IBM Security

November 29, 2017

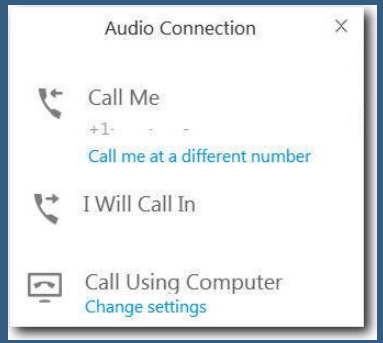
QRadar™ Open Mic: Custom Properties

IBM SECURITY SUPPORT OPEN MIC

To hear the WebEx audio, **select an option** in the Audio Connection dialog or by access the Communicate > Audio Connection menu option. To ask a question by voice, you must either Call In or have a microphone on your device.

You will not hear sound until the host opens the audio line.

For more information, visit:
http://ibm.biz/WebExOverview_SupportOpenMic



Slides and additional dial in numbers:

http://ibm.biz/JoinQRadarOpenMic

IBM

Announcements

- QRadar 7.3.0 Patch 6 is released and includes 57 resolved issues.

- An interim fix 01 for 7.3.0 Patch 6 is being posted today for a list of release notes, see https://ibm.biz/qradarsoftware.

- QRadar Community Edition is now available for all users. QRadar Support does not do phone support for QRadar Community Edition. Administrators can use the tag ‘qradarce’ in the forums to ask questions about QRadar Community Edition.

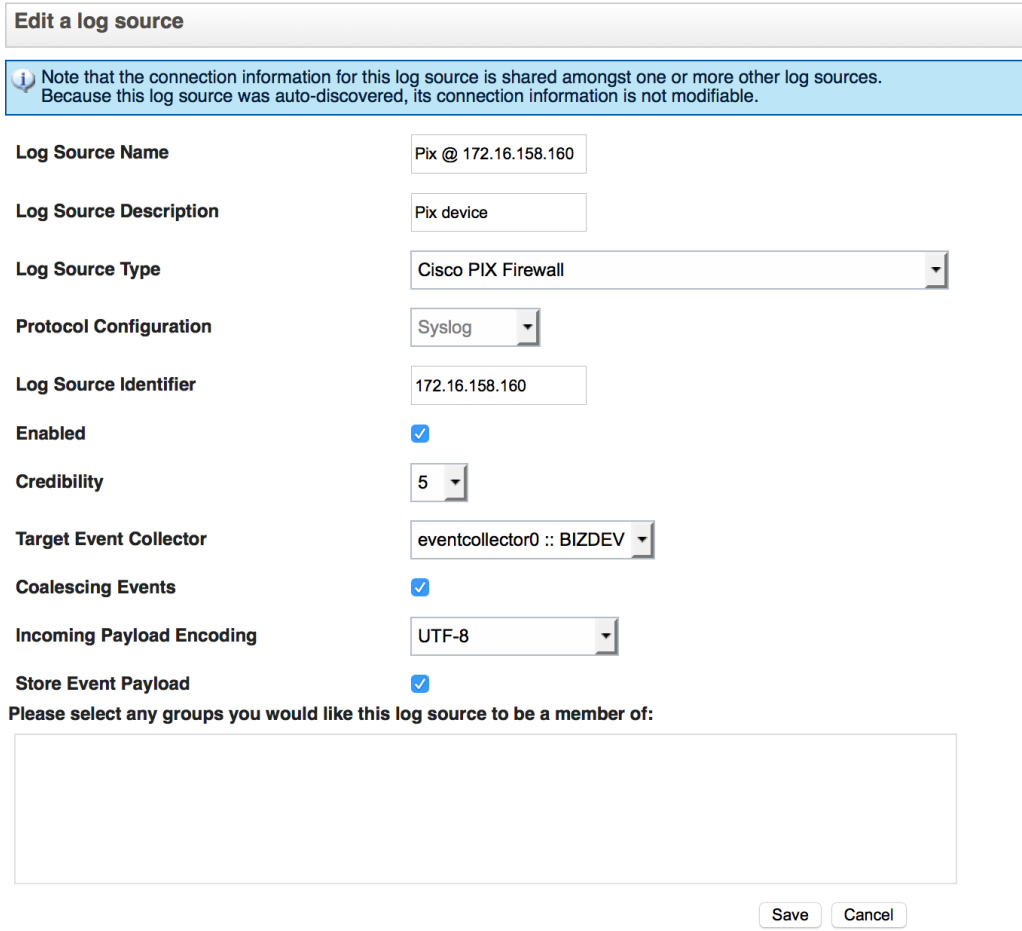
  For questions, see https://ibm.biz/qradarceforums
  For the software, see https://ibm.biz/qradarce

- User Behavior Analytics v2.4.0 is now on the IBM App Exchange.

A Quick Introduction

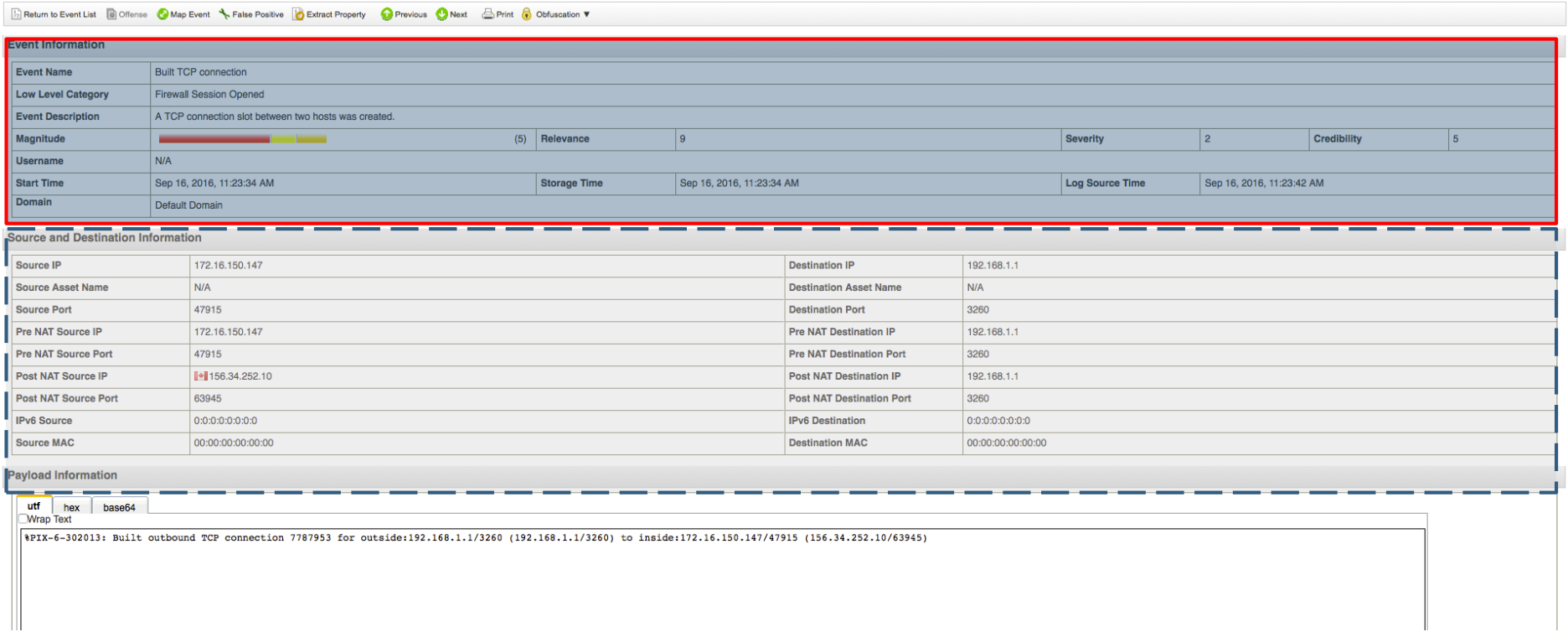
Log Sources

- The primary method for how QRadar gets data from event sources.
- A log source is made up of two components: The Protocol and the DSM.
- The Protocol is how the data gets into QRadar.
- The DSM concerns how the data is parsed.



Device Support Modules (DSMs)

- The parsing component of the log source.
- Normalizes event data to fit into the QRadar Normalized Event Model.
- Custom properties are not part of the DSM to process normalized events.



Normalized Event Data vs Custom Properties

Normalized events are the standard values that we populate in the user interface that present a common and make data which is broadly applicable available in a consistent presentation. Data like the date and time an event occurred, the user involved in the event, and information about endpoints/assets involved in the event (IP addresses, ports, MAC addresses) are almost universally relevant to all events and so these values are considered normalized event data.

Normalized event fields include:

- Source IP
- Destination IP
- MAC Address
- Username
- Port
- Protocol
- Pre-NAT values (source, dest, ports)
- Post-NAT values (source, dest, ports)
- HostName (identity-related)
- GroupName (identity-related)
- NetBIOSName (identity-related)
- ExtraIdentityData (identity-related)

Custom Properties are used to parse values from event payloads which do not align with the Normalized event fields. These allow administrators to display information in the user interface as '**name(custom)**' to be used across QRadar.

Event Information

Event Name	Success Audit: Successful logon with administrative or special privileges
Low Level Category	Admin Login Successful
Event Description	Success Audit: Successful logon with administrative or special privileges
Magnitude	(2)
Username	Administrator
Start Time	Nov 29, 2017, 1:58:06 AM
Accesses (custom)	N/A
AccountDomain (custom)	N/A
AccountID (custom)	N/A
AccountName (custom)	Administrator
ChangedAttributes (custom)	N/A
EventID (custom)	4672
GroupID (custom)	N/A

Normalized Event Data vs Custom Properties (continued)

You can think of custom properties as a quick reference for a value that falls outside of normalized data, such as source zone, destination zone, policy, or server name. As this data might be important and administrators might want to be able to provide these filters to users to assist with searches.

For example, lets look at a payload from a IDP event.

```
<26> 1 2011-05-01T22:43:12 10.10.150.3 Jnpr Syslog 32743 1
[syslog@juniper.net dayId="20170501" recordId="659" timeRecv="2017/05/01
22:43:12" timeGen="2017/05/02 03:13:12" domain="" devDomVer2="751"
device_ip="10.10.150.3" cat="Predefined" attack="HTTP:XSS:X-FORWARDED-FOR-
INJ" srcZn="DMZ" srcIntf="NULL" srcAddr="193.5.216.100" srcPort="47255"
natSrcAddr="169.5.216.100" natSrcPort="47255" dstZn="TRUSTED" dstIntf="NULL"
dstAddr="169.128.28.10" dstPort="80" natDstAddr="10.100.127.1"
natDstPort="80" protocol="TCP" servername="CardServer15" ruleVer="0"
policy="31" rulebase="IDS"
```

In this example you will see common values that are part of our normalized data for the event, such as IP, port information, NAT, etc. This payload also contains a number of highlighted values that might be important to the administrator where a custom property might provide useful data.

Types of Custom Properties

Custom **Event** Properties allow for event payload information to be extracted and presented in its own field in the Log Activity user interface.

Custom **Flow** Properties allow for flow information to be extracted and presented in its own field in the Network Activity user interface.

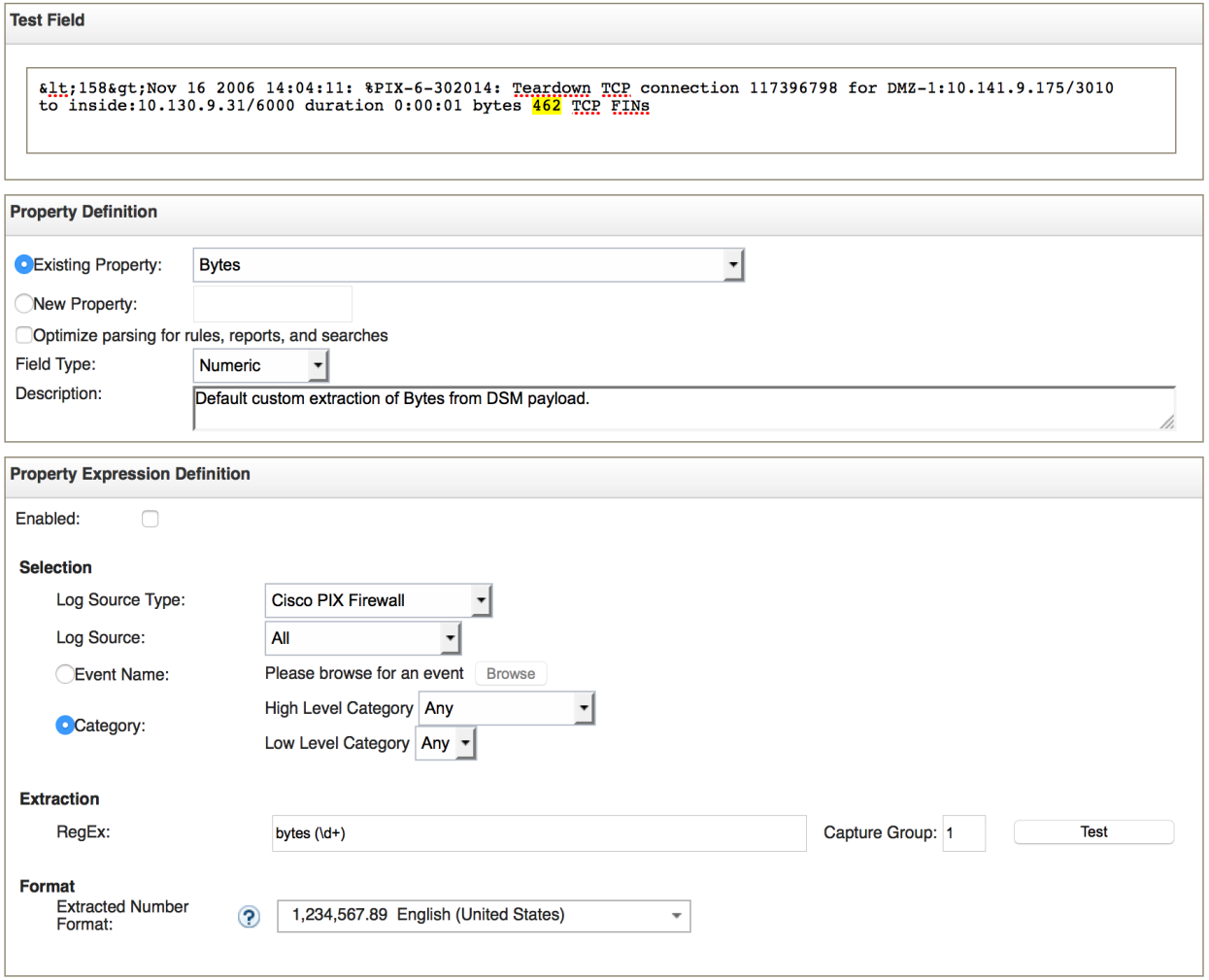
Custom **Asset** Properties allow administrators to assign a name to an asset group, which can then be leveraged in Asset tab searches. These are not regex-based values, but manually assigned definitions, which can then be searched.

AQL Custom Properties (coming soon)

Custom Properties and the User Interface

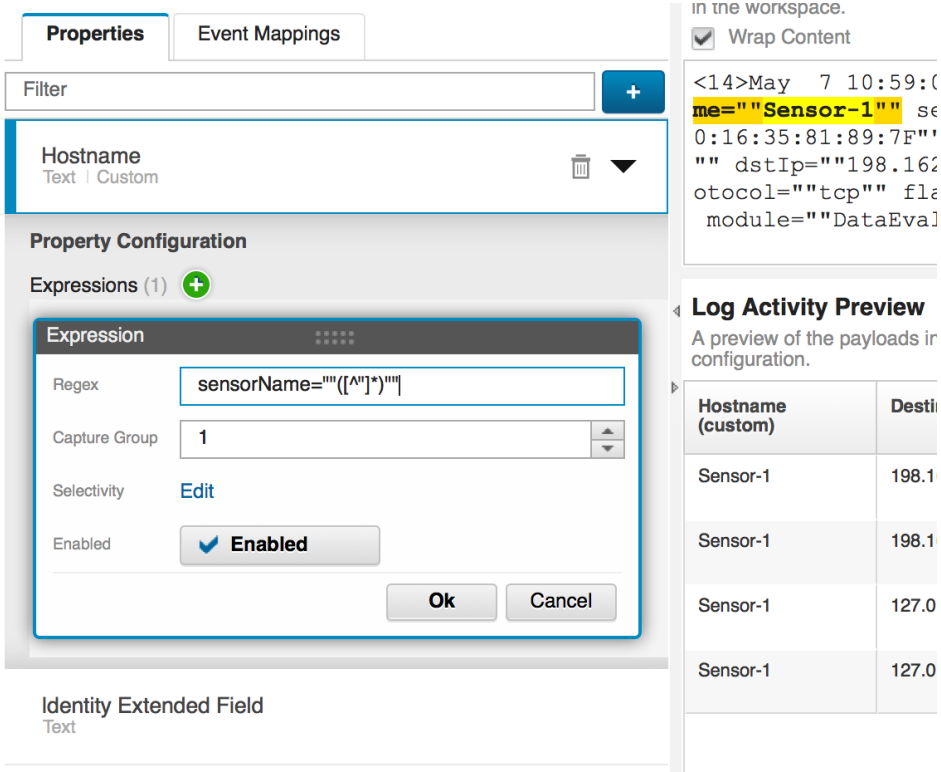
Custom Event Properties

- Allows users to define event properties not covered by the Normalized Event Fields.
- Divided into three parts: The test field, property definition and the expression definition.
- Custom Properties can be associated with specific log source types, log sources, high level categories, low level categories, or even specific QIDmap entries. This ensures not all Custom Properties are applied to all events that are received by QRadar and allows the admin to decide on usage.



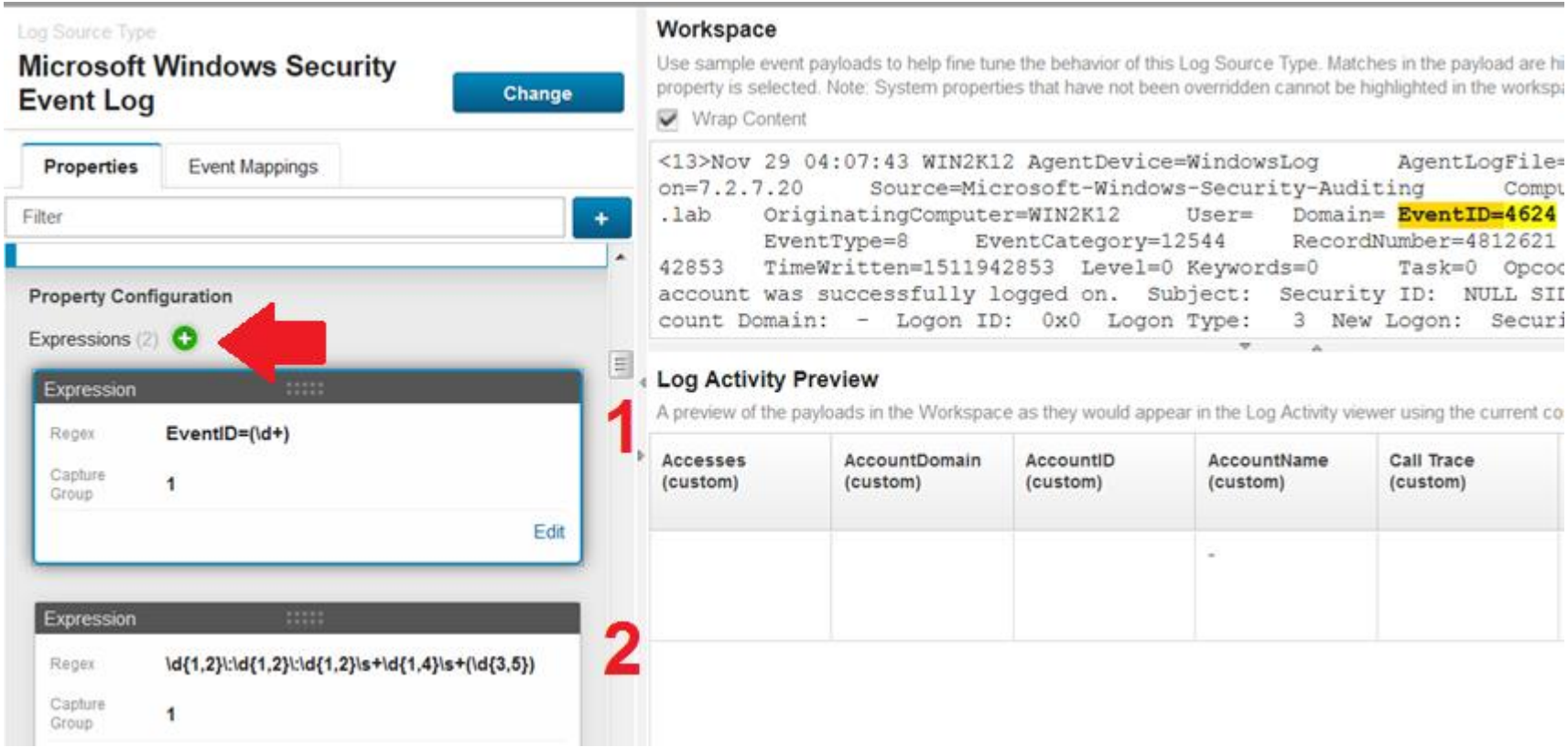
Custom Properties in the DSM Editor (continued)

- To add a custom property to the DSM simply click the plus above the normalized properties.
- Once selected, you can set the property expression like any of the normalized fields.
- You can Change the Selectivity so that the property only fires on certain events rather than all the time
- You can also set to have the property enabled or disabled by default. Custom Properties are calculated in a brute force fashion so customers often like having them disable to start out, and then turn on the ones they see as important.



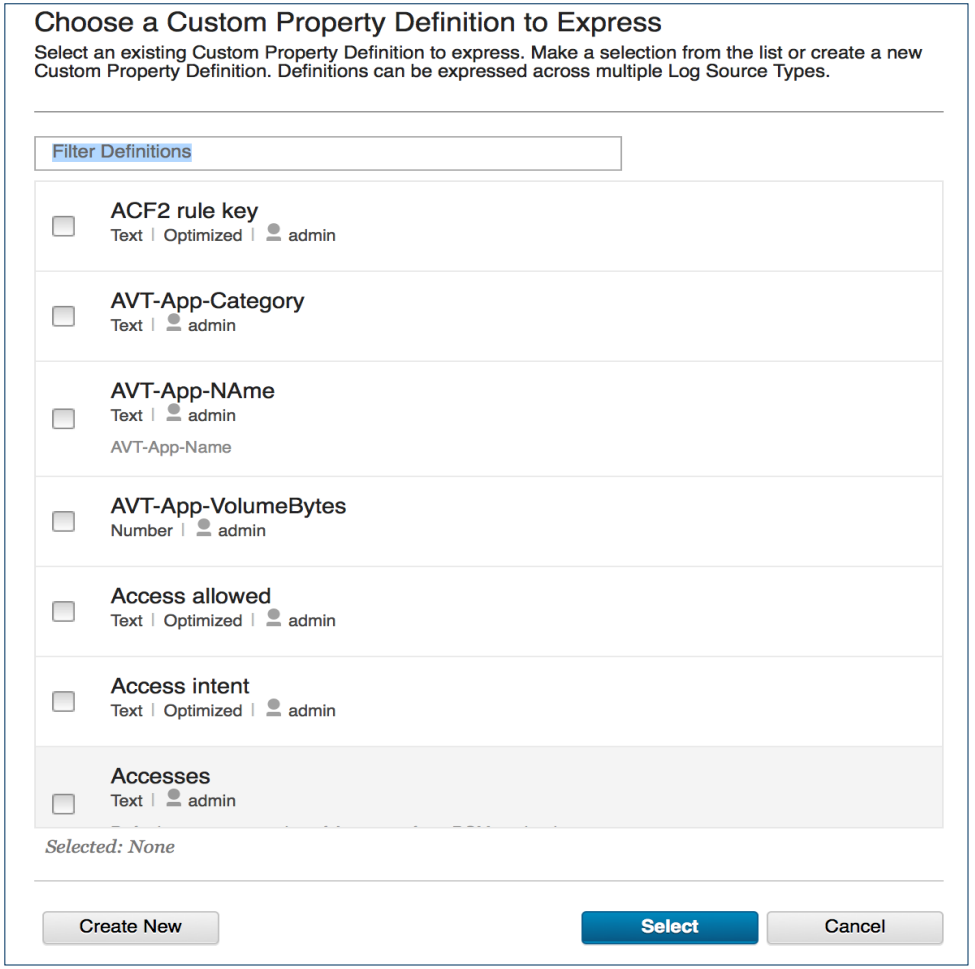
Multiple Custom Properties in the DSM Editor (continued)

Multiple custom properties are represented by Expressions (#) and can be used to deal with variations in format. It is recommended that multiple expressions be used, instead of complex regex when the data differs drastically.



Custom Properties in the DSM Editor

- It is highly recommended to base a custom property on an existing one if something similar already exists in the list.
- Custom Properties are made up of 2 parts. The property itself and an expression There is only ever one property so that it can be shared across DSMs, but each can have it's own expression.
- A DSM can also have multiple expressions for a given property if some event sets give the same information in slightly different ways.
- Properties can be set to be optimized for Rules or indexes can be enabled for searches.



Optimizing & Indexing

Optimized Custom Properties

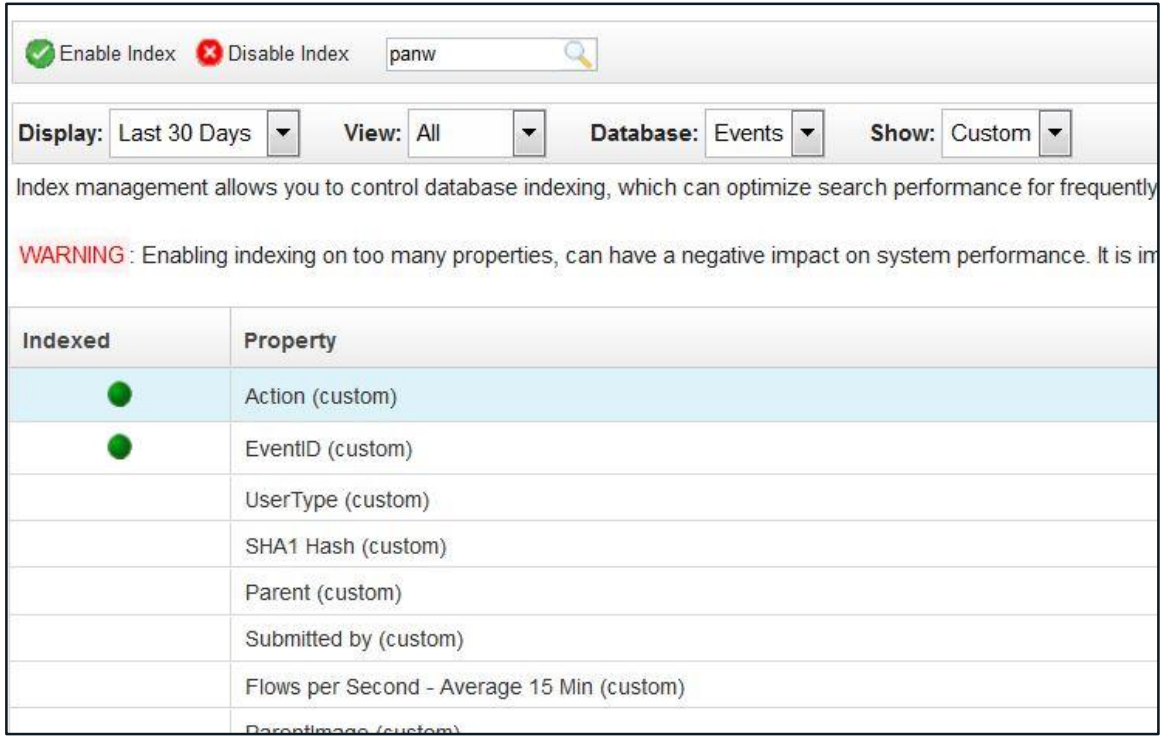
Optimized means that the custom properties are part of the event record written to disk, and therefore any reports and searches run after initial processing that depend on those properties can simply retrieve them, rather than having to parse them out of the payload on demand. Custom Properties which are not optimized parse out the values on demand when something attempts to access the event record. When you optimize, the values are pre-parsed and the data is stored and allows it to run without having to run the regex to retrieve the values.

Only check off ‘Optimize’ if you actually need the properties for rules.

If you have a property used often, optimizing it will help with other parts of the product, such as reports, searches, and dashboards as the pre-parsed data is faster than running the regex. However, using optimization for gaining speed outside of rules should be considered carefully.

Indexed Custom Properties

When you want to leverage certain properties for faster searching in QRadar, administrators can enable an index for a custom property, which requires you to optimize the value. This allows you to use custom properties in searches to get quick results from the indexed values.



Tips and Best Practices

Best practices

- Content packs from the X-Force App Exchange contain custom properties that might be useful for popular event sources.
- Look for existing regular expressions to use as examples.
- Consolidate common properties for data that has structured format where you can.
- Create multiple custom properties to deal with variations in the data format, instead of trying to create complex regex.

AccountName	Microsoft Windows Security Event Log	New Account Name: (.*?)
AccountName	Microsoft Windows Security Event Log	Account Name:\s*(.+?)\s+(Additional Information|Account Domain|Service Infor…
AccountName	Microsoft Windows Security Event Log	Account Name:\s*(.+?)\s+(Additional Information|Account Domain|Service Infor…
AccountName	Microsoft Windows Security Event Log	Target Account Name: (.*?)

- Only optimize when you need to use a custom property in a rule.

Rule

Apply AWS Cloud: Multiple Failed Console Logins from Different Source IPs on events which are detected by the Local system
and when the event(s) were detected by one or more of Amazon AWS CloudTrail
and when the event category for the event is one of the following Audit.General Audit Event
and when any of Action (custom) match Failure
and when at least 25 events are seen with the same Destination IP and different Source IP in 2 minutes

Common mistakes with custom properties

- Do not use greedy regular expressions.

  Using *greedy quantifiers* (*.?) or (.+?) by themselves. If you use them, you are wild card matching against the payload to identify these values. If you know what content you are looking for, then it is better use \d or \w.*

- Combining different formats in to a single property, for example CSV format with name=value pairs in a single custom property regular expression.
- Trying to do too much in a single property, such as large numbers of capture groups. We specifically limit regex to 10 capture groups in the DSM Editor.
- Optimizing too many properties
- Extremely rigid patterns can cause you issues

Using Custom Properties in Advanced Searches

Using Custom Properties in AQL statements

Custom properties can be used throughout your AQL statement. In most cases, you can call the custom property directly, unless in contains spaces where you would require double-quotes.

NOTE: The custom property must be enabled to be used in an AQL statement.

```
SELECT Bluecoat-cs-host, sourceip, Bluecoat-cs-uri FROM events
WHERE LOGSOURCEGROUPNAME(devicegrouplist)
ILIKE '%Proxies%' AND Bluecoat-cs-host ILIKE '%facebook.com%'
GROUP BY sourceip
```

Bluecoat-cs-host = Hostname from the client's requested URL.
Bluecoat-cs-uri = The original URL requested.

```
SELECT "Changed User" from events where "Changed User" = 'admin'
```

New Custom Property Features in QRadar 7.3.1

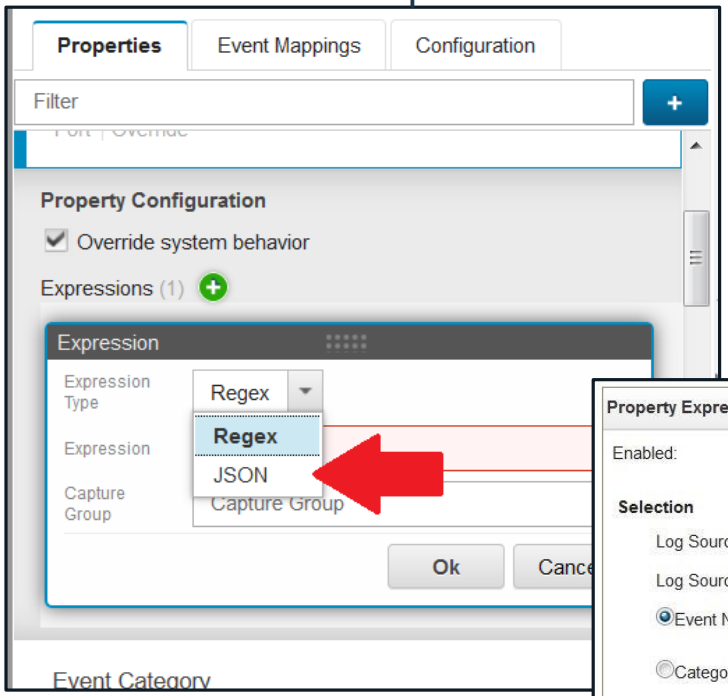
JSON Support in Custom Properties

- In QRadar 7.3.1 a new feature is being provided to assist users with improved JSON property support. This new JSON support allows users to configure parsing of both standard/normalized and custom properties from JSON events without needing to use regex. This makes JSON data easier to consume when there is no DSM available and runs more efficiently for the system then using regex, which is typically a brute-force match for the regex to the payload values.

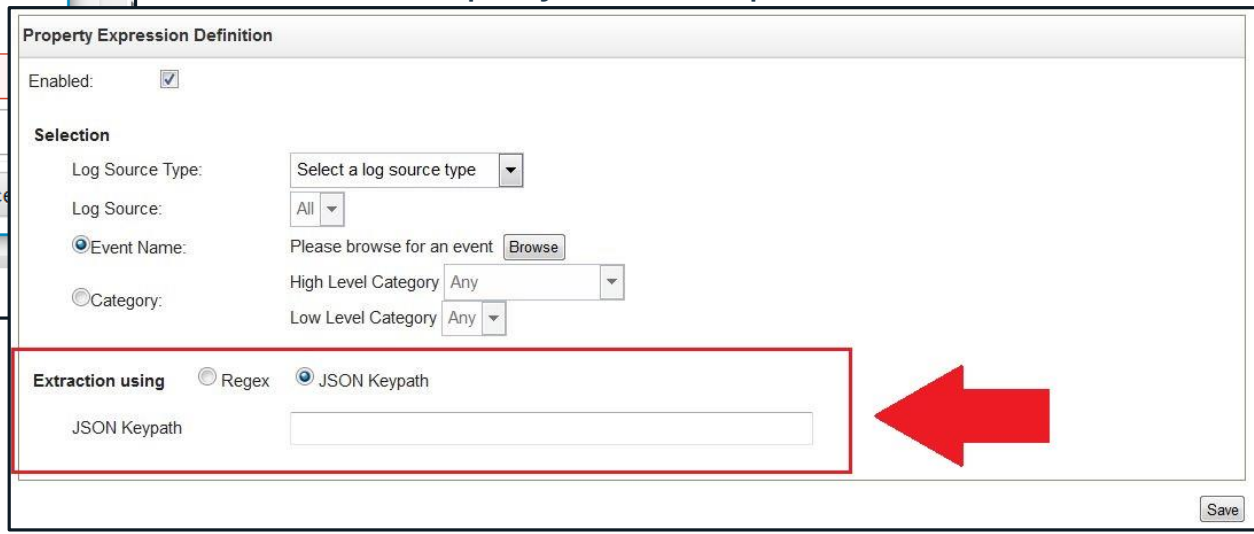
- In Log Source Extensions, users can now put a JSON keypath expression in their <pattern> elements, as long as they set the “type” attribute to “JsonKeypath”. They can then reference these patterns inside their <match-group> elements by using <json-matcher> elements instead of the original <matcher> elements. No capture-group value is necessary because the JSON keypath specifies a particular JSON value (or set of values, if multiple values are used)

JSON Keypaths in the User Interface

DSM Editor JSON Expression Interface



Custom Property JSON Expression Interface



Using JSON Keypaths (continued)

Given the JSON data on the right, the examples on the left show how to reference different fields

- To capture the “action” value, the expression is:

  /“action”

- To capture the “username” value, the expression is:

  /“client”/“username”

- To capture the 1st “address” value, the expression is:

  /“client”/“address”

- To capture the 2nd “address” value, the expression is:

  /“target”/“address”

- To capture the “port” value, the expression is:

  /“target”/“port”

```
{
    "action": "login",
    "client":
    {
        "username": "Bruce",
        "address": "10.0.2.15"
    },
    "target":
    {
        "address": "10.100.100.90",
        "port": 80
    }
}
```

Automatic Custom Property Discovery in the DSM Editor

The DSM Editor can support automatic creation of custom properties for JSON event data. This is toggled using an “Enable Auto Property Discovery” feature.

Work flow for users

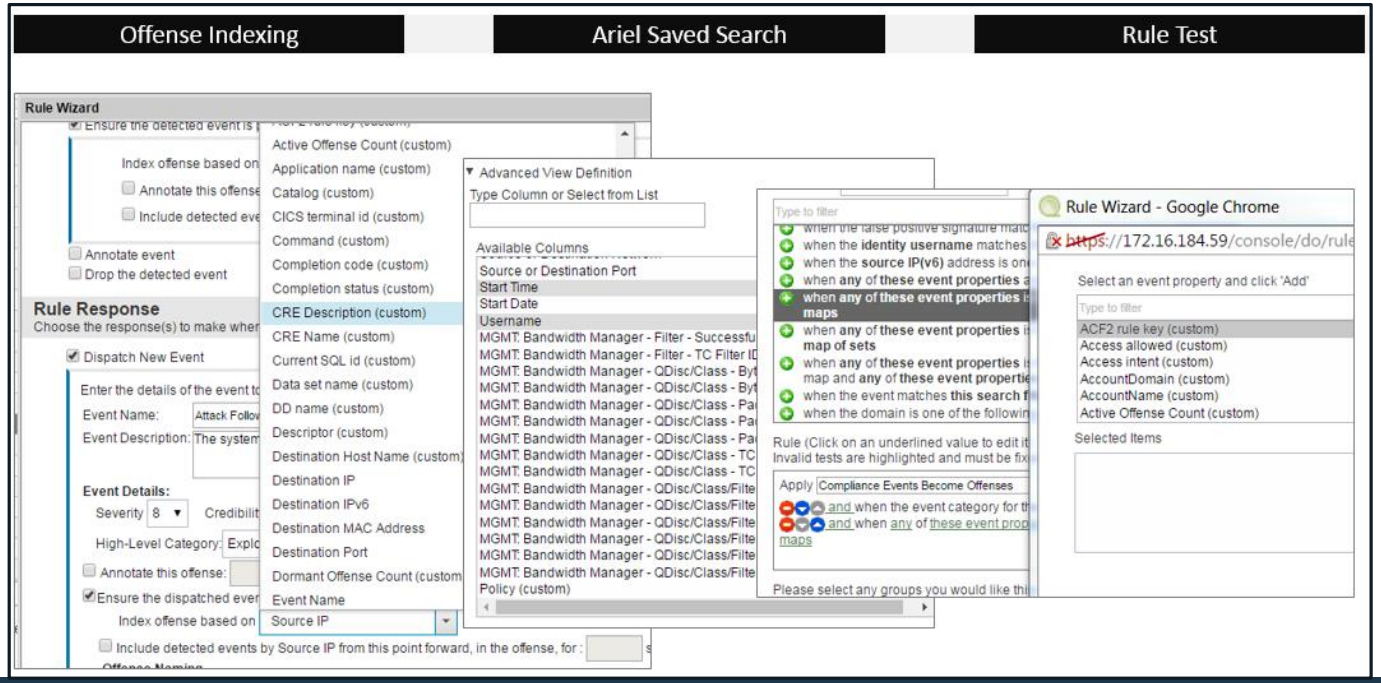
1. Launch the DSM Editor.
2. Create (or select an existing) log source type with has JSON-formatted event data
3. Go to the Configuration tab in the left-side pane of the DSM Editor
4. Click the “Enable Auto Property Discovery” toggle to show additional property discovery configuration
5. Select a “Property Discovery Format” as JSON
6. Toggle the “Enable Properties for use in Rules and Search Indexing” switch if you want discovered properties to be optimized by default.
7. If desired, adjust the Discovery Completion Threshold value. This number represents the number of consecutive events received by this log source type without new properties being discovered that should trigger discovery to turn itself off. The idea being that if X events go by without any new properties, then stop trying to auto create values.
8. After events for this log source type enter the system, the properties will automatically get created. The user may choose to go into the DSM Editor at any time to remove or modify any autodiscovered properties they want to get rid of or adjust.

AQL Custom Property Feature in QRadar 7.3.1

AQL Custom Properties

With AQL-based custom event or custom flow properties, you can use an AQL expression to extract data that IBM QRadar does not typically normalize and display from the event or flow payload. For example, users can create an AQL-based property when they want to combine multiple extraction and calculation-based properties, such URLs, virus names, or secondary user names, into a single property. The new property can be used in custom rules, searches, reports, or they can use it for indexing offenses.

AQL custom properties are used like any other custom property and can enrich user information, or concatenate multiple properties in to a single value.



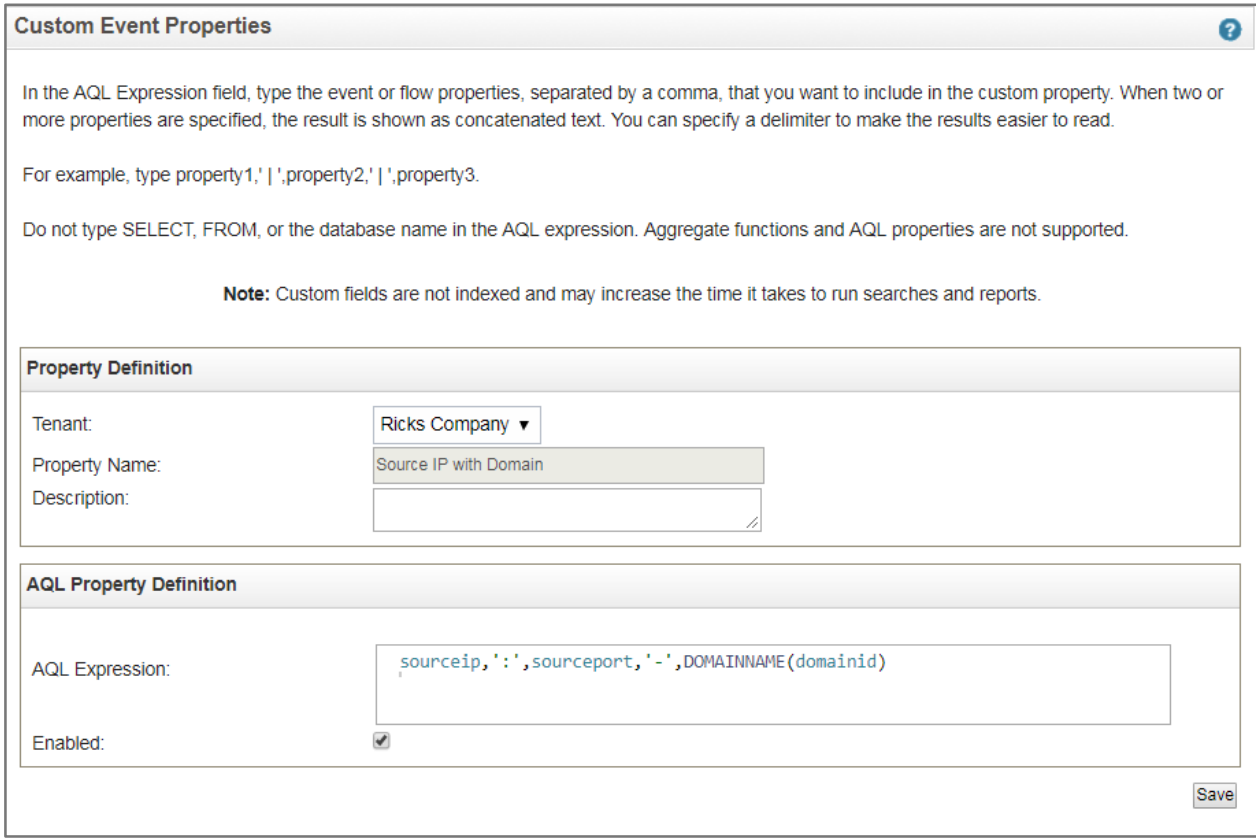
AQL Custom Properties (continued)

For example, in a multi domain environment, an IP address on its own does not hold much meaning for the SOC analyst and should include information about the domain.

AQL custom properties allow users to chain together unique properties, such as:

property 1, property 2, property 3,

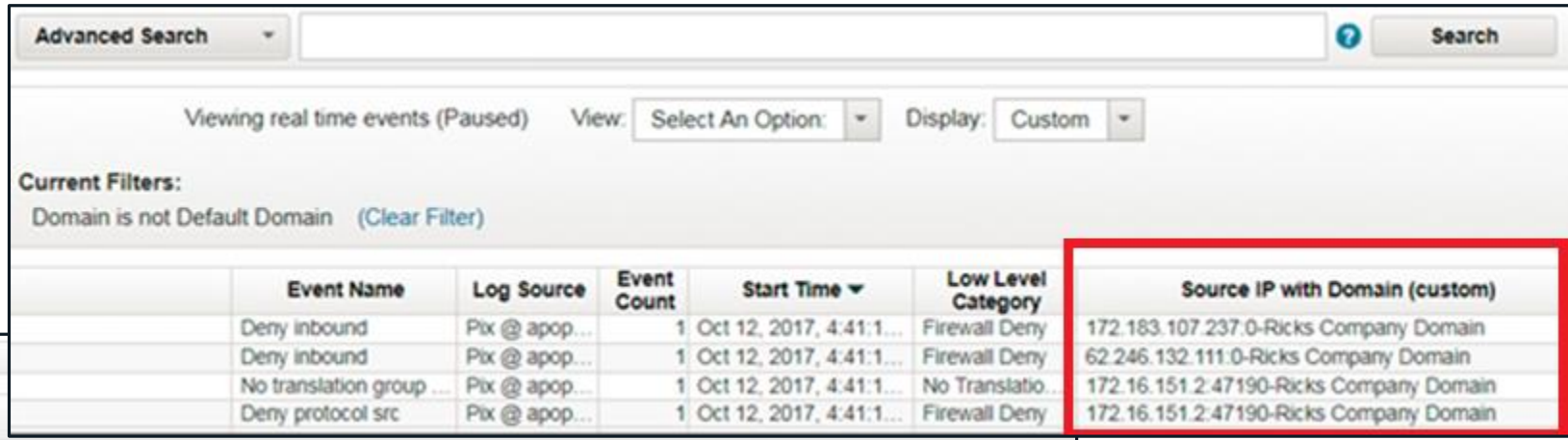
That can then be called using a single custom property value.

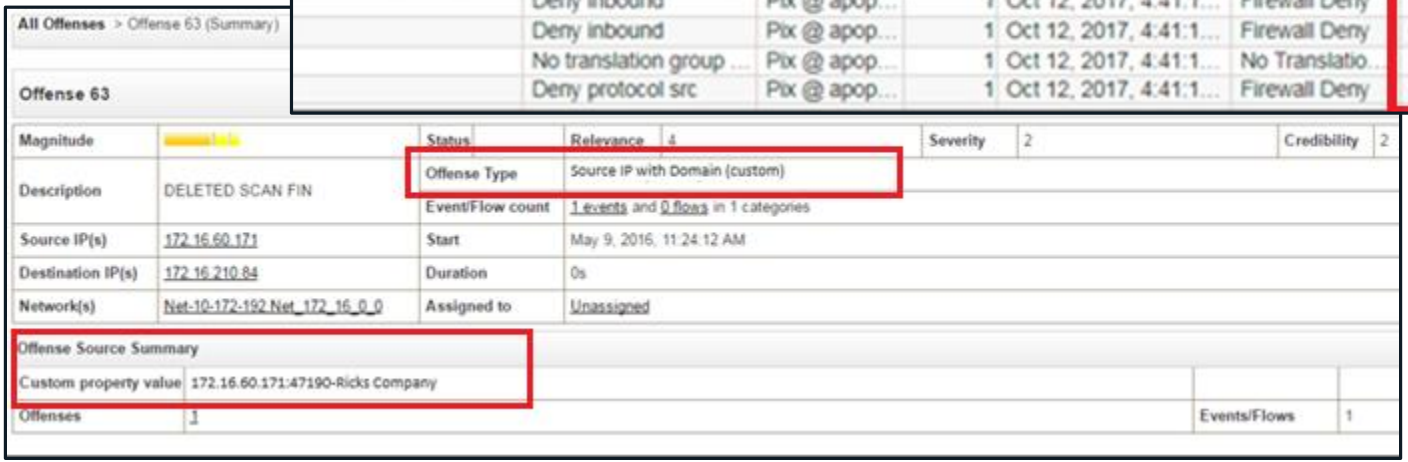


AQL Custom Properties (continued)

Other scenarios for concatenation of values to a single property could be to leverage:

- Hostname and Username
- Source IP and Username
- Username and URL
- Complex calculation through AQL function





Troubleshooting & Support

Troubleshooting

Custom properties will generate notifications for Expensive Custom Properties. There are also messages in /var/log/qradar.log that have data about custom properties and their performance.

For example: QID = 38750138. Performance degradation was detected in the event pipeline. Expensive custom properties were found.

```
Nov 22 16:01:30 127.0.0.1  [Timer-63]
com.q1labs.semsources.filters.normalize.DSMFilter: [WARN]
[NOT:0080014100][10.10.10.10/- -] [-/- -]Expensive Log Source or Log
Source Extensions Based On Average Throughput in the last 60 seconds
(most to least expensive) - (.+?)=19.0eps, (\w+)/\S+=1136.0eps
```

Questions

Questions for the panel

Now is your opportunity to ask questions of our panelists.

To ask a question now:

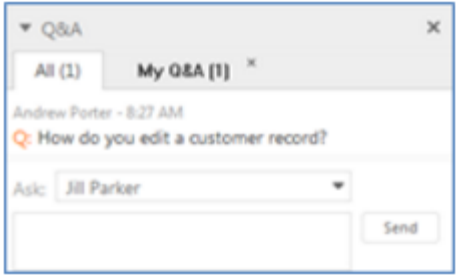
Raise your hand by clicking Raise Hand. The Raise Hand icon appears next to your name in the Attendees panel on the right in the WebEx Event. The host will announce your name and unmute your line.

or

Type a question in the box below the Ask drop-down menu in the Q&A panel.

Select *All Panelists* from the Ask drop-down-menu.

Click Send. Your message is sent and appears in the Q&A panel.



To ask a question after this presentation:

You are encouraged to participate in the dW Answers forum:

https://ibm.biz/qradarforums

IBM Security

THANK YOU

FOLLOW US ON:

https://www.facebook.com/IBM-Security-Support/

QRadar Forums: https://ibm.biz/qradarforums

youtube/user/ibmsecuritysupport

@askibmsecurity

securityintelligence.com

xforce.ibmcloud.com

IBM