



# ThreatConnect® Risk Quantifier Release Notes

Software Version 7.6

November 17, 2023



ThreatConnect® is a registered trademark of ThreatConnect, Inc.  
FAIR™ is a trademark of The FAIR Institute.



# Table of Contents

---

<b>New Features and Functionality</b>	<b>4</b>
Custom Loss Models for Semi-Automated FAIR Scenarios	4
Third Party Partners Configuration Updates	5
Updates to FAIR Calculations	6





**Most Likely** field or select a formula to determine the **Minimum** value from the **Choose Formula** dropdown.

- **Most Likely:** Select a formula to determine the **Most Likely** value.

**Note:** You may not select a **Most Likely** formula with a result that is less than 1.

- **Maximum:** After selecting a formula to determine the **Most Likely** value, either enter a percentage of the **Most Likely** value in the **Percent of Most Likely** field or select a formula to determine the **Maximum** value from the **Choose Formula** dropdown.
- **Confidence:** Select your confidence level for this model.
- **Rationale:** Enter a rationale for the confidence level, if desired.

## Third Party Partners Configuration Updates

The 7.6 update for ThreatConnect RQ also brings you a revamped Third Party Partners configuration that echoes the steps for configuring Applications. Now, when you click **Create** from the **Configuration** screen for **Third Party Partners**, you will see the following series of screens: **General Information** → **Identify Business Assets at Risk** → **Identify Attack Surface** → **Summary**.

**New Third Party** Draft

Follow the steps below in order to configure New Third Party.

1 General Information      2 Identify Business Assets at Risk      3 Identify Attack Surface      4 Summary

**Third Party Name**

New Third Party

**Data Related Questions**

- Does the third party handle classified (or sensitive) information?
- Is the 3rd party's access limited just to the data required?
- Does the third party host sensitive data?

**General Questions**

- Does the third party provide hardware, software or other technology that integrates with internal systems?
- Is the third party provided with administrative privileges for internal systems?
- Does the third party represent a single point of failure?
- Is the third party the only provider of the in-scope systems or services?
- Does the third party directly interact with customers / consumers?
- Does the third party utilize subcontractors in delivering systems or services?
- Is there a network connection established with the third party's systems?
- Does the third party deliver its services from an area considered a high-risk area?

In addition, the **Identify Attack Surface** screen enables you to add external scans to your third-party vendors. These scans use semi-automated FAIR scenarios.



**New Third Party** Draft

Follow the steps below in order to configure New Third Party.

1 General Information      2 Identify Business Assets at Risk      3 Identify Attack Surface      4 Summary

**Identify Attack Surface**  
RQ can use internal controls or third party scans for use in computing technical risk for third parties. Enter the internal controls for the third party you are evaluating below or select External Scans.

> Internal Controls ✕

∨ External Scans ✕

Third-Party Vendor Scans

Choose the company from the existing list of external scans

Select

Previous Step Next Step

## Updates to FAIR Calculations

Minor changes were made to the gamma values used in the FAIR calculations. A high confidence, which translates to high gamma values, means that the interval will close in on the number returned as the most likely. Thus, the minimum will steadily increase, converging closely to the most likely. Similarly, the maximum will steadily decrease. In RQ, the gamma values for Low, Medium and High are now set to 1, 4 and 8, respectively.