IBM Security Resilient Security Orchestration, Automation and Response (SOAR) Platform Privacy Add-On

Highlights

- Orchestrate all aspects of the incident response process
- Support for 174 state, global and industry specific regulations
- Coordinate response process with privacy tasks and workflows
- Risk Assessment tools help evaluate notification requirements

Fast, Intelligent, Proactive Response to Privacy Breaches

State, global and industry-specific breach notification regulations are resulting in additional cost and complexity for organizations worldwide as they look to meet privacy reporting requirements. Security and Privacy teams need to align their processes in order to report privacy data breaches to different regulatory authorities with different reporting requirements and deadlines or risk the impact of negative publicity and costly fines.

The Privacy Add-On for the IBM Security Resilient Security Orchestration, Automation and Response (SOAR) Platform provides organizations with support for 174 privacy incident reporting regulations worldwide, allowing security teams to integrate privacy reporting tasks into their overall incident response playbooks and work together with your privacy and legal teams to address regulatory requirements.

The Resilient SOAR Platform Privacy Add-on

The Resilient Privacy add-on is a key addition to the Resilient SOAR Platform. The solution helps to transform current manual tasks for assessing privacy risk and reporting requirements into an automated, efficient process that can provide a single point for preparation, assessment and management of a data privacy breach.

By integrating privacy reporting deadlines into the broader Incident Response (IR) process, the Resilient SOAR platform helps organizations to maintain a single, auditable record of all aspects of their breach response. This single "system of record" can help provide value to security leaders as they conduct post-incident reviews and create the reporting package for regulators.

A single, integrated system for all aspects of security incident management supports strong alignment between your privacy, legal and security operations teams. The Resilient SOAR platform can become a centralized hub for all breach information, as security teams look to integrate information from different security tools such as Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) and firewalls.

Aligning people, process and technology

Additionally, integrations with IT operations tools , IT Service Management (ITSM) and ticketing systems can help to gather information and assign tasks to team members outside of the core security team.

Third party integrations for the Resilient SOAR platform are available from the IBM Security App Exchange. The App Exchange offers more than 130 validated and community apps, with additional apps being added regularly. Customers also can develop their own integrations for bespoke or customized applications, leveraging fully-documented APIs and supported by IBM developer resources.

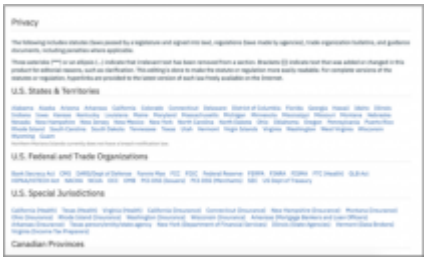
Key features of the Resilient Privacy solution include:

Global Privacy Knowledgebase

At the heart of the IBM Security Resilient Privacy add-on is the global knowledgebase. This database is a regularly updated database of breach notification regulations across US states and countries in Europe, the Middle East and Asia. The database also includes industry-specific regulations with a

privacy breach reporting requirement, such as HIPAA.

An internal team of certified privacy professionals manages the global knowledgebase. These privacy professionals communicate with regulators, privacy professionals from the IBM customer base and the wider privacy community to keep the knowledgebase updated.

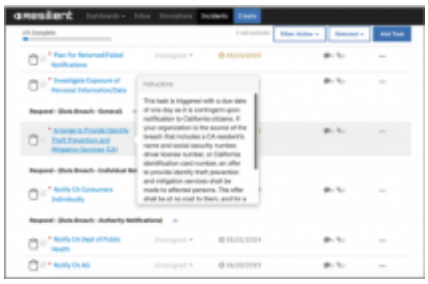


Global Knowledgebase

The Resilient privacy team monitors the regulatory landscape for upcoming and updated regulations and tracks their process. The team works with partners and customers on how to best implement these regulations inside the platform. Regular release notes provide updates on new or upcoming regulations so customers can review their relevance and adjust their breach response plans as appropriate.

Guided Data Breach Notification

The Resilient Privacy Add-on allows customers to integrate breach notification into the wider cybersecurity incident response process, with privacy-specific tasks integrated into the overall incident playbook. Derived from the specific reporting requirement, these tasks detail the steps that the members of the privacy team should take to address the reporting requirements. The privacy add-on tracks data breaches that triggers multiple reporting requirements as separate tasks inside the overall incident. This process gives privacy and security teams a single view of all privacy and security related aspects of an incident.If required by a regulation, operators of the add-on can assign specific users and specific timelines for incident tasks.



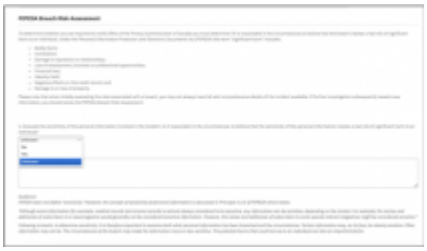
Incident Playbook

While the information varies based on the regulation, these tasks can often include the following items:

Document the breach - Prompts and guides the team on what documentation is required throughout the response process. *Notify regulator/supervisory authority* - Provides guidance on who to notify, what to include in the notification, and how to notify. If applicable, this guidance may include a notification template. *Notify affected individuals/consumers* - Offers detailed guidance on what information should be included in any consumer notification and guidance on acceptable formats. These tasks can also provide a notification template, if available.

Breach risk assessment

Many regulations require completing a breach risk assessment as part of the breach response process, these include GDPR, PIPEDA and HIPAA. The Resilient Privacy Add-On includes a breach risk assessment tool to help guide privacy teams through evaluating the risk of harm associated with a security incident. This tool provides examples and guidance from the regulation as appropriate.



Risk Assessment engine

This feature also can generate a clean report to share with regulators which demonstrate work has been done to ascertain the level of risk, which is a specific requirement under GDPR.

Incident simulation

The Resilient platform allows customers to create realistic simulations of real-world incidents. By simulating privacy incidents, security and privacy teams of organizations can practice and prepare for a data breach incident and exercising the responsible parties. This process can help leaders of organizations understand whether they have the right processes in place and if the right people have a clear understanding of their roles when a data breach occurs.

Practicing in this way can help security and privacy teams become more aligned and better able to respond to real incidents. Organization leaders also can iterate on the process to help improve their incident response plans and processes. This activity is a key part of becoming cyber resilient.

Dashboards and reporting

Senior security and privacy executives, as well as the wider executive team, often need help to understand the security posture of their organization. The Resilient SOAR Platform provides extensive dashboards and reporting that is available to privacy customers. Users can take any data tracked by the Resilient platform to generate dashboards and reports, including incident-specific reports. Customers can review these dashboards and reports to understand how effective their overall response process is for data breach reporting and related issues.

Incident reports and dashboards

The IR dashboards allow security and management leaders to identify potential gaps in their processes and areas where they need additional resources. These reports can also help to identify if particular countries or business units have specific data breach issues for an organization.

Conclusion

To help to meet evolving breach notification requirements, security teams should align with their privacy and legal colleagues. Security orchestration and automation technology is an important tool in helping to enable this alignment. Many current and upcoming regulations require security teams to have a fully documented incident response plan and be able to execute the plan effectively and consistently. To help achieve these goals, privacy and security leaders should have an IR process that is codified, consistent and orchestrated across their organizations. This requires a combination of people, process and technology to enable a consistent, repeatable process for breach response.

The IBM Security Resilient SOAR Platform Privacy Add-On provides security and privacy teams with intelligence and insights to help them respond to rapidly-evolving security incidents. This tool can help security and privacy teams understand and address complex regulatory requirements.

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 https://www.ibm.com/security

Next steps

→ IBM Security Resilient product page

→ IBM Security Resilient Privacy add-on

For more information

To learn more about the IBM Security Resilient SOAR platform Privacy add-on, please contact your IBM representative or IBM Business Partner, or visit the following website(s): https://www.ibm.com/security/intelligent-orchestration/resilient/privacy-breach-preparation-response

This document contains information pertaining to the following IBM products which are trademarks and/or registered trademarks of IBM Corporation:
IBM Security Resilient