IBM Security SOAR and IBM Security QRadar

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

With the volume of threats increasing, security operations teams are having to respond to a higher number of more complex, increasingly destructive cyber-attacks on their organizations. To help accelerate and coordinate their response, security teams are exploring ways they can automate SOC and incident response (IR) processes to reduce their time to contain and remediate security incidents. In fact, Gartner identified alert triage and prioritization as a key capability of security orchestration, automation and response (SOAR) tools.[1]

By integrating IBM Security SOAR with IBM Security QRadar, security teams are able to utilize a market leading threat management solution that covers the detection, investigation and remediation of threats across a wide range of cybersecurity use cases. The technology integration between the solutions allows security analysts to quickly and efficiently escalate suspected offenses from QRadar to IBM Security SOAR, trigger additional automated enrichments, and drive the full investigation process. As the incident evolves, all information is synchronized between QRadar and IBM Security SOAR, ensuring full data integrity. Any new information uncovered by IBM

Highlights

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

[1] Gartner, Market Guide for Security Orchestration, Automation, and Response Solutions, Claudio Neiva, Craig Lawson, TobyBussa, Gorka Sadowsk, September 21, 2020

Security SOAR is fed back into QRadar to improve the detection process.

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

Combine intelligence and insights with automation and integration

QRadar provides your security analysts with comprehensive visibility to maximize threat and risk insights. With IBM Security SOAR, 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

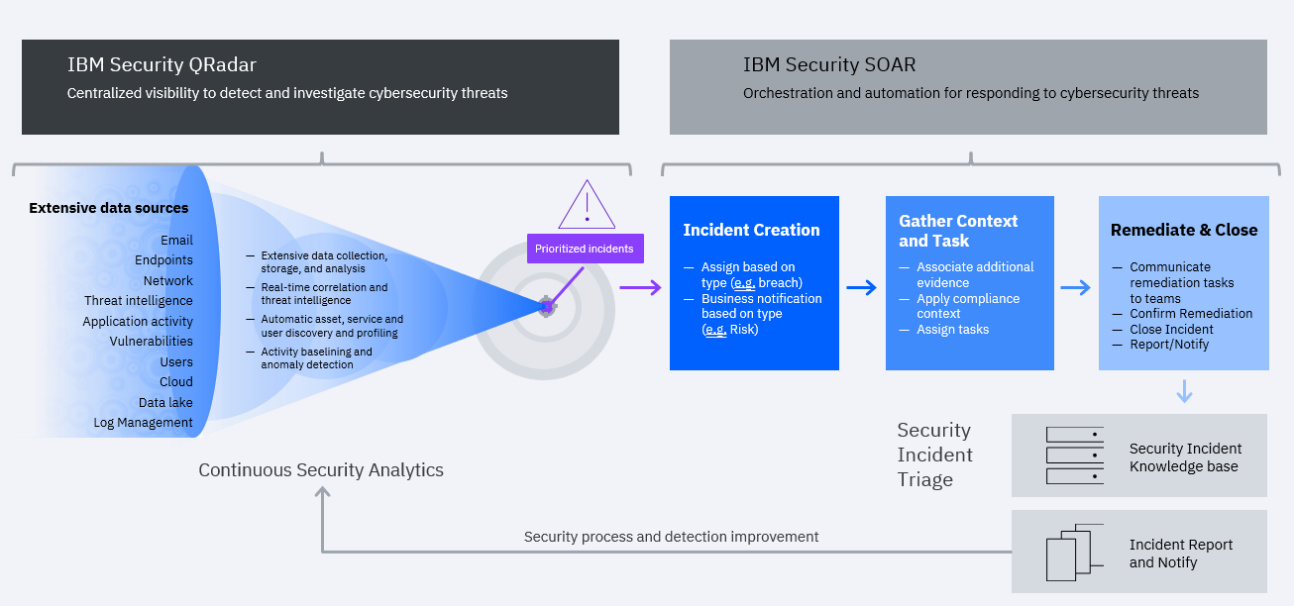
When QRadar has identified a threat early in the cycle, IBM Security SOAR can improve the response process to remediate the threat faster. Through guided response, analysts can leverage proven and tested incident response plans to take them step-by-step from incident investigation to remediation. Support for MITRE ATT&CK® in QRadar also allows IBM Security SOAR 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

IBM Security QRadar and IBM Security SOAR help improve security process before and after an attack occurs. QRadar identifies anomalies early in the attack cycle and enables analysts to continually tune detection mechanisms based on the threat and lessons learned. IBM Security SOAR 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 IBM Security SOAR 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 IBM Security SOAR to respond to the most pressing threats. IBM Security SOAR 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 life cycle

IBM Security SOAR Integrations for QRadar

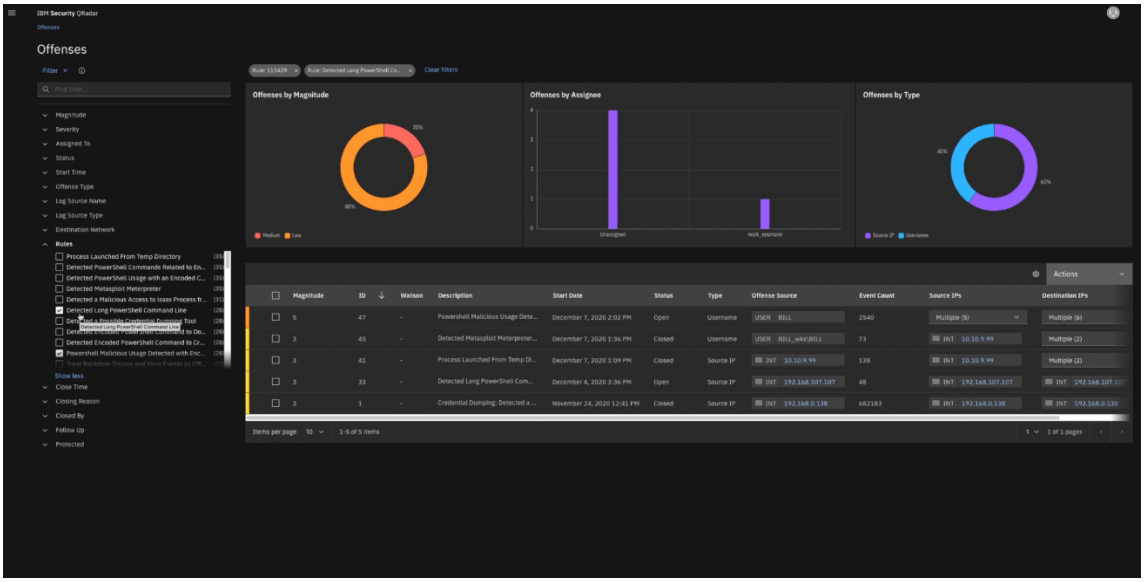
QRadar users can quickly and easily leverage the benefits of IBM Security SOAR through 4 integrations that are available on the IBM Security App Exchange:

IBM Security SOAR + QRadar integration

This integration delivers automated or manual escalation of QRadar offenses into IBM Security SOAR 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 IBM Security SOAR and QRadar to ensure data integrity. This integration also supports the linking of multiple QRadar domains with IBM Security SOAR child orgs to address the MSSP use case.

IBM Security SOAR & QRadar Enhanced Data Migration

The QRadar Enhanced Data Migration integration with IBM Security SOAR provides a rich, simplified and centralized view of Offense data from QRadar. This out-of-the box capability allows access to detailed Offense information through the 'QRadar Offense Details' tab within IBM Security SOAR. Within this tab, security teams can quickly reference the details associated with a QRadar Offense, such as the ID, source and destination IPs, and associated events. In addition, security analysts can easily access event information directly in QRadar, helping speed up the investigation process. Creating an artifact from an event in IBM Security SOAR helps enrich and remediate cases and provide visibility to the incident response team.



Associated QRadar offense accessed through IBM Security SOAR

IBM Security SOAR + QRadar Functions

This packaged integration includes a search function that enhances 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 IBM Security SOAR. Additional functions include managing and connecting QRadar reference set items with IBM Security SOAR incident artifacts, which creates a "paper-trail" of updated notes on each artifact. This package contains five functions, six workflows, and six rules from IBM Security SOAR to run workflows based off incident feedback from QRadar.

[IBM Security SOAR + 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 IBM Security SOAR 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 IBM Security SOAR, 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 IBM Security SOAR with IBM Security 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 IBM Security SOAR'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.

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 drive security into the fabric of their business so they can thrive in the face of uncertainty.

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

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Security SOAR and IBM Security QRadar, please contact your IBM representative or IBM Business Partner, or visit the following websites:

https://www.ibm.com/security/intelligent-orchestration/soar

https://www.ibm.com/security/security-intelligence/qradar