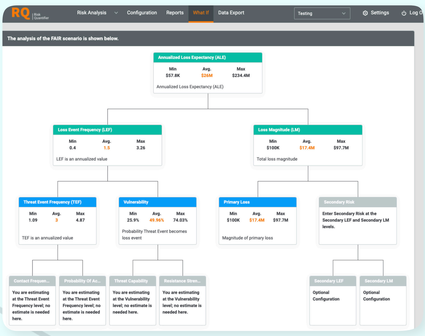
ThreatConnect.

Capability Snapshot

RQ + FAIR = Let's Evolve Together

Evolution without the Revolution – Scale FAIR with Automation

FAIR is the de-facto standard in ThreatConnect Risk Quantifier. RQ supports FAIR by letting users create their own FAIR scenarios. Enter your data into the FAIR taxonomy and run a monte-carlo simulation to get your Loss Exceedance Curve – all within RQ.



Overcoming challenges with FAIR is the key to seeing FAIR adopted at a wider scale in the industry and within companies that are using it today. RQ is introducing semi-Automated FAIR Scenarios that use automation to compute the Loss Event Frequency (LEF) portion of the FAIR taxonomy. Combine that with your Loss Magnitude projections and you have the ability to compute the financial impact of risk scenarios rapidly and at scale.

FAIR | Modified FAIR | RQ

Running FAIR scenarios can be a great way to analyze ad-hoc events or out of band requests. But there are challenges associated with making FAIR operational including:

- Subjectivity of inputs
- Time required to gather data
- Lack of actionable outputs

Computing Loss Event Frequency

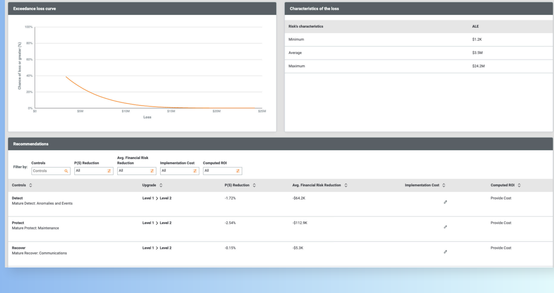
Using RQ you overcome the challenges of scale and speed through a semi-automated FAIR scenario. It uses your inputs for the Loss Magnitude side and the RQ risk engine to compute the ThreatEvent Frequency and Vulnerability side of the taxonomy. RQ runs a simplified kill chain analysis using data from a variety of sources to see what an attacker can do to the defenses you have in place.

Evolve your risk program with semi-automated FAIR scenarios

Leverage your loss data using the RQ risk computation engine capabilities to see what the impacts are to your business, all within the FAIR framework.

Actionability

With semi-automated FAIR scenario's, you can now provide actionable recommendations about what controls will best mitigate risk. No longer do you have to just put in a Loss Exceedance Curve (LEC) for review - you can now show a plan for how mitigations can work to reduce risk for the organization.



Evolution, not Revolution

RQ 6.0 enables FAIR practitioners to use their existing data and processes to model risk as they have been while providing a way to automate and scale the most challenging parts of making FAIR operational.

Cyber risk quantification is something that should be done across the enterprise for all parts of the business. **The way to scale to meet that need is through integration and automation.**

RQ provides the ability to integrate with a variety of tools, including: GRC, Vulnerability scanners, CMBD's and others. It gives you an aggregated view of risk by business unit, application portfolio and business process so you can view organizational risk at multiple organization levels. Combining these features to evolve your application of the FAIR standard provides organizations an easy way to start quantifying cyber risk in a data driven, actionable, and automated manner.

ThreatConnect.

ThreatConnect enables security operations and threat intelligence teams to work together for more efficient, effective, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse threat intelligence and cyber risk quantification into their work, allowing them to orchestrate and automate processes to respond faster and more confidently than ever before. Nearly 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their most critical systems.
Learn more at

ThreatConnect.com
3865 Wilson Blvd., Suite 550 Arlington, VA 22203
sales@threatconnect.com
+1 (800) 965.2708