IBM Security QRadar SOAR and IBM Security QRadar SIEM Integration

Accelerate response times and reduce analyst workload

Highlights

Simplified analyst experience through a seamless integration

Extended visibility for better contextual threat and risk insights

Faster responses and continuous improvement

Proactive attack mitigation with automated workflows

Due to an increase in the volume of threats, security operations teams have to respond to a high number of increasingly complex and destructive cyberattacks on their organizations. Security teams typically purchase a variety of tools and software to combat these attacks and help them remediate issues. The simultaneous use of different tools can sometimes cause problems, creating more work for security analysts. To be efficient, your security personnel need tools that work together.

IBM Security® QRadar® SIEM and IBM Security® QRadar® SOAR integrate together to allow security analysts to quickly and efficiently detect, investigate and respond to threats. QRadar SIEM is a software solution that collects, monitors and correlates events to provide security analysts with prioritized high-fidelity alerts. QRadar SOAR is a solution that provides automatic responses for those high-fidelity alerts, helping your security team respond to threats with confidence. By integrating QRadar SOAR with QRadar SIEM, security teams can utilize a market-leading threat management solution that covers the detection, investigation, and remediation of threats across a wide range of cybersecurity use cases.

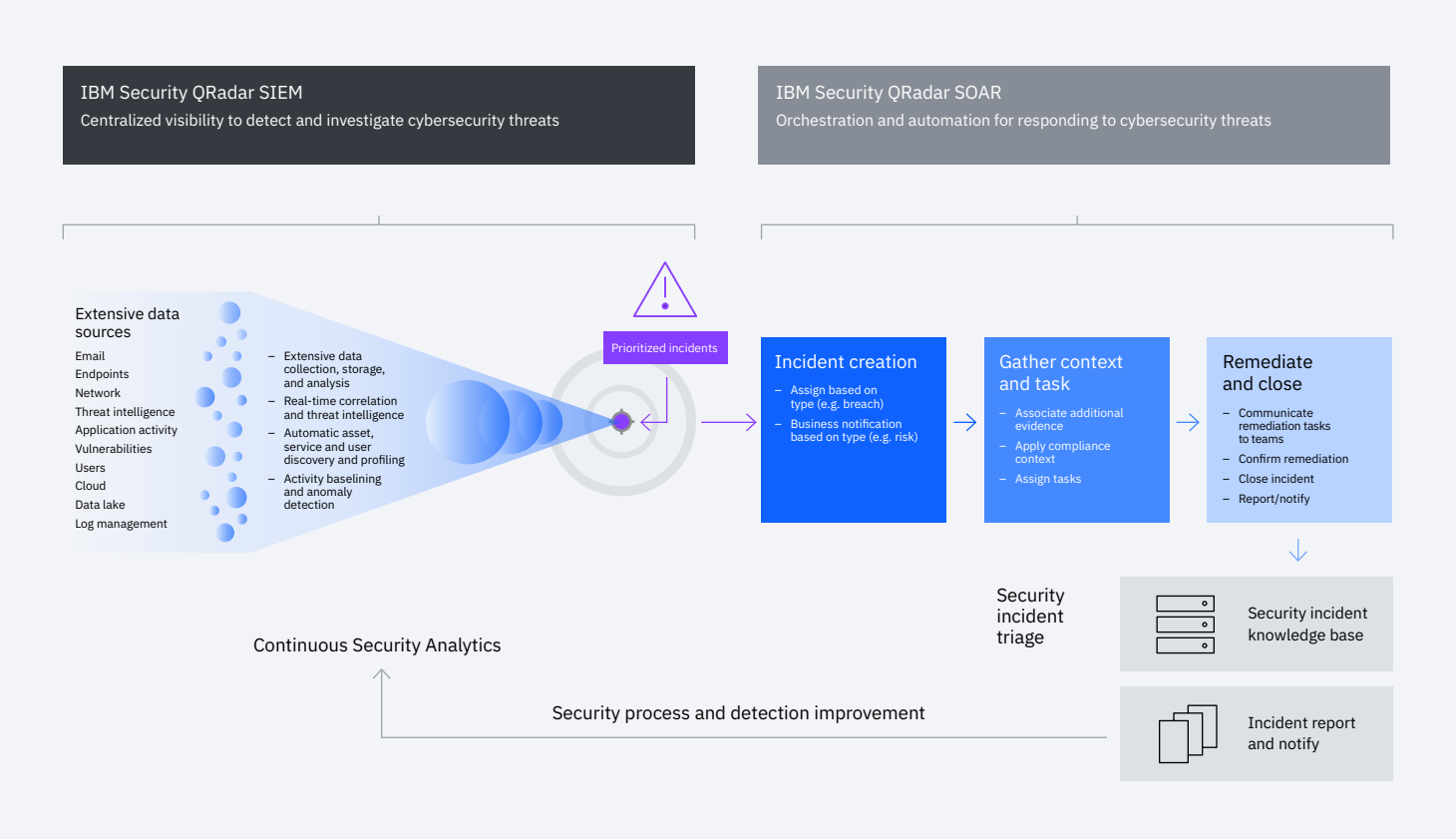

Figure 1. QRadar SIEM and QRadar SOAR integration workflow

Simplified analyst experience through a seamless integration
Combining QRadar SOAR with an existing QRadar SIEM deployment unlocks security orchestration, automation and case management capabilities. This can significantly improve how your organization responds to cyberattacks. QRadar SIEM customers can connect with QRadar SOAR through multiple fully-supported applications on the IBM Security App Exchange. QRadar SOAR can enhance your Security Operations Center (SOC) by seamlessly pairing it with your QRadar SIEM deployment.

QRadar SIEM collects data from your environment with help from more than 700 partner extensions and integrations. This gives you complete visibility of your environment. When threat actors trigger multiple detection analytics, move across the network, or change their behaviors, QRadar SIEM tracks each tactic and technique being used throughout an attack structure. The solution then rates the threat, automatically prioritizing high-fidelity alerts.

QRadar SOAR augments the analyst experience, helping teams work smarter in the face of today's security threats. With a seamless integration into your existing security infrastructure, QRadar SOAR provides tools to help you accelerate incident response times, optimize SOC operations, and connect business stakeholders through a centralized security hub. QRadar SOAR simplifies the analyst experience with automated and intelligent responses. This allows analysts to take remediation and response actions by leveraging over 250 partner extensions and integrations available on the IBM App Exchange.

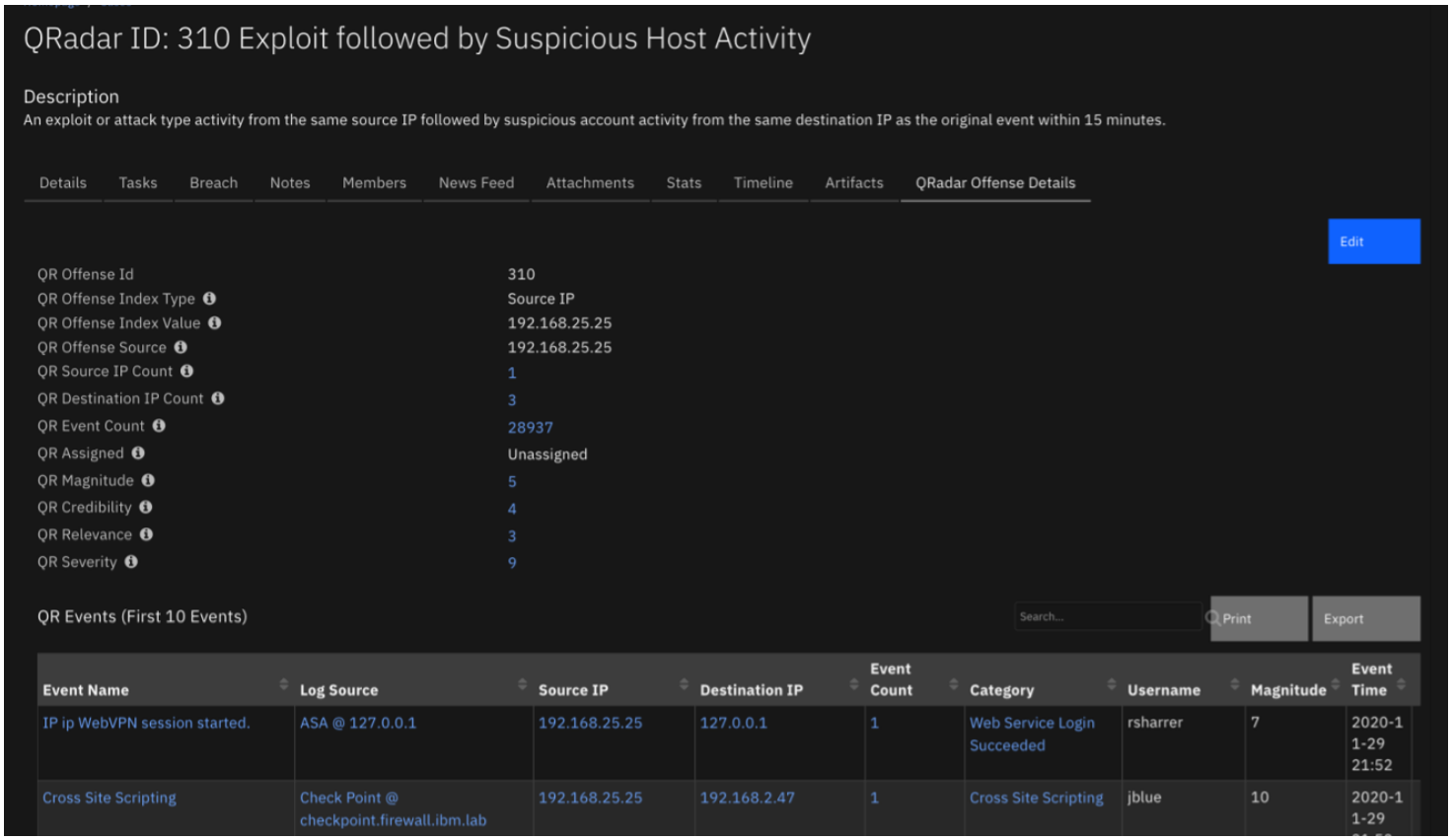

Figure 2. QRadar SOAR case details

Extended visibility for better contextual threat and risk insights
QRadar SIEM provides your security analysts with comprehensive visibility to maximize threat and risk insights. With QRadar 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.

When evaluating third party SIEM integrations for QRadar SOAR, all of our existing integrations provide basic bidirectional synchronization of notes and the ability to close events. However, when evaluating QRadar SIEM and QRadar SOAR, our Enhanced Data Migration (EDM) app is a force-multiplier of QRadar SOAR functionality. With our EDM integration, analysts can see everything related to an offense in a single view; eliminating the need to repeatedly switch between tools. A “QRadar Offense Details” tab is created within a SOAR case, containing auto-generated data tables displaying triggered rules, destination IPs and associated events. In addition, the Live Links feature within the QRadar Offense Details tab enables analysts to quickly navigate back to the QRadar SIEM analyst workflow for further information. As the offense evolves, the EDM app auto-refreshes within SOAR so the analyst is always presented with the latest information.

↓97%

By using QRadar SOAR, formally IBM Resilient, your team could reduce incident response time by 97%[1]

Fast attack response and continuous improvement
When QRadar SIEM has identified a threat early in the attack cycle, it can improve the response process to remediate the threat faster. Through guided response, analysts can leverage incident-response plans to take them step-by-step from incident investigation to remediation. Support for MITRE ATT&CK in QRadar SIEM also allows QRadar SOAR to enrich the incident information and potentially pivot the response process based on insights derived from MITRE tactics, techniques and procedures (TTPs).

When it comes to facilitating responses, analysts can leverage QRadar SOAR's Playbook Designer; a graphical UI intended to lower the barrier to entry for building automation. Playbook Designer provides a streamlined and intuitive experience with in-app guidance and drag and drop automation configurations to help accelerate the playbook creation process. SOC teams can leverage a modern canvas to easily build and manage automation, utilizing manual or automatic triggers.

Proactive attack mitigation with automated workflows
QRadar SIEM identifies anomalies early in the attack cycle and helps analysts continually tune detection mechanisms based on the threat and previous lessons learned. QRadar SOAR enables SOC teams to prepare robust and automated incident response workflows to orchestrate people, processes and technology. After the attack, the platform uses tools to continually assess and refine the process. This learning can be sent back into QRadar SIEM, through the bi-directional integration, helping to improve the detection rules and adding new artifacts to QRadar SIEM reference sets.

QRadar SOAR provides case management, dynamic playbooks with customizable and automated workflows, and a robust ecosystem of third party integrations. This provides analysts with the tools to use the information they have from QRadar SIEM and respond to incidents quickly and efficiently.

Conclusion

By integrating QRadar SOAR with QRadar SIEM, security teams can take advantage of highly integrated solutions to reduce their time to detect and contain complex cyber-attacks. Aligning the security automation, orchestration and case management of QRadar SOAR with the detection and correlation capabilities of QRadar SIEM helps security analysts to prioritize their focus on critical incidents. The integration also helps 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 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. IBM holds over 3,000 security patents and monitors more than one trillion events per month in more than 130 countries. To learn more, visit ibm.com/security.

For more information

To learn more about IBM Security QRadar SOAR and IBM Security QRadar SIEM, please contact your IBM representative or IBM Business Partner, or visit ibm.com/products/qradar-soar or ibm.com/products/qradar-siem.

1. The Total Economic Impact of IBM Resilient, A Forrester study commissioned by IBM, October 2017.

© Copyright IBM Corporation 2022

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
December 2022

IBM, the IBM logo, IBM Security, QRadar, and X-Force are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

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.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

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: 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 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.