IBM Security SOAR Breach Response

Fast, Efficient, Proactive Response to Privacy Breaches

The current regulatory environment is evolving at a rapid pace. Since the introduction of the European Union's General Data Protection Law in 2018, the growth of new and amended regulations at the global, state, and local level has continued to increase, posing challenges for organizations trying to stay abreast of the changes. Regulations such as the California Consumer Protection Act and Brazil's General Data Protection Law have far-reaching implications globally that organizations need to be aware of.

According to Ponemon Institute, 80% of breached organizations stated that customers' personally identifiable information (PII) was the most common and costliest type of compromised record[1]. The implications from a data breach can be wide-ranging, resulting in high costs, a negative impact to brand, and loss of customer trust. As the complexity of regulations increases, so does the responsibility for organizations to manage personal data and ensure their security and privacy teams are aligned to respond to security incidents and potential privacy breaches.

IBM Security SOAR Breach Response provides organizations with support for over 180 privacy regulations worldwide, allowing security

Highlights

- Orchestrate the incident response process
- Support for 180+ state, global and industry specific regulations
- Coordinate response process with privacy tasks and workflows
- Risk Assessment tools help evaluate notification requirements

[1] Cost of a Data Breach Report 2020, Ponemon Institute

teams to integrate privacy reporting tasks into their overall incident response playbooks and work together with privacy, HR and legal teams to help them address regulatory requirements.

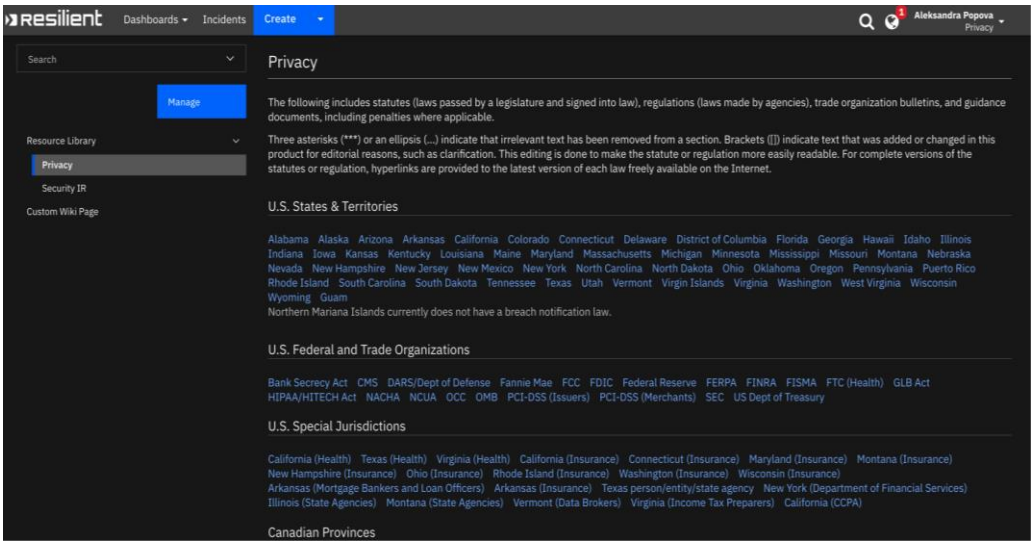
IBM Security SOAR Breach Response helps to transform current manual tasks for assessing privacy risk and reporting requirements into an automated, efficient process that can provide a single point for preparation, assessment and management of a data privacy breach. Furthermore, IBM Security SOAR Breach Response can become a centralized hub for breach information, as security teams look to integrate information from different security tools. Third party integrations for the IBM Security SOAR are available from the IBM Security App Exchange, where there are more than 180 validated and community apps.

Stay ahead of rapidly evolving privacy regulations

At the heart of IBM Security SOAR Breach Response is the global knowledgebase. This database includes breach notification regulations across the world such as GDPR, CCPA, and LGPD. The database also includes industry-specific regulations with a privacy breach reporting requirement, such as HIPAA.

An internal team of 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.

The IBM Security SOAR Breach Response team monitors the regulatory landscape for upcoming and updated regulations and tracks their process. Release notes provide updates on new or upcoming regulations so customers can review the irrelevance and adjust their breach response plans as appropriate.



Regulations in the global knowledgebase in IBM Security SOAR Breach Response

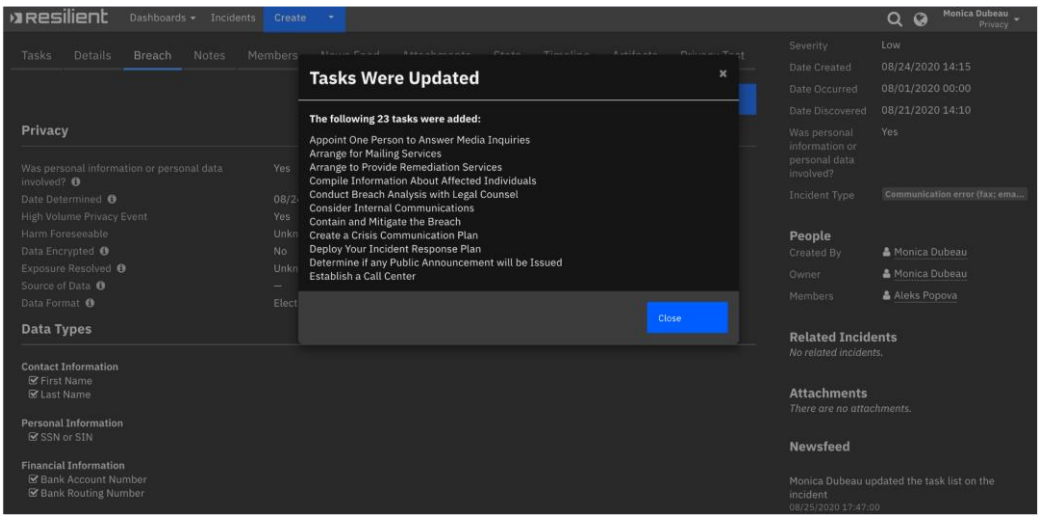
Accelerate breach response with privacy-related tasks and best practices

IBM Security SOAR Breach Response 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 recommended steps that members of the privacy team should take to address the reporting requirements. IBM Security SOAR Breach Response tracks data breaches that trigger multiple reporting requirements as separate tasks inside the overall incident. This process gives privacy and security teams a single view of the privacy and security related aspects of an incident. If required by a regulation, users can assign specific users and specific timelines for incident tasks.

By integrating privacy reporting deadlines into the broader incident response process, IBM Security SOAR Breach Response helps organizations to maintain a single, auditable record 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.

IBM Security SOAR Breach Response optimizes and can enhance response efforts by leveraging best practices for non-regulatory activities. Data Breach Best Practices, available from the IBM App Exchange, provides tasks that are recommended and supplemental to required privacy-tasks to help ensure a comprehensive response across the organization. These tasks can be easily assigned rules and conditions to ensure that they only appear in privacy playbooks as necessary.



Data Breach Best Practices in IBM Security SOAR Breach Response

Conduct breach risk assessments

Many regulations require completing a breach risk assessment as part of the breach response process, such as GDPR, PIPEDA and HIPAA. IBM Security SOAR Breach Response 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.

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

Practice and prepare with incident simulation

IBM Security SOAR Breach Response allows customers to create realistic simulations of real-world incidents so that security and privacy teams can practice and prepare for a data breach incident. 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.

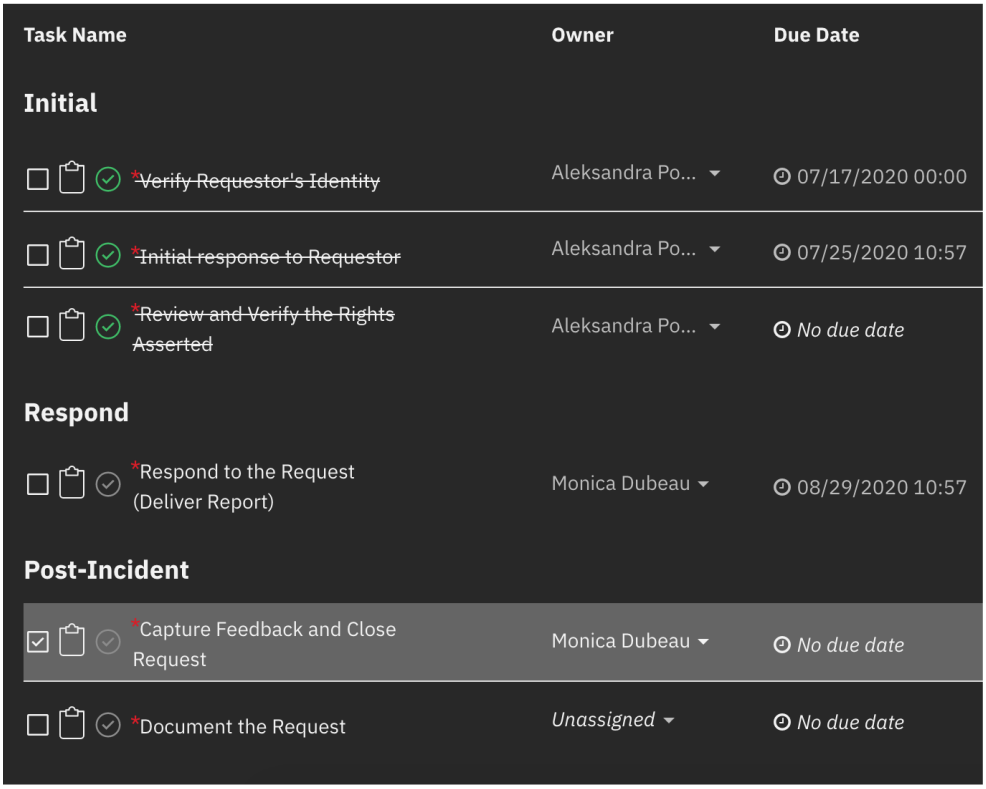
Practicing in this way can help security and privacy teams become more aligned and better able to respond to real incidents. Organization leaders also can iterate on the process to help improve their incident response plans and processes. This activity is a key part of becoming cyber resilient.

Manage Data Subject Access Requests with automation

IBM Security SOAR Breach Response can help organizations manage data subject access requests (DSAR) by building a programmatic response plan using customization to reflect their unique needs, timeframe, and processes. By leveraging integrations, organizations can automate portions of DSAR workflows to monitor the progress of a data subject request from initial request to final fulfillment. The case management capabilities of SOAR allow privacy, legal and HR teams to collaborate on requests, with clear roles and responsibilities, in order to produce an efficient and guided response to meet reporting timeframes.

Automation of tasks can be orchestrated through integrations to transition parts of the manual process to a repeatable, auditable, and

automated process. Customers can develop their own integrations for bespoke or customized applications, leveraging fully documented APIs and supported by IBM developer resources.

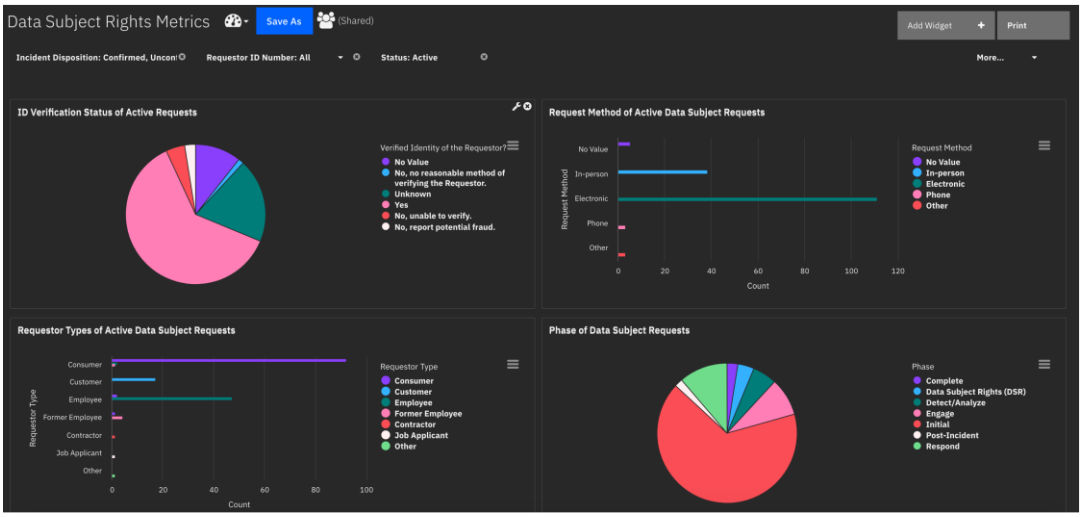


List of tasks for a Data Subject Access Request in IBM Security SOAR Breach Response

Gain visibility into your privacy program

Senior security and privacy executives often need help meeting internal and external reporting requirements. IBM Security SOAR Breach Response provides simple, visual dashboards and reporting to track volume, status, and outcome of privacy breaches and DSARs across the business. Customers can review these dashboards and reports to understand how effective their overall response process is. Furthermore, security and privacy teams can export information

about the breach response to external tools to update regulators or external counsel as required.



Dashboards and reporting in IBM Security SOAR Breach Response

Conclusion

To help to meet evolving breach notification requirements, security teams should align with their privacy and legal colleagues. 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 incident response 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. IBM Security SOAR Breach Response provides security and privacy teams with intelligence and insights to help them respond to rapidly evolving security incidents while helping 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 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.

For more information

To learn more about IBM Security SOAR Breach Response, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/security/intelligent-orchestration/soar/privacy-breach-preparation-response.