QRadar on Cloud - Quick Start Guide

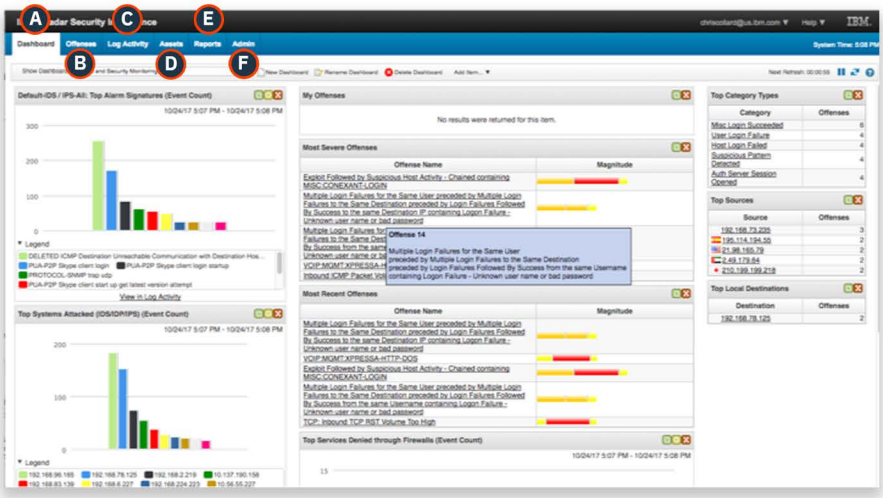
Welcome to the IBM QRadar on Cloud Free Trial! Here are some key activities that you can perform in your trial environment.

1 Login and familiarize yourself with the interface and the QRadar Tabs

(A) Dashboard - A customizable view of offenses, sources, categories & top systems impacted.

(B) Offenses – As events and data pass through the Custom Rules Engine (CRE), it is correlated against configured rules. Offenses are potential incidents identified during correlation and analysis

(C) Log Activity – See a list of live, raw incoming events, add filters and add additional rules based on incoming events.



QRadar on Cloud Interface

(D) Assets – Search and view assets (e.g. servers) and associated details.

(E) Reports – View existing reports; create, edit, or duplicate reports.

(F) Admin – Administer your SaaS instance.*

2 Investigate an offense

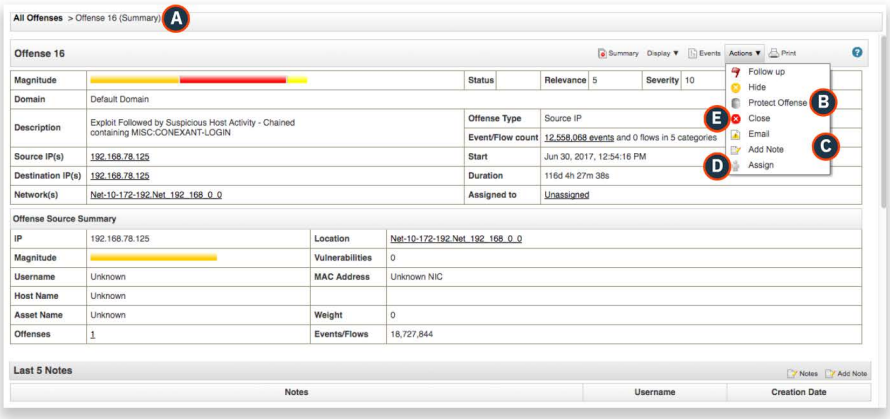
(A) Analyze and Assess – Open the Offense Tab and select a specific Offense for further drill down.

(B) Protect the Offense - The Offense will be protected and not removed from QRadar.

(C) Add a Note - Add comments to the Offense to collaborate on resolution

(D) Assign the Event - Delegate the event to an individual or team for follow up.

(E) Close the Offense - Mark the generated Offense as closed.



Sample Offense View

** Trials do not have full administrative access*

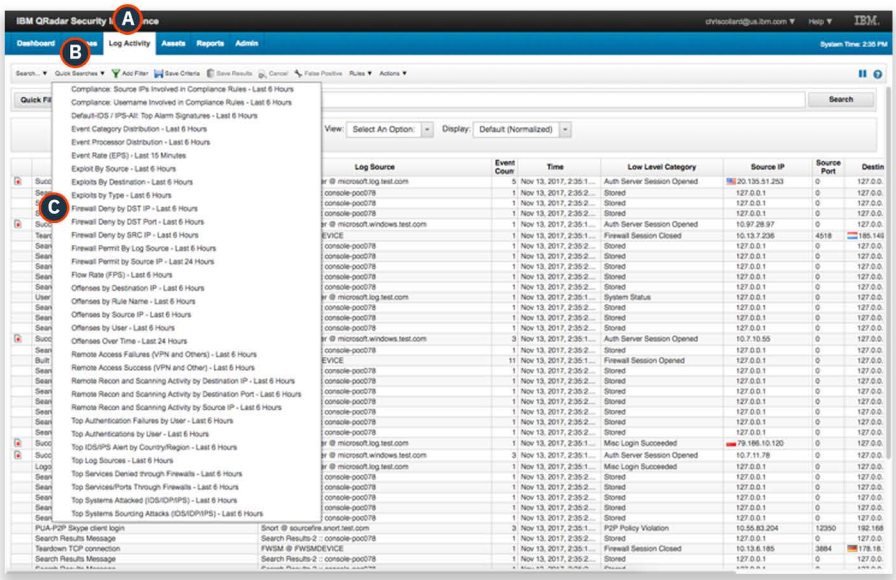
3 Conduct a search

A simple way to use QRadar on Cloud is to conduct a **Quick Search**

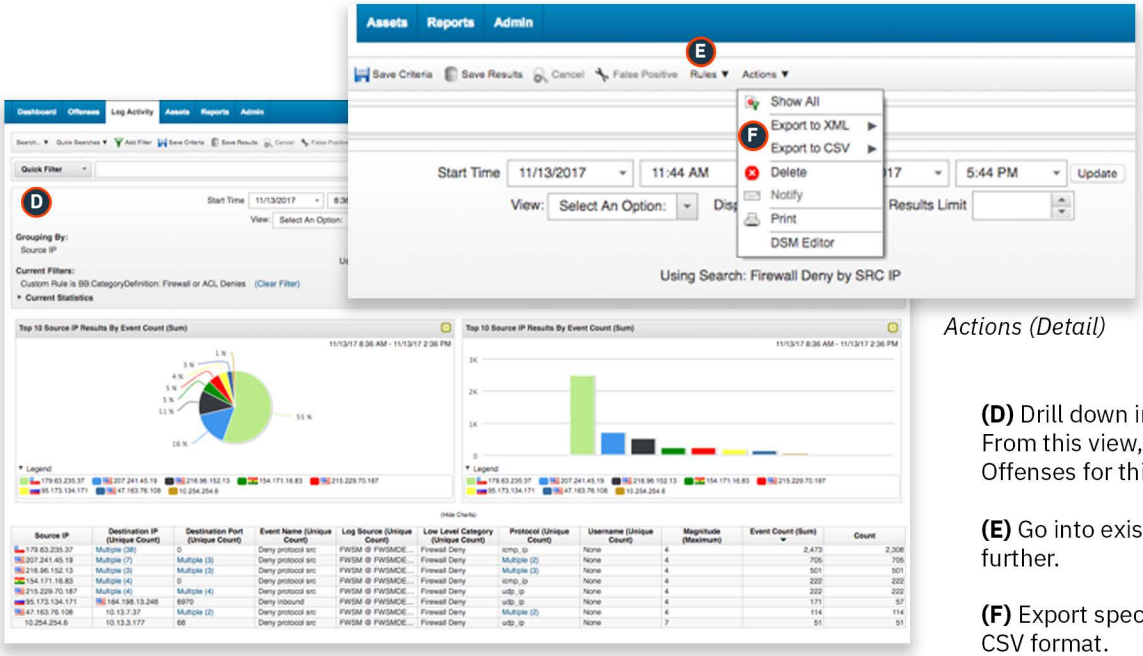
(A) Click on the **Log Activity** Tab.

(B) Click **Quick Search**. From here, you will see a full list of available searches.

(C) Explore this list and select a Quick Search. For example, select a **Firewall Deny rule** - IPs denied by the firewall based on configured rules.



Quick Search View



Actions (Detail)

Firewall Deny Rule View

(D) Drill down into the Firewall Deny rule. From this view, you can view specific Offenses for this rule.

(E) Go into existing rules and modify further.

(F) Export specific log activity in XML or CSV format.

Advanced Search Capabilities

QRadar has a full set of advanced search capabilities – here is an overview from the QRadar community.

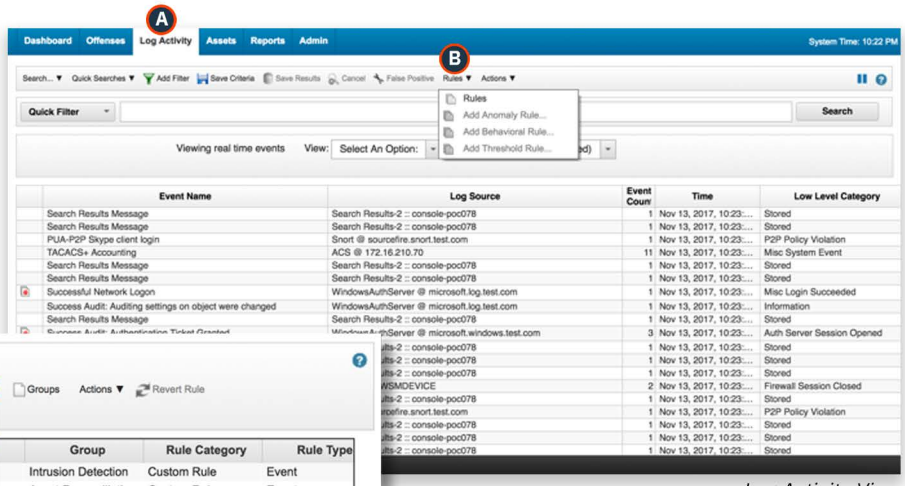
4 Customize a Rule

QRadar allows you start quickly with preset rules while also enabling you to create custom rules specific to your environment. Here are the steps that you can take to create a custom rule.

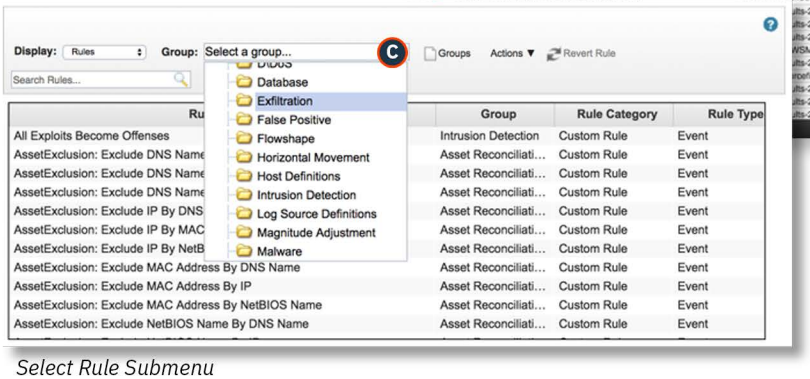
(A) Click on the **Log Activity** Tab.

(B) Select the **Rules** submenu.

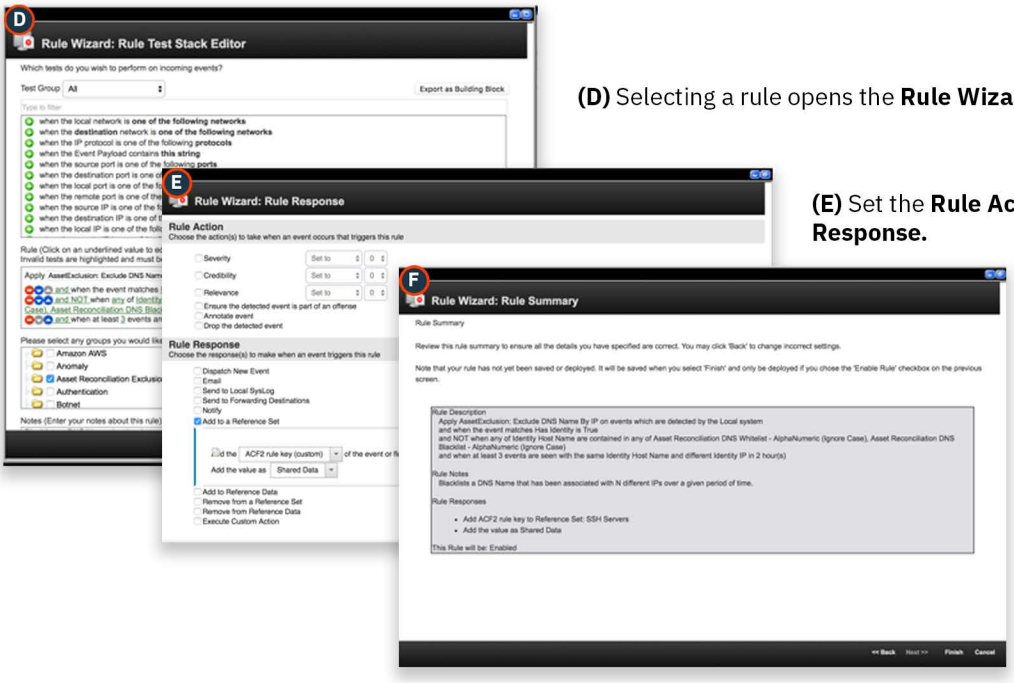
(C) Select from **Rules** directory or select from a group.



Log Activity View



Select Rule Submenu



(D) Selecting a rule opens the **Rule Wizard.**

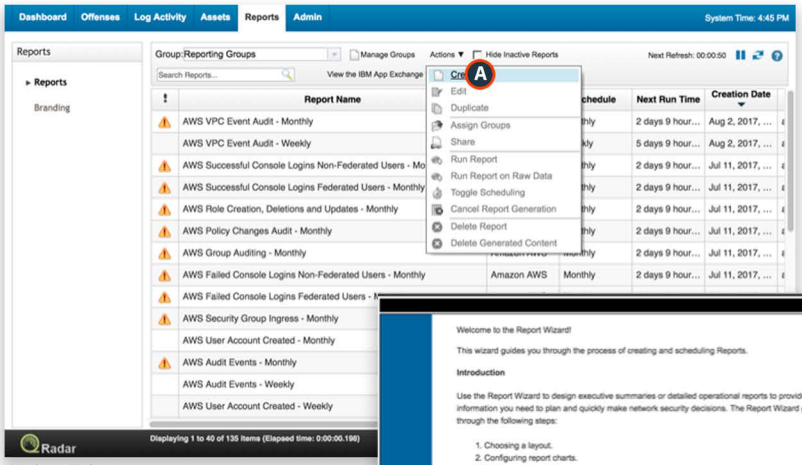
(E) Set the **Rule Action** and the required **Rule Response.**

(F) Confirm the rule change.

5 Creating a Report

You can create reports for a specific interval and can choose a chart type.

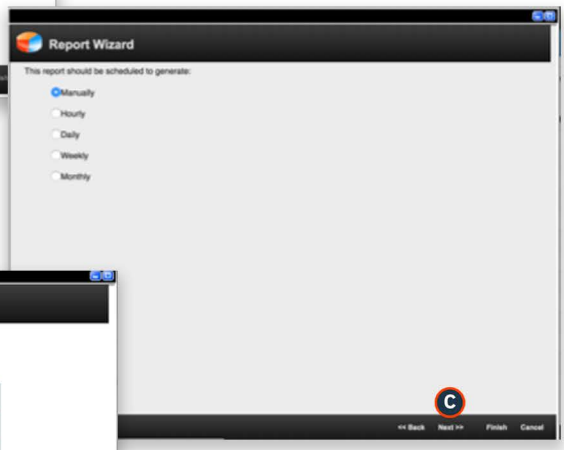
(A) Click on the **Reports** Tab and select from the **Actions** list, then select **Create**.



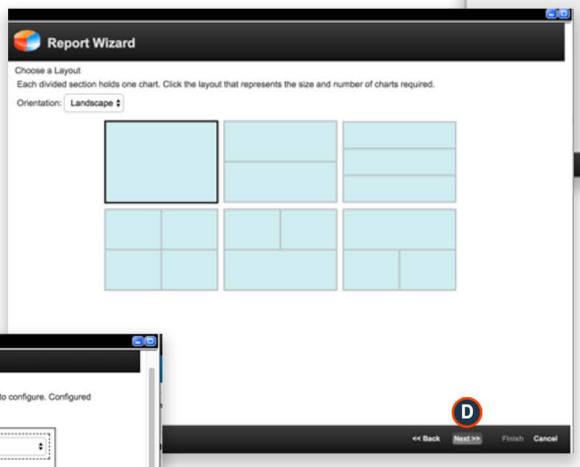
Rules Tab

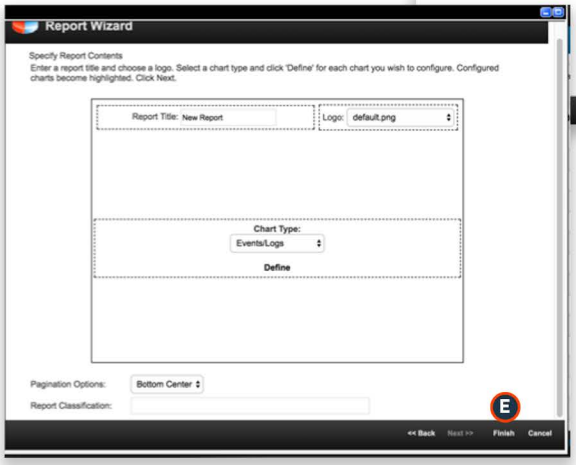
(B) Click **Next** to move to the **Report Wizard**

(C) Select reporting schedule frequency and click **Next.**



(D) Choose a layout for your report; click **Next**.





Add a report title, logo, chart type, and click **Finish**. You can also select the groups to which you want to assign this report.

You can also select to run this report when the wizard setup is complete. Click **Next** to view the report summary.

6 Definitions & Terminology

Custom Rules Engine (CRE)

The Custom Rules Engine (CRE) displays the rules and building blocks that are used by IBM® Security QRadar®. Rules and building blocks are stored in two separate lists because they function differently. The CRE provides information about how the rules are grouped, the tCustom Rules Engine (CRE)

The Custom Rules Engine (CRE) displays the rules and building blocks that are used by IBM® Security QRadar®. Rules and building blocks are stored in two separate lists because they function differently. The CRE provides information about how the rules are grouped, the types of tests that the rule performs, and the responses that each rule generates.

Rules

A rule is a collection of tests that triggers an action when specific conditions are met. Each rule can be configured to capture and respond to a specific event, sequence of events, flow sequence, or offense. The actions that can be triggered include sending an email or generating a syslog message. A rule can reference multiple building blocks by using the tests that are found in the function sections of the test groups within the Rule Editor.

Offenses

As event and flow data passes through the CRE, it is correlated against the rules that are configured and an offense can be generated based on this correlation. You view offenses on the Offenses Tab.

Building Blocks

Building blocks group commonly used tests, to build complex logic, so that they can be used in rules. Building blocks use the same tests that rules use, but have no actions that are associated with them, and are often configured to test groups of IP addresses, privileged user names, or collections of event names. For example, you might create a building block that includes the IP addresses of all mail servers in your network, then use that building block in another rule, to exclude those hosts.

QFlow

Qflows (for the most part) will have a start and end time, or a life of multiple seconds. For example, when you connect to a website, the communication will include HTML files, images, flash files, longer file downloads, etc, and may take some time to transfer the data.

Device Support Module (DSM)

A Device Support Module (DSM) is a configuration file that parses received events from multiple log sources and coverts them to a standard taxonomy format that can be displayed as output. Each type of log source has a corresponding DSM. For example, the IBM Fiberlink MaaS360 DSM parses and normalizes events from a IBM Fiberlink MaaS360 log source.