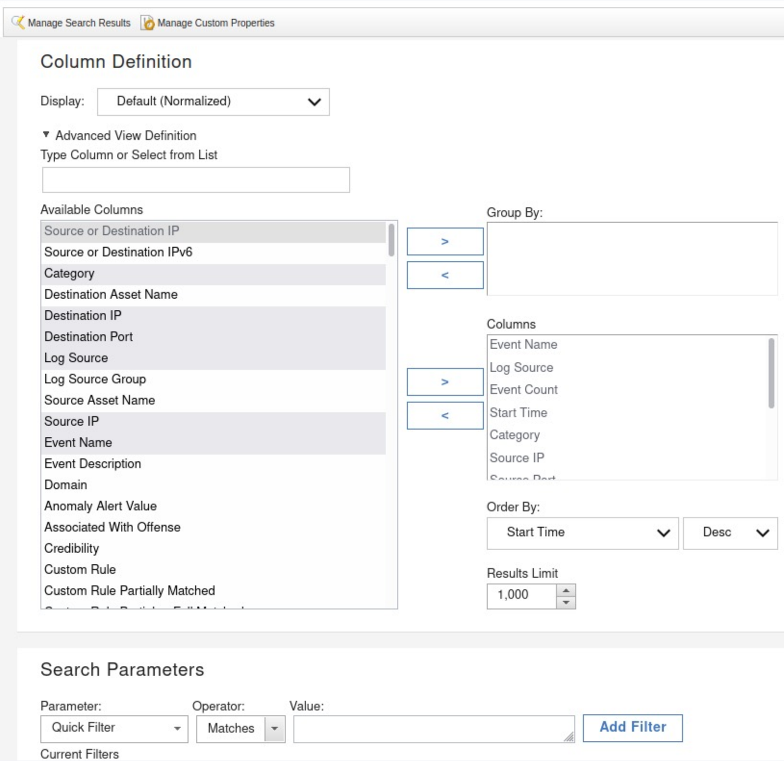
- Special characters

QRadar Searches

Basic Searches

Basic Searches

- GUI editor is accessed via the *New Search* and *Edit Search* items in the *Search* menu for *Log Activity* and *Network Activity* tabs.
- This image shows the sections most used for creating new or editing existing searches:
  - Selecting the columns to display or group by.
  - The search parameters used for the search.
- Column definitions can be saved as different views to apply as needed against a search.
- Add new filters before removing existing filters. This allows for faster search pivoting.
- Use basic searches if changing the *Display* (group by) menu is required. This menu is disabled for AQL searches.



Column Definition

Display: Default (Normalized)

▾ Advanced View Definition

Type Column or Select from List

Available Columns

Source or Destination IP
Source or Destination IPv6
Category
Destination Asset Name
Destination IP
Destination Port
Log Source
Log Source Group
Source Asset Name
Source IP
Event Name
Event Description
Domain
Anomaly Alert Value
Associated With Offense
Credibility
Custom Rule
Custom Rule Partially Matched

Group By:

Columns

Event Name
Log Source
Event Count
Start Time
Category
Source IP

Order By: Start Time Desc

Results Limit 1,000

Search Parameters

Parameter: Quick Filter

Operator: Matches

Value:

Current Filters

Tips for Basic Searches

One tip to rule them all – limit the scope of the search, be as specific as possible

Start with small time ranges, then expand the duration of the search gradually
- There is a near linear relationship to time frame and duration to complete a search
- Interim results may show opportunities of further refining the search criteria

Always try to have at least one **`[Indexed]`** property in your search criteria
- Searches without any indexed properties will take much longer to complete

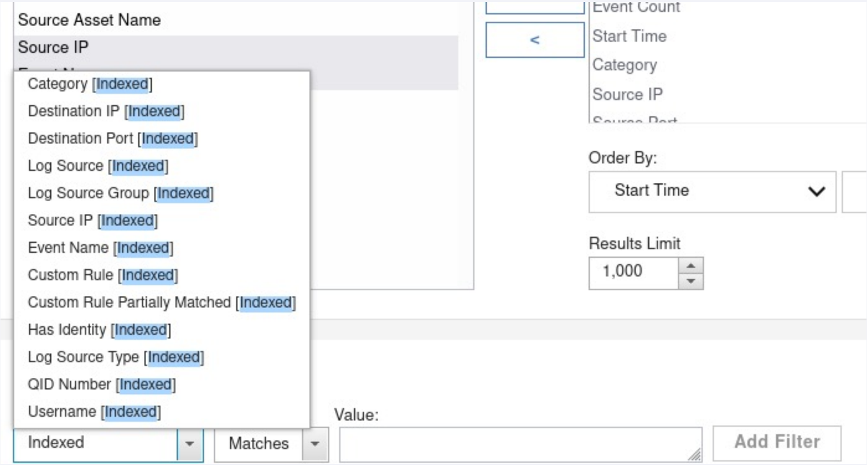
Using indexed properties is a must for “expensive” searches
- Any type of payload search

If possible, add an Event or Flow processor filter
- These are special filters that tell QRadar to restrict a search to a specific processor or type of processor
- But you need to know where the data is stored in order to use them

QRadar Searches

Indexed Properties

Using Indexed Properties



Adding at least one filter for an indexed property will improve search speed in QRadar. When the search is first started the search engine filters the data set based on the indexed property first.

Look for properties with the tag **`[Indexed]`** after its name. Searching on “Indexed“ will list all of them.

Default Indexed Properties

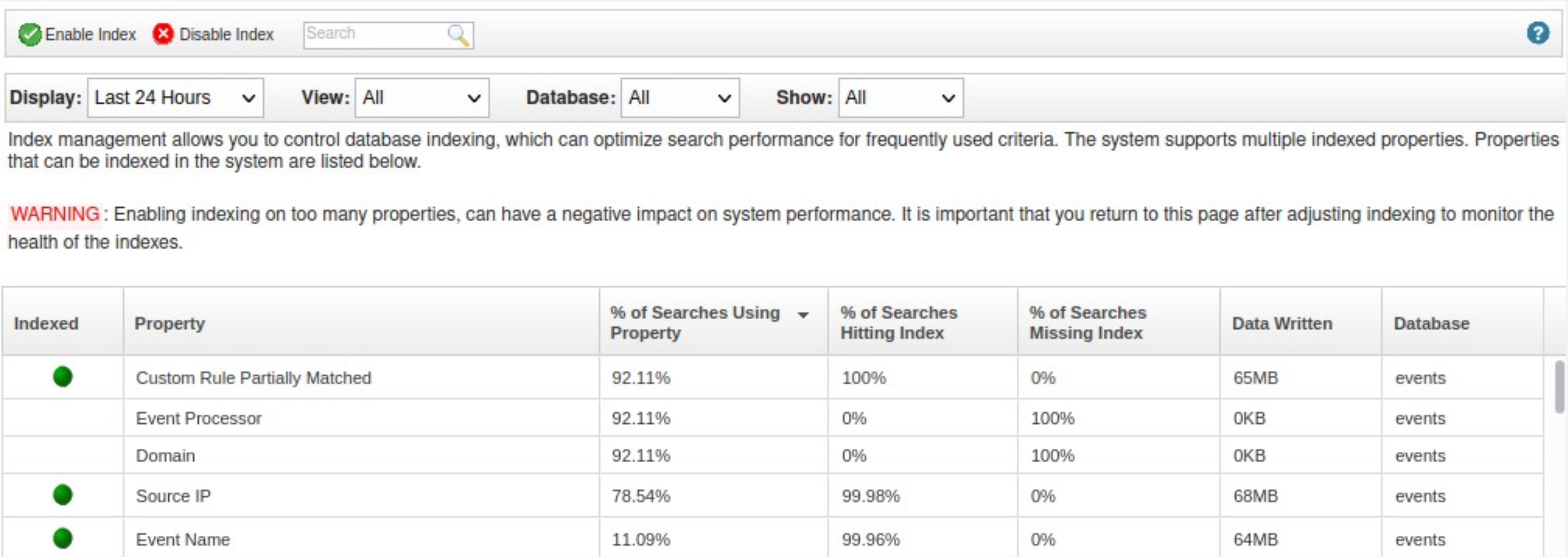
Events

Custom Rule
Custom Rule Partially Matched
Destination IP
Destination Port
Event Name
Has Identity
Log Source
Log Source Type
Low Level Category
Quick Filter
Source IP
Username

Flows

Application
Custom Rule Partially Matched
Destination IP
Destination Port
Flow ID
Quick Filter
Source IP

Index Management



Display: Last 24 Hours **View:** All **Database:** All **Show:** All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING : Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Custom Rule Partially Matched	92.11%	100%	0%	65MB	events
	Event Processor	92.11%	0%	100%	0KB	events
	Domain	92.11%	0%	100%	0KB	events
●	Source IP	78.54%	99.98%	0%	68MB	events
●	Event Name	11.09%	99.96%	0%	64MB	events

When to Enable/Disable an Index

Enable index when:

- **`% of Searches Using Property`** >= 30%
- **`% of Searches Missing Index`** >= 30%
- Across all three timeframes; 24 hours, 7 days, and 30 days

Disable index when:

- **`% of Searches Using Property`** = 0% last 30 days

The above apply for properties that are frequently used.

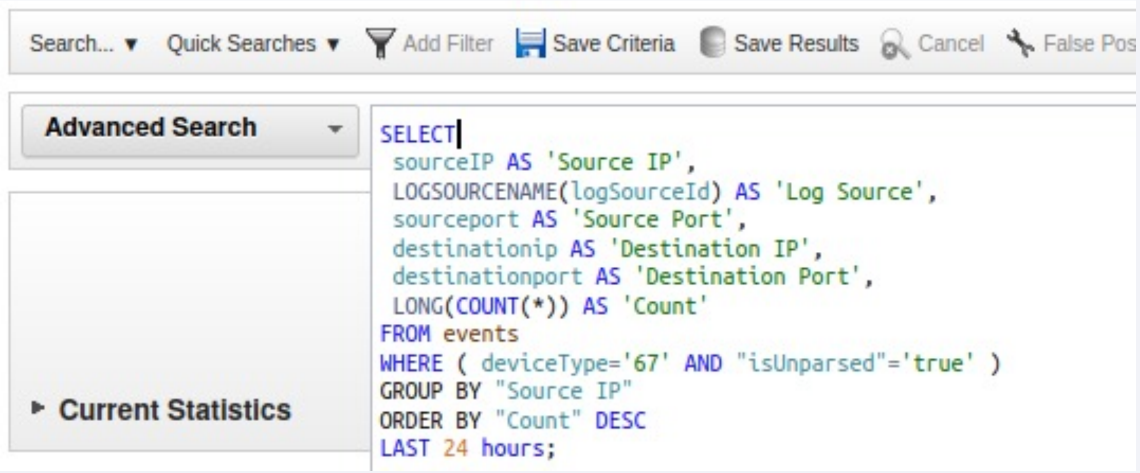
If users are performing searches with many different saved searches that use properties that are not widely used across all searches, a threshold lower than 30% should be used.

Indexes are updated once a minute and indexing too many properties can potentially lead to performance issues in the event pipeline and could also impact disk storage.

QRadar Searches

Advanced Searches

Advanced Search



```
SELECT
 sourceIP AS 'Source IP',
 LOGSOURCENAME(logSourceId) AS 'Log Source',
 sourceport AS 'Source Port',
 destinationip AS 'Destination IP',
 destinationport AS 'Destination Port',
 LONG(COUNT(*)) AS 'Count'
FROM events
WHERE ( deviceType='67' AND "isUnparsed"='true' )
GROUP BY "Source IP"
ORDER BY "Count" DESC
LAST 24 hours;
```

Advanced searches support the use of a SQL-like language called Ariel Query Language (AQL).

Advanced Search - Features

SQL-like Support

- Mathematical and string operations
- Boolean conditionals (AND / OR / NOT)
- Result column naming
- 'Having' and 'Group by' support
- Full text search support
- Quickfilter search support
- Time and Date formatting

Functions and Analytics

- Event category, name, etc.
- Logs: source name and group
- Asset data and categories
- External threat intelligence and IAM data
- Time series anomaly detection
- Scheduled offenses
- 'Hot', 'Warm', 'Cold' data
  - Data nodes

Advanced Search Example – Hourly Beaconing

```
SELECT
 sourceip AS ‘Source IP’,
 destinationip AS ‘Destination IP’,
 UNIQUECOUNT(DATEFORMAT(starttime,’hh’)) AS ’Different Hours’,
 COUNT(*) as ’Total Flows’
FROM flows
WHERE flowdirection = ‘L2R’
GROUP BY “Source IP”, “Destination IP”
HAVING ’Different Hours’ > 20
AND ’Total Flows’ < 25
LAST 24 Hours
```

Advanced Search Example – External Threat Intelligence

```
Select
 REFERENCETABLE('ip_threat_data','Category',destinationip) AS 'Category’,
 REFERENCETABLE('ip_threat_data','Rating', destinationip) AS 'Threat Rating’,
 UNIQUECOUNT(sourceip) as 'Source IP Count’,
 UNIQUECOUNT(destinationip) as 'Destination IP Count'
FROM events
GROUP BY 'Category', 'Threat Rating'
LAST 1 Days
```

QRadar Searches

Resources

Resources

Open Mic Webcast #6: Searching Your QRadar Data Efficiently
– http://www-01.ibm.com/support/docview.wss?uid=swg27044066

Searching Your QRadar Data Efficiently
– https://www.ibm.com/support/pages/searching-your-qradar-data-efficiently-start

Lucene Query Parser Syntax
– https://lucene.apache.org/core/5_3_1/queryparser/org/apache/lucene/queryparser/classic/package-summary.html#package_description

Sharing Dashboard Items from QRadar Saved Searches
– https://www.ibm.com/support/pages/qradar-sharing-dashboard-items

Event and Flow Searches
– https://www.ibm.com/docs/en/qsip/7.5?topic=siem-event-flow-searches

Resources - continued

Using Search Efficiently in QRadar

- https://www.securitylearningacademy.com/enrol/index.php?id=4791

Advanced Search and Use Cases

- https://www.securitylearningacademy.com/enrol/index.php?id=1441

Using AQL for Advanced Searches in IBM QRadar SIEM

- https://www.securitylearningacademy.com/enrol/index.php?id=4683

Ariel Query Language (AQL) Guide

- https://www.ibm.com/docs/en/qsip/7.5?topic=aql-learn-about-ariel-query-language

Questions?

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM **Security**

IBM