ThreatConnect | **IBM Security**

ThreatConnect IBM QRadar Integration

Use Validated Threat Intelligence to Easily Spot Trends and Patterns

ThreatConnect® and IBM® have partnered to enable users to detect and act on ThreatConnect intelligence from within IBM QRadar®.

This integration allows users to combine validated Threat Intelligence in ThreatConnect with their aggregated internal logs from QRadar. Users can easily spot trends or patterns that are out of the ordinary and act on them efficiently.
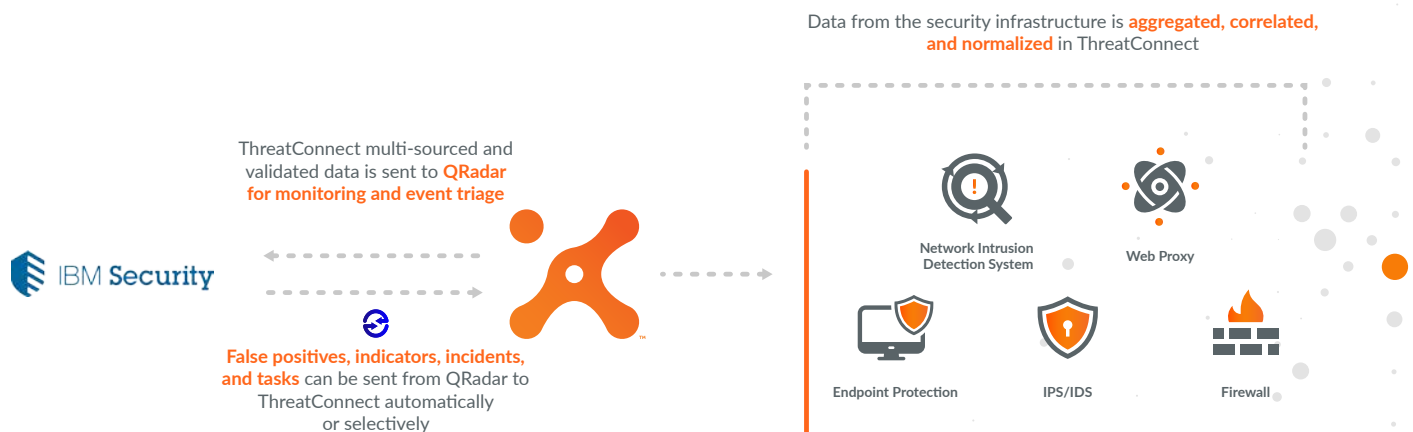
The Challenge

Organizations of all sizes suffer from fragmentation in their security operations.

When security teams don't collaborate and tools don't communicate, critical gaps emerge. By making ThreatConnect intelligence data available in QRadar, you are able to build rules and alerts to identify the most relevant threats, proactively protect your network, and quickly respond to incidents in a measurable way.

The Solution

The integration ensures validated and actionable intelligence is being sent from ThreatConnect to QRadar.

First, intelligence from ThreatConnect is sent to QRadar for monitoring. Then, the additional context provided by ThreatConnect enables the security team to act more efficiently when reviewing alerts. Lastly, this bi-directional integration allows you to send data back to ThreatConnect.

Data from the security infrastructure is **aggregated, correlated, and normalized** in ThreatConnect

ThreatConnect multi-sourced and validated data is sent to **QRadar for monitoring and event triage**

IBM Security

False positives, indicators, incidents, and tasks can be sent from QRadar to ThreatConnect automatically or selectively

Network Intrusion Detection System

Web Proxy

Endpoint Protection

IPS/IDS

Firewall

Features & Benefits

Sends available threat data from ThreatConnect into QRadar for validated alerting

Hover over an indicator in QRadar to see a real-time summary of what ThreatConnect knows about that indicator

Provides the necessary context to be able to take action on indicators

Lookup and create indicators, or report false positives to ThreatConnect from within QRadar

Search QRadar events for matching ThreatConnect indicators using ThreatConnect Playbooks

How to Get Started

If you are a ThreatConnect customer, contact your Customer Success Representative for more information.

If you are not a customer and would like to learn more about this integration or see a demo of the ThreatConnect Platform, please contact sales@threatconnect.com.

ThreatConnect™

Designed by analysts but built for the entire team (security operations, threat intelligence, incident response and security leadership), ThreatConnect's intelligence-driven security operations platform is the only solution available today with intelligence, automation, analytics, and workflows in a single platform. Centralize your intelligence, establish process consistency, scale operations, and measure your effectiveness in one place. To learn more about our threat intelligence platform (TIP) or security orchestration, automation, and response (SOAR) solutions, visit ThreatConnect.com.

ThreatConnect.com

📍 **3865 Wilson Blvd., Suite 550 Arlington, VA 22203**

✉️ **sales@threatconnect.com**

📞 **1.800.965.2708**