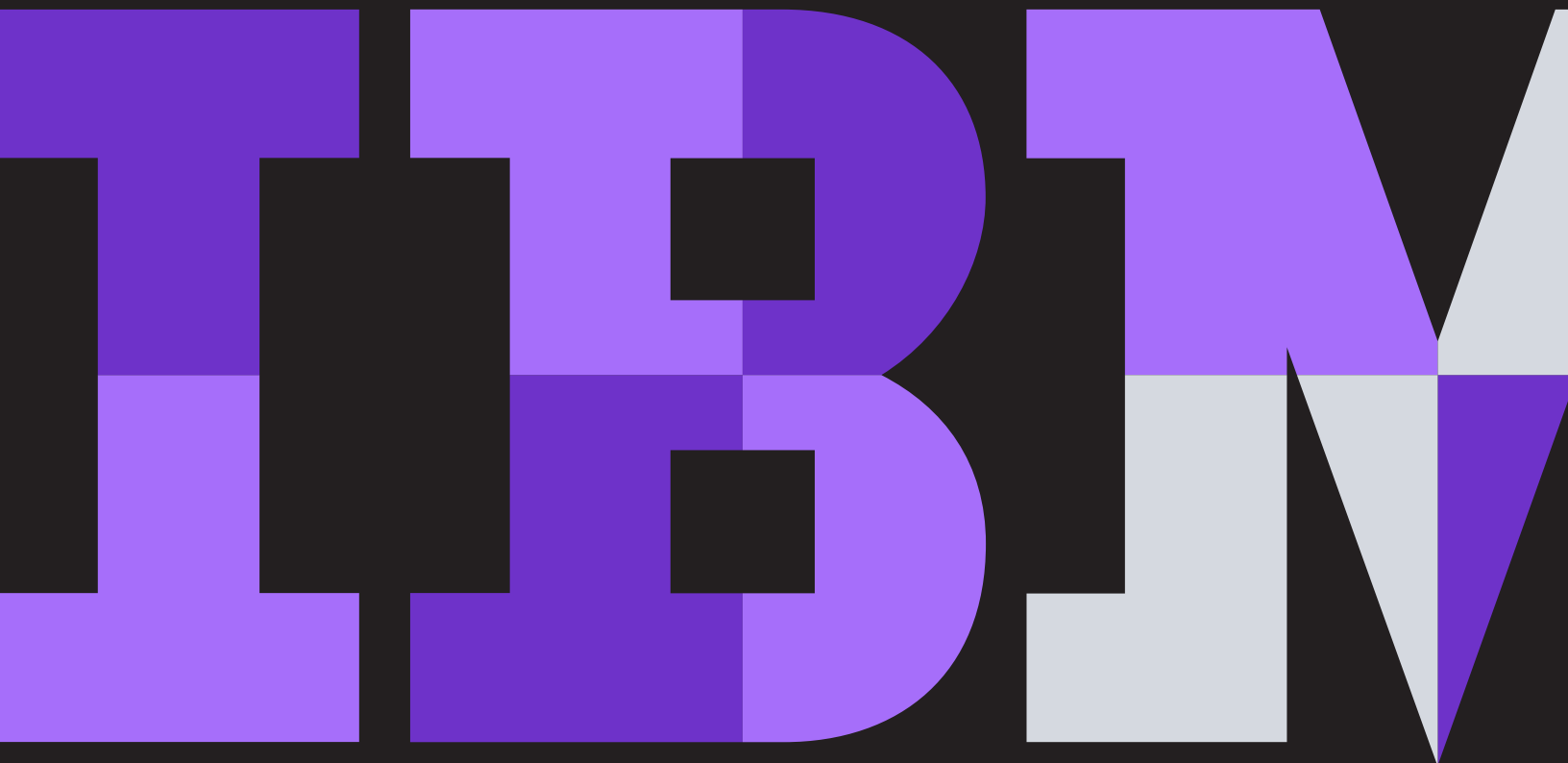


How to be a SOAR winner:

8 successful strategies to unlocking more value from your security orchestration, automation and response (SOAR) solution

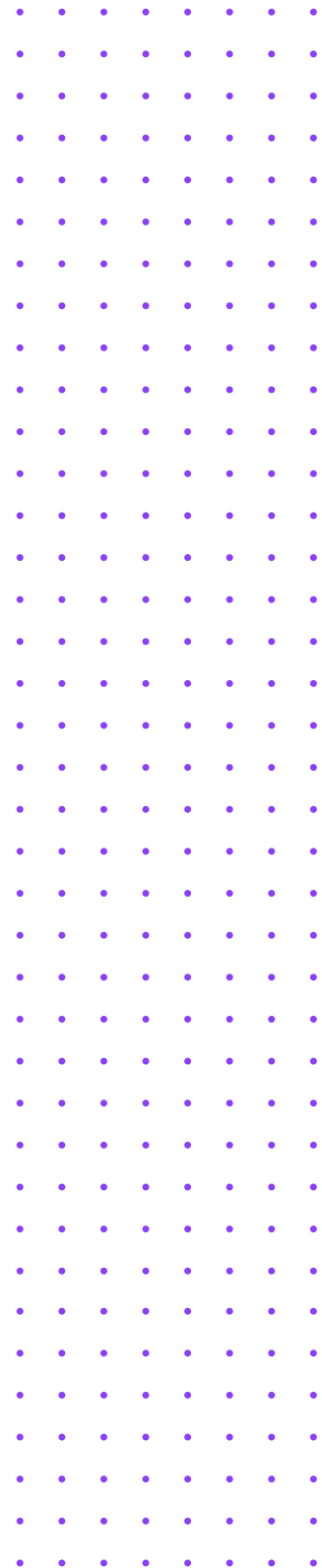


Contents

- 3 If you want your SOAR solution to really soar, start here
- 4 The ABCs of SOAR
- 5 Don't just build playbooks — build them into your daily workflow
- 6 Integrate your security environment
- 7 Create flexible playbooks that can tie different techniques together (and don't tie you down)
- 8 Connect security stakeholders through communication, collaboration and cross-organizational workflows
- 9 Use automation intelligently and effectively
- 10 Practice fire drills before the heat is on
- 10 Prepare for compliance audits and reports before an attack — because you won't have much time after it happens
- 11 Quickly incorporate lessons learned into your playbooks for the next incident
- 11 Why IBM

Key points

- Security platforms that provide an integrated, unified view of security data are faster and more accurate
- Automation of security processes should be done dynamically and intelligently to be effective
- Practice drills and compliance audits ensure that when the heat is on, your security teams stays cool
- Always update and expand your security playbooks as new tactics, techniques and procedures emerge



If you want your SOAR solution to really soar, start here

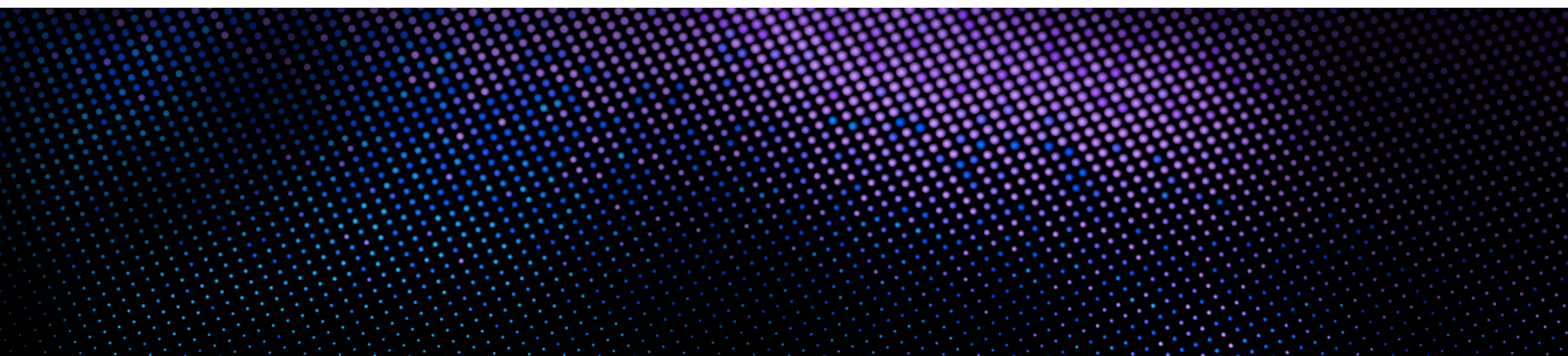
Automated, orchestrated security. The words conjure the image of a security operations center (SOC) humming smoothly as machines effortlessly detect and deflect cyberthreats. The reality, however, is more complicated. Malware detection is a moving target, SOC teams are living organisms and security environments are anything but seamless. The goal of a security orchestration, automation and response (SOAR) solution isn't to replace human intelligence with machine intelligence, but to empower security analysts to be more effective and efficient through the intelligent application of automation and orchestration.

In today's security landscape, there are a variety of tools that position themselves as SOAR solutions. Some are more robust than others, yet few of them deliver on the promise of bringing people, processes and technology products together in an intelligently orchestrated, automated fashion.

At IBM, we believe that SOAR can lift your SOC to a higher level of efficiency. But we also know that many organizations struggle to achieve the full benefits of a SOAR solution because of misconceptions, misunderstandings and missed opportunities. In the following pages, we'll highlight the most critical success factors in creating and sustaining an intelligently automated, orchestrated security team.

What does truly intelligent orchestration look like?

- It enables human agents to respond to security incidents confidently
- It automates incident response and enriches it with intelligence
- It fosters collaboration and consistency across the decision chain



The ABCs of SOAR

With all the talk around security these days, it's important to make sure that everyone is speaking the same language. To that end, we've prepared a short primer of security terms you'll encounter in this paper:

Automation

The ability to perform functions without human intervention. These functions may be internal — e.g., escalating an incident's urgency, adding members to an incident response chain — or they can be external, such as querying an SIEM tool or external threat Intelligence feed for more information on Indicators of Compromise (IoC).

Orchestration

The creation of a sequence of multiple steps and/or actions that drive a particular process or response. Orchestration typically involves human action as well as automated steps. An example of orchestration might be a security analyst who suspends a user account in Active Directory, where the account suspension process had been pre-configured but still requires a manual decision to execute the process.

Case/Incident

This refers to the end-to-end process of investigation, containment and remediation. A case/incident may include multiple workflows, depending on how an attack evolves — e.g., a simple phishing attack could become part of a broader data exfiltration attack, requiring additional steps.

Playbook

A set of tasks that may or may not include external automation, which is associated with a specific threat type such as phishing or network intrusion. A playbook determines the organizational response to a particular threat and should include business processes as well as technical tasks. Playbooks are additive, such that a complex incident may consist of multiple playbooks.

Workflow

A workflow describes a specific set of actions around a particular security process. A playbook is made up of multiple workflows.

App/Integration

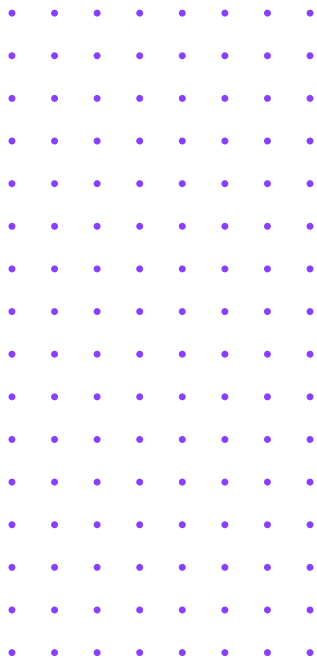
An Application (App) or Integration is a packaged set of functions, rules, scripts and workflows that links the IBM Security SOAR API to third-party security or IT ops tools in order to leverage that external tools capabilities as part of the incident response process. More than 170 Validated and Community apps are available from the [IBM Security AppExchange](#). It is easy to develop additional further integrations using the full-documented RESTful API, and developer documentation and sample code is also available to assist the process.

Success factor #1

Don't just build playbooks — build them into your daily workflow

Preconfigured Incident Response (IR) playbooks allow SOC teams to respond quickly and consistently to threats. Consistency is especially important because organizations should have the same security response, whether a threat is being handled by a Level 1 SOC analyst or a Level 3 incident responder, in Boston or in Bangalore. Yet the reality is that many organizations have found themselves reacting to the same attack differently based on who and where the analyst is, because of the lack of a standard playbook.

Creating security playbooks is an important step, but don't stop there. Integrating those playbooks into your security processes will reduce critical response times and ensure that security analysts can make better decisions during moments of crisis. For example, if you know that a particular type of malware attack has certain characteristics, you might create a playbook that prompts a security analyst with a series of yes/no questions to speed up the investigative process.



Key considerations

- IBM Security SOAR starts you off with pre-built playbooks for phishing, malware, ransomware and other common use cases, based on industry standards (such as NIST and SANS) and best practices.
- Playbooks are fully customizable. Security teams can quickly update tasks and conditions in the rules engine or through a visual workflow editor.
- Security analysts can easily add existing third-party integrations into their playbooks and workflows through the visual workflow editor.



70%

of highly cyber resilient organizations significantly use automation to strengthen cyber resilience¹

Success factor #2

Integrate your security environment

Most organizations opt for a best-of-breed security approach that features solutions from a variety of vendors. While this can provide SOC teams with a host of different and useful tools, each vendor tends to collect and organize data in a slightly different way, making it difficult for analysts to get a unified view of security data. A SOAR solution can help unify data by integrating different data sources through APIs.

Unified security data enables security teams to enrich data with intelligence from other applications. For example, by adding data from an employee directory to a phishing scam alert, security analysts could see not only the name and role of the phishing victim, but also when they last logged onto the network and which files they have authorization to access. This information, in turn, could allow security analysts to quarantine specific users or files until a further investigation can be made. A single view of security data is also important for communication and collaboration, as it ensures that analysts and decision makers are seeing the same thing and can react consistently and confidently.


In some cases, the SOAR solution itself serves the purpose of tying together the disparate security tools into a single environment, eliminating the need for analysts to toggle through different applications as they investigate and remediate threats. This can save crucial minutes during the threat investigation phase and allow analysts to make connections that might otherwise have gone undetected.

Key considerations

- There are over 170 published third-party applications available for IBM Security SOAR on [IBM Security AppExchange](#) featuring detailed workflows and use cases for common security problems.
- Developers can quickly add custom integrations to tools and apps through the RESTful API. For third-party tools without an accessible API, the IBM Security SOAR platform can consume email alerts and parse them, building new incidents or updating existing ones.

Disseminate critical intelligence across your team and security tools

Watch this video to find out how IBM Security SOAR interacts with Threat Intelligence Platforms (TIPs) allowing for incident enrichment and better alert triage.

[Watch the video](#) 

Success factor #3

Create flexible playbooks that can tie different techniques together (and don't tie you down)

One of the major benefits of a SOAR solution is the ability to automate security tasks for greater consistency and efficiency. As the [MITRE ATT&CK™ matrix](#) has shown, different cyberthreat tactics employ a wide range of techniques, resulting in an almost endless number of possibilities. For example, a cybercriminal might use spear phishing, a corrupted file attachment and a link redirect in one attack and then change those tactics and techniques in another attack.


Dynamic playbooks are the cornerstone of an effective SOAR solution because cyberattacks are dynamic entities. The tactics, techniques and procedures (TTPs) of cybercriminals are constantly evolving in an effort to stay one step ahead of blacklists, anti-malware tools and other protective measures. SOC teams need playbooks that can pivot and change based on human intelligence and new discoveries. Remember: the goal of automation is to empower human analysts by eliminating repetitive tasks, not replace human analysts entirely by automating every aspect of the SOC. Ultimately, security automation should be a balance of science and art, humans and machines, that leverages both internal intelligence and threat intelligence from the wider cybersecurity community.

Key considerations

- IBM Security SOAR's playbooks are dynamic and additive. For example, you can start a phishing investigation with a basic phishing playbook and then, as the investigation unfolds, add other playbooks to address further actions as needed.
- Security analysts can quickly add new tasks to reflect decisions made outside of the preconfigured playbook, ensuring all aspects of the incident are captured in the platform.
- IBM Security SOAR can leverage and enrich MITRE ATT&CK TTPs from third-party tools and use this information to dynamically update response plans.

Leverage MITRE ATT&CK™ for security operations platforms

The MITRE ATT&CK™ framework allows you to map the techniques of an attacker to the various threat groups known to use it, the software they may have used, so that you can customize your playbooks to detect and mitigate for those techniques.

[Watch the video](#) 

Incident response (IR) preparedness was the highest cost saver for businesses, decreasing the average total cost of a data breach by an average of

\$2M²

Success factor #4

Connect security stakeholders through communication, collaboration and cross-organizational workflows

Security conversations aren't contained to the SOC; they're happening in board rooms, on investor calls and in customer communications. The new reality is that security is everybody's business, and that means communication and collaboration around security is more important than ever before. Yet, too often, different business constituents aren't speaking the same language when it comes to security. They may have different definitions of compliance, have opposing views on what constitutes a serious threat or simply disagree on which security initiatives are most important for the future. And these differences create a breakdown in communication and collaboration.

The first step for organizations is to establish a common security language. Some of this may involve education, such as defining what the difference is between a data breach and data exfiltration. Much of the commonality can be communicated through shared data and metrics, so that everyone can quickly get on the same page. Security analysts will find they collaborate better when Level 1 analysts have visibility into Level 2 and Level 3 analyst responsibilities so they can better assist them. CSOs and SOC managers will find they meet with less resistance on budget requests when they can have informed conversations with the CIO, CEO and CFO.

As part of this process, organizations should identify who owns the security responsibilities within each organization. Assigning points of contact in each appropriate department (e.g., finance, public/investor relations, marketing, legal) will allow organizations to complete their playbook in the event of a data breach, for example, to ensure that each department has the information it needs to react and respond in a timely manner. This becomes increasingly important as organizations take next steps after attack discoveries, from communicating with customers to filing compliance reports with regulatory agencies.

Key considerations

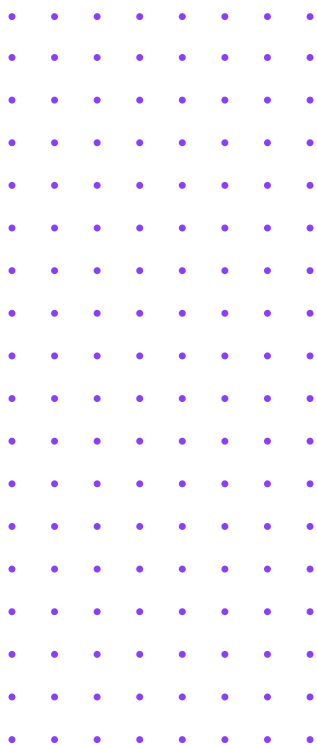
- IBM Security SOAR allows security teams to customize and generate relevant response playbooks that include business processes and technical response steps. With support from IBM Security Services, new playbook content can be generated to align with different business units.
- IBM Security SOAR integrates privacy use cases into security case management to help track breach reporting regulations around the world and add relevant tasks to the data breach response, ensuring that your privacy and security teams are aligned.

Success factor #5

Use automation intelligently and effectively

Automation has become a popular buzzword in security, and there's a tendency among organizations to see automation as pure good in every situation. But in fact, automating everything can be worse than not automating anything at all, if it means that what is being automated is fundamentally flawed. The value of SOAR lies in intelligent automation: choosing processes that are predictable and repeatable, and automating those processes first.

As an example, let's say that your Level 1 security analysts perform the same task multiple times per day, such as enriching each new incident record with data intelligence from a trusted source. Automating this step might save analysts an hour or more each day. But what if an organization were to automate a response by blocking every email from a country suspected of phishing attacks? That could have unintended, negative consequences, even though it might seem like a good deterrent at the time.




Key considerations

- With IBM Security SOAR, security analysts are able to automate any step of the incident response lifecycle if it makes sense. By building effective, repeatable playbooks, security analysts can quickly identify suitable use cases for automation, deploy them and measure their results.
- IBM Security SOAR contains support for more than 10 preconfigured external threat intelligence feeds. This means that all artifacts associated with new incidents can be automatically checked against these feeds for known threats before the analyst has even started the investigation.

Automation in Incident Response

Reduce your time to respond and accelerate the learning skills of your security team with IBM Security SOAR - put the right information in front of the right person at the right time through effective dynamic playbooks.

[Watch the video](#) 

Success factor #6

Practice fire drills before the heat is on

Practice fire drills before the heat is on

Firefighters train on simulated fires to prepare for real emergencies. SOC teams should do the same thing. Practice drills that simulate cyberattacks can help security analysts build the confidence and composure they need to handle real threats in real time. Equally important, simulations can help organizations identify skills and process gaps before an attack rather than after.

Cyberattack simulations also allow security teams to formulate and test threat playbooks that can aid them during a real attack. Organizations should consider simulating different attacks to generate a variety of different playbooks for ransomware, malware delivered via email phishing, denial-of-service attacks and so on. A SOAR solution should include the ability to run a variety of different attack simulations and allow security teams to then tweak and customize playbooks depending on different outcomes.

Key considerations

- IBM Security SOAR has a built-in simulation setting that allows security teams to test the validity of their playbooks and build muscle memory for real incident scenarios.

43%

of highly cyber resilient organizations have an incident response plan that is consistently applied across the entire enterprise¹

Success factor #7

Prepare for compliance audits and reports before an attack — because you won't have much time after it happens

SOC teams can quickly find themselves in battle conditions during a cyberattack. No one has the time to think about audits and filing breach reports during an attack, but they're very necessary steps that need to take place quickly after an attack is over. The General Data Protection Regulation (GDPR), for example, requires that the relevant Supervisory Authority (SA) should be notified within 72 hours of the discover of a personal data breach. If your organization doesn't have the data or the expertise to file that report, the follow-up can be more painful than the original breach.

SOAR solutions can help organizations meet complex reporting requirements by automating much of the discovery process and creating a detailed audit trail of the attack. Breach reports require that the right people be looped into the process — legal, privacy, security, etc. — which can be automated to improve internal communications. Organizations make a grave mistake when they think of reporting as an afterthought; it needs to be part of the response process, as much as the mitigation/remediation phase.

Key considerations

- IBM Security SOAR can include detailed assistance for privacy breach reporting. It supports more than 180 global, state and industry-specific regulations for breach reporting, enabling organizations to better understand their obligations and meet different regulatory deadlines.
- Security analysts can track privacy tasks for incident documentation, regulator reporting and consumer notification within the incident record, ensuring that all relevant data is maintained in a time-stamped, auditable record.

Success factor #8

Quickly incorporate lessons learned into your playbooks for the next incident

The post-remediation clean-up phase is the perfect time for security teams to assess what went right, what went wrong and fold their new-found knowledge into future playbooks through automation. A SOAR solution should allow organizations to easily revise and expand their playbooks based on newly evidenced TTPs (tactics, techniques and procedures) — whether those TTPs come from personal experience or from threat intelligence sources such as the MITRE ATT&CK™ matrix.

Key considerations

- IBM Security SOAR generates incident-specific reports that can assist security teams with the post-incident review process, capturing the incident timeline and key decisions made. This allows SOC managers to review the effectiveness of their playbooks and look for areas for improvement.
- IBM Security SOAR can generate detailed dashboards and reports to help organizations capture common IR metrics and track important KPIs such as meantime to respond (MTTR) and meantime to contain (MTTC).
- IBM Security SOAR integrates with SIEM platforms, such as QRadar, to help improve detection capabilities by providing information on new threats and false positives.
- IBM Security SOAR for IBM Cloud Pak for Security integrates with other native applications like Threat Intelligence Insights and Data Explorer to help prioritize and investigate threats.

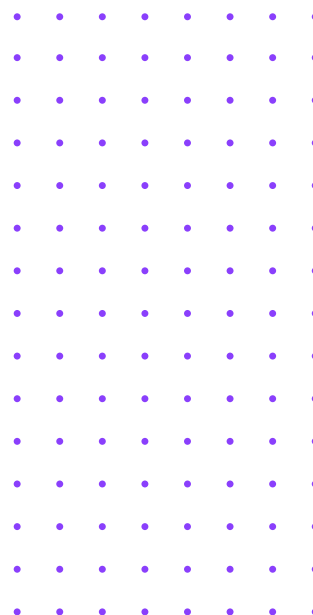
Why IBM

IBM Security SOAR helps organizations unify people, processes and technology for automated, orchestrated incident response. It provides a single platform that allows security analysts to access their entire ecosystem of security tools and data from one environment. IBM Security SOAR features flexible automation and orchestration controls that enable playbooks and processes to be quickly created and integrated into business workflows and security applications for a faster and more effective response to threats and attacks.

[Learn more about IBM Security SOAR solutions and capabilities.](#) →

Next steps:

- Read the [2020 Market Guide](#) for Security Orchestration, Automation and Response Solutions.
- [Request a demo](#)



Sources

1. Ponemon Institute, “2020 Cyber Resilient Organization Report”, IBM Corp., June 2020
2. Ponemon Institute, “2020 Cost of a Data Breach Study: Global Overview,” IBM Corp., July 2020.
3. Ibid.

© Copyright IBM Corporation 2020

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
November 2020
All Rights Reserved

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.



Please Recycle