Publication date:
04 Feb 2021

Author:
Maxine Holt
Senior Director, Cybersecurity

On the Radar: IBM Security SOAR Breach Response enables organization-wide responses to data breaches

Brought to you by Informa Tech

Table of Contents :

Table of Figures :

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Summary

Catalyst

Data privacy is a bigger issue than ever, with hundreds of varying regulations around the globe dictating the use of personally identifiable information (PII). The COVID-19 pandemic has shone a spotlight on the importance of protecting and respecting the data that individuals provide, and consumers are increasingly aware of the need for data privacy. These dynamics have led to data privacy becoming a strategic focus for many companies, with some using it as a differentiator. Although data privacy was originally a compliance issue, much of the requirement is enabled with data security controls to safeguard data and prevent security breaches. In the event of a breach, a security orchestration, automation, and response (SOAR) solution helps an organization respond quickly and efficiently. In this arena, the IBM Security SOAR Breach Response offering helps facilitate a coordinated response across the organization by leveraging case management, automation of manual tasks, and incident response playbooks, which can incorporate a raft of regulations from different countries and regions as part of the response.

Omdia view

Security incidents and breaches continue to hit the headlines. Far too often, there are examples of PII being exposed, whether through lax security controls or the subject of a targeted and sophisticated attack.

IBM Security SOAR has been a mature and well-adopted security orchestration, automation, and response solution for several years. It helps organizations respond to security incidents and breaches. IBM Security SOAR Breach Response incorporates over 180 global regulations with customized and automated playbooks to enable a comprehensive response to data privacy incidents and breaches. It also helps organizations comply with regulations within required timeframes.

Organizations challenged by a range of compliance obligations will find that the offering provides a step-by-step approach to enable efficiency and compliance in meeting various expectations. Security operations center (SOC) leaders will value the available automation in addition to proactive threat intelligence and flexible deployment options (on-premises, software as a service [SaaS], and on the hybrid multicloud platform).

Why put IBM Security SOAR Breach Response on your radar?

IBM Security SOAR Breach Response is designed to help organizations understand the myriad data privacy regulations that they must comply with. When a security incident or breach affecting any of these regulations does happen, the IBM offering initiates dynamic playbooks that provide guided workflows to help teams collaborate and coordinate the specific steps needed as part of the regulatory response. Visibility into compliance, playbooks, and response is enabled across the business. IBM Security SOAR Breach Response is available as part of IBM Security SOAR and can be deployed via on-premises, SaaS, and within the IBM Cloud Pak for Security platform.

Market context

Information security focuses on protecting the confidentiality, integrity, and availability of information—frequently referred to as the CIA triumvirate. The confidentiality portion focuses on data privacy, and this has been a key legal requirement for enterprises for decades. However, preventing the disclosure of PII is not always successful. On one end of the scale, an organization might be subject to a highly sophisticated and targeted attack to steal specific information; on the other end of the scale, an organization might employ few or no security controls to provide data protection. The outcome is the same across this scale: PII that should have remained private has been exposed.

Governments around the globe have implemented increasingly stringent legislation designed to protect the individual when it comes to maintaining data privacy. In Europe, there is the General Data Protection Regulation (GDPR), enacted in law in EU member states in 2018 and adopted by the UK post-Brexit. GDPR applies to any organization globally that processes the personal data of EU/UK citizens. In California, the US, the California Consumer Privacy Act (CCPA) has been law since the beginning of 2020, and across the US, the Health Insurance Portability and Accountability Act (HIPAA) has been around for almost a quarter of a century. The Personal Information Protection and Electronic Documents Act (PIPEDA) applies in Canada. In Brazil, there is the Lei Geral de Proteção de Dados Pessoais (LGPD) general data protection law, and so on—regulation after regulation across the globe.

These regulations can vary quite significantly region by region. Organizations operating in multiple locations can sometimes have conflicting regulations to deal with, creating challenges when demonstrating compliance in the event of a data privacy incident or breach. Incident response playbooks are crucial, particularly when some legislation requires notification within hours of breach discovery. Being ready and prepared to respond with a set of predefined processes and workflows in the event of a breach supports compliance with requirements in the region(s) where the legislation applies. Furthermore, a centralized source of regulations, playbooks incorporating as much automation as possible, and case management capabilities help accelerate response and facilitate coordination across the different functions involved, such as HR, Legal, and Marketing (among others).

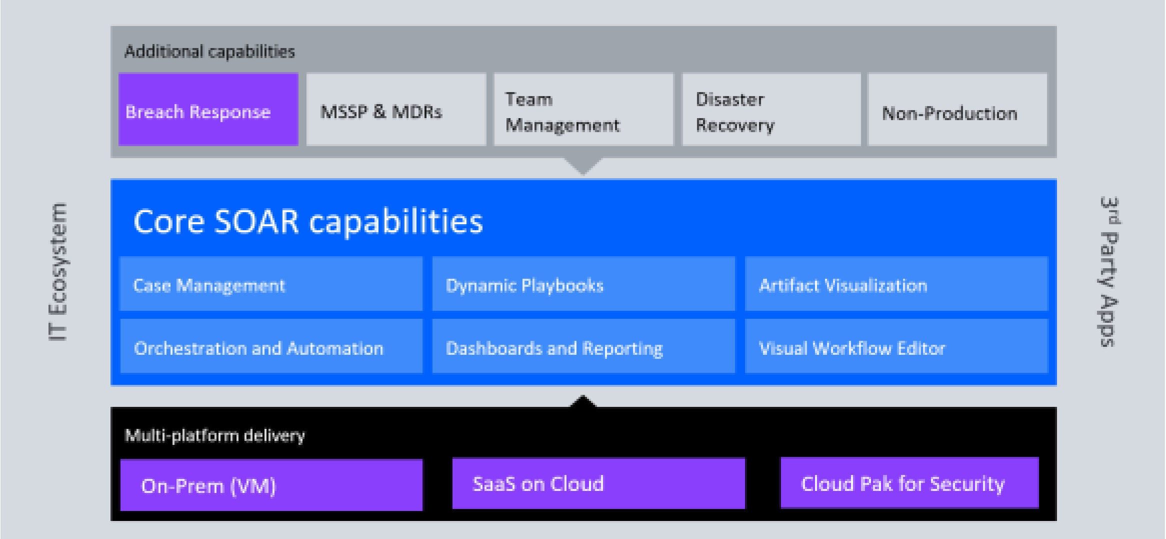
This market is not going away anytime soon—data privacy requirements are only going to increase. Organizations must be able to manage security incidents and breaches quickly and effectively. Complying with data privacy regulations can help mitigate the impact of a breach, including any short- or longer-term damage to organizational reputation.

IBM Security SOAR Breach Response

The IBM Security SOAR Breach Response offering leverages core SOAR capabilities, such as case management, dynamic playbooks, orchestration and automation, and dashboards and reporting (see **Figure 1**). The offering integrates breach notification into the overall incident response process, providing centralized visibility across the organization when dealing with security incidents and breaches.

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.

1. Figure 1: IBM Security Soar with Privacy



Source: IBM

IBM Security SOAR Breach Response is available via multiple deployment options: on-premises, SaaS, and on the IBM Cloud Pak for Security platform. It helps organizations keep abreast of and comply with various data privacy breach notification regulations. It also helps organizations build and manage workflow-based processes for use in circumstances where a security incident or breach occurs.

The offering includes a knowledgebase of over 180 breach notification regulations such as GDPR, CCPA, and LGPD, and it is updated on a regular basis. The database also includes industry-specific regulations with a privacy breach reporting requirement, such as HIPAA.

IBM Security SOAR Breach Response aims to improve the organization’s ability to respond to data privacy incidents and breaches through the creation of incident playbooks. The privacy-related tasks provide recommended steps and can support compliance with, for example, specific notification timescales. They can also provide additional support to the SOC in responding to an attack in progress. For each of the incorporated regulations, the offering includes the required regulatory tasks supplemented by Data Breach Best Practices for non-regulatory activities, available via the IBM App Exchange.

The range of regulations that organizations operating in multiple jurisdictions must comply with is only getting longer, and the ability to comply with each of these regulations is an essential component of incident response. Usability is integral to IBM Security SOAR Breach Response, which focuses on enabling users to follow dynamic playbooks for a security incident or breach without having to wade through reams of “legalese” to meet compliance requirements. The playbooks created in the offering are dynamic and will respond to the facts and circumstances associated with an incident or event. For example, if a company in Brazil has a data breach, the security and privacy team can pull in tasks specific to the LGPD’s regulatory requirements, indicating specific actions based on the number of individuals affected, where they reside, and the data compromised as well as how the notification needs to occur and the timeframe for notification.

Beyond the direct users for data privacy purposes, SOC managers are frequently looking to streamline and automate essential but repetitive tasks, enabling SOC analysts to focus on the more human resource-intensive requirements and streamline the workload. The automation of tasks can be orchestrated through integrations with third-party tools, such as external threat intelligence platforms. Third-party integrations

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.

for IBM Security SOAR are available from the IBM Security App Exchange, where there are more than 160 validated and community apps.

Most security incidents or breaches affect multiple parts of an organization and, frequently, other organizations in the supply chain. As such, IBM Security SOAR Breach Response provides SOC analysts and beyond with case management, allowing the sharing of information so there is a single source of truth in addition to taking advantage of the most effective communications channels. In the event of a breach, the IBM offering incorporates a risk assessment to review the level of risk for the individuals breached.

Data subject access requests (DSAR) are not available out-of-the-box but can be managed by building a response plan with customizations. Similar to a data breach, DSAR workflows can be automated to monitor the progress of each request. Organizations typically build this with IBM services via customer-defined playbooks, but they could also do it directly themselves or with IBM privacy consultants if help is needed to define frameworks.

Reporting can be done via dashboards to track the volume, status, and outcome of incidents and breaches across the organization, providing visibility to security and privacy teams to help meet requirements. Information can also be exported to external tools to support other parts of the business in reporting, such as compliance or legal functions.

Company information

Background

IBM Security is a division of IBM, providing a range of software and services to support enterprises in preventing, detecting, and responding to security incidents and breaches. IBM Security SOAR Breach Response, formerly the Privacy add-on, was part of the acquisition of Resilient Systems by IBM back in 2016. Organizationally, the Resilient capabilities (founded in 2010 to address the increase in cybersecurity risks and threats) are part of IBM Security.

Current position

IBM Security SOAR is part of an integrated Threat Management portfolio within IBM Security to help security teams detect, prevent, investigate, and respond to cybersecurity threats. IBM Security SOAR Breach Response helps security and privacy teams stay abreast of changing regulations, accelerate response times through automation and orchestration, and coordinate responses across the organization with case management.

IBM Security SOAR has customers globally and in a wide range of industries. The offering is sold by IBM sellers and through business partners.

IBM Security SOAR Breach Response is available in a variety of deployment options to give customers flexibility: on-premises, SaaS, and on IBM Cloud Pak for Security (an open, multicloud platform built on Red Hat OpenShift). IBM Cloud Pak for Security is IBM's integration enablement solution, or security platform integration framework (SPIF) in Omdia parlance, designed to enable the rapid integration of best-of-breed security tools, helping organizations generate deeper security insights. IBM Security's SOAR capabilities for breach response are built-in, providing the ability to enable orchestrated and automated response actions across products integrated with the SPIF while meeting compliance requirements.

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Key facts

Table 1: Data sheet: IBM Security SOAR Breach Response

Product/Service name	IBM Security SOAR Breach Response	**Product classification**	Security orchestration, automation, and response (SOAR)
Version number	v40 and higher (on-premises and SaaS)	**Release frequency**	Monthly
Industries covered	All	**Geographies covered**	All
Relevant company sizes	Large and midsize	**Licensing options**	Subscription or perpetual
URL	https://www.ibm.com/security/intelligent-orchestration/resilient/privacy-breach-preparation-response	**Routes to market**	Direct and via business partners
Division headquarters	Cambridge, MA, US		

Source: Omdia

Analyst comment

IBM is indeed an extremely well-established player in the security market in general. With the acquisition of Resilient Systems back in 2016, it has consolidated its position within the data breach response market. However, as the landscape for data privacy grows ever more stringent, more enterprises will need help and support to navigate this landscape and maintain compliance. For example, although some (not all) regulatory authorities have perhaps become slightly more “relaxed” for DSARs, partially recognizing the challenges that remote working brought during the COVID-19 pandemic, they have become stricter on breach response times. Other regulatory authorities have not relaxed at all and expect enterprises to maintain compliance irrespective of the situation. It is these developments that enterprises are quite rightly concerned about and that IBM has an opportunity to capitalize on further.

Although the process of creating and changing regulations can be slow, the data privacy market is fast-moving in some respects, the pandemic being a prime example of external influences that affect an organization’s ability to be compliant. IBM must continue to build out the regulations and best practices it incorporates and make the capabilities as easy as possible for all involved to use. It must be practical for the SOC analyst, the Compliance function, and the IT function. Organizations operating in single jurisdictions might find the offering too much for their needs, but any organization operating in multiple data privacy jurisdictions can benefit.

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.

IBM Security SOAR Breach Response provides enterprises with several options that will appeal—as an add-on within IBM Security SOAR, as a standalone SaaS or on-premises deliverable, and via the IBM Cloud Pak for Security. This is the main differentiator for the IBM Security SOAR Breach Response offering—tying SOAR and Privacy together and supporting the enterprise in the complex cybersecurity technology environments that the vast majority operate through years of accumulation. IBM is looking to have existing customers upgrade and adopt this offering, and there are organizations new to IBM Security that would benefit from this broad offering.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Author

Maxine Holt, Senior Director, Cybersecurity

askananalyst@omdia.com

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia’s consulting team may be able to help you. For more information about Omdia’s consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com

© 2021 Omdia. All rights reserved. Unauthorized reproduction prohibited.