

IBM Security Webinar

# QRadar Analyst Workflow App – Ask Us Anything

## Panelists

- Rick Sobiesiak  
Design Researcher
- Rick McCaskill  
Design Manager
- David Chun  
Offering Manager
- Shane Stewart  
Product Owner
- Omar Imam  
QRadar Support
- Jonathan Pechta  
QRadar Support

# Agenda

Introduction

Features and overview

Installation overview

Demo

Common Questions

Q&A

Jonathan Pechta

Rick Sobiesiak

Shane Stewart

Rick McCaskill

Panelists

Panelists

# Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

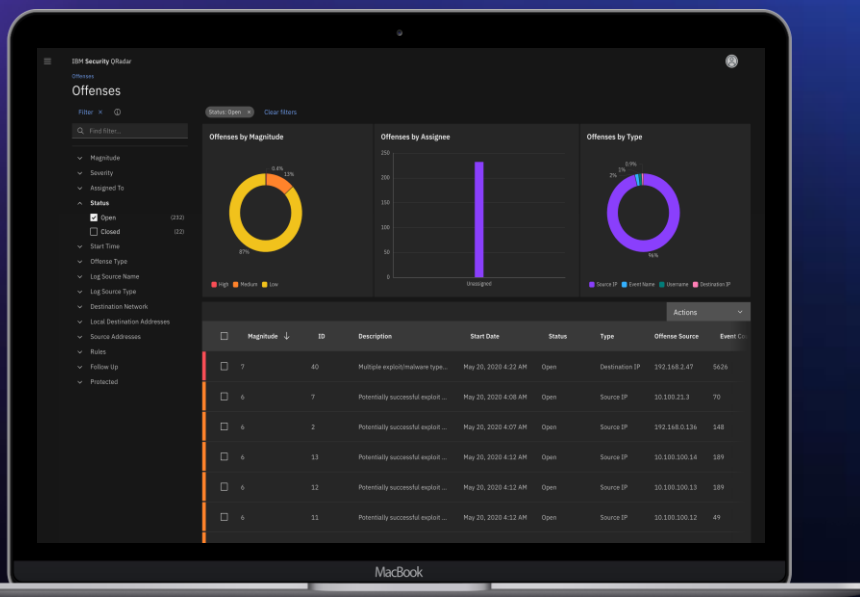
The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

IBM QRadar Analyst Workflow

# Features and overview

# QRadar Analyst Workflow



# Streamlined Offense & Search

## Investigate offenses faster

Understand why an offense was created, who/what was involved, networks/networks impacted, and analytics that lead to the creation of the offense within a single investigation workflow

## Drill down with a single click

View asset details, threat intelligence, payload information, rule details without leaving the screen

## Automatically defined AQL queries

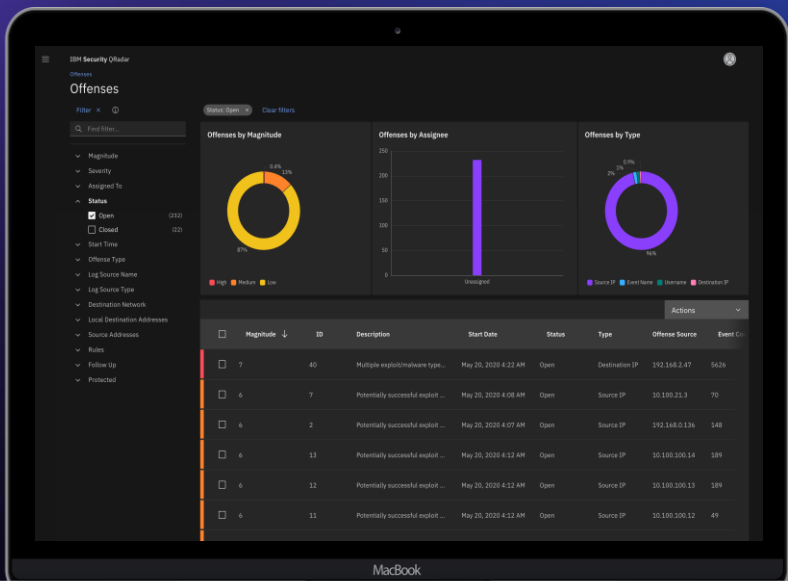
Query type-ahead can build out complete AQL queries for IP, Hash, Domain, and more so a user can search without previous knowledge of AQL

# QRadar Analyst Workflow

# Offenses Overview

## View of all offenses

- Graphical overviews that summarize offenses by magnitude, assignee, and type
- Sortable, filterable table of offenses
  - Magnitude
  - Time
  - Log source
  - Assigned To
  - Status
  - Rule information
  - ...and more
- Decorated addresses in table brings out additional details from side panels

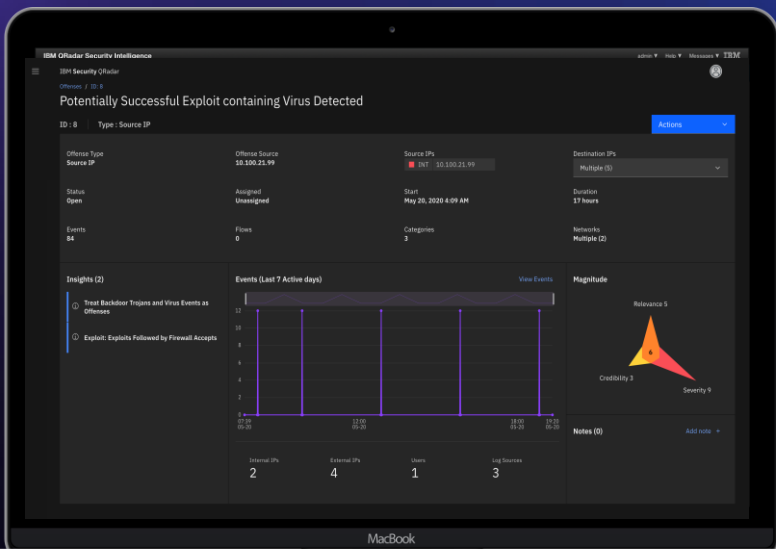


# QRadar Analyst Workflow

# Offenses Details

## Drill into details within an offense

- Summary table with offense type, # of events, source and destination addresses, time
- Insights layer provides list of all analytics and rules that contributed to offense
- Source IP drill down provides information from QRadar Asset Database (name, type, location, network, etc.)
- Destination IP drill down surfaces information from IBM X-Force (category, WHOIS, etc.)
- Link into the events of the offense

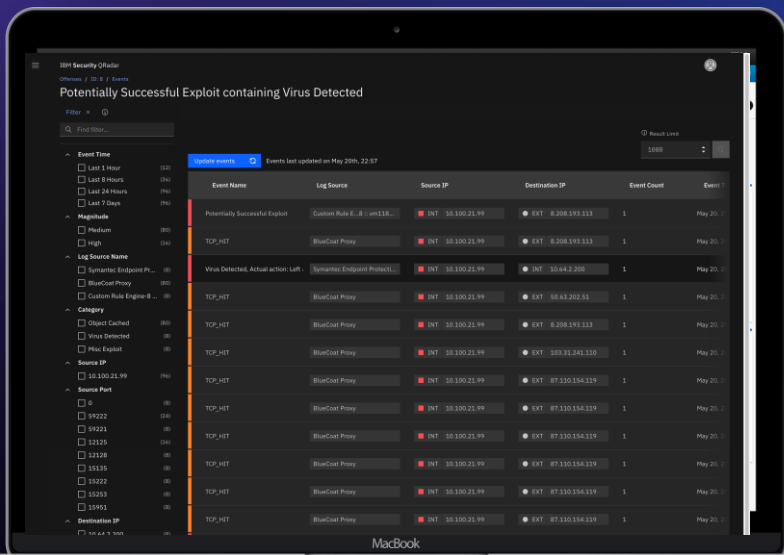


# QRadar Analyst Workflow

# Events of the Offense

Sort, filter, narrow down the events

- Shows events of the offense at the time of the offense
- Option to update to get latest events
- Sortable, filterable by event type, log source, source IP, dest IP, name, user, etc.
- Exclude certain results with IS NOT filter
- Event row drill down provides information about event magnitude, category, log source, protocol, payload, custom rules matched, and more
- Custom columns and custom column widths on roadmap\*



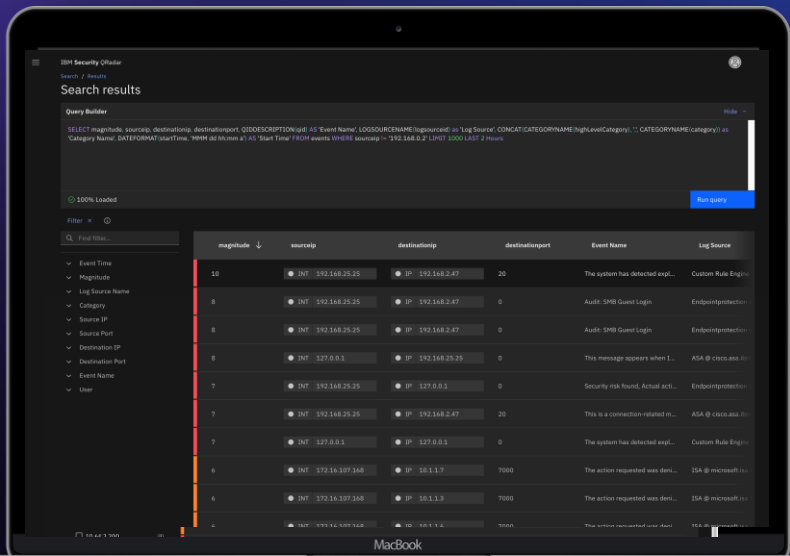


# QRadar Analyst Workflow

# Search

## Automatically built AQL queries

- Search using AQL without previous expertise
- Start typing an IP address, URL, or Hash to build out a predefined AQL query
- Syntax highlighting and error states to show where the query is invalid
- AQL best practices implemented to warn users of risky searches



IBM QRadar Analyst Workflow

# Installation overview

# Get the Analyst Workflow Application

## Compatibility

## Memory requirement

## Requires Internet

## Supported 64-bit browsers

The QRadar Analyst Workflow app uses Console RAM.

For X-Force Exchange lookups.

QRadar  
7.4.0+

600 MB

Yes

Chrome (latest)  
Firefox (60 ESR+)  
Microsoft Edge  
(38.14393 and later)

# Limitations

- QRadar Analyst Workflow V1.0.0 must run on the Console.

Note: You cannot move this app to an App Host or a QRadar Cloud Applications (QCA) appliance.

- QRadar on Cloud users must wait until DevOps upgrades your Console.
  - Current version: 7.3.3 Fix Pack 1
  - Planned upgrades to 7.4.0 Fix Pack 2
- QRadar Community Edition users will need to wait on a 7.4.x version to use the Analyst Workflow application.
- The Analyst Workflow zip file **CANNOT** be installed from **Admin > Extension Management**.

# Installation

1. If you have custom certificates, type the following commands on your QRadar Console (any directory):
  - `update-ca-trust`
  - `docker restart`
2. Download the [QRadarAnalystWorkflow1.0.0.zip](http://ibm.biz/analystworkflow) (<http://ibm.biz/analystworkflow>) app.
3. Copy the file onto your QRadar Console.  
For example: `scp QRadarAnalystWorkflow1.0.0.zip <QRadar host>:/<directory>`
4. Create a directory for the application: `mkdir qradar-ui`
5. To extract the QRadarAnalystWorkflow1.0.0.zip:  
`unzip **QRadarAnalystWorkflow1.0.0.zip -d qradar-ui`
6. To start the application, type: `./qradar-ui/start.sh`

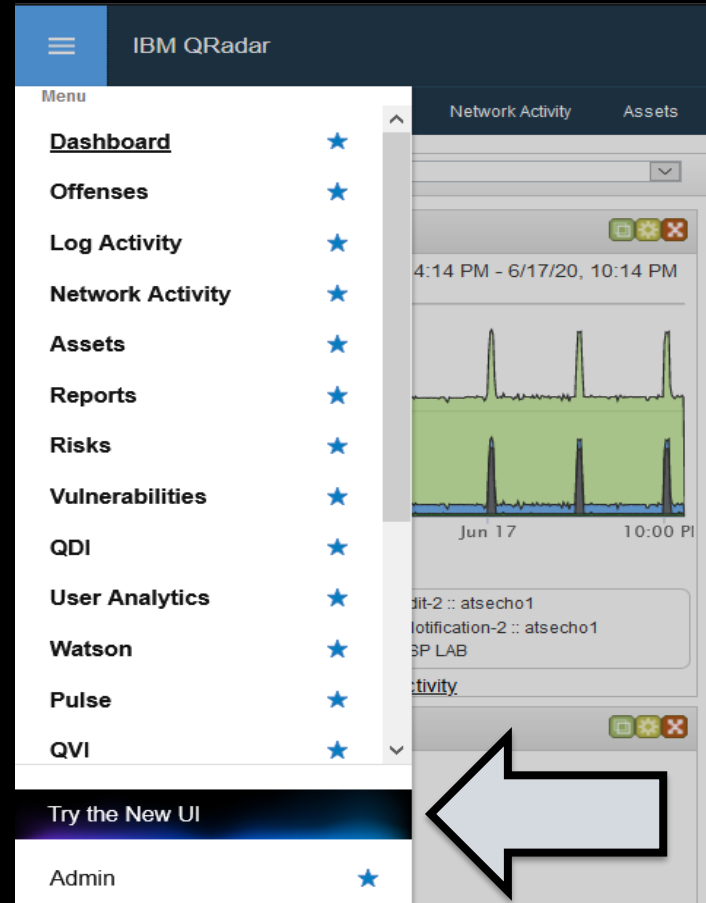
```
[root@qradardev qradar-ui]# ./start.sh
Starting Falcon UI
  UI version - 1.0.0-RC.10
  GraphQL version - 1.0.0-RC.10
QRadar version 7.4.0 or greater is required, found: 7.3.2
```

**Note:** If you experience a '**workload already exists**' message it can be ignored. This is a benign message that displays when someone attempts to reinstall the Workflow Analyst app at the same version.

# Accessing the app

Optional method from your browser address bar:

<https://<QRadar IP address>/console/ui>



IBM QRadar Analyst Workflow

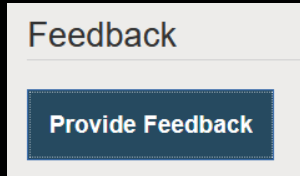
# Demo

# Submitting enhancements

Requests for enhancement allow users to submit features to QRadar Offering teams and product owners for review.

Two methods to submit feature requests:

- QRadar app enhancements (<https://ibm.biz/qradarapprfe>)
- X-Force App Exchange feedback (<http://ibm.biz/analystworkflow>)



## What to include

- Description of your feature enhancement
- Your current app version
- Your current QRadar version
- Use case information you can provide as an example
- Business importance of this feature for your organization

A screenshot of a feedback form. At the top left, there is a speech bubble icon followed by the text "Feedback". Below this, there are five gray stars. A large white text area contains the text "Enter your feedback comments here. Your feedback is only visible to you and IBM." At the bottom of the form, there are two buttons: "Cancel" and "Submit".



IBM QRadar Analyst Workflow

# Common questions

# Questions

Q1: Does the QRadar Analyst Workflow app cost anything?

A1: No, it is a free application.

Q2: Is the QRadar Analyst Workflow app supported?

A2: Yes, entitled users can open cases for issues. What to include in your case:

- Description of your issue
- Add logs to your case
- Your current app version
- Your current QRadar version
- Any troubleshooting you have completed
- Screen capture of the issue

Q3: Does the QRadar Analyst Workflow app V1.0.0 support multitenancy?

A3: Not yet, it is a feature in development.

Q4: Can I still use the old/existing user interface?

A4: Yes, the new interface runs in parallel to the old one

# Questions (continued)

Q5: What do the color codes boxes next to the destination IP represent?

A5: The color of the icon indicate the risk score of the destination IP from X-Force (red=high, orange=medium, yellow=low).



Destination IPs		Don
Multiple (5)		0
▲ EXT	59.154.60.160	0

Q6: Can columns be adjusted or reordered?

A6: Not yet, this is a feature coming soon.

Q7: Does this impact search performance if this app is installed in console?

A7: Not yet, it is a feature in development.

Q8: Is event streaming available in the user interface?

A8: Not yet. This would be a feature request for the development team to review.

Q9: Will this new UI be available in other tabs, like assets and admin?

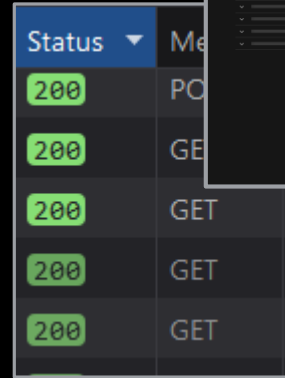
A9: Additional data for more UI functionality is planned for future releases to show data from other applications.

# Questions (continued)

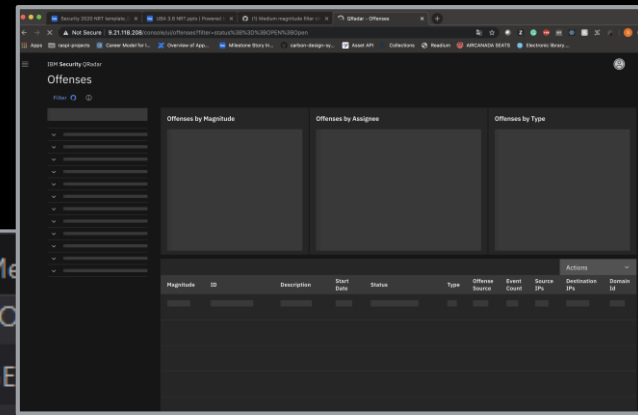
Q10: I installed the application, but do not see data.

A10: Steps the administrator can take:

- Developer tools in your browser can help indicate issues. Click the Network tab and look for connection failures.
- Run `recon ps` to determine if you can connect to the API.
- Verify the container reports OK. How?  
`<ip_address>/console/graphql/readiness`
- Open a case to have your logs reviewed.
- Confirm that certificates are valid in the application logs.



Status	Method
200	POST
200	GET
200	GET
200	GET
200	GET



Q11: Will this application be available as a default app in the future?

A11: Not yet, as this app is in continued development it will eventually be added by default during software upgrades.

Q12: Is a light theme available for the QRadar Analyst Workflow app?

A12: The default theme is dark, but a light theme can be available in a future release.

# Questions (continued)

Q13: Can we search notes added by users?

A13: Not yet, this should be a feature request so note searching can be reviewed.

Q14: When I talk with support, what areas might they check for error messages?

A14: Errors can be identified in the following locations or logs:

- Browser Console/Network tab
- GraphQL container logs
- UI container logs
- QRadar error logs

Q15: What containers are part of this application?

A15: There are two containers that make up the QRadar Workflow Analyst app:

- A UI container
- A GraphQL container

```
[root@qradar ~]# docker ps
CONTAINER ID          IMAGE
db2c935b7cc0         066e413cbd7352c63aec.localdeployment:5000/qradar-graphql:1.0.0-RC.1
eb6833842c79         066e413cbd7352c63aec.localdeployment:5000/qradar-user-interface:1.0.0-RC.1
12a81e93c6da         registry:2.6.2
```

IBM QRadar Analyst Workflow

# Questions and answers

# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://twitter.com/ibmsecurity)

[youtube.com/ibmsecurity](https://youtube.com/ibmsecurity)

© Copyright IBM Corporation 2020. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.

The image features the classic IBM logo, which consists of the letters 'IBM' in a bold, sans-serif font. Each letter is formed by eight horizontal white stripes of equal thickness, set against a dark blue background that has a subtle gradient from top to bottom.