

BEST PRACTICE REPORT

How To Measure The Effectiveness And Value Of Threat Intelligence

December 10, 2024

By Brian Wrozek with Merritt Maxim, Kaylee Mahoney, Christine Turley

FORRESTER

Summary

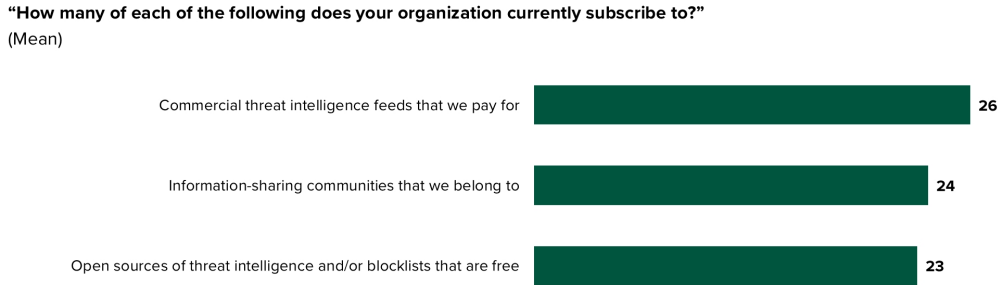
Security and risk (S&R) pros frequently struggle to measure the value and effectiveness of threat intelligence, resulting in wasted or misallocated resources. This report highlights the most common and beneficial quantitative and qualitative metrics you can use to demonstrate the value and effectiveness of threat intelligence to your organization.

Threat Intelligence Metrics Need A Revamp

Organizations are consuming more threat intelligence to counter the rising volume and sophistication of threats. In [Forrester's Security Survey, 2024](#), organizations subscribe to 26 paid commercial threat feeds on average (see Figure 1). Despite this conscientiousness, identifying and reporting on appropriate metrics to measure its value and effectiveness is challenging. According to a group of external threat intelligence service providers (ETISP) surveyed in Forrester's Q1 2024 Measuring The Value And Effectiveness Of Threat Intelligence Survey, less than half of their customers had excellent or good threat intelligence metric programs; this was determined by the number and type of measurements in place plus the maturity level of their overall threat intelligence program (see Figure 2). Measuring the value and effectiveness of threat intelligence is challenging because:

- **Too many variables cloud attribution.** It's difficult to attribute threat intelligence directly to a positive outcome when many other factors are intertwined. A decrease in incident response time could be due to insights gained from the tactics, techniques, and procedures (TTP) of threat actors documented in threat intelligence reports or to a more robust response plan, better experienced incident responders, insights from new event log sources, or even less-skilled threat actors. Threat intelligence plays a role, but it's difficult to isolate and quantify how much it contributes to the outcome.
- **Threat intelligence is poorly integrated into existing security tools and processes.** Organizations struggle to capitalize on useful threat intelligence due to the lack of interoperability between indicators of compromise (IOC) data feeds and lack of automation across security tools such as network and endpoint protection technologies. Threat intelligence must be quickly and efficiently transformed into the right format consistent with the security technology syntax, often requiring human involvement which impedes adoption and complicates accurate metric computations.
- **Competing metrics complicate results.** Some metrics are naturally antagonistic, forcing organizations to balance quality against quantity and accuracy versus richness. Fine-tuning requirements to reduce false positives will minimize analyst churn but may also result in an increase of false negatives when potential threats are missed — leading to higher risks to the organization.

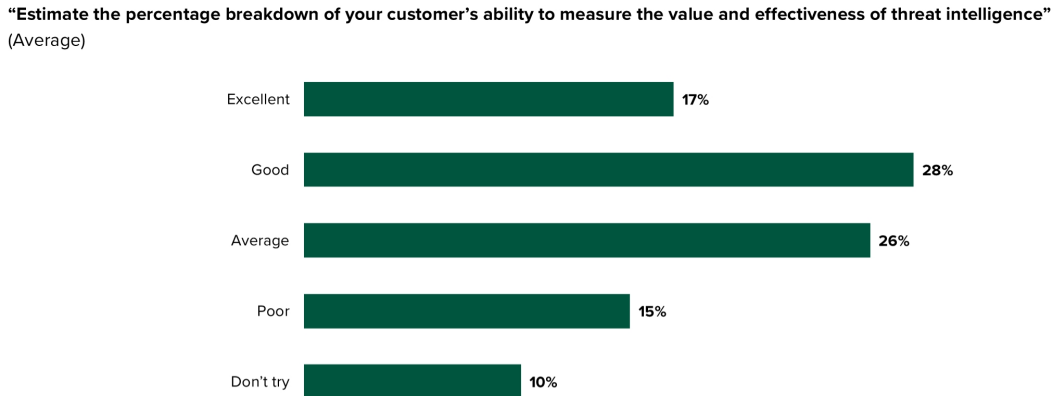
Figure 1
Organizations Subscribe To Multiple Threat Intelligence Feeds



Base: 464 security decision-makers who are a major influencer or final decision-maker in threat intelligence for their organization
Source: Forrester's Security Survey, 2024

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Figure 2
Less Than Half Of ETISP Customers Have Above Average Metric Programs



Note: This data is indicative and may only be used directionally. Percentages have been rounded.
Base: 23 external threat intelligence service providers
Source: Forrester's Q1 2024 Measuring The Value And Effectiveness Of Threat Intelligence Survey

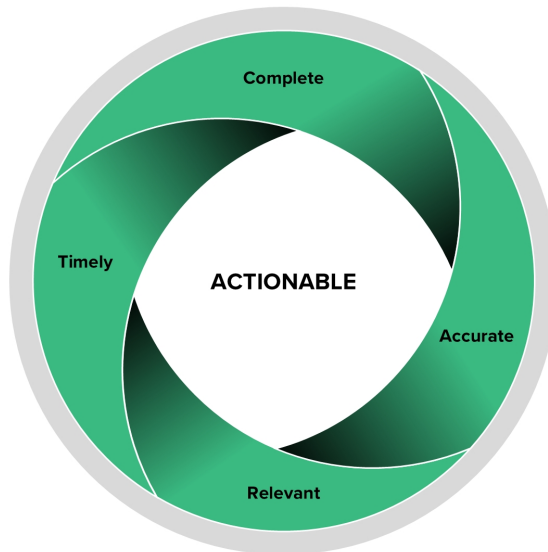
© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Focus On Quantitative Metrics To Measure Effectiveness

Credible threat intelligence must be complete, accurate, relevant, and timely (CART) for you to act on it (see Figure 3). Even then, you need to apply it correctly to improve decision-making and operational efficiency. Metrics are essential for you to demonstrate the effectiveness of threat intelligence, but resist the temptation to rely solely on consumption-based metrics such as the number of IOCs delivered and threat reports read. Forrester asked threat intelligence providers to rank various metrics (see Figure 4). The results show that more does not necessarily mean better. The right target value for a given metric is unique to each organization’s cybersecurity maturity and risk profile. You can measure how effective threat intelligence is in achieving the desired results by using the metrics from each of the CART categories.

Figure 3

Credible Threat Intelligence Must Be Complete, Accurate, Relevant, And Timely (CART)



© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Completeness

Threat intelligence is complete when it has progressed through the threat intelligence lifecycle and provides tangible benefits to the organization. The threat intelligence lifecycle is a cyclical process composed of six stages: requirements, collection,

How To Measure The Effectiveness And Value Of Threat Intelligence

Forrester Report Copy Prepared Exclusively For Zuzana Legathova With Eset, spol s r.o. Distribution and reproduction are prohibited. For more information, see the [Terms Of Use Policy](#) and [Ways To Share Research](#).

processing, analysis, dissemination, and feedback. Completeness provides greater assurance that potential threats are properly identified and that relevant contextual information is considered during decision-making. The desire for completeness drives organizations to leverage multiple threat intelligence solutions. You can't measure an unknown, but you can use the following metrics to gauge the level of completeness of your threat intelligence:

- **Requirements met.** Tactical, operational, and strategic use cases are effective when they meet the stated objectives of the threat intelligence program and produce the desired outcomes. An effective threat intelligence program must track the performance of threat intelligence against the original use case requirements. Refine your threat intelligence requirements as your needs and risk appetite change. Pay close attention to ETISP roadmaps to ensure they are anticipating and responding to the dynamic threat landscape.
- **Number of sources.** This includes both the breadth and depth of threat intelligence sources from public open-source channels, dark web forums, malware samples, lessons learned from incident response engagements, honeypots, system logs, network telemetry, and collaboration with trusted partners and industry groups. A rich variety of unique sources provides different perspectives and enables stronger contextual relationships between objects and a more thorough understanding of the threat landscape.
- **Number of objects.** A large data lake of IOCs and artifacts provides a centralized repository of diverse threat intelligence data from multiple sources. This provides the foundation for thorough analysis leading to detailed profiles, complex pattern associations, and stronger relationships between objects, driving higher levels of confidence in threat intelligence accuracy. It enables historical trending and the ability to scale as data volumes grow.

Accuracy

Accuracy is a critical measure of the quality and correctness of threat intelligence information, ensuring that the IOCs, reports, and alerts are reliable and pertinent to the threats faced by an organization. Accuracy is closely related to completeness and relevancy. The most common accuracy metrics are the number of false positives and negatives encountered.

- **False positives.** False positives are known as a Type 1 error, and they are more than just an annoyance. They distract your team from working on valid threats and necessary tasks. Spending limited time and resources on non-value-added tasks

How To Measure The Effectiveness And Value Of Threat Intelligence

Forrester Report Copy Prepared Exclusively For Zuzana Legathova With Eset, spol s r.o. Distribution and reproduction are prohibited. For more information, see the [Terms Of Use Policy](#) and [Ways To Share Research](#).

contributes to alert fatigue and employee burnout. False positives can lead to business disruption as necessary tasks go uncompleted. Eliminating all false positives is difficult, and an acceptable number depends on your risk tolerance and capacity to process all the inputs. If the number is trending up, make adjustments to reduce the volume to a level that meets the organization's risk appetite and resource capacity. One way to do this is to narrow the scope of sources and refine the analysis process by strengthening the associations and increasing the number of contextual relationships between threat artifacts before acting.

- **False negatives.** False negatives are known as a Type 2 error, and not surprisingly, they're the opposite of false positives. False negatives give you a false sense of security by leaving companies exposed, putting them at greater risk of compromise. Eliminating all false negatives isn't possible, but if your existing threat intelligence isn't keeping pace with the volume and sophistication of the threat actors targeting your organization then you should look for alternative providers and consider leveraging multiple threat intelligence feeds.

Relevancy

Relevant threat intelligence focuses on an organization's specific industry, region, environment, and potential threat landscape. Relevance ensures that the provided threat intelligence is directly applicable to the organization's needs, enhancing the effectiveness of their security posture. Relevancy metrics include:

- **Events and incidents detected and prevented.** Threat intelligence will improve the performance of your security controls. You can achieve this by tracking metrics like how many attacks are successful and how many are being prevented and detected. For example, track the number of malicious URLs blocked or the number of phishing emails quarantined versus the number delivered to employee inboxes.
- **Compromised assets discovered.** A common [threat intelligence use case](#) is to have ETISPs send alerts to organizations when they find evidence of compromised accounts in a repository on the dark web. Organizations should also track the number of accounts that need password resets. Industry benchmarks can be used to calculate the potential costs if those compromised accounts led to a breach of PII.
- **Rogue domains, social media profiles, or mobile applications taken down.** These are common service offerings provided by ETISPs and are easy to track. They're visible, tangible actions that demonstrate intent to protect the company, brand, employees, and customers. Besides just tracking raw totals, measure

success percentages to track effectiveness over time. If you're evaluating threat intelligence providers, compare their takedown SLAs and performance records to find the one right for you.

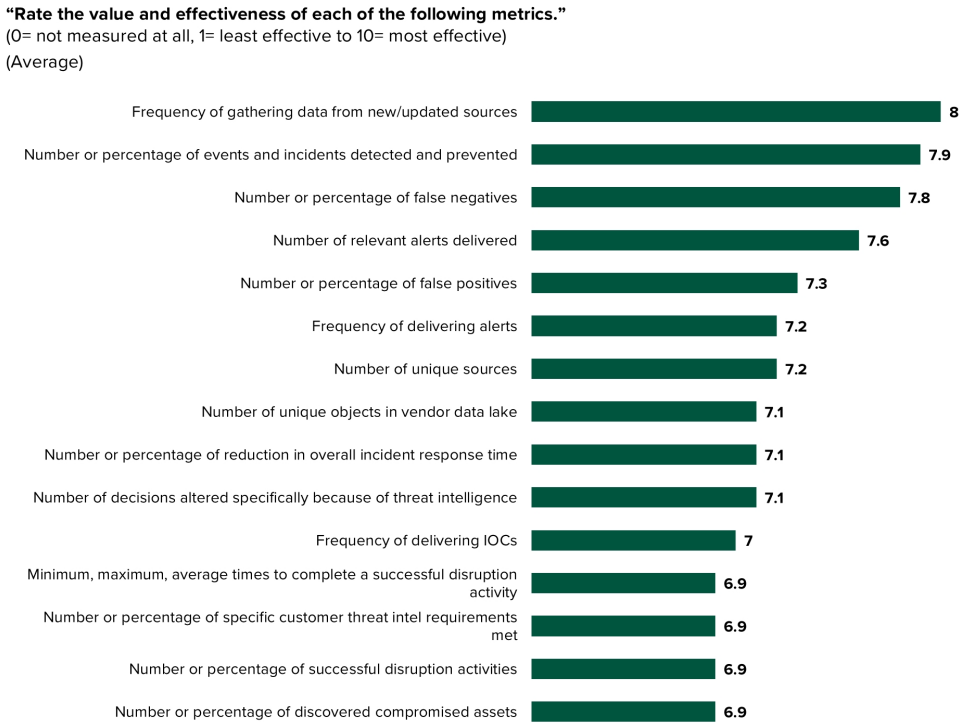
- **Decisions altered.** This is a broad category that encompasses a range of use cases and scenarios. Don't take a haphazard approach; tailor a few metrics to what is most important and relevant to your security program and be willing to adjust in the future as emphasis changes. For example, if you are improving your vulnerability management program, track how the contextual risk score from ETISPs changes the priority of patch distributions relative to the raw CVSS value.

Timeliness

The speed at which threat intelligence is provided is critical. When proactively preventing or detecting threats, timeliness ensures that organizations can respond to threats quickly to mitigate potential damage or exposure. It also ensures that existing threat intelligence is not becoming stale. Measure the time-related impact of threat intelligence for the following activities:

- **Frequency of gathering data from new and existing sources.** Threat actors quickly change their attack infrastructure, and new social media channels arise to evade detection. ETISPs must routinely update their search criteria and hunt for new sources of threat intelligence to keep their data inventory current.
- **Frequency of delivering relevant IOCs and alerts.** Gathering new threat intelligence is not enough. ETISPs must constantly refresh their data analysis or risk missing new, vital contextual relationships by processing outdated information. The quicker this new threat intelligence is delivered to the customers the better they can update their defenses against new threats to minimize the impact of attacks.
- **Time to complete disruption services.** Go beyond tracking the sheer number of disruption events and monitor the time to successfully complete them. ETISPs should be able to disclose the minimum, maximum, and average time to successfully take down a rogue domain and remove a fake social media profile.
- **Reduction in incident response time.** Be diligent in tracking the amount of time spent in each phase of the [incident response lifecycle](#). Threat intelligence provides early warning of attacks and insights into the TTPs of threat actors and malware campaigns. This intel points responders in the right direction quickly. By reducing the time spent responding to incidents and investigations, personnel are more effective and efficient, and the impact of incidents is reduced.

Figure 4
ETISPs Show That Threat Intelligence Metrics Vary In Success



Note: This data is indicative and may only be used directionally. Not all response options shown.

Base: 23 external threat intelligence service providers

Source: Forrester's Q1 2024 Measuring The Value And Effectiveness Of Threat Intelligence Survey

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Rely On Qualitative Criteria To Demonstrate Value

Determining the return on investment for threat intelligence can be difficult. How much revenue is gained or how much expense is avoided by taking down a rogue domain? Our gut tells us this is beneficial, but estimating the monetary value is dubious. Don't waste energy on trying to use metrics to provide a dollar value for the threat intelligence program. Be wary of complex cyber threat exposure calculations. Instead, focus on articulating how and why you use threat intelligence. Let the narrative guide your audience in connecting the dots between the threat intelligence, use case, and respective value. Use these qualitative techniques to demonstrate the value of threat intelligence:

How To Measure The Effectiveness And Value Of Threat Intelligence

Forrester Report Copy Prepared Exclusively For Zuzana Legathova With Eset, spol s r.o. Distribution and reproduction are prohibited. For more information, see the [Terms Of Use Policy](#) and [Ways To Share Research](#).

- **Craft anecdotes and reference threat intelligence sources.** Whenever possible, link threat intelligence to the decision as part of the justification. If you are trying to secure funding for a ransomware tabletop exercise consulting engagement, show ransomware statistics from reputable annual threat reports. Go a step further by weaving a story of a known threat actor who routinely uses ransomware malware common to your industry. Map the TTPs to the MITRE ATT&CK framework illustrating how a threat actor could compromise your environment because of gaps in your controls. Illustrate how threat intelligence helps make better decisions.
- **Take stakeholder satisfaction surveys.** Security teams are not the only group that benefits from threat intelligence. IT, business leaders, marketing, and physical security departments benefit from threat intelligence. Obtain feedback from these stakeholders regarding the usefulness of threat intelligence. Are their requirements and expectations being met? Is the physical security team more confident in protecting the CEO on business trips thanks to the travel protection intelligence regarding pending weather conditions, local crime statistics, and the nature of threats on social media? ETISPs should routinely ask you for feedback on their threat intelligence feeds, performance, and recommendations for improvement.
- **Don't strive for perfection.** A common saying is that “perfection is the enemy of good.” An exact valuation of threat intelligence is hampered because other factors come into play and not everything is completely under your control. Hardware and software fail. People make mistakes. Threat actors change their approach. You can't prove a negative. If there's no threat intelligence about an impending attack, is it because no attack is imminent, or was it just not found? Value is fluid. Threat intelligence that was good enough last year may not be good enough today. Despite these challenges, you should use metrics to monitor your threat intelligence program rather than just accepting that it's a necessary component of your security program.

Supplemental Material

Survey Methodology

Forrester fielded the Q1 2024 Measuring The Value And Effectiveness Of Threat Intelligence Survey from March to June 2024. The survey used a convenience sample of a self-selected group of respondents knowledgeable of threat intelligence and is therefore not random. This data is not guaranteed to be representative of the population, and, unless otherwise noted, statistical data is intended to be used for

How To Measure The Effectiveness And Value Of Threat Intelligence

Forrester Report Copy Prepared Exclusively For Zuzana Legathova With Eset, spol s r.o. Distribution and reproduction are prohibited. For more information, see the [Terms Of Use Policy](#) and [Ways To Share Research](#).

descriptive and not inferential purposes. While nonrandom, the survey is still a valuable tool for understanding where users are today and where the industry is headed.

Companies We Interviewed for This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

AlertMedia

Blackbird.AI

Censys

CrowdStrike

CTM360

Cyble

Doppel

ESET

Flare.io

Flashpoint

Fortinet

Intel 471

Intrinsec

Lumen

NSFOCUS

OpenText

QAX

ReliaQuest

Team Cymru

Tencent Cloud

Viattel Cyber Security

How To Measure The Effectiveness And Value Of Threat Intelligence

Forrester Report Copy Prepared Exclusively For Zuzana Legathova With Eset, spol s r.o. Distribution and reproduction are prohibited.
For more information, see the [Terms Of Use Policy](#) and [Ways To Share Research](#).

ZeroFox



We help business and technology leaders use customer obsession to accelerate growth.

FORRESTER.COM

Obsessed With Customer Obsession

At Forrester, customer obsession is at the core of everything we do. We're on your side and by your side to help you become more customer obsessed.

Research

Accelerate your impact on the market with a proven path to growth.

- Customer and market dynamics
- Curated tools and frameworks
- Objective advice
- Hands-on guidance

[Learn more.](#)

Consulting

Implement modern strategies that align and empower teams.

- In-depth strategic projects
- Webinars, speeches, and workshops
- Custom content

[Learn more.](#)

Events

Develop fresh perspectives, draw inspiration from leaders, and network with peers.

- Thought leadership, frameworks, and models
- One-on-ones with peers and analysts
- In-person and virtual experiences

[Learn more.](#)

Contact Us

Contact Forrester at www.forrester.com/contactus. For information on hard-copy or electronic reprints, please contact your Account Team or reprints@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
Tel: +1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com