IBM Resilient SOAR Platform and IBM QRadar® Security Intelligence

Highlights

- Escalate suspected incidents quickly to streamline the investigation
- Prioritize analyst workload through automated enrichment
- Synchronize all incident data between QRadar and Resilient
- Leverage MITRE ATT&CK tactics and techniques
- Continuous feedback loop to improve detection accuracy

Aligning SIEM and SOAR to accelerate response times and reduce analyst workload

In a recent market guide report, Gartner identified 'improving alert triage quality and speed' as a key driver for the adoption of security orchestration, automation and response (SOAR) tools.[1] Security operations teams are having to respond to a higher number of more complex, increasingly destructive cyber attacks on their organizations and are looking at how they can automate SOC and incident response (IR) processes to reduce their time to contain and remediate security incidents.

By integrating the IBM Resilient Security Orchestration, Automation and Response (SOAR) Platform with IBM QRadar® Security Intelligence, security teams are able to build out a market leading threat management solution that covers the detection, investigation and remediation of threats across a wide range of cyber use cases. The technology integration between the two solutions allows security analysts to quickly and efficiently escalate suspected offenses from QRadar to Resilient, trigger additional automated enrichments and drive the full investigation process. As the incident evolves, all information is synchronized between QRadar and Resilient, ensuring full data integrity, and any new information uncovered by Resilient is fed back into QRadar to improve the detection process.

Combining the Resilient SOAR platform with an existing QRadar deployment unlocks market-leading security orchestration and automation and case management capabilities, which enable significant improvements to how your organization responds to cyberattacks. QRadar customers can connect with Resilient through multiple fully-supported applications on the IBM Security AppExchange. Resilient can enhance your Security Operations Center (SOC) by seamlessly pairing with your QRadar deployment.

- Match Intelligence and Insights with Automation and Integration

QRadar provides your security analysts with comprehensive visibility to maximize threat and risk insights. With Resilient, analysts can take these threat insights and act quickly to remediate them through customizable workflows and Dynamic Playbooks. Analysts can leverage automation for repetitive and time-consuming tasks, streamlining the entire process.

- Respond Faster When an Attack Hits

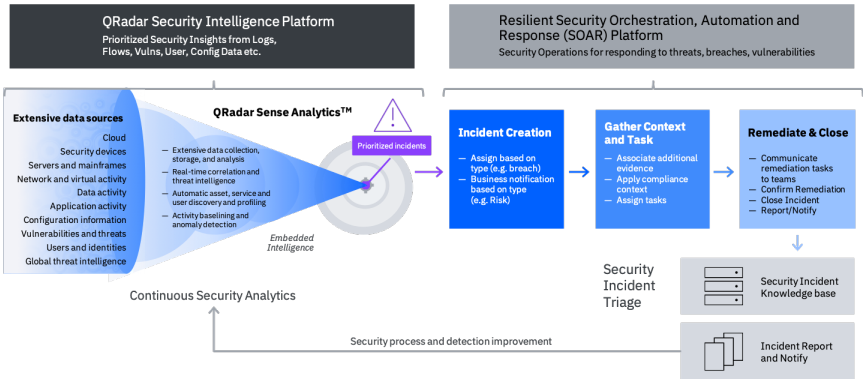
When QRadar has identified a threat early in the cycle, Resilient can improve the response process to remediate the threat faster. Through Guided Response, analysts can leverage proven and tested incident response plans to take them step-by-step from incident investigation to remediation. The introduction of support for MITRE ATT&CK™ in QRadar Advisor with Watson also allows Resilient to enrich the incident information and potentially pivot the response process based on insights derived from MITRE tactics, techniques and procedures (TTPs).

- Improve Processes Before and After an Attack

QRadar and Resilient help improve security process before and after an attack hits. QRadar identifies anomalies early in the attack cycle and enables analysts to continually tune detection mechanisms based on the threat and lessons learned. Resilient enables SOCs to prepare robust and automated IR workflows to orchestrate people, process, and technology. After the attack, the platform has tools to continually assess and refine the process. This learning can be fed back into QRadar, through the bi-directional integration, helping to improve the detection rules and adding new artifacts to QRadar reference sets.

Together, QRadar and Resilient deliver an end to end threat management solution which can accelerate and sharpen the incident response process by combining accurate threat detection, case management, orchestration and automation, and artificial and human intelligence. By quickly and efficiently triggering the investigation of QRadar offenses, analysts can shorten the time to incident remediation.

Analysts can take the insights learned from QRadar and feed them directly into Resilient to respond to the most pressing threats. Resilient provides case management, Dynamic Playbooks with customizable and automated workflows, as well as a robust ecosystem of 3rd party integrations to provide analysts with the tools to use the information they have from QRadar and respond to incidents quickly and efficiently.



The Incident Response lifecycle

Resilient Integrations for QRadar

QRadar users can quickly and easily leverage the benefits of Resilient benefits through 4 integrations that are available on the IBM Security App Exchange:

Resilient + QRadar integration

Delivering automated or manual escalation of QRadar offenses into the Resilient SOAR platform for investigation and remediation. IP addresses and other artifacts can be added to existing or new incidents as part of the integration. Changes to offenses are automatically pushed to existing incidents and notes are bi-directionally synchronized between Resilient and QRadar to ensure data integrity. This integration also supports the linking of multiple QRadar domains with Resilient child orgs to address the MSSP use case.

Resilient + QRadar Functions

This packaged integration includes a search function that enhance workflows by performing actions on reference set items and updating an incident artifact. The search function allows users to manually or automatically execute a search for username, IP address, or offense ID in QRadar, and generate the search results into a custom data table in Resilient. Additional functions include managing and connecting QRadar reference set items with Resilient incident artifacts, which creates a “paper-trail” of updated notes on each artifact. This package contains four functions, five workflows, and five rules from Resilient to run workflows based off incident feedback from QRadar.

Resilient + QRadar Advisor with Watson

This integration allows QRadar Advisor with Watson customers to leverage Watson investigations of Indicators of Compromise to enrich threat insights, map the full scope of the threat, then package and send the threat data and impacted systems to Resilient to remediate the threat. This process substantially expands the capabilities and efficiencies of an incident response process. The power of Watson allows a security analyst to dive deeper into artifacts and provide context surrounding them, making the remediation process faster and more

accurate. The integration also adds MITRE ATT&CK tactic information from a QRadar offense if available.

QRadar-MITRE content package

Working together with QRadar Advisor with Watson, this app includes workflows to retrieve analysis and insights from QRadar Advisor, including ATT&CK tactics and techniques. This information is enriched from the MITRE ATT&CK knowledgebase and can then be converted to incident tasks for follow-up actions, to assist with incident prioritization or to change the response process based on this new information

---

"We refer to Resilient, QRadar and the whole IBM ecosystem as a force multiplier, we've evolved into an organization with a completely comprehensive and dynamic program around security incident response."

—Brian Herr, Chief Security and Privacy Officer, Secure-24

By integrating the Resilient SOAR platform with IBM QRadar, security teams are able to take advantage of highly integrated solutions across detection and response to reduce their time to detect and contain complex cyber attacks.

Aligning Resilient's security automation and orchestration and case management with QRadar's detection and correlation helps security analysts to prioritize their focus on critical incidents, reduce the manual workload on incident investigation and drive a faster, more efficient security operations process.

[1] Gartner, Market Guide for Security Orchestration, Automation and Response Solutions, Claudio Neiva, Craig Lawson, Toby Bussa, Gorka Sadowski, 27 June 2019

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations stop threats, prove compliance, and grow securely.

IBM operates one of the broadest and deepest security research, development and delivery organizations. It monitors more than two trillion events per month in more than 130 countries, and holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

To learn more about the IBM Resilient SOAR Platform, please contact your IBM representative or IBM Business Partner, or visit the following website(s): https://www.ibm.com/security/intelligent-orchestration/resilient