IBM Security
Data Sheet

IBM QRadar and the Resilient Incident Response Platform

Fast, intelligent, proactive response from IBM Resilient

Overview

With IBM QRadar® and IBM Resilient®, customers now have access to the industry's first, integrated, end-to-end security operations and incident response platform.

Integrating IBM QRadar into the Resilient Incident Response Platform (IRP) allows you to manually or automatically escalate QRadar offenses into Resilient incidents and enrich Resilient artifacts with data from QRadar.

The Resilient integration for QRadar is available on the IBM Security App Exchange.

Benefits

By integrating IBM QRadar and the Resilient IRP, you empower your security team to:

- **Unify your security solutions within the IBM Security ecosystem, providing fast and seamless integration and quick time to value**
  IBM QRadar and Resilient IRP integration creates a bidirectional channel of communication, escalating offenses into Resilient incidents and providing access to QRadar's data and intelligence sources from inside the Resilient IRP. This ensures you have the full scope of an incident inside your Resilient IR hub, and that the data will map onto the right workflows and tasks automatically.

- **Ask intelligent questions in QRadar directly from Resilient IRP to gain context and save time**
  To further enrich artifacts and other data inside the Resilient platform, you can ask intelligent questions from inside the Resilient IRP UI via Ariel queries. For example, you can ask, "Which machines connected to this C2 IP in this timeframe?" The query is answered quickly without leaving the Resilient IRP single pane of glass.

- **Enrich Resilient incidents with relevant data from QRadar offenses so you can identify, understand and respond faster**
  IBM QRadar and Resilient IRP integration makes it faster and easier to add artifacts to existing Resilient incidents. If you notice a group of events that share an artifact, just right-click on the IP address (or other artifacts in the QRadar UI) and select your Resilient incident from the context menu.

- **Improve your security posture by closing the loop on false positives from within the Resilient IRP**
  As you investigate incidents in Resilient, you may come across false positives and other false alarms based on potentially unimportant artifacts. From within the Resilient UI, you can quickly add artifacts to QRadar Reference Sets. For example, you can add IPs to “False Positive IPs” or automatically add usernames that are appearing in an “Affected Users” Data Table to a Reference Set.

IBM Resilient Incident Response Platform (IRP) is your hub for incident response

By integrating IBM Resilient IRP with QRadar, you arm your IR teams with the technology and intelligence they need to take action quickly and effectively. Resilient IRP helps define, orchestrate, automate, and streamline response processes with built-in workflows based on industry best practices (including NIST and SANS), regulatory guidelines, and customization determined by organizational needs.

Resilient IRP becomes a hub for your IBM Security ecosystem — an integrated security solution with the correct workflows, enriched intelligence, deep-data analytics, and simulation capabilities you need to respond to threats effectively and correctly every time.

With IBM Security, you get access to the industry’s first, integrated, end-to-end Security Operations and Response Platform. By combining the power of QRadar and the Resilient IRP, you can seamlessly take information from the leading detection technology, and leverage it for a faster, more effective, and more intelligent response to security incidents or offenses.

Every organization needs the full suite of prevention, detection and response. Resilient IRP acts as a central hub for managing all three. With the addition of the Resilient platform, you can:

- Increase the ROI of your QRadar deployment
- Bridge the gap between the SOC and your board room
- Create faster time to value

It also provides seamless integration and easy vendor management.

This empowers your security team to build consistent, repeatable, and effective processes for managing and resolving security incidents — and it ensures no security alerts are forgotten.

Free your teams to spend more time focusing on triaging and remediating incidents and less time manually searching for information from different systems. Your IBM representative is committed to your success and will work with you to ensure all of your use cases and processes are covered, and that the Resilient IRP can meet your needs as an IR hub.

About IBM Resilient

The mission of IBM Security is to help organizations thrive in the face of any cyberattack or business crisis. The Resilient Incident Response Platform (IRP) empowers security teams to analyze, respond to, and mitigate incidents faster, more intelligently, and more efficiently. The Resilient IRP is the industry's only complete IR orchestration and automation platform, enabling teams to integrate and align people, processes, and technologies into a single incident response hub. Many Fortune 500 companies, and hundreds of partners globally depend upon IBM for Resilient best-in-class security solutions.

IBM Resilient IRP empowers organizations to thrive in the face of cyberattacks and business crises.

The Resilient Incident Response Platform (IRP) enables faster and more effective response through the orchestration and automation of IR processes. It works seamlessly seamlessly with the prevention and detection systems you use today to create a central hub for IR management.

For more information about IBM Resilient IRP, schedule a demonstration today at: http://info.resilientsystems.com/incident-response-platform-schedule-a-demo

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2018

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

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.