Sponsored by:
Recorded Future

Authors:
Harsh Singh
Martha Vazquez

August 2018

Business Value Highlights

284%
three-year ROI

32%
more efficient IT security teams

4 months
to payback

10 times
faster identification of threats

22%
more security threats identified before impact

86%
less unplanned downtime

1 million
in potential penalties/fines per breach avoided

63%
faster resolution of threats

Organizations React to Security Threats More Efficiently and Cost Effectively with Recorded Future

This IDC Business Value White Paper has been updated with an additional "Message from Sponsor" section which was not in the previous publication of the paper.

EXECUTIVE SUMMARY

The threat intelligence security services (TISS) market in the early stages was defined as the collection of multiple data feeds and sources about vulnerabilities or threats in an IT environment. In the past three to five years, the definition of the TISS market has evolved from just multiple sources of data feeds to include the context around the information or data entering the environment. Today, threat intelligence (TI) services involve using the data to present deeper analysis to the IT analyst. IDC defines TISS to include not only data feeds but also additional context around the vulnerability or threat and the use of iterative intelligence — a process that incorporates past experiences and mistakes into future planning. Threat intelligence needs to provide information that goes beyond the data points and also actionable recommendations around the data being presented to the organization. Threat intelligence should identify historical trends, much like a forecast that is then used in telling a story that can easily help organizations make strategic decisions about their security posture.

Recorded Future, a vendor in the TISS market, provides an all-in-one universal TI solution that combines machine learning along with human analysis to create real-time and relevant data. The technology is built on machine learning and automation, and in the past few years, the company has added experts to its team to provide detailed analysis of the content as well. Recorded Future's technology is created to save time and improve efficiency as opposed to humans looking through vast amounts of data for context around security alerts or incidents that may need further investigation to determine the organization's security risk.

IDC interviewed organizations that are utilizing Recorded Future for IT security threat intelligence. The interviews reveal that these organizations were realizing significant benefits by leveraging Recorded Future's solution across their entire IT security organization. Based on IDC's calculations, these organizations were realizing benefits worth about $806,000 per organization per year ($39,638 per internal IT security team member) by:

- Driving higher staff productivity for the entire IT security team, including staff responsible for operations, investigation, report compilation, and threat resolution
- Giving security teams more time to proactively attack threats before they impacted the wider organization
- Helping organizations avoid damaging penalties and fines for each security breach

SITUATION OVERVIEW

In today's cyberthreat landscape, adversaries are smarter, posing serious challenges for organizations. Security teams are trying to stay ahead of advanced persistent threats (APTs) and zero-day threats, but the unknown bad actors continue to be one step ahead, employing multiple techniques and tools at their targets while maintaining a low profile and slow infiltration speed. Typical firewalls and signature-based antimalware solutions work well but are not always suitable to keep up with the malicious threats of today. While some enterprises still rely primarily on signature-based methods, many are integrating threat intelligence services into their security operations and taking an analytical, predictive stance to help reduce risk and potential business disruption.

While organizations may install security tools that integrate data feeds onto their network, many do not recognize what to do with the information that is coming in. Organizations often do not understand the term threat intelligence and the benefits to the organization if used effectively or correctly. The amount of data coming into an IT environment is enormous, making organizations even more perplexed and confused as to how to make effective decisions around this incoming content. An organization may subscribe to data feeds but not have the staff to dissect and research which threat is more important than the others and then, once this is found, to actually conduct the analysis to see whether the threat needs to be taken seriously and how the organization should proceed after that.

The TISS market is relatively new and has been growing steadily in the past several years. It reached $1.3 billion in 2017 and is forecast to grow at a CAGR of 11.2% from 2016 to 2021. The TISS market will continue to grow as organizations look to secure their own investments, data, and intellectual property. It is increasingly overwhelming and complex for an organization to keep up with the threat profile across the organization because of the rise of Internet of Things

(IoT), software-defined networks, and cloud computing — all of which open doors to new threats. As a result, organizations are taking the opportunity to partner with TISS vendors to create concrete actionable data points from their security analysis, therefore assisting them in the fight against adversaries.

RECORDED FUTURE

Recorded Future is one vendor that provides a universal threat intelligence solution to global organizations. One theme mentioned previously discusses how threat intelligence needs to consist of data that provides actionable content. Organizations today struggle with gathering tons of data and making sense of what the data means and whether it's a true threat. Deciphering a security incident takes time and expertise, which is where Recorded Future comes into play. Recorded Future delivers a unified solution by combining subscription feeds, open source and dark web intelligence, and analyst reports and aggregates the data on one platform. Recorded Future's threat intelligence combines machine learning and human expertise to create real-time and relevant data. In addition, in the past few years, the company has added experts to its team to provide detailed analysis of the content. Recorded Future's technology is created to save time and improve efficiency as opposed to humans looking at possible security incidents that are coming in from devices, such as security information and event management (SIEM) systems or vulnerability scanners, and then taking the time to determine which vulnerabilities or security incidents are more serious. In addition to trying to decipher which events represent real threats, the IT security team must prioritize the high volume of alerts entering the environment. With Recorded Future's TI offering, teams can assess which threats are most important and mitigate or patch them immediately.

The amount of threat and vulnerability data available from hundreds of thousands of external sources is extremely difficult for security teams to look through because they must decipher language and cross-correlate and conduct in-depth research to determine what this threat data means and which threat data is relevant to their organization. By utilizing machine learning and automation, Recorded Future's solution can take in data from technical sources, technical research, open sources, and closed/dark sources. Recorded Future's newest platform, Fusion, can also take in customer sources, which include other third-party feeds and internal threat data. The Recorded Future solution takes in a large volume of these resources and will aggregate and analyze the data in one place. Within the universal TI solution, the technology uses natural language processing to read in any language and can quickly identify in real time words that are related to a threat actor or target or malware and so forth. The solution utilizes ontologies to represent hierarchical relationships and organize the data; for example, if an organization is researching threats in France, the system automatically includes threats relevant to every city, town, and so forth in France.

Recorded Future connects the dots and presents customers with all intelligence relevant to threat actors; tactics, techniques, and procedures (TTPs); and indicators of compromise (IOCs). If a customer wants to know more about a certain IP address, for example, the compiled reports (intelligence cards) can be pulled on demand with real-time intelligence, delivering valuable context. Intelligence cards can provide customers with a glance into understanding top attack vectors, affected technologies that can exist in the enterprise, and related IOCs. In addition, customers can ask for on–demand reports, customized to their specific requirements and areas of interest, as well as weekly reports to determine their security risk and other security threat analysis.

Another key feature of Recorded Future's TI offering is the ability to integrate within security environments. As mentioned previously, SIEM systems and vulnerability scanners can be integrated, but a number of other security devices can also be integrated to consume threat intelligence. In addition, multiple solutions can be integrated to support different IT security roles such as security operation, incident response, vulnerability management, or executive teams. For the security operation teams, Recorded Future can help triage faster, reduce manual research time, and help discover unknown threats, assisting in determining the level of risk around alerts and event prioritization. For incident response teams, the solution can assist in reducing response time by providing real-time and rich context around the incident, therefore minimizing the need for manual research and time wasted on identifying false positives. Vulnerability management teams can determine prioritization from the high amount of vulnerabilities coming in and which vulnerabilities should be patched first. To further speed prioritization, intelligence cards provide risk scores to help organizations quickly understand the level of risk associated with an event. Executive teams that do not need as much detailed information can also see high-level reports and dashboards that show them just enough information to understand their overall security risk posture.

The interviewed Recorded Future customers were all very enthusiastic about Recorded Future's TI offering and how it helped them become more efficient and work more effectively. Customers commented on the solution's ability to provide real-time analysis to make their teams work more efficiently by helping them make better decisions around the security incidents entering the IT environment. They also mentioned cost effectiveness and efficiency, easy integration, wider visibility, and actionable information around the latest security incidents.

THE BUSINESS VALUE OF RECORDED FUTURE

Study Demographics

IDC interviewed six organizations for this study by asking participants a variety of quantitative and qualitative questions about the impact of deploying the Recorded Future solution on their IT and security operations, businesses, and costs. Table 1 characterizes the firmographics of these organizations.

The size of the companies surveyed represented a diverse mix, ranging from very large enterprises to small and medium-sized organizations. This is reflected in the average employee base of 51,725. A significant IT presence was also apparent across all companies with the average number of IT staff at 4,072, supporting an average total of 43,292 internal users. All the companies surveyed were located in the United States. In addition, the companies represented a broad mix of vertical industries: financial services, automotive, manufacturing, and information technology.

TABLE 1 Demographics of Interviewed Organizations

	Average	Median
Number of employees	51,725	17,500
Number of IT staff	4,072	880
Number of users of IT services	43,292	17,500
Number of business applications	742	475
Number of connected devices	64,100	36,250
Revenue per year	$6.2 billion	$1.9 billion
Countries	United States (6)	
Industries	Financial services (3), automotive, manufacturing, information technology	

n=6 Source: IDC, 2018

Use of Recorded Future

In today's business environments, first-rate security capabilities are essential for both IT and business operations. IT organizations and their security teams need analytics-driven solutions that can provide proactive security by automating the collection and analysis of threat data in real time. In addition, solutions need to complement existing security systems, such as network-based firewalls and endpoint security.

The companies that IDC interviewed stressed the need for having these capabilities in place to meet the increasing number of threats and attacks on their IT infrastructure and data. Interviewed organizations told IDC that the Recorded Future solution has helped them monitor and address security issues by providing better real-time notifications and insights. Study participants provided a number of reasons for choosing Recorded Future over alternative approaches, including:

- **Cost-effective enhanced security:** "Recorded Future will cost less than two security engineer FTEs and will increase the access and improve the relevant intelligence analysis and reporting of all existing security efforts across our organization."
- **Better insights into vendors:** "Recorded Future provides insight such as the risk of doing business with vendors. When our procurement people evaluated vendors, they used a financial report but never thought of doing a cybercheck on them. We did it one time for them, and the reaction was, 'Who are these people?'"
- **Ability to automate more security processes:** "One strategic objective is to implement more automation features within our security detection and response capabilities. Recorded Future plugs right in and complements our network-based firewalls and endpoint security."

To develop a full picture of usage patterns within surveyed companies, IDC gathered data on how study participants were deploying the Recorded Future platform as well as detailed information about their IT and network environments. For example, as shown in Table 2, the average number of business applications across all companies was 322. These applications were used by a large base of 31,617 internal users. Table 2 also provides additional metrics on the use of the Recorded Future solution.

TABLE 2 Recorded Future Environment by Organization

	Average	Median
Number of branches/sites	238	200
Number of internal users	31,617	10,800
Number of business applications	322	155
Total revenue supported	88%	100%

n=6 Source: IDC, 2018

Business Value of Recorded Future

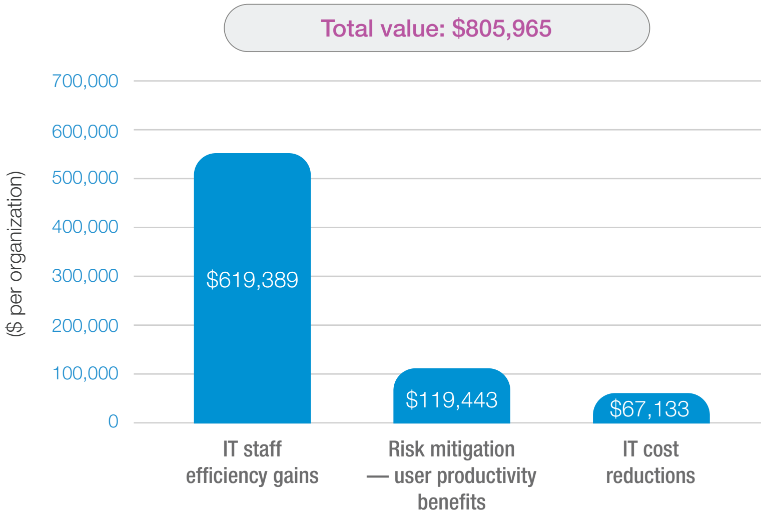
Participating organizations stated that the intelligence they received from Recorded Future is relevant and timely, based on two primary capabilities: the automation of information-related threats generated through machine learning/artificial intelligence and the improving awareness of these threats through visibility and timeliness. Instead of spending significant time investigating potential threats and remediating them, organizations can be more proactive in their approach to security threats and concerns. IDC calculates that customers/participants will achieve benefits worth an annual average of about $806,000 per organization ($39,638 per internal IT security team member) in the following areas (see Figure 1):

- **IT staff productivity benefits:** IT security teams have time freed up from investigating and compiling reports to work on other critical security operations. Meanwhile, security resolution teams have more time to anticipate incoming threats, which allows them to be more proactive. IDC calculates that these organizations are realizing productivity benefits worth $619,389 per organization ($30,462 per internal IT security team member).

- **Risk mitigation — user productivity benefits:** Organizations have reported seeing reduced unplanned downtime because of fewer security breaches impacting their operations. IDC places a value of $199,443 per organization ($5,874 per internal IT security team member) on these productivity gains.

- **IT cost reductions:** Interviewed organizations told IDC they were seeing savings in the cost of external reports and consulting, which IDC estimates to be worth $67,133 per organization ($3,302 per internal IT security team member).

FIGURE 1 Average Annual Benefits per Organization



Source: IDC, 2018

More Efficient IT Security Operations

Study participants described how deployment of the Recorded Future solution increased the efficiency of security teams. This included improvements in two key areas: threat intelligence compilation and threat investigation procedures. As a result, security teams can address issues more proactively using the solution.

The Recorded Future solution is built to utilize the scale and speed of machine learning for threat intelligence compared with manual human labor. Organizations are able to achieve time savings because Recorded Future offers an API to integrate threat intelligence into the other solutions these IT organizations are deploying.

Study participants described several specific attributes that drove these efficiencies:

- **Improvement of existing security solutions:** "Recorded Future enriches the data. I pull off some information and using Recorded Future get a whole lot more data out of it. For example, we use domain tools for domain monitoring. By plugging them into Recorded Future, I could get information that a particular IP address was involved in suspect activity."
- **Accurate reporting:** "Recorded Future's on-demand reports … are precise and the level of detail is unbelievable. Turnaround time is really good as well. The data in the report is valuable because it is very actionable."
- **Relevant and actionable information:** "Our team gets constant updates about our products. But it is nice to see high-level reports such as what is in the news today. With Recorded Future, we have seen a legitimate uptick in useful information. For a C-level, it's nice to have that report in the morning before meetings. Recorded Future puts out valuable information that you can sink your teeth into."

These quotes illustrate how Recorded Future has impacted various levels of security teams. Table 3 provides specific improvement metrics for Recorded Future's impact on the productivity of security threat intelligence compilation tasks. The fact that staff time costs for these tasks showed a 34% improvement is noteworthy.

TABLE 3 Productivity Impact of Security Report Compilation

	Before Recorded Future	With Recorded Future	Difference	Benefit (%)
Threat intelligence compilation staff impact (equivalent FTEs)	6.1	4.1	2.0	34
Staff time per security team member per year (hours)	564	375	189	34
Staff time cost for report compilation	$610,200	$405,400	$204,800	34

Source: IDC, 2018

Interviewed organizations spoke to IDC about how threat intelligence teams are no longer required to manually search for threats because the Recorded Future solution compiles them automatically. This core benefit substantially reduces the time required to investigate threats.

Commenting on this benefit, one study participant noted: "Recorded Future allows us to produce more meaningful data around potential threats. It has allowed us to get a clearer picture of everything. Previously, our team would have had to do a manual search for a particular event. Recorded Future is able to pull in more sources than we could. Without it, we would have to sift through Google or social media for potential activity." On the ability to identify issues faster, another participant said: "Recorded Future is really security focused when it comes to incident response. We are finding out about incidents faster, and we are able to respond and remediate even if those incidents are not on our networks and are out in the wild."

Table 4 provides specific improvement metrics on the productivity impacts for threat investigation processes. For example, the overall staff time required for these tasks showed an average 13% improvement.

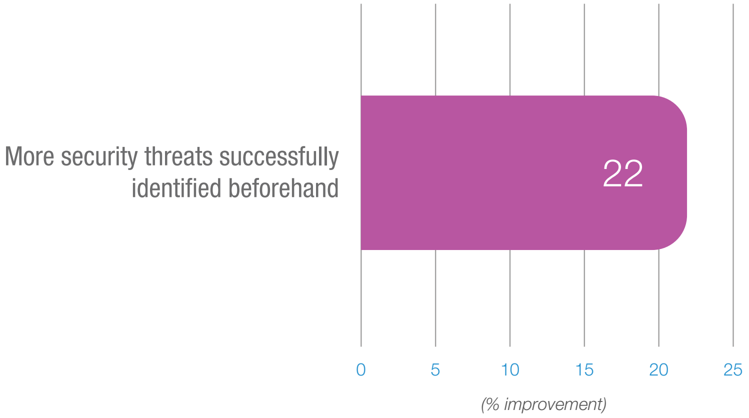
TABLE 4 Productivity Impact of Threat Investigation Staff

	Before Recorded Future	With Recorded Future	Difference	Benefit (%)
Threat investigation staff impact (equivalent FTEs)	18.2	15.7	2.4	13
Staff time per security team member per year (hours)	1681	1455	226	13
Staff time cost for threat investigation	$1,818,600	$1,574,000	$244,600	13

Source: IDC, 2018

Another aspect of the overall security challenge for the organizations surveyed is to successfully identify more threats before they can impact their organization. As one organization noted: "Recorded Future helps us assess our risk profile. As we have grown and acquired new technologies and expanded into new areas, it allows us to monitor for threats in areas where we are fairly new entrants and where we might not have the same security infrastructure as we would have in our existing business." As shown in Figure 2, these organizations are able to detect 22% more threats before these threats impact their organization.

FIGURE 2 Threat Resolution



Source: IDC, 2018

Table 5 shows the productivity impacts for these teams after deploying and using the Recorded Future offering. These organizations are able to identify potentially impactful threats 10 times faster than before deploying Recorded Future, from 0.4 days advance notice to about 4.1 days advance notice with Recorded Future. The time savings also means that security resolution teams can resolve threats 63% faster on average. As a result of these time savings — due to more timely threat visibility — security resolution teams are averaging a 78% increase in productivity.

TABLE 5 Productivity Impact of Security Resolution Staff

	Before Recorded Future	With Recorded Future	Difference	Benefit (%)
Time that threats are identified before becoming impactful (days)	0.4	4.1	3.7	1,000
Time to resolve issues (hours)	15.6	5.7	9.9	63
Security resolution staff impact (equivalent FTEs)	2.4	0.5	1.9	78
Staff time per security team member per year (hours)	223	50	173	78
Staff time cost for security resolution	$241,100	$54,000	$187,400	78

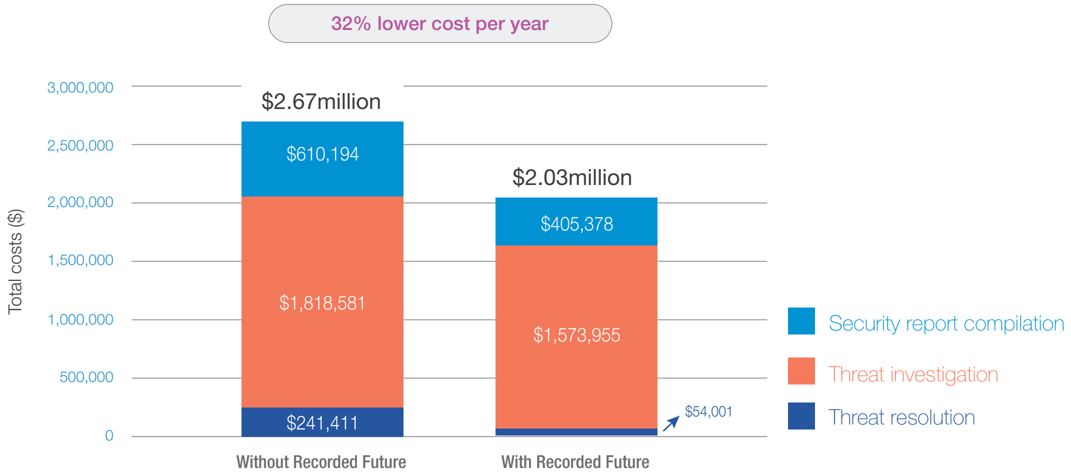
Source: IDC, 2018

Productivity improvements lead to benefits involving total cost of operations. As shown in Figure 3, the security team cost impacts are associated with the three key areas already discussed:

- Security report compilation
- Threat investigation
- Threat resolution

As Figure 3 indicates, IT security teams' costs are 32% lower with Recorded Future.

FIGURE 3 Total IT Security Team Time Cost Impact



Source: IDC, 2018

Risk Mitigation Impact

In today's business environments, unplanned downtime is a line-of-business productivity killer. Study participants spoke to IDC about how the functionality of the Recorded Future solution has led to fewer instances of unplanned downtime.

Security teams keep unplanned downtime in check because they are better able to handle threats before they become serious issues. This is the result of reducing the number of users impacted by security-related unplanned downtime and the number of incidents experienced per user.

As shown in Table 6, organizations are able to gain back 86% of end users' lost productivity due to security threat–related unplanned outages.

TABLE 6 Unplanned Downtime Impact

	Before Recorded Future	With Recorded Future	Difference	Benefit (%)
FTE impact of lost productivity due to unplanned outages	2.1	0.3	1.8	86
Hours per year per security team member	193	27	166	86
Value of lost productivity per year	$145,800	$20,300	$125,600	86

Source: IDC, 2018

According to some sources, in 2018, companies in the United States paid significantly more for every data breach than companies in any other country. Actual breaches may involve monetary exposure, the much publicized risk of data theft, or the more intangible but still troublesome problems associated with loss of reputation or customers.

Mitigating risk is a means of reducing these costs. More reliable handling of actual and potential security threats reduces overall risk to the organizations surveyed. Commenting on this benefit, one study participant noted: "We have better visibility using Recorded Future. The number of incidents didn't change, but it changed the level of risk."

As shown in Table 7, the risk mitigation impact after deployment and use of the Recorded Future solution is significant, allowing customers to avoid an average of $1,033,300 in potential losses per breach.

TABLE 7 Risk Mitigation Impact

	Per Organization
Potential losses per breach	$1,033,300
Reduction in fines/penalties	2%

Source: IDC, 2018

ROI Analysis

Table 8 presents IDC's analysis of the benefits and costs related to participating organizations' use of Recorded Future. IDC projects that over three years, these organizations will invest a discounted average of $0.50 million ($24,656 per security team member) in the Recorded Future solution. IDC expects that in return, these customers will realize discounted benefits of $1.92 million per organization ($94,639 per security team member). This would result in an ROI of 284% and a breakeven on their investment in four months.

TABLE 8 ROI Analysis

	Per Organization	Per Security Team Member
Benefit (discounted)	$1.92 million	$94,639
Investment (discounted)	$0.50 million	$24,656
Net present value (NPV)	$1.42 million	$69,983
Return on investment (ROI)	284%	284%
Payback period	4 months	4 months
Discount rate	12%	12%

Source: IDC, 2018

CHALLENGES AND OPPORTUNITIES

One of the challenges of utilizing threat intelligence is learning what it is and how to use it. End users typically want to receive threat intelligence data but don't know how to create valuable insight from the data. For the end user, receiving raw data feeds from multiple sources does not make the data valuable to use. The end user needs to know what the data means to the company and if it is something to worry about. The importance of the threat feeds and other threat data is not only the collection of indicators of compromise but also the actionable content that can help companies make decisions about their security posture and events detected within the organization.

In the TISS market, a number of vendors provide only feeds, but the feeds lack essential details such as historical information, threat trends, and context around the initial indicators being evaluated. Organizations today still struggle with what to do with the intelligence they receive and how to go about making decisions with the information they have.

Recorded Future is one provider that has turned those challenges into opportunities to penetrate the TISS market. Its solution includes an aggregation of dozens of threat feeds with surface, deep, and dark web data along with expert analysis to provide relevant threat intelligence in real time. Its new platform, Fusion, integrates other third-party feeds and customer proprietary data, which makes the solution a one-stop shop for enterprises. The combination of rich external threat intelligence and internal data to help companies make informed decisions around their security has become a game changer in the TISS market.

SUMMARY AND CONCLUSION

Overall, organizations today struggle with gathering vast quantities of data and making sense of what the data means and whether it's a true threat. To decipher a security incident takes time and expertise, which is where Recorded Future comes into play. Based on the customer data collected during the interview process, Recorded Future's threat intelligence customers can expect higher staff productivity and efficiency across the entire IT security team. The solution also allows IT teams to have wider visibility into security threats that are occurring and assists teams in making strategic decisions around the latest threats. Recorded Future's ability to provide a universal threat intelligence platform to organizations differentiates the company's offering from those of other vendors by aggregating the data, analyzing the data in real time, and giving customers the real intelligence needed to make an actionable decision. As a result, the organizations that participated in this study were achieving impressive financial results of 284% on their investment over three years.

APPENDIX

Methodology

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from current users of Recorded Future as the foundation for the model. Based on interviews with organizations using Recorded Future, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of Recorded Future.** In this study, the benefits included staff time savings and productivity benefits and operational cost reductions.
2. **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Recorded Future and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of Recorded Future reports over a three-year period. ROI is the ratio of the net present value (NPV) and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

Message From Sponsor

Interested in a better understanding of the Business Value of Threat Intelligence and how that effects your organization directly?

Visit the IDC ROI Threat Intelligence Assessment Tool Sponsored by Recorded Future to help transform your cybersecurity. By completing the tool you will receive a personalized report that focuses on an assessment of your current threat intelligence operations plus business outcome improvements you can expect with Recorded Future.

Link to Tool: https://threatintelligenceroi.com/

IDC Research, Inc.

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC
ANALYZE THE FUTURE