A Forrester Total Economic Impact™
Study Commissioned By IBM
August 2020

The Total Economic Impact™ Of IBM Security SOAR

Cost Savings And Business Benefits Enabled By IBM Security SOAR

FORRESTER®

Table Of Contents

Project Director:
Mary Anne North

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Key Benefits

Orchestration and automation savings for security incident response:
$3,190,436

Existing security asset value realization improvement:
$1,330,128

Reduction in per-incident security analyst time:
66% to 97%

Executive Summary

IBM Security SOAR helps organizations address cybersecurity incidents faster and more consistently through a combination of orchestration, automation, and case management. It guides and standardizes incident response with customized dynamic playbooks. By leveraging security automation and third-party integrations to decrease manual tasks and increase security analyst productivity, IBM Security SOAR reduces the effort needed to investigate and resolve a cybersecurity incident.

IBM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying IBM Security SOAR. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of IBM Security SOAR on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with experience using IBM Security SOAR. Prior to using IBM Security SOAR, the interviewees' organizations took variable and highly manual approaches to incident response, using notes on spreadsheets, informal knowledge sharing, and a ticketing system for simple incident tracking. They lacked technology that would enrich the outputs from their various security tools to inform and shorten their incident response.

After deploying IBM Security SOAR, the organizations found that their security analysts could investigate and resolve an incident in a fraction of the time they previously spent, freeing up analyst time for higher-value security initiatives. The organizations reduced end user downtime as well as IT staff effort to remediate those end users' machines. They compiled better reporting metrics in less time, enhancing visibility for the CISO and senior leadership. With IBM Security SOAR acting as the central dashboard orchestrating the response to security incidents, they gained visibility into the efficacy of existing security tools. This enabled their security professionals to realize the full potential of those tools and eliminate tools or switch to more effective replacements when warranted.

Customer quotes highlight IBM Security SOAR's impact on the interviewed organizations:

"Our mean time-to-resolution has been drastically reduced." – *Senior manager, cybersecurity operations center, retailer*

"IBM Security SOAR just pulls a lot of information into one place, and it makes things happen." – *Cyberthreat analyst, utility*

"The analysts now have time to do things that actually improve our overall security posture, versus responding to things that are potentially compromising it." – *Manager, information security, information services company*

"Our threat responses are much more effective, and we have much better reporting for management and regulators." – *Vice president and information security officer, financial services company*

"It's an extremely flexible platform and your mind is the limit. We're finding new use cases all the time. And if we didn't have IBM Security SOAR, we would probably need two or three different products, all costing individually more than IBM Security SOAR does to get the effectiveness that we're getting out of IBM Security SOAR." – *Manager, information security, information services company*

FORRESTER®

ROI
444%

Benefits PV
$4.6 million

NPV
$3.8 million

Payback
<6 months

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits (totaled over an initial three years of using IBM Security SOAR) are representative of those experienced by the companies interviewed and applied to a composite organization that Forrester synthesized based on those experiences:

- **Security orchestration and automation savings of $3.2 million for incident response.** By automating many previously manual efforts (especially enrichment) for security analysts and by guiding those analysts to efficiently address cybersecurity incidents, IBM Security SOAR saved organizations an average of more than one hour of analyst time for each security incident.
- **Existing security asset value realization improvement of $1.3 million.** Because IBM Security SOAR enabled organizations to centrally collect data and determine points in their security architecture that were less responsive, the organizations could identify points of failure to reconfigure, eliminate, or replace with alternate security tools.
- **End user and IT productivity capture of $71,656 from improved incident response capabilities.** By accelerating incident response, IBM Security SOAR reduced end user downtime and IT time for remediation or reimaging of machines.
- **Audit efficiency gains of $19,042.** Organizations needed less time to compile compliance metrics due to the visibility and querying and reporting capabilities that IBM Security SOAR provides.

Unquantified benefits. The interviewed organizations experienced the following benefits, which are not quantified for this study:

- **Ability to focus security analysts on higher-value activities.** With many time-intensive tasks now addressed by security orchestration and automation, analysts had time to contribute to broader initiatives that improved their organization's overall security posture.
- **Consistent high-quality incident response.** Dynamic playbooks ensured an effective response regardless of which analyst picked up an incident.
- **Better and faster reporting for management on security incident metrics.** Security teams delivered more comprehensive security metrics in less time for the CISO and senior leadership, aided by the ease of creating and automatically updating dashboards in IBM Security SOAR.
- **Time savings from IBM Security SOAR use outside of the incident response team.** Individuals in other cybersecurity roles or other areas of an organization (e.g., payment fraud departments) saved time by using information from IBM Security SOAR or actively working in it.

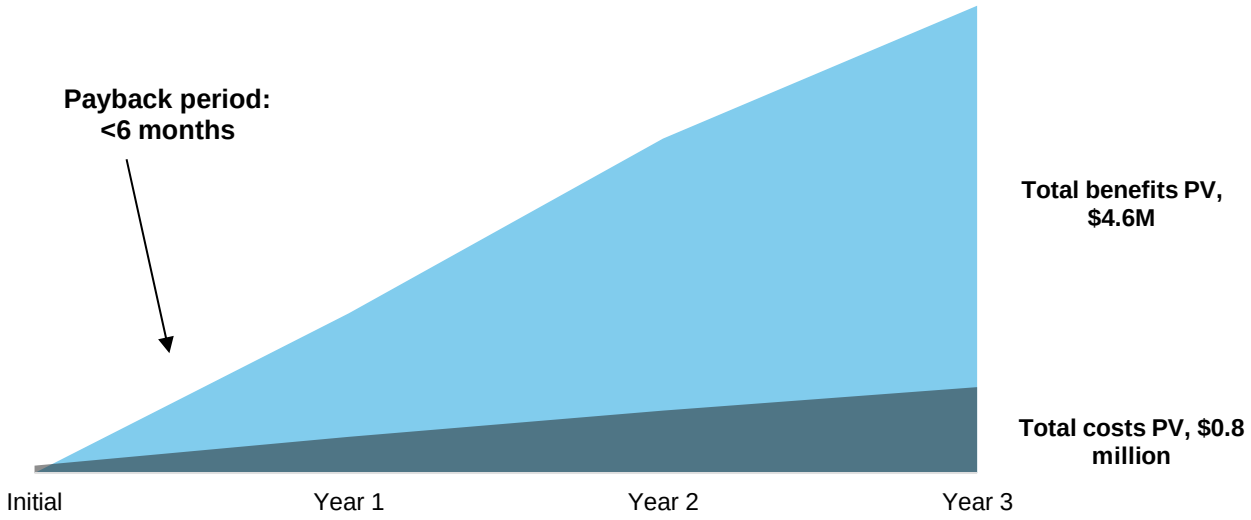
Costs. The interviewed organizations experienced the following risk-adjusted PV costs (totaled over their initial three years of using IBM Security SOAR and applied to the composite organization):

- **IBM fees of $684,299.** IBM fees included annual subscription costs for IBM Security SOAR and one-time professional services fees for implementation assistance.

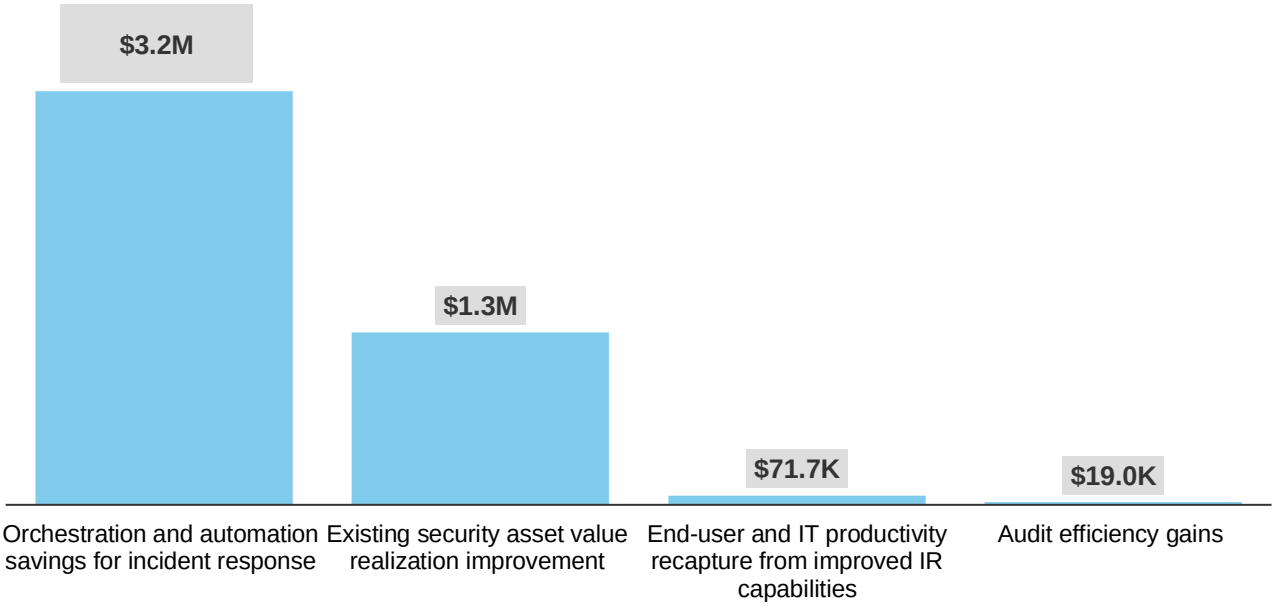
› **Internal labor for implementation and ongoing management of $163,172.** Internal labor costs included IT staff time to implement IBM Security SOAR and then manage its use and to continue to further leverage its capabilities.

Forrester's interviews with five customers and subsequent financial analysis found that the composite organization based on the interviewees' organizations would experience benefits of $4,611,262 over three years versus costs of $847,471, adding up to a net present value (NPV) of $3,763,791 and an ROI of 444%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing IBM Security SOAR.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that IBM Security SOAR can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed IBM stakeholders and Forrester analysts to gather data relative to IBM Security SOAR.

CUSTOMER INTERVIEWS
Interviewed five organizations using IBM Security SOAR to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed organizations.

FINANCIAL MODEL FRAMEWORK
Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling IBM Security SOAR's impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by IBM and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in IBM Security SOAR.

IBM reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

IBM provided the customer names for the interviews but did not participate in the interviews.

The IBM Security SOAR Customer Journey

BEFORE AND AFTER THE IBM SECURITY SOAR INVESTMENT

Interviewed Organizations

For this study, Forrester conducted interviews with five IBM Security SOAR customers. Interviewed customers included the following:

INDUSTRY	SCOPE OF OPERATIONS	INTERVIEWEES
Financial services	Global	Lead cybersecurity engineer
Retail	North America	Senior manager, cybersecurity operations center
Information services	Global	Manager, information security
Financial services	North America	Vice president and information security officer
Utility	Regional operations, headquartered in North America	Cyberthreat analyst

Key Objectives

The interviewees described a range of challenges and objectives that drove their organizations' decisions to deploy IBM Security SOAR:

- **Improve security incident processing and security analyst productivity.** Organizations sought to make their security incident responses more consistent, repeatable, effective, and efficient to reduce both security analysts' effort and the elapsed time needed to contain and resolve an incident. Any existing documentation of those response processes was typically rudimentary, static, and out of date, requiring analysts to handle incidents on a largely ad hoc basis with little standardization. Incident response efforts were highly manual and time-intensive, requiring analysts to check numerous individual security tools and copy information from them, and email or call colleagues in other areas to initiate and follow up on incident resolution. Analysts could not readily identify correlations over time or among data from multiple tools or sources. If the organization used a ticketing system to track incidents, that system delivered only a simple list of incidents (since it was not purpose-built for security incidents) and no further security orchestration or automation.
- **Free up security analyst time for higher value work.** With both the volume and complexity of security incidents continuing to increase, interviewees said their organizations wanted their security analysts to have time to do more than address each day's security incidents. By decreasing security analysts' manual and repetitive work, the organizations envisioned tapping the analysts' expertise for higher-value security initiatives.
- **Assess performance of security tools.** The organizations used an array of security tools, but they lacked insights on which of those tools needed reconfiguration to improve their performance or did not merit renewal.

> "Our functionality was limited to noting and tracking incidents. There weren't any tools to actually address the problem and do that efficiently. There was no filtering of what you needed to figure out, so you had to go through a lot of stuff and just assume most of it was wrong."
>
> *Senior manager, cybersecurity operations center, retailer*

> "It could take 8 to 10 hours for an analyst just to collect evidence related to an incident and determine what was going on."
>
> *Vice president and information security officer, financial services company*

- **Gain better visibility to incident metrics and trends across the organization.** Interviewees were frustrated by their lack of visibility to trends, pain points, and what was happening from a security perspective across their organizations. They wanted to be able to create, access, and share reports about incidents and incident response faster and with less effort.
- **Decrease time spent supporting regulatory and compliance audits.** Organizations wanted to be able to support recurring and one-off internal and external compliance audits with better data while spending less staff time to gather that data.

Solution Requirements

The interviewees said their organizations searched for a solution that could:

- Enable security orchestration and automation to decrease analyst effort and elapsed time to investigate, contain, and resolve cybersecurity incidents.
- Provide dynamic playbooks that facilitate handling multistage and evolving incidents.
- Support automation of security incident response, either partial or full (where appropriate).
- Integrate fully with security tools, not simply with intake logs.
- Help identify false positives and false negatives so they can be reduced.
- Deliver dashboards that provide visibility to security metrics across the organization.
- Work well across diverse infrastructures and network topologies, including emerging and legacy technologies and cloud and on-premises environments.

Key Results

The interviews revealed that key results from the IBM Security SOAR investment include:

- **Reduction in security analyst time needed to investigate, contain, and resolve a cybersecurity incident.** Analysts resolved an incident with less effort because of IBM Security SOAR's security orchestration and automation capabilities including dynamic playbooks, automated enrichment and remediation (via integration with security tools), and case management. Instead of manually checking many sources for information on an incident, they consulted a single central source into which IBM Security SOAR had compiled information from those different sources. Playbooks guided them through effective and efficient processes tailored to various types of incidents. Depending on the type of incident, some containment and remediation actions were automated.

> "If an analyst needs to gather and analyze data from multiple tools, it's very easy to use the automations that we build using IBM Security SOAR. Otherwise the analyst would have to go to each of those tools, then search for and collect that data."
>
> *Lead cybersecurity engineer, financial services company*

- **Enhanced ability to realize the value of existing security assets.** By tracking key metrics that can inform strategic business decisions such as eliminating redundant security tools, and also helping identify less responsive points in the security architecture, IBM Security SOAR enabled organizations to affirm that their investments are working as anticipated.
- **Improved productivity for end users and IT support staff.** With the time to resolve an incident shortened by IBM Security SOAR's security orchestration and automation, end users had fewer hours of downtime. IT staff needed to remediate fewer of the affected machines, because a swifter response to an incident can reduce the need for IT staff to pursue deeper-level remediation/recovery techniques.
- **Decreased effort needed to compile compliance metrics.** The querying and reporting capabilities provided by IBM Security SOAR reduced the time spent gathering compliance metrics by 67% to 86%, saving several weeks of staff time every year.
- **Capacity to leverage analysts' capabilities on higher-value activities.** With many formerly manual tasks now addressed by security orchestration and automation, analysts were able to spend time helping strengthen their organization's security programs.
- **Consistent and effective incident response.** With IBM Security SOAR playbooks guiding and orchestrating incident response, organizations ensured a high-quality approach across the analyst team.
- **Better reporting on security incident metrics, in less time.** IBM Security SOAR's reporting capabilities enabled organizations to easily create and update reports from security data for the CISO and senior leadership.
- **Greater productivity in other areas of the organization and improved collaboration.** Although security analysts are the primary IBM Security SOAR users, individuals in other areas accessed data from IBM Security SOAR or worked actively in it, improving their productivity. IBM Security SOAR also improved incident-related collaboration and data sharing across an organization's overall cybersecurity team, and with other departments.

"We use IBM Security SOAR to let machines do what machines do best, and let humans focus on higher-value activities instead of pulling information and connecting the dots."

Cyberthreat analyst, utility

"It had been very difficult to see where our pain points were and to identify trends. Now, with IBM Security SOAR, we can create dashboards, data points, and metrics that seamlessly allow us to get that visibility."

Manager, information security, information services company

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five interviewees' companies and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. The composite is a multibillion-dollar global financial services organization serving businesses and consumers through a physical and online presence. Its diverse technology environment spans data and applications hosted on-premises as well as a growing number of workloads hosted in public or private clouds. Its 16,000 security incidents annually are equally diverse and include malware, phishing-related emails, suspicious login attempts, and penetration testers. The organization is held accountable to multiple regulatory bodies, with effective security posture and processes

Key assumptions

Multibillion-dollar global organization

On-premises and cloud technology environment

16,000 incidents addressed annually

important in meeting regulatory standards. Prior to deploying IBM Security SOAR, the organization responded to security incidents with extensive manual effort but no supportive technology beyond crib notes on spreadsheets about potential responses, and a ticketing system used simply to list incidents. It lacked time-saving orchestration of security information, playbooks to ensure consistent and swift response, and security automation to further reduce response time and effort (including fully automated response to certain types of incidents).

Deployment characteristics. After evaluating multiple vendors, the composite organization selected IBM Security SOAR and implemented cloud-based IBM Security SOAR using internal staff assisted by IBM professional services. In addition to establishing direct integrations, the organization integrated IBM Security SOAR with some tools indirectly via a security information and event management (SIEM) system. Although implementation included initial integrations and use cases, the organization has expanded its use of IBM Security SOAR's extensive functionality over time by adding more integrations and use cases. Similarly, it continues to modify or add playbooks to address emerging threats. Before going live, the organization trained end users. Internal staff members provide ongoing management and maintenance of IBM Security SOAR.

Analysis Of Benefits

QUANTIFIED BENEFIT DATA AS APPLIED TO THE COMPOSITE

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Orchestration and automation savings for incident response	$1,060,800	$1,283,568	$1,550,978	$3,895,346	$3,190,436
Btr	Existing security asset value realization improvement	$640,000	$760,000	$160,000	$1,560,000	$1,330,128
Ctr	End user and IT productivity recapture from improved IR capabilities	$27,137	$28,928	$30,718	$86,783	$71,656
Dtr	Audit efficiency gains	$7,657	$7,657	$7,657	$22,971	$19,042
	Total benefits (risk-adjusted)	$1,735,594	$2,080,153	$1,749,353	$5,565,100	$4,611,262

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $4.6 million.

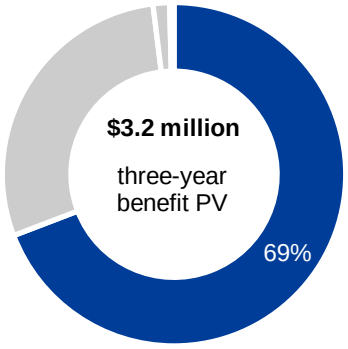
Orchestration And Automation Savings For Incident Response

The interviewees said their organizations reported significant reductions in the average amount of time needed for a security analyst to investigate, contain, and resolve a cybersecurity incident compared to their experiences before implementing IBM Security SOAR. Those reductions were apparent upon IBM Security SOAR implementation, and they increased over time as the organizations integrated additional security tools and sources with IBM Security SOAR for further enrichment and continued to refine and automate their incident response processes.

The interviewees said the amount of time saved per incident varied significantly — from less than half an hour to many hours — depending on the prior state of each organization's incident response. The percentage reduction in an analyst's average time spent per incident (compared to before IBM Security SOAR) ranged from 66% to 97%.

Interviewees noted that IBM Security SOAR reduced their organization's security analysts' effort across the lifecycle of an incident in multiple ways, including:

- **Security orchestration through dynamic response plans.** IBM Security SOAR guides and orchestrates analysts' incident response through playbooks that codify incident processes including dynamic adjustments if warranted by new information over the course of an incident. Organizations can use the playbooks that IBM Security SOAR provides (either as is or modified to suit their organization) or embed their own response plans and team expertise into IBM Security SOAR. The playbooks accelerate analyst response and ensure that analysts of all experience levels address each kind of incident in the most efficient and effective way. This provides immediate and substantial benefits for organizations, and it also establishes a foundation for later automating some aspects of the response, if desired.



Orchestration and automation savings for incident response: **69%** of total benefits

FORRESTER®

- **Reduced investigation time via automated enrichment.** By leveraging third-party integrations, IBM Security SOAR automatically consolidates threat intelligence and incident data from many security tools and sources. This automates enrichment tasks that analysts previously handled manually related to compiling knowledge of an incident (and, in some organizations, it enables employees to be able to do some of those tasks at all). These tasks include gathering current and historical information from endpoints, external networks, VPN logs, DNS records, network infrastructure, and endpoint forensics, and also internal data sources like a configuration management database (CMDB) and a lightweight directory access protocol (LDAP); checking indicators of compromise (IOCs) against threat intelligence feeds; identifying affected users and assets; and correlating historical incidents and data. Because IBM Security SOAR makes this information available from a central source (which several interviewees described as a "single pane of glass"), analysts quickly gain the insights they need in order to determine their decisions and actions.
- **Case management and orchestration of communication among various parts of an organization.** IBM Security SOAR's case management capabilities not only drive down response effort, but they also ensure that organizations document who is doing what and when and why. If an incident response process degrades, IBM Security SOAR automatically provides visibility and escalates efforts so that tasks get closed out within internal service-level agreements (SLAs). IBM Security SOAR's orchestration of communications saves time and improves collaboration between security analysts and other teams such as IT by replacing the numerous emails and phone calls previously needed to initiate, follow up on, and confirm actions.
- **Automation of application or system containment and remediation.** Once an organization has well-defined playbooks, it can begin to automate some further investigation, containment, and remediation actions that lend themselves to being done programmatically, saving additional analyst time.
- **Reduction in extraneous triage and analysis related to underperforming security tools.** Because IBM Security SOAR helps organizations recognize points of failure in their security architecture, security teams save time that they otherwise would have spent passing false negatives or exerting additional effort on false positives.

"The playbooks save time and make it easier for an analyst to know what to do."

Cyberthreat analyst, utility

"IBM Security SOAR correlates information and tells us if several things that have come in are related to each other. So rather than looking at three events as separate, you might look at them as a single event."

Manager, information security, information services company

"IBM Security SOAR may take an analyst's effort from an hour to a couple of minutes because they can see 'Well, these seven incidents are all the same, so I'm going to close all of them at the same time.'"

Manager, information security, information services company

The percentage reduction in analyst time varies not only across organizations but also across incident types within the same organization, depending on the nature of the incident response. A manager of information security at an information services company described reductions by incident type that ranged from 47% to 99%.

For some organizations, automating the entire response for some types of incidents contributed to the per-incident percentage reduction in analyst time. A vice president and information security officer at a financial service company noted that 20% of the organization's total number of incidents flowing through IBM Security SOAR were addressed automatically. Examples include quarantining, scanning, and neutralizing threats on machines where malware was detected, and blocking outbound traffic and terminating a VPN session for a particular user where the VPN detects malicious activity. A manager of information security at an information services company reported automating the closing of one-half to two-thirds of its phishing incidents by automatically pulling URLs, IPs, and attachment file hashes out of email reports and

automatically checking these artifacts against threat feeds. Security automations help that organization identify duplicate or near-duplicate emails already classified in the past. Then, when classifying an email, IBM Security SOAR checks all open incidents for duplicates and near-duplicates in order to auto-close with the same classification.

In addition to incident response, the information services company also uses IBM Security SOAR to automate virtually all aspects of tracking resolution of identified application security vulnerabilities, a process that may extend over several weeks. Prior to IBM Security SOAR, an analyst would have to log into multiple sources to identify vulnerabilities, and then rely on lengthy emails chains to ensure their resolution. With IBM Security SOAR, the analyst automatically sees all vulnerabilities and the communications about them in one place, and most communications are automated. If an analyst is out of the office, others can check vulnerability status or update the incident as needed.

For the composite organization, Forrester models orchestration and automation savings for incident response as:

- 16,000 cybersecurity incidents during Year 1, increasing to 17,600 and 19,360 in Years 2 and 3 due to corporate growth and more prevalent cybersecurity incidents.
- Reduction in per-incident triage and incident analysis effort of 1.20 hours in Year 1, increasing to 1.32 and 1.45 hours in Years 2 and 3.

Orchestration and automation savings for incident response will vary based on:

- An organization's prior state and maturity level for incident response.
- Nature of an organization's incidents and resulting per-incident analyst effort to address.
- Number of incidents.
- Extent to which an organization has leveraged IBM Security SOAR's functionality.
- Number and type of integrated security tools.
- Security analyst experience and capabilities.
- Prevailing local compensation rates.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $3,190,436.

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Orchestration And Automation Savings For Incident Response: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
A1	Cybersecurity incidents annually		16,000	17,600	19,360
A2	Triage and incident analysis effort reduced with automation and orchestration, in hours per incident		1.20	1.32	1.45
A3	Hours saved annually by security analysts with IBM Security SOAR orchestration and automation	A1*A2	19,200	23,232	28,072
A4	Cybersecurity analyst hourly compensation, fully burdened	$135,200/2,080	$65	$65	$65
At	Orchestration and automation savings for incident response	A3*A4	$1,248,000	$1,510,080	$1,824,680
	Risk adjustment	↓15%			
Atr	Orchestration and automation savings for incident response (risk-adjusted)		$1,060,800	$1,283,568	$1,550,978

Existing Security Asset Value Realization Improvement

Although organizations allocated increasing amounts to their security budgets, including acquisition of additional security tools, they found it difficult to determine the efficacy of those individual tools once they were deployed. With IBM Security SOAR as a central point of security orchestration and data collection, organizations were better able to evaluate the value of those tools for detecting or containing malicious activity. Security teams were able to identify underperforming or redundant security assets in order to either reconfigure them to improve performance or stop using them. For instance, the lead cybersecurity engineer at a financial services firm said: "From IBM Security SOAR, we can see what tools are generating more true positive alerts or false positive alerts. That means we know that these tools need to be tuned — or tuned more." As a result, they fully realized the value of security assets they had purchased and avoided continued payment for assets that were not delivering. They also saved analyst effort that otherwise would have been spent passing false negatives or acting on false positives.

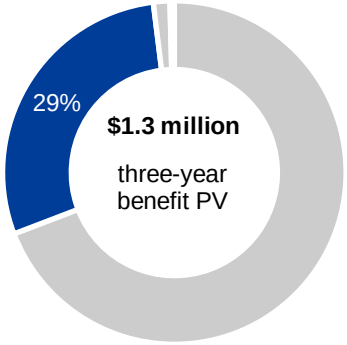
Improvement in realizing the value of existing security assets was generally largest in the first year or two of using IBM Security SOAR as an organization integrated some of its existing security tools. Value realization improvement persisted (although at a lower rate) as the organization integrated additional tools and continued to monitor performance.

For the composite organization, Forrester models existing security asset value realization improvement as:

- $800,000 in Year 1, $950,000 in Year 2, and $200,000 in Year 3.

Existing security asset value realization will vary based on:

- The number of security tools integrated with IBM Security SOAR and thus more readily evaluated.
- The annual fees for individual security tools.



Existing security asset value realization improvement: **29%** of total benefits

"We were able to show that some of our tools needed to be reconfigured and others weren't needed at all because the information they provided was also coming from other sources."

Senior manager, cybersecurity operations center, retailer

FORRESTER®

To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year risk-adjusted total PV of $1,330,128.

Existing Security Asset Value Realization Improvement: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Value of assets found to be misconfigured or underperforming		$800,000	$950,000	$200,000
Bt	Existing security asset value realization improvement	B1	$800,000	$950,000	$200,000
	Risk adjustment	↓20%			
Btr	Existing security asset value realization improvement (risk-adjusted)		$640,000	$760,000	$160,000

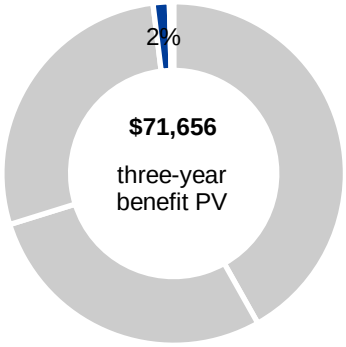
End User And IT Productivity Recapture From Improved Incident Response Capabilities

IBM Security SOAR does not enable quicker detection of malicious activity, which is a function of the existing security infrastructure. It does accelerate the incident response workflow once an incident has been detected, significantly reducing the time needed to enact remediation and containment procedures. End users who operate on the enterprise network would often find that their machines were locked out upon detection, resulting in a period of downtime until the endpoint was contained and remediated. By reducing the time between detection and containment, IBM Security SOAR enables end users to regain productive time.

In addition, incidents may cause deeper and collateral damage as time passes. A swifter response to an incident can reduce the need for IT staff to pursue deeper-level remediation/recovery techniques. IBM Security SOAR also speeds communications because an analyst can initiate automated notifications to both the end user and the IT staff who handle reimaging or remediation.

For the composite organization, Forrester models end user and IT productivity recapture from improved IR capabilities as:

- Annual number of incidents causing end user downtime increasing from 75 to 85 due to organization growth and increased frequency of cybersecurity incidents.
- One end user affected by each incident.
- A reduction in the percentage of downtime incidents that require reimaging or full-scale remediation effort from 95% to 20%.
- A total of 3.5 hours of IT effort for each reimaging or remediation.



End user and IT productivity recapture from improved incident response capabilities: **2%** of total benefits

FORRESTER®

End user and IT productivity recapture from improved IR capabilities will vary based on:

- Number of endpoints and end users affected.
- The detection efficacy of security measures already in place.
- Nature and severity of incidents, number of applications affected, and resulting remediation or reimaging processes needed.
- Prevailing local compensation rates.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $71,656.

> "Our analysts previously would designate a machine for reimaging because they lacked information to make a better decision. Now that information is in one place."
>
> *Senior manager, cybersecurity operations center, retailer*

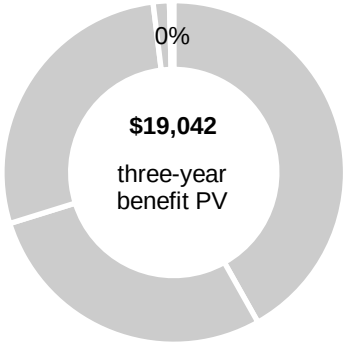
End User And IT Productivity Recapture From Improved IR Capabilities: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Incidents causing end user downtime		75	80	85
C2	Number of users affected per incident		1	1	1
C3	End user uptime improvement from automation and orchestration of containment, in hours per incident		5.25	5.25	5.25
C4	Total hours saved annually by end users from uptime improvement	C1*C2*C3	394	420	446
C5	End user hourly compensation, fully burdened	$93,600/2,080	$45	$45	$45
C6	Reimage/full-scale remediation effort avoided, measured in IT hours needed to address incidents	B1 * 75% of incidents * 3.5 hours per incident	197	210	223
C7	IT support staff hourly compensation, fully burdened	$114,400/2,080	$55	$55	$55
Ct	End user and IT productivity recapture from improved IR capabilities	(C4*C5)+(C6*C7)	$28,565	$30,450	$32,335
	Risk adjustment	↓5%			
Ctr	End user and IT productivity recapture from improved IR capabilities (risk-adjusted)		$27,137	$28,928	$30,718

Audit Efficiency Gains

The interviewees' organizations span a range of industries and geographies, and thus contend with varied security and privacy regulations and compliance measures. However, all were able to collect and present required cybersecurity information faster due to the visibility and the querying and reporting capabilities provided by IBM Security SOAR. Interviewees reported a 67% to 86% reduction in the time needed to compile compliance metrics, saving several weeks of staff time every year. A senior manager, cybersecurity operations center, for a retailer explained: "Before IBM Security SOAR, we had to go through a lot of different systems trying to collect information the auditors needed. If they came back with questions, we couldn't provide details. Now I just put in the timeframe and export the data. If they need details, I can pull individual incidents and export a more in-depth PDF for each incident they've requested."

For the composite organization, Forrester models audit efficiency gains as:



Audit efficiency gains:
<1% of total benefits

FORRESTER®

› Reduction in total annual IT staff time spent compiling metrics from 156 to 32 hours each year.

Audit efficiency gains will vary based on:

› Nature of regulations and required reporting.

› Prevailing local compensation rates.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $19,042.

Audit Efficiency Gains: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	IT staff time spent annually compiling compliance metrics before IBM Security SOAR		156	156	156
D2	IT staff time spent annually compiling compliance metrics after IBM Security SOAR		32	32	32
D3	Blended IT staff hourly compensation, fully loaded	$135,200/2,080	$65	$65	$65
Dt	Audit efficiency gains	(E1-E2)*E3	$8,060	$8,060	$8,060
	Risk adjustment	↓5%			
Dtr	Audit efficiency gains (risk-adjusted)		$7,657	$7,657	$7,657

Unquantified Benefits

The interviewed organizations reported other significant benefits that are not quantified for this study:

› **Ability to focus security analysts on higher-value activities.** With many time-consuming and repetitive incident response tasks now addressed by security orchestration and automation, organizations leveraged their security analysts' capabilities on higher-value activities. Instead of those analysts struggling to resolve each day's barrage of cybersecurity incidents, they are able to apply time freed up by IBM Security SOAR to help further strengthen their organization's security programs such as penetration testing and vulnerability management and tracking. Interviewees perceived that this resulted in greater job satisfaction for these highly skilled individuals.

> "Our analysts can get ahead of the game instead of just constantly fighting the onslaught."
>
> *Manager, information security, information services company*

› **Consistent high-quality incident response.** By encoding their security team's collective expertise within IBM Security SOAR playbooks, organizations ensured a consistent response regardless of which analyst picked up an incident. Less-experienced team members learned faster, and the team elevated its collective capabilities.

› **Better and faster reporting on security incident metrics**. Since every field within IBM Security SOAR is exposed to its reporting capabilities, organizations can easily create and update reports from their security data. They found that IBM Security SOAR cut the time needed to prepare reports on security metrics for the CISO and senior leadership, and it enabled preparation of better reports. A senior manager, cybersecurity operations center, for a retailer noted: "IBM Security SOAR provides a one-stop shop for metrics. We no longer have to collect them."

> "None of our metrics now are manually calculated. It all happens automatically, so we don't have to touch anything."
>
> *Cyberthreat analyst, utility*

- **Time savings and improved collaboration from IBM Security SOAR usage outside of the incident response team.** Although security analysts are the primary IBM Security SOAR users, individuals in other areas accessed data from IBM Security SOAR or worked actively in it, improving their productivity. That included threat hunters, threat intelligence researchers, and security engineers, along with other IT staff. IBM Security SOAR also improved collaboration and data sharing across an organization's overall cybersecurity team, and with other departments. A senior manager, cybersecurity operations center, for a retailer estimated that half of their organization's security incidents require notifying other parts of the company, with three to five individuals being notified.

  Both of the interviewees from financial services companies reported that their payment fraud departments use IBM Security SOAR. A vice president and information security officer at one of them indicated that using IBM Security SOAR decreased the time for the fraud department to understand if an account opening was fraudulent or not from as much as two days to 2 to 4 hours. That vice president explained: "IBM Security SOAR's ability to ingest data helps a lot in terms of the investigation time as well as determining if an account is actually fraudulent or instead the alert was a false positive. A fraud investigator can easily respond, as well as stop the threat." The financial services company was able to reduce its fraud losses and also redeploy 60% of a 50-person fraudulent account team to other needed roles.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement IBM Security SOAR and later realize additional uses and business opportunities, including:

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

- **Integrating IBM Security SOAR with additional security tools.** For further enrichment and automation and greater visibility to the performance of security tools, interviewees said their organizations anticipate integrating IBM Security SOAR with additional security tools and information sources. Through IBM Security SOAR integration, these additional tools can be leveraged to further automate the investigatory or remediation process and tie that into incident response workflows.
- **Further automating incident response.** Whether through these additional integrations or via process refinements, interviewees anticipate additional automation of their organization's incident responses, either partially or in full.
- **Using IBM Security SOAR for purposes other than cybersecurity incident response.** Interviewees said their organizations have leveraged or are considering leveraging IBM Security SOAR for use by other security staff outside of the incident responders (such as threat hunters, threat intelligence researchers, and security engineering), by IT staff outside of the cybersecurity team (e.g., disaster recovery), or even by staff outside of the IT department (physical security, legal).
- **Capitalizing on new IBM Security SOAR capabilities as they are launched.** Organizations anticipate further utilizing IBM Security SOAR as its capabilities continue to evolve.

- **Deploying related IBM security products**. IBM Security SOAR can be readily integrated with additional IBM security products, such as the IBM Security SOAR Privacy add-on for privacy breach reporting.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

QUANTIFIED COST DATA AS APPLIED TO THE COMPOSITE

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	IBM fees	$31,500	$262,500	$262,500	$262,500	$819,000	$684,299
Ftr	Internal labor for implementation and ongoing management	$44,363	$47,775	$47,775	$47,775	$187,688	$163,172
	Total costs (risk-adjusted)	$75,863	$310,275	$310,275	$310,275	$1,006,688	$847,471

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than $0.8 million.

IBM Fees

IBM fees reflect annual subscription costs for IBM Security SOAR along with one-time professional services fees for implementation assistance. The subscription fee includes a standard level of support.

Since subscription costs are determined by customer-specific factors, consult with IBM for likely costs specific to your organization when conducting your own analysis. Your organization's subscription fees may be lower or higher than the composite organization's fees.

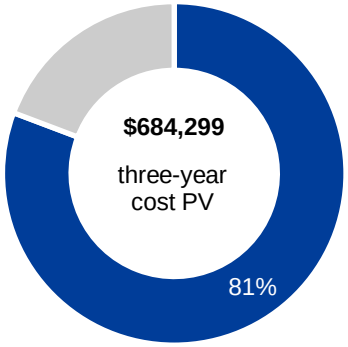
For the composite organization, Forrester models IBM fees as:

- Annual subscription fees of $250,000 for cloud-based IBM Security SOAR.
- IBM professional services of $30,000 during implementation.

IBM fees will vary based on:

- Scope of the IBM Security SOAR implementation.
- Choosing cloud or on-premises deployment.
- Whether or not and to what extent an organization augments its internal labor with IBM professional services during implementation and/or ongoing operations.
- Level of IBM support selected.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $684,299.



IBM fees:
81% of total costs

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

FORRESTER®

IBM Fees: Calculation Table						
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Subscription fees			$250,000	$250,000	$250,000
E2	Professional services		$30,000			
Et	IBM fees	F1+F2	$30,000	$250,000	$250,000	$250,000
	Risk adjustment	↑5%				
Etr	IBM fees (risk-adjusted)		$31,500	$262,500	$262,500	$262,500

Internal Labor For Implementation And Ongoing Management

Initial costs: Interviewees said their organizations typically implemented IBM Security SOAR using internal security and other IT staff with assistance from IBM professional services. Although as a software-as-a-service (SaaS) product, IBM Security SOAR could be functional quickly, interviewees described their full implementation in broader terms. Most of their organizations began with a proof of concept, followed by full implementation, and that combined effort spread across two to three months. Implementation included technical deployment of IBM Security SOAR, tuning IBM Security SOAR to fit an organization's environment and processes, customizing IBM Security SOAR playbooks or entering an organization's own response plans into IBM Security SOAR, establishing role-based access control, integrating with the organization's SIEM system and several security tools, and integrating IBM Security SOAR with the ticketing system IT support staff members use to facilitate and track follow-up. Training was typically brief and conducted by internal staff, as security analysts found IBM Security SOAR intuitive and easy to use.

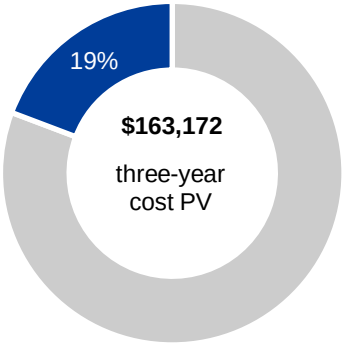
For the composite organization, Forrester models initial internal labor as:

› A total of 650 IT hours for implementation from a team of two security engineers and a manager.

Ongoing costs: Ongoing internal labor costs cover not only general management and support of IBM Security SOAR, but also additional efforts to build out security orchestration and automation capabilities since interviewees said their organizations typically took a phased approach to deployment. With consistent incident response processes established, organizations began to automate some of their investigatory and remediation efforts (whether partial or full for certain incident types). They integrated IBM Security SOAR with more of their existing security tools as well as newly acquired tools, adjusting their response processes and workflows as needed. They modified or created processes and remediation approaches to address emerging threats and embedded them in their IBM Security SOAR playbooks.

For the composite organization, Forrester models ongoing internal labor as:

› A total of 700 IT hours annually for ongoing management and support and further development of IBM Security SOAR's capabilities.



Internal labor for implementation and ongoing management: **19%** of total costs

FORRESTER®

Internal labor costs will vary based on:

- Scope and complexity of the implementation.
- Extent to which an organization continues to expand its use of IBM Security SOAR.
- Staff experience and capabilities.
- Prevailing local compensation rates.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $163,172.

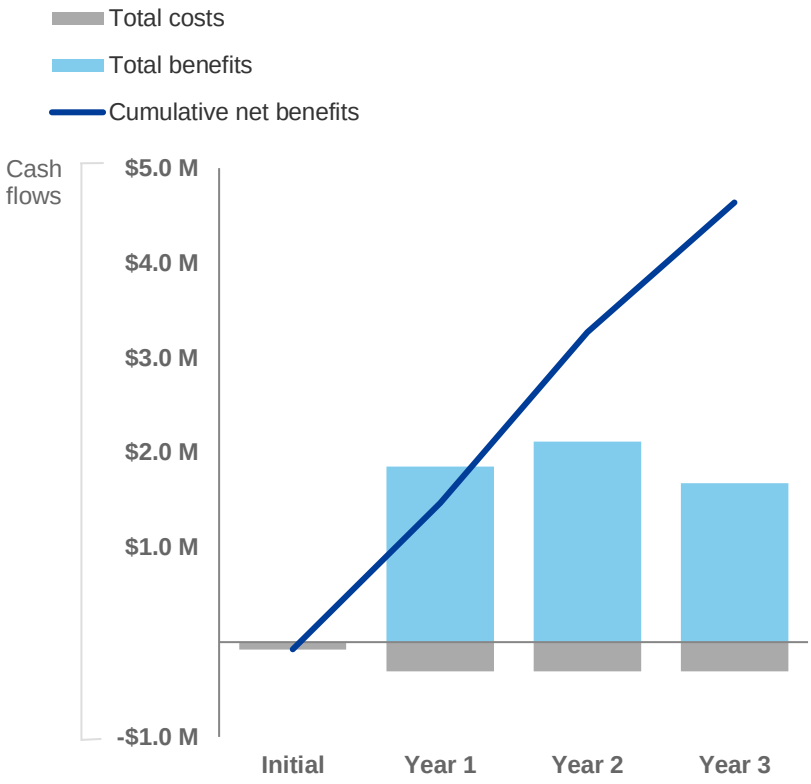
Internal Labor For Implementation And Ongoing Management: Calculation Table

REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
F1	IT hours required for implementation and ongoing support, per year		650	700	700	700
F2	Blended IT staff hourly compensation, fully loaded	$135,200/2,080	$65	$65	$65	$65
Ft	Internal labor for implementation and ongoing management	G1*G2	$42,250	$45,500	$45,500	$45,500
	Risk adjustment	↑5%				
Ftr	Internal labor for implementation and ongoing management (risk-adjusted)		$44,363	$47,775	$47,775	$47,775

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($75,863)	($310,275)	($310,275)	($310,275)	($1,006,688)	($847,471)
Total benefits	$0	$1,735,594	$2,080,153	$1,749,353	$5,565,100	$4,611,262
Net benefits	($75,863)	$1,425,319	$1,769,878	$1,439,078	$4,558,412	$3,763,791
ROI						444%
Payback period						<6 months

FORRESTER®

IBM Security SOAR: Overview

The following information is provided by IBM. Forrester has not validated any claims and does not endorse IBM or its offerings.

IBM Security SOAR is a leading Security Orchestration, Automation and Response (SOAR) platform designed to empower security teams to respond to security incidents with confidence. With IBM Security SOAR, organizations can introduce efficiency into their Security Operations Center (SOC) by leveraging its orchestration and automation capabilities to maximize existing security and IT tools, and to eliminate repetitive tasks. IBM Security SOAR enables security analysts to focus on high-level investigations and to take remediation action from a single hub.

As a SaaS offering, IBM Security SOAR enables security teams to deliver rapid time to value by providing a predictable, scalable cost model that allows security teams to start a SOAR project without significant upfront investment. Organizations can expand their business geographically with the confidence that control standards can be met using the service without having to commit and tie up capital assets. IBM Security SOAR can also be deployed on-premises with IBM Cloud Pak for Security platform, supporting on-premises and hybrid multi-cloud use cases. IBM Security SOAR helps accelerate your incident response with:

- **Dynamic playbooks:** IBM Security SOAR codifies incident response plans into workflows that, combined or independently, form playbooks that are dynamic and additive. Playbooks are incident-type-specific and provide security teams with a recommended course of action, therefore amplifying their ability to respond to incidents and giving them the agility to pivot and adapt to real-time incident conditions.
- **Case management:** IBM Security SOAR allows incident response teams to collaborate with consistency and share timely information about incidents through tasks, notes, and attachments. Teams have visibility into the relevant incident tasks, the team members working on them, and the due dates. Every action is recorded and time-stamped to assist in preparing for an audit. Furthermore, IBM Security SOAR ensures that key stakeholders in other business units are part of the incident response effort and are equipped to fulfill their roles and complete their tasks.
- **Robust orchestration and automation ecosystem:** With more than 150 applications published in the IBM Security App Exchange, IBM Security SOAR integrates with numerous security and IT tools, including Red Hat Ansible Automation, which opens the door to thousands of additional automation playbooks.
- **Data privacy breach assistance:** IBM Security SOAR maps privacy breach reporting requirements with security incident case management. The Global Privacy Regulations Knowledgebase tracks more than 170 regulations and can help your team navigate the complex regulatory environment and notification requirements with a guided process.

IBM Security SOAR Enables Cyber Resilience Across The Organization		
Outside the SOC	**For the organization**	– Captures repeatable processes and ensures standard operating procedures are in place – Documents evidence of abiding to rules and regulations for compliance audits – Extends incident response to include other business units (legal, marketing, HR) necessary in the incident response process
	For the CISO	– Provides visibility into incident response program via dashboard and reporting – Enables measurable time-to-value of security spend – Maximizes ROI of security tools and demonstrates security's value to the business

Inside the SOC	**For the SOC manager**	– Tracks key metrics like mean time to resolve (MTTR) to measure and improve SOC productivity – Elevates staff effectiveness with tools that help them focus on the right tasks – Allows for consistent response across regions/departments
	For the analyst	– Provides a guided response plan through playbooks to resolve different types of incidents – Helps analysts focus on investigation and response instead of pivoting between tools – Helps reduce repetitive tasks like alert triage and enrichment with automation

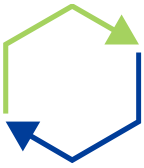
Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.



Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

FORRESTER®