

Threat Intelligence Benchmark: Stop Reacting; Start Anticipating

Harness AI And Expert Insights To Transform Threat Intelligence
From Overwhelming To Actionable

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY GOOGLE CLOUD, JULY 2025



Table Of Contents

3	<u>Executive Summary</u>
4	<u>Key Findings</u>
5	<u>Growing Threat And Data Volumes As Well As Skills Shortages Leave Organizations Vulnerable</u>
10	<u>Organizations Struggle To Operationalize Threat Intelligence</u>
13	<u>Overcoming Intelligence Overload: The Importance Of Actionable Insights</u>
15	<u>The Role Of AI And External CTI Experts In Operationalizing Threat Intelligence</u>
18	<u>Key Recommendations</u>
20	<u>Appendix</u>

Project Team:

Mandy Polacek,
Principal Market Impact Consultant

Contributing Research:

Forrester's [Security & Risk](#) research group

ABOUT FORRESTER CONSULTING

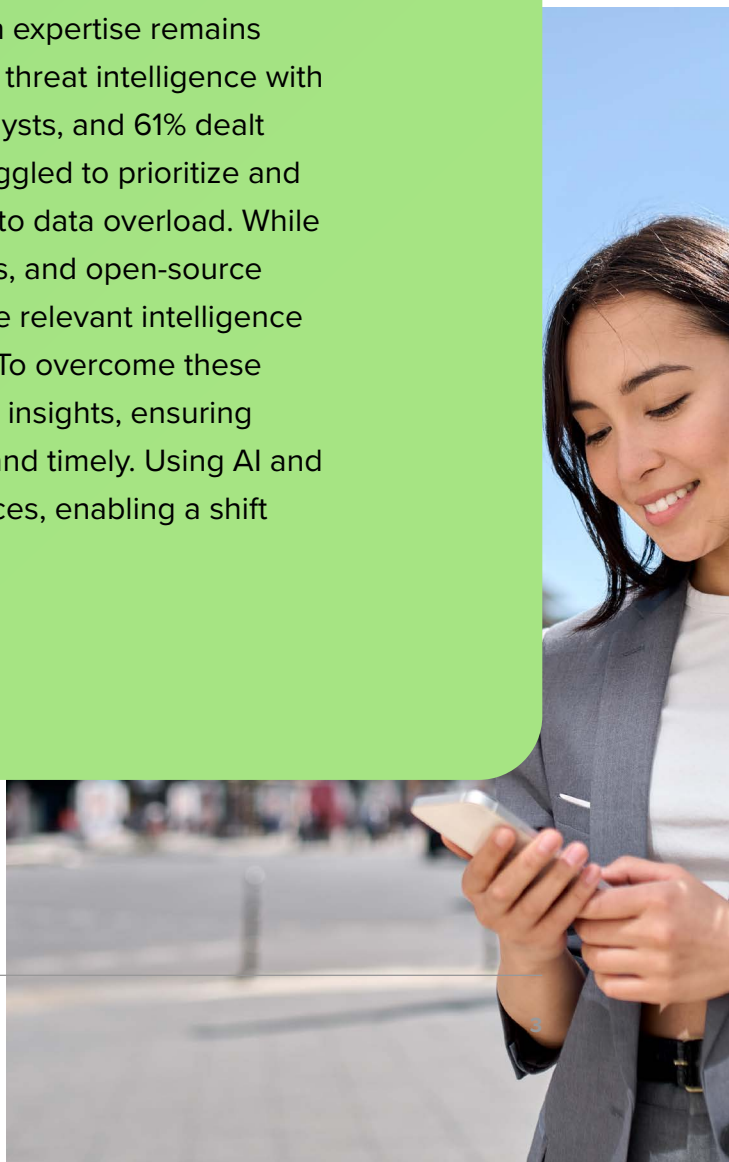
Forrester provides independent and objective [research-based consulting](#) to help leaders deliver key outcomes. Fueled by our [customer-obsessed research](#), Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. [E-62162]

Executive Summary

As cyberattacks grow in frequency and sophistication, organizations struggle to keep up due to challenges like increasing, siloed threat intelligence feeds. Rather than aiding efficiency, myriad feeds inundate security teams with data, making it hard to extract useful insights or prioritize and respond to threats. Security teams need visibility into relevant threats, AI-powered correlation at scale, and skilled defenders to use actionable insights, enabling a shift from a reactive to a proactive security posture.

In January 2025, Google Cloud commissioned Forrester Consulting to evaluate the state of cyberthreat intelligence (CTI) practices and strategies. Forrester conducted a double-blind online survey with 1,541 director+ IT and cybersecurity leaders at global enterprises across 12 industries to explore this topic. The survey found that organizations are increasingly vulnerable due to the vast amount of threats and data and a shortage of skilled threat analysts. Despite the use of AI, human expertise remains essential to help security teams interpret and apply threat intelligence with confidence: 60% of respondents lacked skilled analysts, and 61% dealt with too many threat intelligence feeds. Teams struggled to prioritize and respond to threats, often missing critical alerts due to data overload. While many relied on information sharing, analysis centers, and open-source threat intelligence, they found it difficult to parse the relevant intelligence and fully utilize it to improve their security posture. To overcome these challenges, organizations must prioritize actionable insights, ensuring threat intelligence is complete, accurate, relevant, and timely. Using AI and external CTI experts can help boost internal resources, enabling a shift from reactive to proactive security measures.



Key Findings

Data overload and skills gaps leave analysts drowning in information and organizations at risk. A shortage of skilled threat analysts plus an overwhelming volume of threat data leave organizations vulnerable. While 61% of respondents said their teams are overwhelmed by too many threat intelligence feeds, 60% said they lack skilled analysts — leading to gaps in security.

Organizations struggle to operationalize threat intelligence. Respondents said their organizations rely on many threat intelligence sources, but most find it challenging to fully use this information to improve their security posture. Many also found it hard to turn raw data from feeds into a decision support system. In turn, they fail to contextualize the intelligence for their environment, operationalize it, and use it to shape strategy.

Organizations are stuck in a reactive state. Due to the shortage of analysts and data overload, 72% of respondents said they can only react to cyberthreats; they struggle to prioritize threats and respond quickly and effectively.

Becoming proactive will require actionable insights, supercharged by AI and embedded skilled analysts (as needed). To overcome these key challenges, organizations need actionable threat intelligence that is complete, accurate, relevant, and timely. They must lay the right foundation with threat intelligence tied to business risk — and then use AI and embed skilled analysts from trusted partners to help support and enhance their internal teams.



Growing Threat And Data Volumes As Well As Skills Shortages Leave Organizations Vulnerable

Organizations today face a shortage of personnel who can effectively interpret and act on threat intelligence. While AI is helping uplevel defenders, organizations struggle to use it consistently. At the same time, analysts are drowning in too many threat intelligence data feeds. If not managed appropriately, the growing volume of threats and data will exacerbate the skills shortage, widening the gap between organizations' capacity to act and the complexity of the threat landscape.¹ In this study, we found that:

- **Too few analysts are working with too many data feeds.** Sixty percent of respondents reported that the lack of skilled threat analysts prevents them from improving their threat intelligence capabilities, and 61% said their teams deal with too many threat intelligence feeds (see Figure 1). The combination of a shortage of threat analysts and an overwhelming volume of data and threat intelligence feeds can significantly hinder an organization's ability to prioritize and respond to threats effectively.

FIGURE 1

Data And Analytical Challenges In Improving Threat Intelligence Capabilities



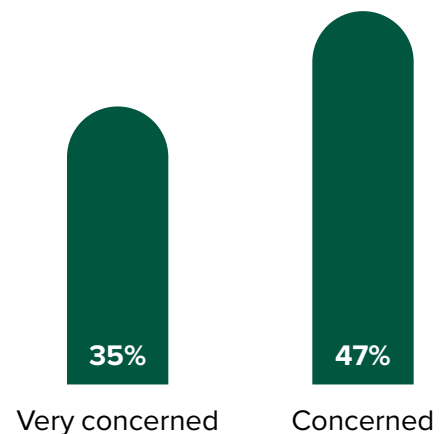
Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

- **Organizations are turning to AI to ease the burden.** Eighty-six percent of respondents agreed that their organization must use AI to improve its ability to operationalize threat intelligence. Respondents expected AI to benefit their organizations in many ways, with use cases varying widely by region and industry.

- **Mounting issues leave organizations in a reactive and vulnerable state.** Eighty-two percent of respondents were concerned their organizations are missing real threats due to the alert and data volumes they face (see Figure 2). Respondents in APAC were the most concerned; they also used the highest number of threat intelligence sources (see Figure 11 in Appendix E). When analysts are inundated with vast amounts of data and alerts from various sources, they can struggle to prioritize and respond to potential threats effectively. Individual alerts might have preconfigured priority ratings, flagging some as critical — but multiple lower-priority alerts, when considered together, may indicate a significant attack. When they gather intelligence, 59% of respondents said it's difficult to act on that data and 66% struggle to share it with relevant teams (see Figures 1 and 3). Validating and prioritizing threats and communicating relevant information can be time-consuming, leaving organizations in a reactive state with little bandwidth or ability to keep an eye on emerging threats or address critical threats in a timely manner. When paired with a lack of sufficient automation, this problem only gets worse: 72% of respondents say their organizations are mostly reactive when it comes to cybersecurity threats.

FIGURE 2

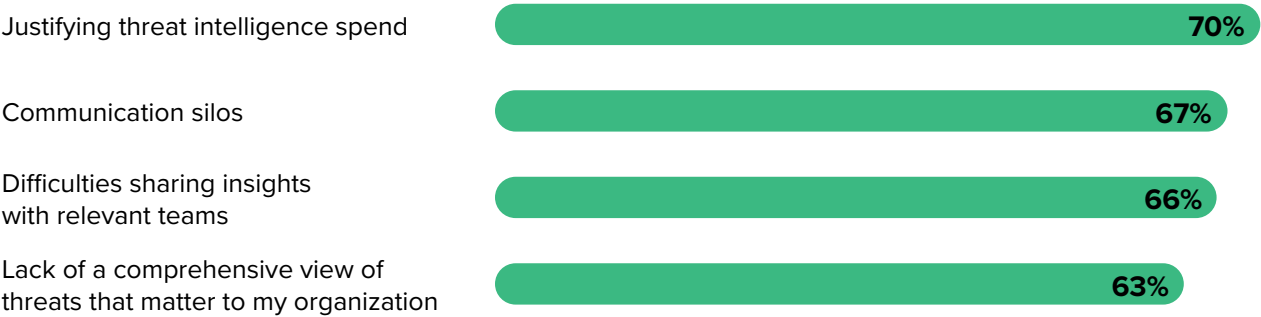
“What level of concern do you have that your organization might be missing real threats/incidents due to the amount of alerts and data you are faced with?”



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 3

Organizational And Communication Challenges In Improving Threat Intelligence Capabilities



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

- **By industry, manufacturing respondents were most concerned, with 89% worried that they’re missing real threats due to alert and data volume.** Most threat intelligence is built for IT environments, but manufacturers have a lot of operational technology, such as PLCs and SCADA systems, so they need highly tailored intelligence. Dealing with such tech can be tricky, and attack detection could be missed due to the nature of their environments. And not all outsourcers understand the sheer diversity of operational technology out there or how to analyze it and respond accordingly (see Figure 12 in Appendix E).
- **Executives must urgently prioritize a proactive approach to security as attacks grow in size and complexity.** Eighty percent of respondents say their senior leadership team underestimates their organization’s cyberthreats (see Figure 4). The speed of attacks and the complexity of the threat landscape continue to increase. Respondents were most concerned about phishing and ransomware attacks, and these types of attacks are only growing in volume. Roughly a third of respondents cited newer or future types of attacks like AI prompt injections and quantum computing breaking encryption as top concerns for their organizations in the next 12 months (see Figure 5).

By industry, technology/technology services felt the most strongly that their leadership underestimates their organization’s cyberthreats, with 84% agreeing. This could be due to leaders prioritizing innovation and speed to market over security and/or this industry being less regulated than others, such as financial services and healthcare (see Figure 13 in Appendix E).

FIGURE 4

“Please rate your level of agreement with the following statements.”

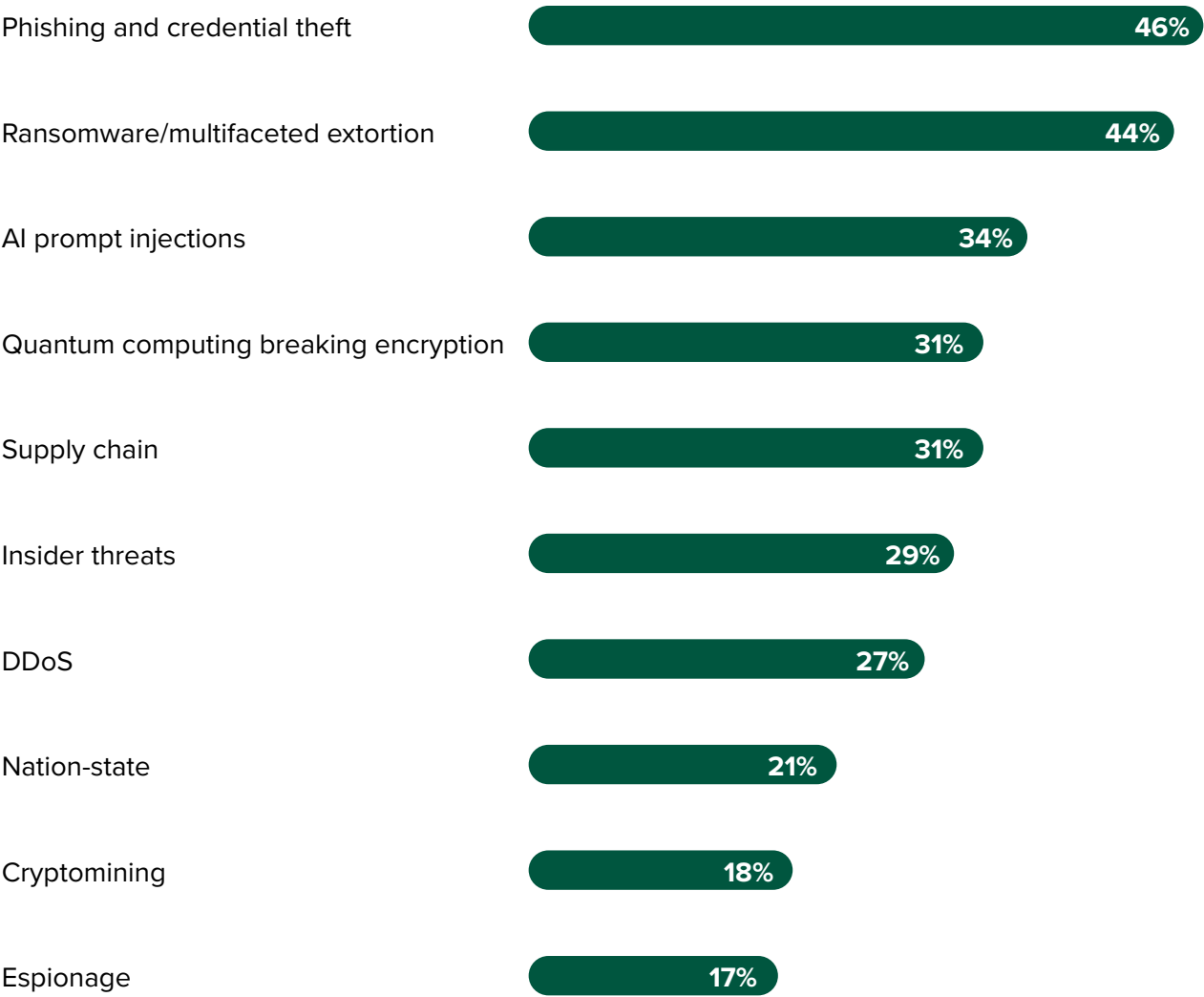
(Responses of agree/strongly agree)



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 5

**Attacks/Threats That Respondents Are Most Concerned About
In The Next 12 Months**



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

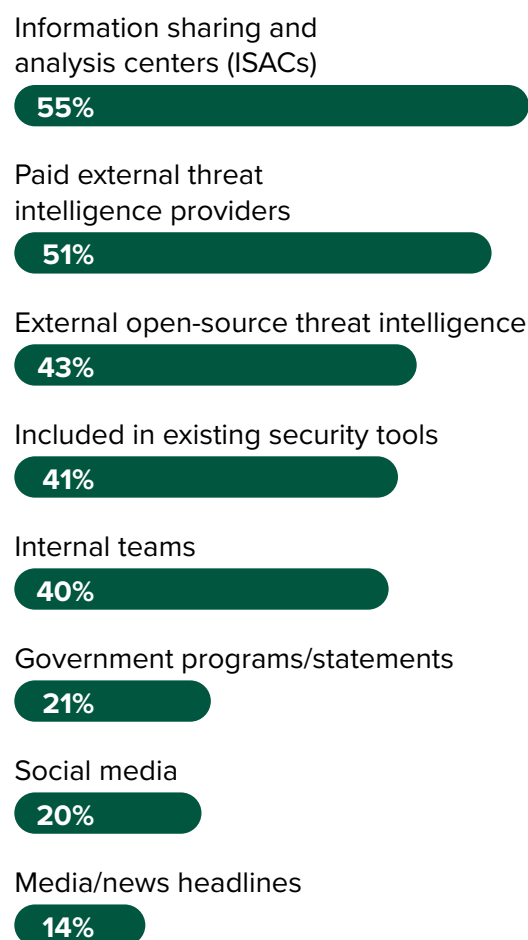
Organizations Struggle To Operationalize Threat Intelligence

Organizations rely on many information sources to stay abreast of vulnerabilities and emerging threats: Respondents cited information sharing and analysis centers (ISACs) and paid external threat intelligence solution providers as the most valuable. Yet most organizations find it difficult to turn available information into actionable outcomes. In this study, we found that:

- **Organizations gather threat intelligence from a variety of sources but value curated insights from paid threat intelligence providers and ISACs the most.** Respondents, and especially those in APAC, rely on many sources for cyber intelligence, including ISACs, paid and open-source threat intelligence solutions, social and traditional media, and information sharing among internal teams. When asked which sources were most valuable, respondents selected community-based ISACs and paid external threat intelligence providers (see Figure 6). These sources provide organizations with the most relevant insights — such as industry-specific intelligence, vulnerability intelligence, and current threat actor tactics, techniques, and procedures (TTPs) — all curated to an organization's unique threat profile.

FIGURE 6

Most Valuable Cyber Intelligence Sources



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Note: Respondents were first asked which cyber intelligence sources they use and then which of those sources are most valuable. Responses show the percentages ranking them as one of the top-three most valuable sources.
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

- **Most struggle to take full advantage of the information available to them.** Applied correctly, threat intelligence can produce tangible results and improve an organization's security program at the tactical, operational, and strategic levels. Respondents said they want to use threat intelligence to be more proactive; to improve their ability to prioritize and respond faster to threats; to educate their broader organization on relevant trends; and to keep improving their security strategies. But for most, these are future goals: They find it challenging to use threat intelligence in this way with the resources currently available (see Figure 7). North American respondents were slightly ahead in their use of threat intelligence: This is likely because this region experiences elevated threats, as it's an attractive target for adversaries; it also has a more mature cybersecurity market and stricter controls like the Cybersecurity Information Sharing Act and industry-specific regulations. That said, even in North America, most respondents said their organization struggles to fully leverage threat intelligence today (see Figure 14 in Appendix E).
- **Paid external threat intelligence tools and services can help organizations overcome operational hurdles.** While threat intelligence sources like ISACs are credible and beneficial in terms of sharing knowledge within the community and other free/reliable sources provide helpful insights, paid threat intelligence solutions help alleviate alert fatigue and minimize the risk of hunting with blinders on. These solutions provide insights tailored to an organization's unique threat profile, which minimizes the risk of dealing with inaccurate or incomplete information and its outcomes. They also provide actionable insights (and services, if needed) to improve efficiency and ease the resource burden many enterprises face today. The value and accuracy of the intelligence embedded in many of these solutions will also scale over time.

FIGURE 7

Threat Intelligence Adoption Across Use Cases

- We use threat intelligence in this way today
- We have plans to use threat intelligence in this way in the future
- We are interested but have no plans to use threat intelligence in this way
- We are not interested in using threat intelligence in this way

Putting preventive controls in place ahead of attacks/threats



Prioritizing the most critical vulnerabilities and addressing those first



Educating the organization on relevant trends and strengthen security posture as a whole



Knowing how to respond to an attack



Acting as the guiding light for security strategy



Hunting



Informing investment strategy



Understanding the threat profile in M&A/supply chain



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

Overcoming Intelligence Overload: The Importance Of Actionable Insights

To overcome their challenges, organizations must prioritize providing analysts and other stakeholders with actionable information, meaning it must be complete, accurate, relevant, and timely.² Respondents in this study agree: 82% said it is important or critical that they are able to act on the threat intelligence provided by external partners. Forrester recommends measuring how effective threat intelligence is in achieving desired outcomes by using metrics that measure:

- **Completeness.** Complete threat intelligence ensures potential threats are accurately identified and relevant contextual information is considered during decision-making. It involves using multiple sources and tracking performance against an organization's original requirements to refine its strategies. This thorough approach enables organizations to prioritize and respond to threats effectively, educate their teams, and continuously improve their security posture. In terms of complete intelligence, 82% of respondents said it's important that external partners provide a comprehensive view of the threat landscape; 80% said it's important that they leverage a rich variety of unique information sources.
- **Accuracy.** Accuracy is a critical measure of the quality and correctness of threat intelligence information, ensuring that indicators of compromise, attributions, reports, and alerts are reliable and pertinent to the threats faced by an organization. Accuracy is closely related to completeness and relevance. The most common metrics are the number of false positives and negatives encountered.
- **Relevance.** Relevant threat intelligence focuses on an organization's specific industry, region, environment, and potential threat landscape. It ensures that the threat intelligence provided applies directly to the organization's needs, enhancing the effectiveness of its security posture. The more relevant the threat intelligence is, the less time security

analysts waste and the more proactive they can be in setting their security posture. Eighty-one percent of respondents said it's important or critical that providers offer contextualized threat intelligence relevant to their organization. Relevancy metrics include events and incidents detected and prevented; compromised assets recovered; rogue domains, social media profiles, or mobile applications taken down; and decisions altered.

- **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 the potential damage or exposure. It also ensures that existing threat intelligence doesn't become stale. Eighty percent of respondents said it's important that providers continuously update information based on the latest attacker TTPs. Security and risk leaders can measure the timeliness of complete, accurate, and relevant information via the frequency with which data is gathered data from new and existing sources, the frequency with which relevant IOCs and alerts are delivered, the time to complete disruption services, and the reduction in incident response time.

The Role Of AI And External CTI Experts In Operationalizing Threat Intelligence

Equally important as having actionable information is the ability to apply it. Both AI and external analyst resources can elevate employees' capabilities, improve efficiency, and give individual contributors and leaders alike more time to focus on high-value work.

- **AI empowers organizations to understand, respond to, and mitigate threats quicker, but many are still navigating how to harness its full potential.** Security teams currently spend a lot of time identifying and prioritizing threats and communicating information to stakeholders across the organization. Respondents expected AI to improve their ability to summarize, contextualize, and prioritize threats and vulnerabilities as well as improve the efficiency and effectiveness of internal communications. This should free up resources and support their organization's shift to a more proactive security posture: 60% of respondents expected AI to give them more time to focus on higher-priority tasks, while 59% expected AI to improve decision-making (see Figure 8). Organizations are likely on a journey to adopt and apply AI most effectively, since (as previously stated) threat intelligence capabilities are on their roadmaps but not being used by many organizations today.
- **Top AI benefits vary by industry and region.** For example, while 75% of respondents in North America said improving the efficiency of generating easy-to-read summaries is most important, 71% in EMEA also said providing actionable recommendations and next steps to uplevel junior analysts is most important, and 73% in APAC said improving the capability to prioritize threats and vulnerabilities is most important (see Figures 15 and 16 in Appendix E).

FIGURE 8

“What benefits does or could AI in the use of threat intelligence bring to your organization?”

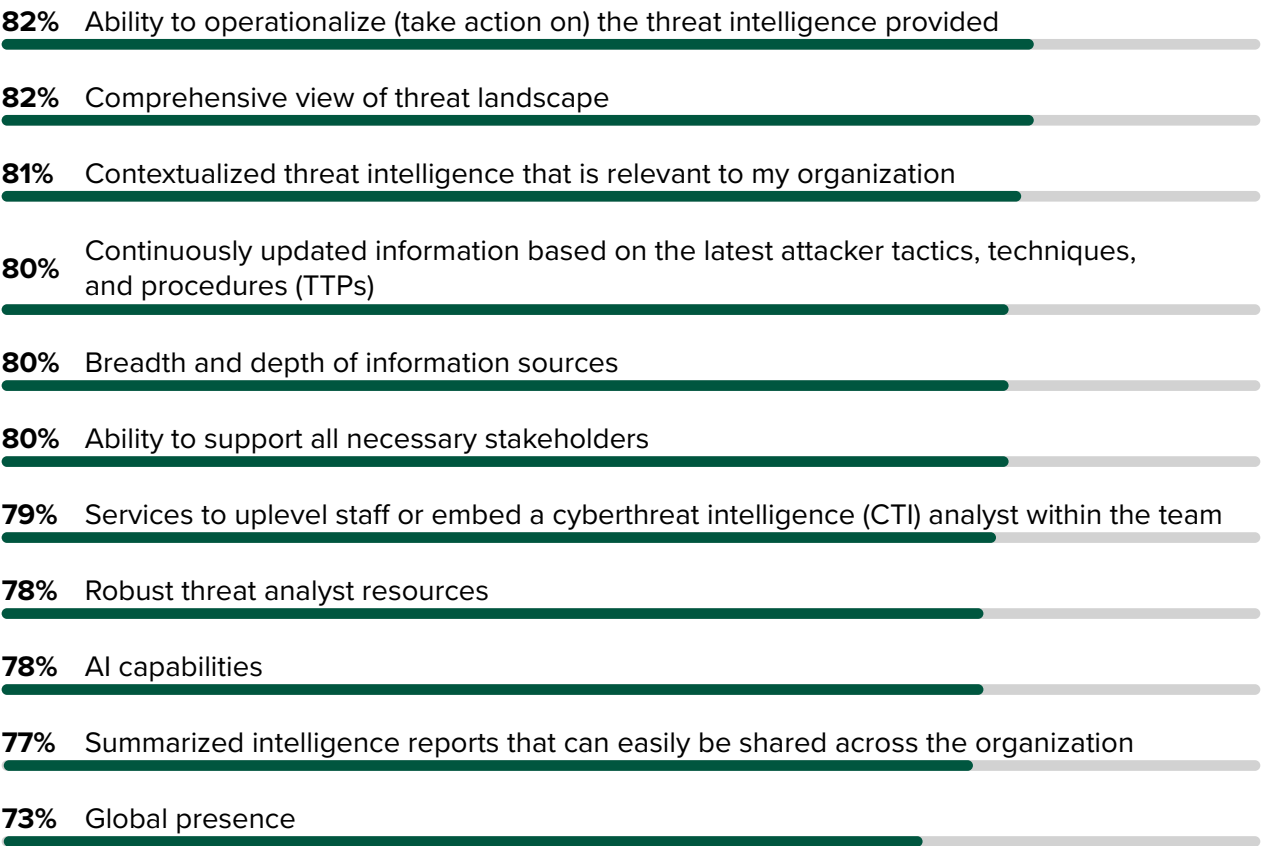


Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

- **External CTI experts help elevate internal teams, easing the strain on resources.** As skill shortages are a key challenge, it's no surprise that respondents turn to external providers to fill the gap: 79% said it's important that a provider offers services to help uplevel junior staff or embed a threat intelligence analyst into their team (see Figure 9). Transportation and logistics respondents were the most likely to cite this as a partner requirement, with 85% agreeing. This could be because respondents in this industry see fewer reasons to build up a robust internal security staff, believing that they can continue operating just fine with legacy tech. And many of these organizations have low margins and decentralized operations, which adds to the complexity. As a result, cybersecurity budgets can be low, making outsourcing appealing (see Figure 17 in Appendix E).

FIGURE 9

External Threat Intelligence Provider Requirements

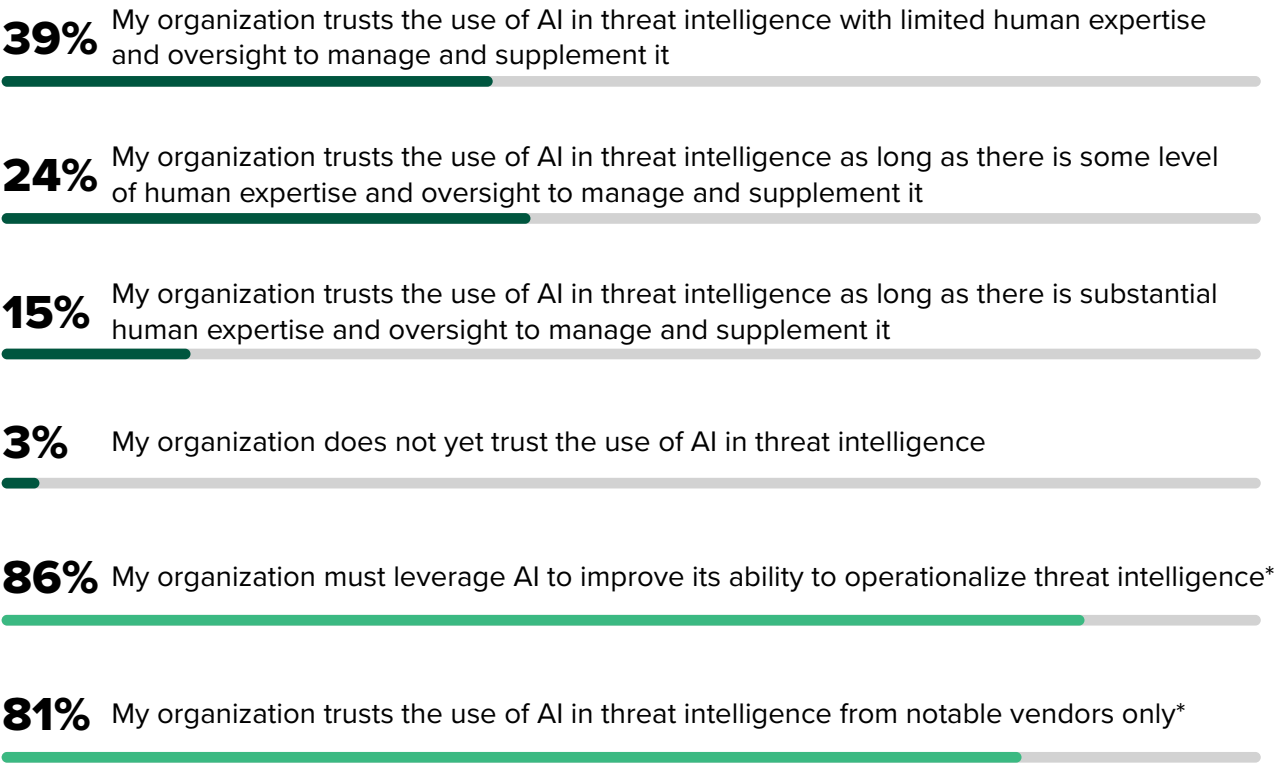


Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

- **Trust and AI go hand in hand.** Respondents are willing to trust AI for threat intelligence. They said that AI embedded in threat intelligence solutions could enhance their trust in a vendor’s ability to gather and analyze information. At the same time, most respondents said they want assurance that humans are managing and supplementing AI with their own expertise. Vendor trust is also really important: 81% of respondents said they trust the use of AI from notable vendors only (see Figure 10). In North America and EMEA, this could be due in part to having stricter AI and data privacy regulations. In APAC, regulatory frameworks are more fragmented, with some countries having stringent policies and others not: As a result, a lower 77% of APAC respondents said they trust the use of AI from notable vendors only (see Figure 18 in Appendix E).

FIGURE 10

Trust In AI For Threat Intelligence



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
*Note: Responses of 4 and 5 on a scale from 1 (Strongly disagree) to 5 (Strongly agree).
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

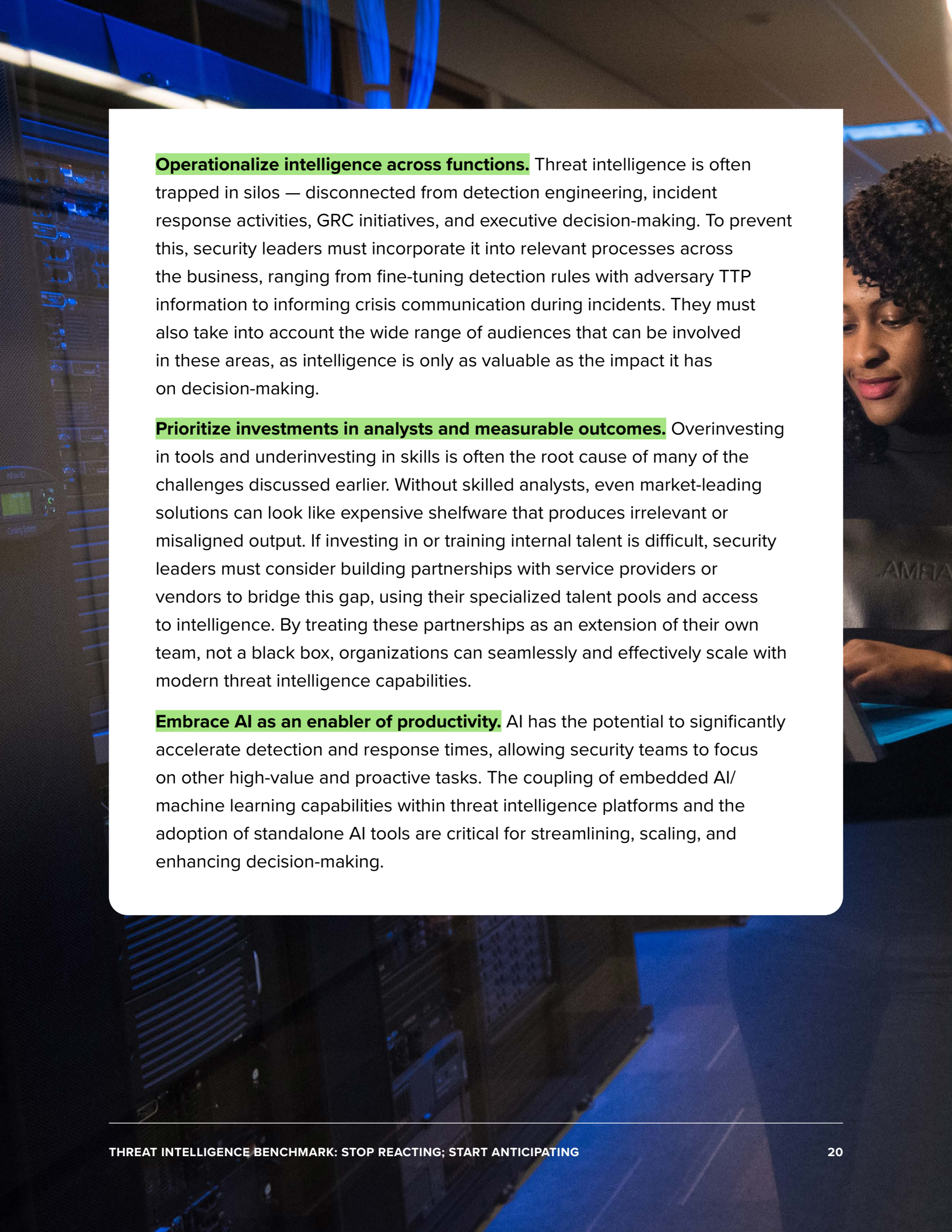
Key Recommendations

Despite significant investments in threat intelligence, it remains an underused capability in many organizations. While data is easily accessible from various sources, many organizations struggle to apply it in a way that enables strategic decision-making or a proactive security practice. Security and risk leaders might miss opportunities due to the misalignment of intelligence efforts with business objectives, a lack of clearly defined use cases, or ineffective process enhancements. To extract the true value of threat intelligence, organizations must reframe their approach by deeply embedding it into both security initiatives and enterprise risk strategies.

Forrester's in-depth survey of security and risk leaders about threat intelligence yielded several important recommendations:

Reframe threat intelligence as a capability, not a feed. Mistaking raw data for insights leads to an overwhelming number of indicators with little context or the ability to act on them. Security leaders can extract the true value of threat intelligence by treating it as a process, rather than a product; they must leverage skilled resources for activities like analysis, enrichment, contextualization, and alignment with real-world threats. They must follow structured intelligence lifecycle models to establish intelligence functions that produce tailored, relevant, and impactful outcomes.

Define intelligence requirements and use cases. Most organizations dive into adopting threat intelligence capabilities without laying out clear intelligence requirements for their business, leading to outcomes that fail to support decision-making. Security leaders must prioritize this effort in order to answer the “so what” of intelligence rather than “reporting the news.” This ensures that intelligence translates into decision-quality information that is complete, accurate, analyzed, timely, and predictive in the context of their business and its unique needs.



Operationalize intelligence across functions. Threat intelligence is often trapped in silos — disconnected from detection engineering, incident response activities, GRC initiatives, and executive decision-making. To prevent this, security leaders must incorporate it into relevant processes across the business, ranging from fine-tuning detection rules with adversary TTP information to informing crisis communication during incidents. They must also take into account the wide range of audiences that can be involved in these areas, as intelligence is only as valuable as the impact it has on decision-making.

Prioritize investments in analysts and measurable outcomes. Overinvesting in tools and underinvesting in skills is often the root cause of many of the challenges discussed earlier. Without skilled analysts, even market-leading solutions can look like expensive shelfware that produces irrelevant or misaligned output. If investing in or training internal talent is difficult, security leaders must consider building partnerships with service providers or vendors to bridge this gap, using their specialized talent pools and access to intelligence. By treating these partnerships as an extension of their own team, not a black box, organizations can seamlessly and effectively scale with modern threat intelligence capabilities.

Embrace AI as an enabler of productivity. AI has the potential to significantly accelerate detection and response times, allowing security teams to focus on other high-value and proactive tasks. The coupling of embedded AI/machine learning capabilities within threat intelligence platforms and the adoption of standalone AI tools are critical for streamlining, scaling, and enhancing decision-making.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 1,541 senior IT and cybersecurity leaders at organizations in North America, Europe, and Asia Pacific to evaluate the state of enterprise threat intelligence. Questions provided to the participants asked about top priorities, challenges, risks, and threats, and the approaches and resources being used to address them. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study began in January 2025 and was completed in February 2025. The survey was conducted in a double-blind fashion.

Appendix B: Demographics

COUNTRY	
US	24%
UK	17%
Singapore	13%
Canada	11%
Australia	11%
Japan	9%
Germany	9%
France	7%

INDUSTRY (TOP 10)	
Financial services and/or insurance	19%
Manufacturing and materials	16%
Technology and/or technology services	15%
Retail	11%
Healthcare	10%
Energy, utilities, and/or waste management	9%
Telecommunications services	5%
Transportation and logistics	4%
Consumer product goods	4%
Government	3%

COMPANY SIZE	
1,000 to 4,999 employees	51%
5,000 to 19,999 employees	34%
20,000 or more employees	16%

RESPONDENT LEVEL	
C-level executive	20%
Vice president	36%
Director	44%

DEPARTMENT	
Cybersecurity	41%
IT	59%

CYBERSECURITY THREAT INTELLIGENCE RESPONSIBILITY	
Final decision-maker	79%
Part of decision-making team	21%

Note: Percentages may not total 100 due to rounding.

Appendix C: Supplemental Material

ADDITIONAL RESOURCES

- [How To Measure The Effectiveness And Value Of Threat Intelligence](#), Forrester Research, Inc., December 10, 2024
- [The External Threat Intelligence Service Providers Landscape, Q1 2025](#), Forrester Research, Inc., January 9, 2025
- [How To Make Your Threat Intelligence Actionable](#), Forrester Research, Inc., September 18, 2023
- [The Top 10 Technologies For Operational Resilience](#), Forrester Research, Inc., February 4, 2025

Appendix D: Endnotes

- ¹ Source: [The External Threat Intelligence Service Providers Landscape, Q1 2025](#), Forrester Research, Inc., January 9, 2025.
- ² Source: [How To Measure The Effectiveness And Value Of Threat Intelligence](#), Forrester Research, Inc., December 10, 2024.

Appendix E: Regional And Industry Data

FIGURE 11

“What level of concern do you have that your organization might be missing real threats/incidents due to the amount of alerts and data you are faced with?”

● Very concerned
● Concerned



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 12

“What level of concern do you have that your organization might be missing real threats/incidents due to the amount of alerts and data you are faced with?”

(Showing “Concerned” and “Very concerned”)

Manufacturing and materials	89%
Transportation and logistics	85%
Technology and/or technology services	85%
Energy, utilities, and/or waste management	84%
Healthcare	80%
Financial services and/or insurance	80%
Telecommunication services	79%
Consumer product goods	77%
Retail	76%

Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 13

“My organization’s senior leadership underestimates the cyberthreat to the organization.”

(Showing “Agree” and “Strongly agree”)

Technology and/or technology services	84%
Transportation and logistics	83%
Energy, utilities, and/or waste management	82%
Manufacturing and materials	81%
Financial services and/or insurance	78%
Consumer product goods	78%
Healthcare	77%
Retail	77%
Telecommunication services	76%

Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 14

How Organizations Use Threat Intelligence Today



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 15

Top AI Benefits By Region

NORTH AMERICA	
Making threat intelligence more accessible to different stakeholders	69%
Improving the capability to prioritize threats and vulnerabilities	67%
Improving efficiency of generating easy-to-read summaries	75%
EMEA	
Improving the capability to prioritize threats and vulnerabilities	65%
Improving efficiency of generating easy-to-read summaries	71%
Providing actionable recommendations and next steps to uplevel junior analysts	71%
APAC	
Making threat intelligence more accessible to different stakeholders	70%
Improving the capability to prioritize threats and vulnerabilities	73%
Improving efficiency of generating easy-to-read summaries	63%

Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Note: Colors correlate to responses across categories.
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 16

Top AI Benefits By Industry

CONSUMER PRODUCT GOODS	
Making threat intelligence more accessible to different stakeholders	74%
Improving efficiency of generating easy-to-read summaries	69%
Providing actionable recommendations and next steps to uplevel junior analysts	74%
ENERGY, UTILITIES, AND/OR WASTE MANAGEMENT	
Improving the capability to prioritize threats and vulnerabilities	69%
Improving efficiency of generating easy-to-read summaries	74%
Providing actionable recommendations and next steps to uplevel junior analysts	67%
FINANCIAL SERVICES AND/OR INSURANCE	
Making threat intelligence more accessible to different stakeholders	69%
Improving the capability to prioritize threats and vulnerabilities	72%
Improving efficiency of generating easy-to-read summaries	68%

FIGURE 16 (CONT.)

Top AI Benefits By Industry

HEALTHCARE	
Making threat intelligence more accessible to different stakeholders	67%
Improving the capability to prioritize threats and vulnerabilities	73%
Improving efficiency of generating easy-to-read summaries	68%
MANUFACTURING AND MATERIALS	
Making threat intelligence more accessible to different stakeholders	67%
Improving the capability to prioritize threats and vulnerabilities	68%
Improving efficiency of generating easy-to-read summaries	74%
RETAIL	
Making threat intelligence more accessible to different stakeholders	71%
Improving the capability to prioritize threats and vulnerabilities	63%
Improving efficiency of generating easy-to-read summaries	64%
TECHNOLOGY AND/OR TECHNOLOGY SERVICES	
Making threat intelligence more accessible to different stakeholders	64%
Improving the capability to prioritize threats and vulnerabilities	64%
Improving efficiency of generating easy-to-read summaries	70%
Providing actionable recommendations and next steps to uplevel junior analysts	67%
TELECOMMUNICATIONS SERVICES	
Making threat intelligence more accessible to different stakeholders	62%
Improving decision-making with more complete, accurate, relevant, and timely information	62%
Improving the capability to prioritize threats and vulnerabilities	68%
TRANSPORTATION AND LOGISTICS	
Enabling the ability to focus on higher-priority tasks via time saved	70%
Improving the capability to prioritize threats and vulnerabilities	68%
Improving efficiency of generating easy-to-read summaries	70%

Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific

Note: Colors correlate to responses across categories.

Source: Forrester's 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 17

“How important are the following to your organization when engaging an external threat intelligence provider?”

(Showing “Important” and “Critical”)

Services to uplevel staff or embed a CTI analyst within my team	
Transportation and logistics	85%
Healthcare	82%
Technology and/or technology services	81%
Manufacturing and materials	81%
Retail	79%
Financial services and/or insurance	79%
Telecommunication services	76%
Consumer product goods	74%
Energy, utilities, and/or waste management	73%

Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

FIGURE 18

“My organization trusts the use of AI in threat intelligence from notable vendors only.”

(Showing “Agree” and “Strongly agree”)



Base: 1,541 senior IT and cybersecurity leaders at enterprise organizations in North America, Europe, and Asia Pacific
Source: Forrester’s 2025 State Of Threat Intelligence Survey [E-62162]

The background is a glowing green circuit board. In the center, there is a rectangular chip with a stylized 'F' logo. The word 'FORRESTER' is written in white capital letters across the chip. The entire image has a green monochromatic color scheme with a glowing effect.

FORRESTER®