IBM Security QRadar SOAR

Improve SOC efficiency. Respond quicker. Help close skill gaps.

Highlights

Streamlines security center response with automation and intelligence

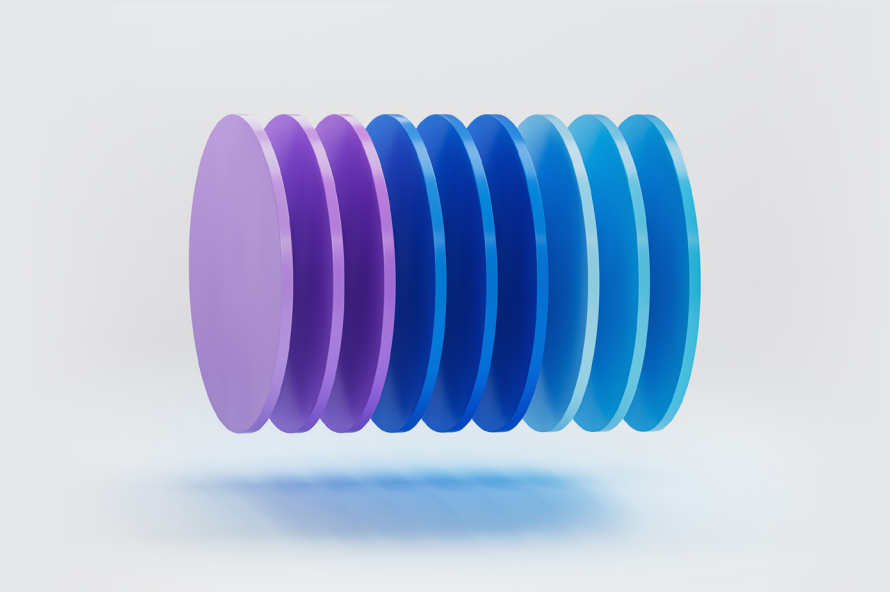
Accelerates incident response with automated investigations

Integrates and responds quickly with over 300 integrations

Helps maintain compliance throughout data breach incident response

The early decisions you make when responding to a potential security incident often make the difference between containment or crisis. Unfortunately, most organizations rely heavily on manual processes or custom code. This lack of automation can contribute to the growing cost of data breaches and the associated legal, regulatory and lost business expenses. In 2023, the average cost of a data breach globally was USD 4.45 million, a 15% increase in just 3 years.[1]

IBM Security® QRadar® SOAR software helps automate and orchestrate incident investigation and response. It can reduce the complexity of responses and uses a broad ecosystem of connectors and dynamic playbooks that are built to help your security operations center (SOC) team respond faster.



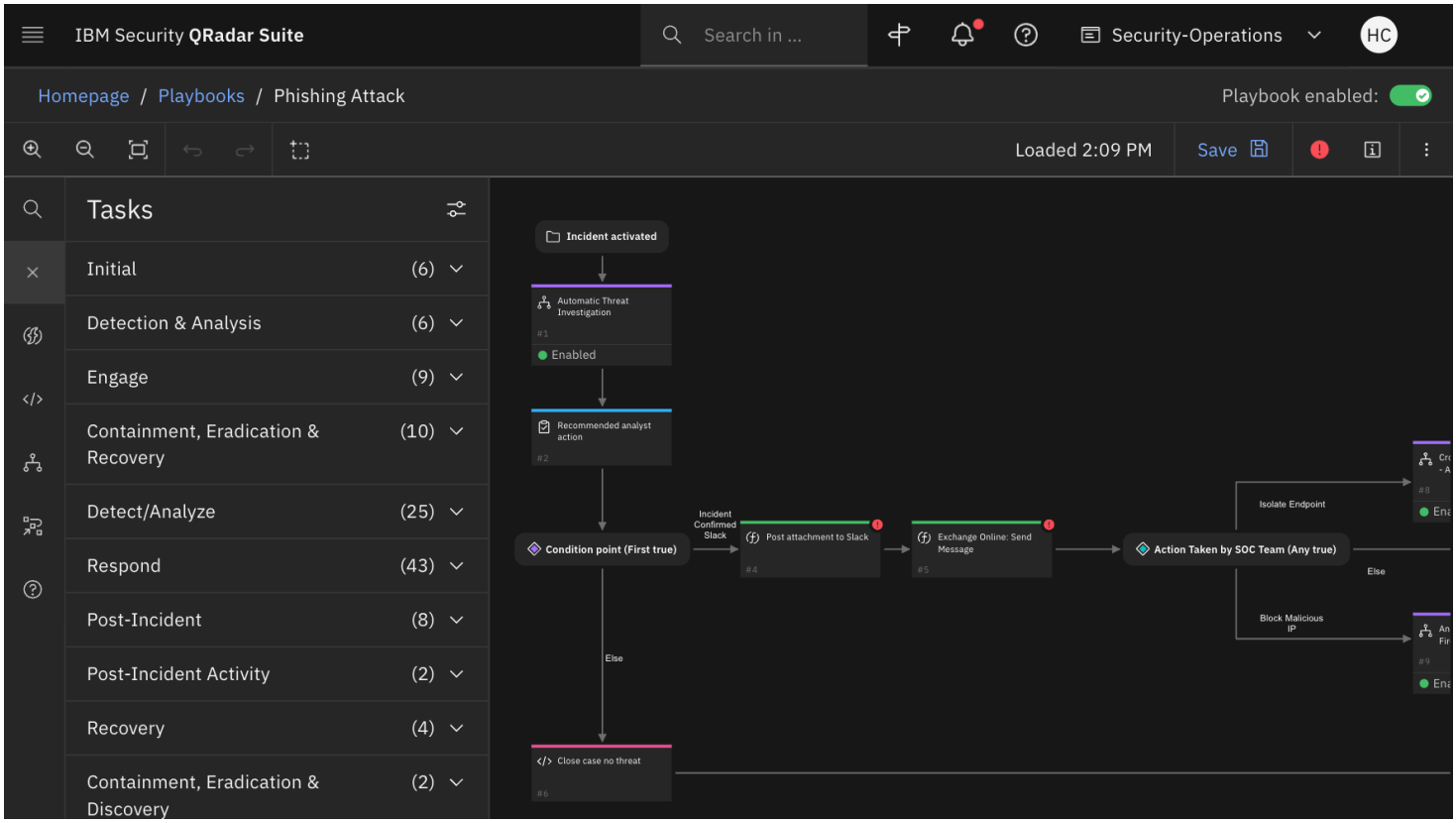


Figure 1. The Playbook Designer in QRadar SOAR helps analysts accelerate response.

Streamline response with automation and intelligence

QRadar SOAR offers a powerful playbook designer so your security team can respond to incidents quickly and decisively. As a recent winner of the Red Dot Design Award, the Playbook Designer presents a modern, graphical canvas that makes it easier for security analysts to build and manage automation tasks. By design, QRadar SOAR playbooks are dynamic, so teams can react with confidence as incident conditions evolve. Reusable sub-playbooks help standardize activities and accelerate development across common, repeatable use cases.

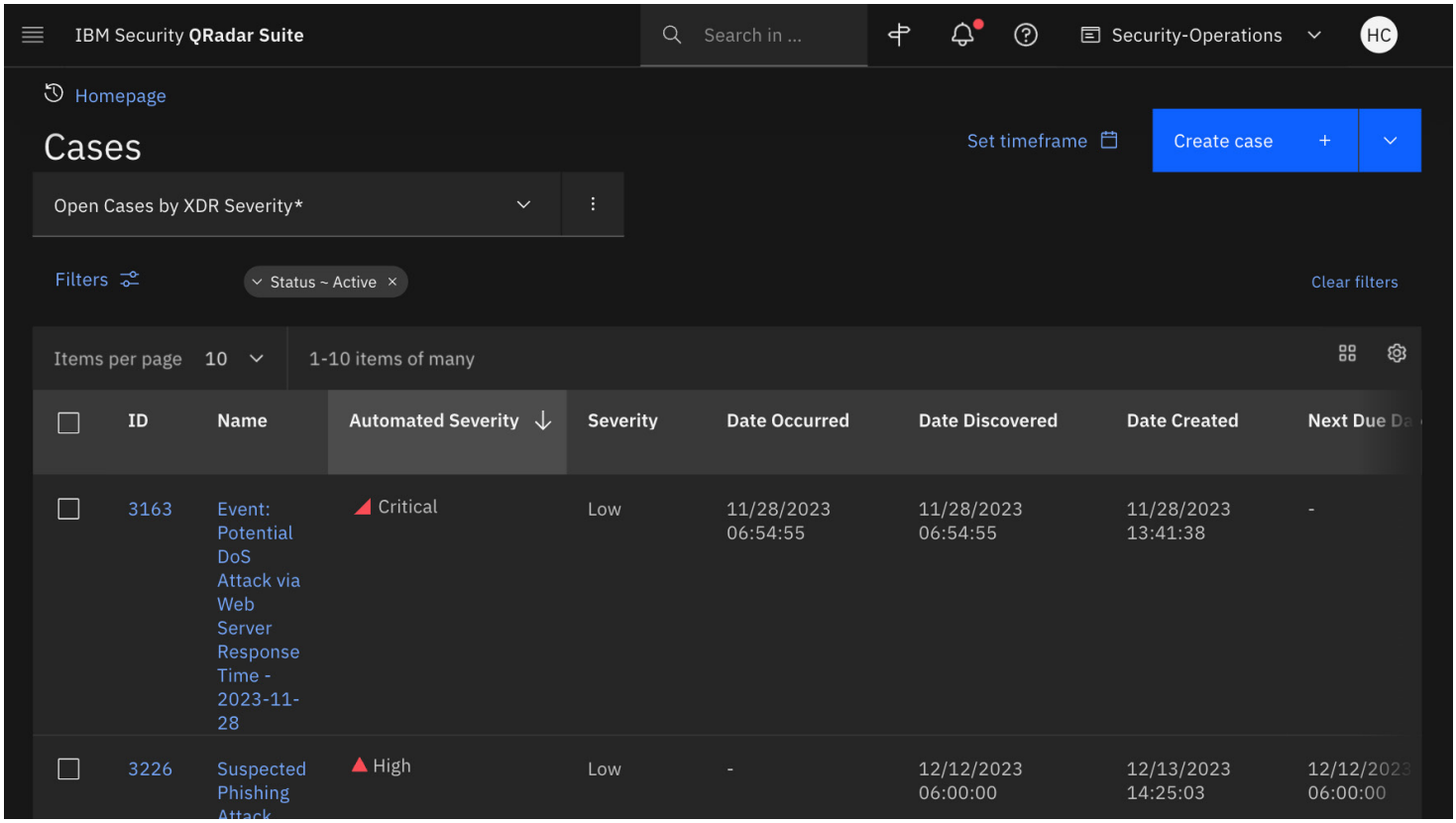


Figure 2. The cases view in QRadar SOAR, which is enriched and correlated by the UAX, provides a contextualized view of incidents.

Accelerate incident response with automated investigations

With the combined power of QRadar SOAR and the included Unified Analyst Experience (UAX), security analysts can get immediate incident context through automated investigations, check root cause analysis, and identify response recommendations. The software correlates, enriches and prioritizes the incident before analysts even begin an investigation.

Within an identified case, UAX gives security analysts an automated severity score. They can click to get more context and transparency about how the severity score was calculated. The analysts can also see a machine learning generated confidence score as well as the related artifacts and findings that contributed to the score. The QRadar SOAR threat investigation tab gives analysts a chronological view of the entire incident and displays the pre-enriched artifacts and associated data sources that contributed to the larger case.

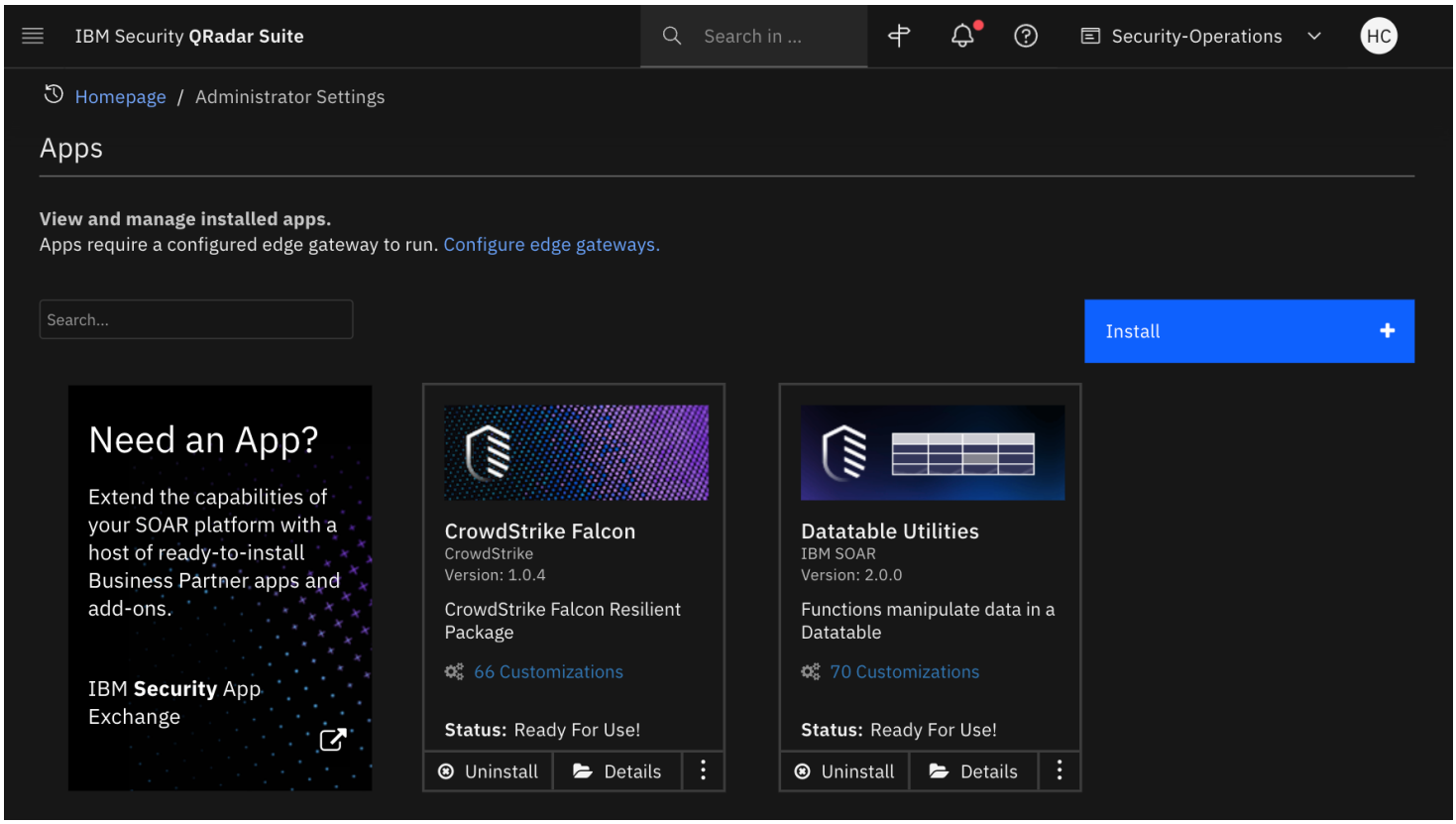


Figure 3. QRadar SOAR supports a wide ecosystem of integrations into response plans.

Integrate and respond quickly with over 300 integrations
QRadar SOAR offers more than 300 no-cost integrations and content packs including some of the industry's most widely adopted security solutions. The integration materials are all available through the IBM Security App Exchange. With these integrations, teams can achieve faster time-to-value using the solution's included capabilities and content to extend their existing security investments.

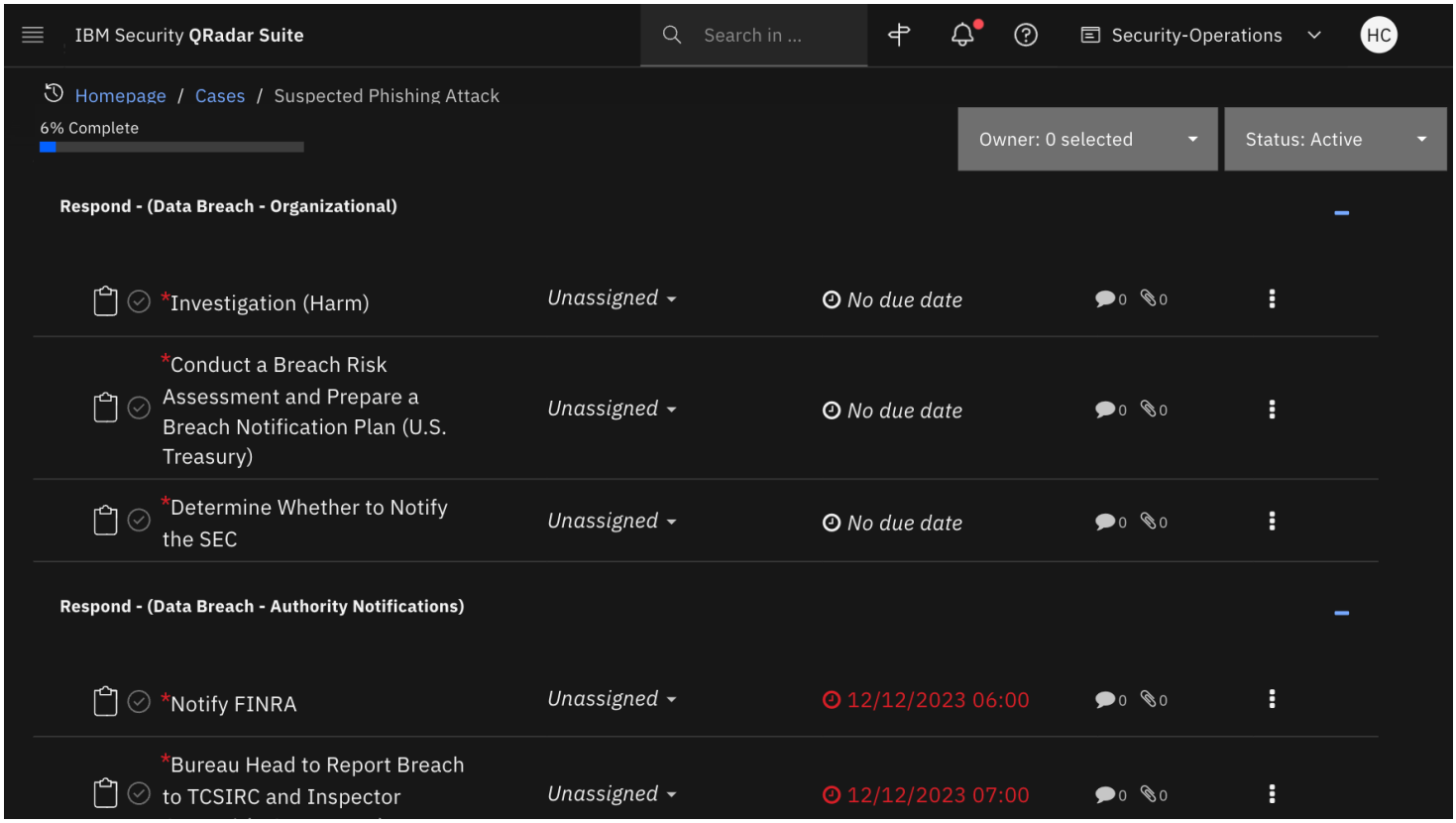


Figure 4. QRadar SOAR breach response helps organizations address compliance in their response.

Help maintain compliance throughout data breach incident response
QRadar SOAR breach response supports over 200 privacy regulations worldwide. This support allows security teams to integrate privacy reporting tasks into overall incident response playbooks. It facilitates collaboration across privacy, HR and legal teams by giving them guidance focused on addressing regulatory requirements. It helps security teams transform current manual tasks required for privacy and compliance into an automated, efficient process. This automation guidance can provide a single point for preparation, assessment and management of a data privacy breach.

Conclusion

For security teams responding to incidents, QRadar SOAR helps analysts use automation and intelligence that can streamline and optimize the response process for faster response times. QRadar SOAR makes it easier for security analysts to dedicate their time and energy where it's needed most so they can respond with greater confidence to help organizations minimize losses.

Why IBM?

IBM Security—supported by world-renowned IBM X-Force® research—offers one of the most advanced and integrated portfolios of enterprise security products and services. IBM security solutions help organizations spread security throughout the fabric of their business so they can thrive—even in the face of uncertainty. IBM holds over 3,000 security-related patents and monitors more than one trillion events per month in more than 130 countries. To learn more, visit www.ibm.com/security.

For more information

Find out more about IBM Security QRadar SOAR by contacting your IBM representative, or IBM Business Partner or visiting ibm.com/products/qradar-soar.

1. IBM Security, Cost of a Data Breach Report 2023, July 2023.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
March 2024