CRA | Business Intelligence
A CyberRisk Alliance Resource

Threat Intelligence:
Critical in the Fight Against Cyber Attacks, But Tough to Master

December 2022

SPONSORED BY

mimecast

Contents

Threat Intelligence: Critical in the Fight Against Cyber Attacks, But Tough to Master

FINDINGS FROM JUNE 2022 AND OCTOBER 2022 CYBERRISK ALLIANCE BUSINESS INTELLIGENCE RESEARCH STUDIES

Background

Threat intelligence has long posed a conundrum. Any program using robust, reliable data sources should help reduce response times and prevent existing and emerging threats from penetrating networks and databases. But without proper mechanisms to manage the volume and velocity of threat feeds, security analysts are easily overwhelmed, and security operations are stymied by an inability to turn off a firehose of feed data and false positives.

Yet the value of threat intelligence solutions is widely understood — and increasingly embraced.

The global threat intelligence industry is set to double within the next five to eight years to surpass **$20 billion in annual sales**, according to Emergen, a research firm tracking that space. Solutions that aggregate, correlate, and analyze data from a variety of vetted sources are increasingly seen as a necessity rather than nice-to-have. They help organizations brace for an attack and prevent future ones. Organizations choose between commercially available products and services or cobble together their own program using various, vetted resources.

No one wants to miss something — be it an exploitable vulnerability or advanced persistent threats. That's why more cybersecurity decisions rely on relevant threat data analyses to help address threats like ransomware.

Organizations want their threat intelligence programs to ease workloads, not add to them. They want to remain confident in their threat intelligence investments, given the wrong choice or response can destroy both companies and careers.

Research methodology

The data and insights in this report are based on two online surveys conducted among respondents from CRA's research panel: one in June 2022 among 183 respondents and another in October 2022 among 208 respondents. Respondents' roles include security and IT leaders and executives, security administrators, and compliance professionals. All respondents are based in the United States. CRA Business Intelligence conducted its first threat intelligence survey in June to assess organizations' threat intelligence usage and capabilities as well as their future plans for these types of solutions at their organizations. A follow-up survey conducted in October among many of the same research panelists also covered use cases as well as additional topics such as threat intelligence sources and data feeds.

The respondent profile in the October survey (similar to the June survey) is as follows:

Roles/titles:

- CISOs/CROs/CIOs/CTOs (8%)
- VPs/SVPs/EVPs in IT security/risk/compliance (6%)
- Directors of IT/IT security/audit, risk, and compliance (29%)
- Managers of IT/IT security/audit, risk, and compliance (29%)
- IT security admins (18%)
- Analysts/consultants (10%)

Organization sizes:

- Small (1 to 99 employees) (9%)
- Medium (100 to 999 employees) (30%)
- Large (1,000 to 9,999) (37%)
- Enterprises (10,000 or more) (24%)

Industries:

- High-tech, IT software and telecom (18%)
- Education (16%)
- Financial services (10%)
- Healthcare (9%)
- Manufacturing (10%)
- Retail, trade, or eCommerce (6%)
- Other (business/professional services, media/communications/advertising, transportation/warehousing, non-profit, energy, government, utilities, military/defense, construction, hospitality, and real estate) (31%)

Executive summary

Organizations understand the important role threat intelligence solutions play in maintaining a strong cybersecurity posture, particularly with the rise of ransomware. In today's rapidly changing threat landscape, early actionable access to credible threat intel is critical. According to survey respondents, it arms their Security Operations Centers (SOCs) and Incident Response teams with operational threat intelligence to help them make timely, informed decisions to prevent system downtime, thwart the theft of confidential data, and protect intellectual property.

Many also claim it is extremely important in protecting their company and customer data — and potentially saving their organization's reputation. Some maintain that with threat intelligence, there's no better way to keep leadership informed so that security efforts can be prioritized. "Without threat intelligence you would be chasing ghosts," commented one respondent from the June 2022 survey.

Key takeaways from the June 2022 and October 2022 surveys:

- About two-thirds (64%) of respondents from the June survey said they are very or extremely concerned about cyberthreats in the next 12 months. Their main concerns are ransomware (70%), followed by expanding attack surfaces (55%). Accordingly, for most respondents (62%), a fear of ransomware attacks is the top strategic driver of their threat intelligence strategies, followed by regulatory requirements (48%) and recommendations from industry experts (39%).
- Virtually all respondents from the October survey indicated they use threat intelligence at some level within their organization. A large majority of respondents (70%) said security operations is among their top use cases for threat intelligence. Threat intelligence is also used to increase the utility of the vulnerability management process, as reported by 64%. Other top uses for threat intelligence include incident response (53%) and risk analysis (53%).
- A large majority of respondents from the October survey said they use threat intelligence data for operational (70%) purposes, which helps in predicting future attacks and planning defense strategies. About two-thirds (67%) said they used threat intelligence data for technical objectives, primarily focusing on attackers' resources and tools and the specific implementations used for the attacks. Strategic data, which provides a more high-level view of threats to help management plan resources and make decisions about future cybersecurity, is somewhat less common at 53%. Slightly less than half of all respondents (46%)

said they use tactical data, which is typically used by incident response teams to help rapidly respond to security incidents.

- Many respondents from the June survey pointed out that having access to early and credible intelligence is a core requirement for their organization. About six in 10 (57%) said they subscribe to up to 10 threat intelligence feeds while another quarter (26%) gather their intelligence from 11 to 50 feeds. The largest shares of respondents said they use threat data from malware analyses (75%) or IoCs (indicators of compromise) (72%).
- Respondents said they use a variety of information in their organization's threat intelligence program, according to the October survey findings. The most common types are data from IDS, firewall, endpoints, etc. (reported by 67%), network traffic analysis packs and flow (62%), incident response and live forensics (57%), application logs (56%) and email or spreadsheets (55%). Use of information from the Dark Web (39%), MSSPs (36%), industry groups such as CERT (34%), and media/news sources (33%) are slightly less common.
- In the June survey, respondents indicated the importance of having an automated action and response capability as part of their chosen solution now and in the future. Nearly half (46%) said they already incorporate automation in their threat intelligence strategies, and almost as many (41%) said they plan to add that capability, making this the top planned component of their threat intelligence strategies.
- About 66% of respondents from the June survey anticipated spending more on threat intelligence in the coming year. This bodes well for security operations centers hoping to boost defense capabilities through improved threat intelligence, particularly as it relates to patching security flaws in current software and responding more quickly to security events.

Using threat intelligence to proactively fight ransomware attacks

Virtually all respondents from the June survey reported they have some level of concern with current cyber threats infiltrating their organizations — about two-thirds (64%) said they are very or extremely concerned about cyberthreats in the next 12 months. Their main concerns are ransomware (70%), followed by expanding attack surfaces (55%). Nearly three out of 10 respondents (29%) indicated the rise in nation-state attacks (particularly with the ongoing war between Russia and Ukraine), shortage of skilled security labor (27%), budget shortfalls (26%), and supply chain attacks (25%) were also among their concerns.

Respondents repeatedly underscored the critical role that threat intelligence plays in their security operations against these types of threats.

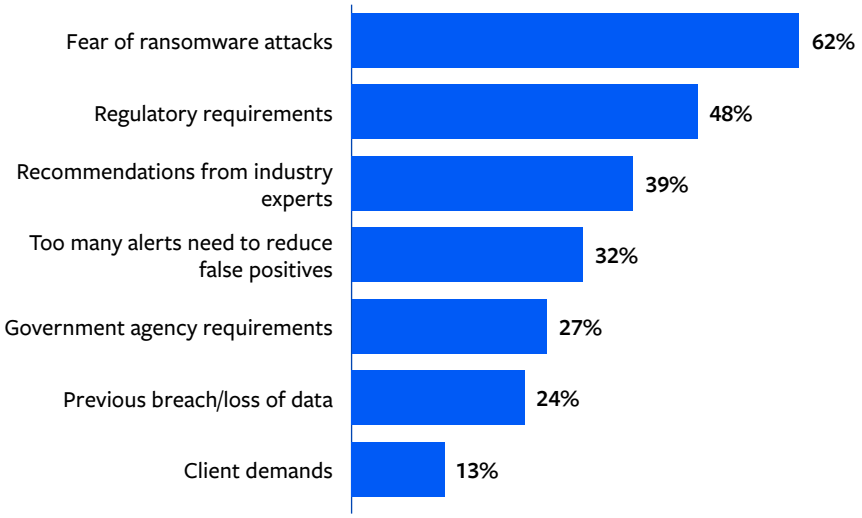
> **"We are able to get actionable information in a more timely manner through the various threat intelligence threads we are connected to than we would be able to ascertain on our own. In today's rapidly changing security landscape and threat sources, having access to early and credible intelligence is a core requirement."**

Accordingly, nearly two out of three respondents (62%) from the June survey said their fear of ransomware attacks was the top strategic driver of their threat intelligence strategies, followed by regulatory requirements (48%) and recommendations from industry experts (39%).

This ever-looming fear of ransomware continues to be a major concern as high profile ransomware attacks make headlines daily. In July, for example, approximately 1.29 million patients of Texas Tech University Health Sciences Center were added to the **ongoing fallout from the Eye Care Leaders ransomware attack and data theft** from December 2021. Meanwhile, in May 2022, **the Costa Rican government** became the first nation to declare a national emergency in response to a ransomware attack.

Which of the following are the top drivers of your organization's threat intelligence strategy?

Select up to three choices.



Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022

> **"Threat intelligence enables us to make faster, more informed, data-backed security decisions and change our behavior from reactive to proactive in the fight against threat actors."**

Threat intelligence data used at all levels of defense

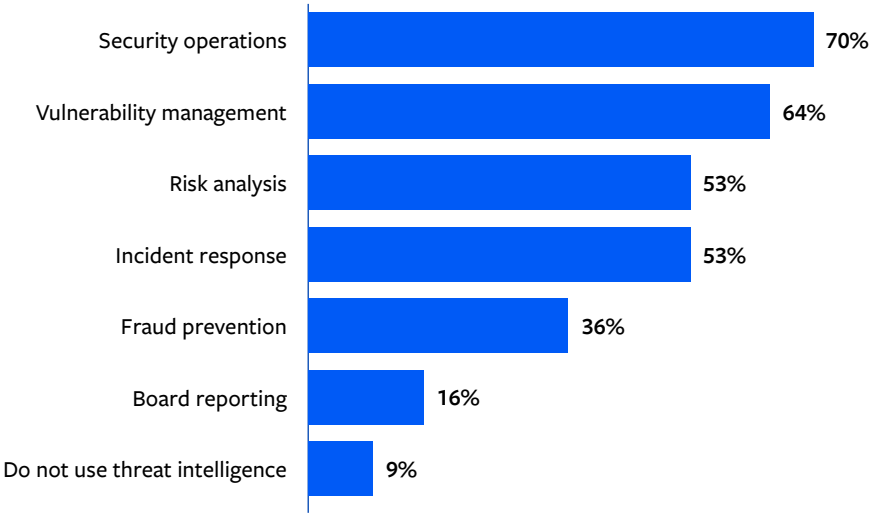
Virtually all respondents indicated they use threat intelligence data at some level within their organization, according to the October survey findings. A large majority of respondents (70%) said security operations is among their top use cases for threat intelligence. Also, threat intelligence is used to increase the utility of the vulnerability management process, as reported by 64%. Other top uses for threat intelligence include incident response (53%) and risk analysis (53%).

Most respondents from the October survey said they use threat intelligence data for operational (70%) and technical (67%) purposes. With operational threat intelligence, organizations can receive warnings and technical details on specific attacks, including the identity and capabilities of the threat actors, their attack behaviors, motives, and timing of attacks, in order to predict future attacks and plan their defense strategies. Technical threat intelligence data primarily focuses on attackers' resources and tools, and specific implementations used for the attacks.

Strategic data, which provides a more high-level view of threats to help management plan resources and make decisions about future cybersecurity, is slightly less common at 53%. Less than half of respondents (46%) said they use tactical data, which is primarily used by incident response teams to help in their rapid response to security incidents.

For which of the following does your organization use threat intelligence?

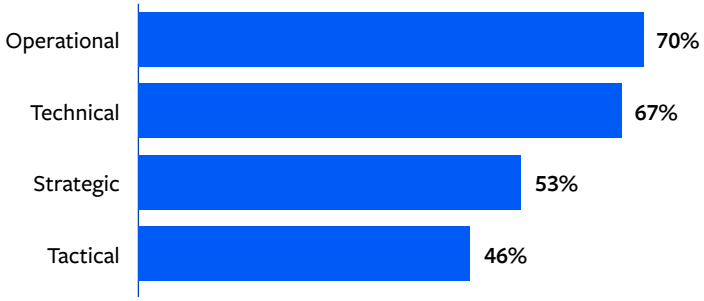
Select up to three choices.



Source: CRA Business Intelligence *Threat Intelligence Survey*, October 2022

Overall, which types of threat intelligence data does your organization currently use?

Select up to three choices.



Source: CRA Business Intelligence *Threat Intelligence Survey*, October 2022

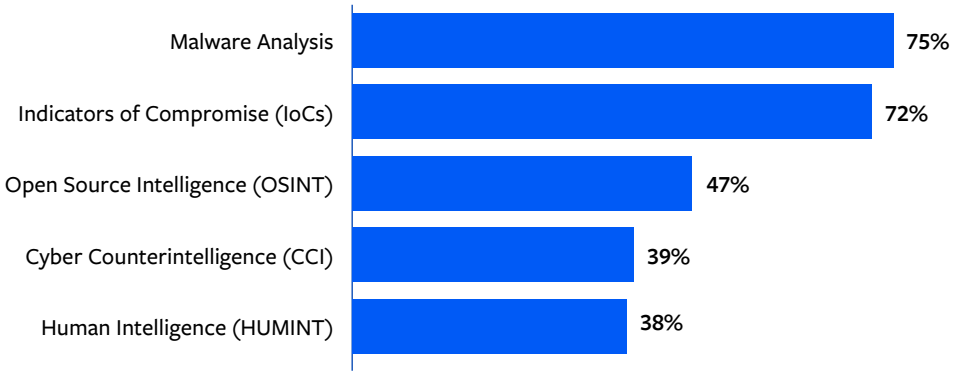
Real-time threat data provides a key advantage for organizations

Many respondents pointed out in the June survey that having access to early and credible intelligence is a core requirement for their organization. About six in 10 (57%) respondents said they subscribe to up to 10 threat intelligence feeds while another quarter (26%) gather their intelligence from 11 to 50 feeds. Only a small minority (7%) subscribe to more than 100.

The largest shares of respondents from this survey also said they use threat data from malware analyses (75%) or IoCs (Indicators of Compromise) (72%). Other, less common sources included open-source communities, cyber counterintelligence, and human/expert resources. Anomalous network traffic, such as a surge in outbound traffic, suggest data exfiltration, while an unusually high volume of authentication requests may signal a phishing attack is underway.

Which types of threat data collection does your organization currently use?

Select up to three choices.

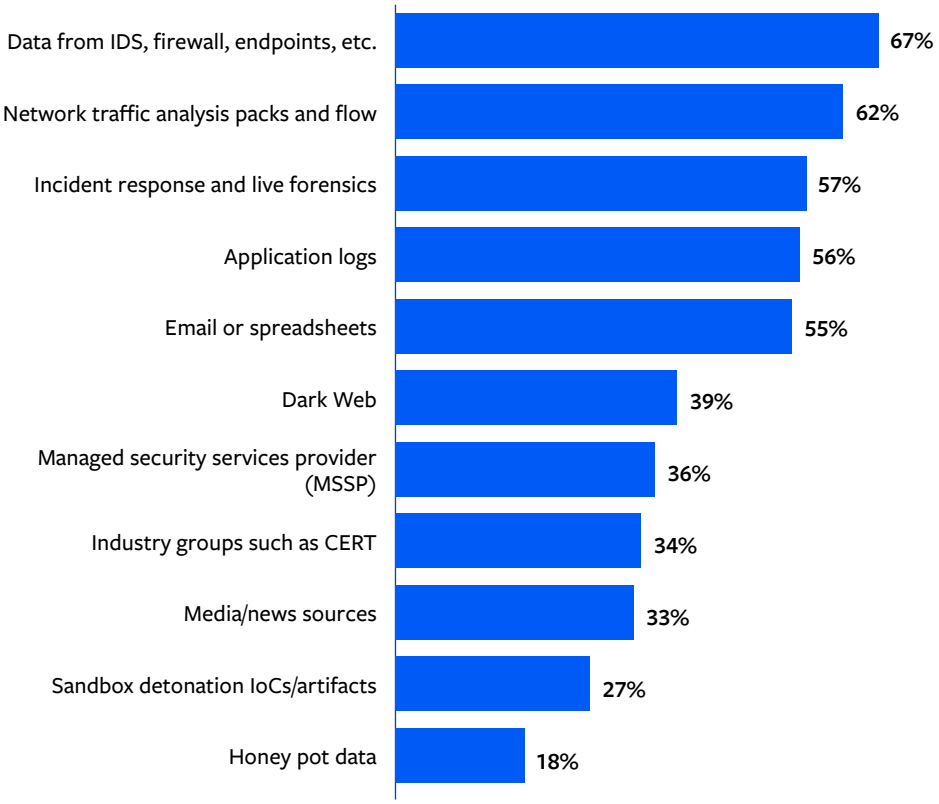


Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022

Respondents from the October survey indicated they use a variety of information in their organization's threat intelligence program. The most common types are data from IDS, firewall, endpoints, etc. (reported by 67%), network traffic analysis packs and flow (62%), incident response and live forensics (57%), application logs (56%) and email or spreadsheets (55%). Use of information from the Dark Web (39%), MSSPs (36%), industry groups such as CERT (34%), and media/news sources (33%) are slightly less common.

Which of the following types of information do you include in your organization's intelligence?

Select all that apply.



Source: CRA Business Intelligence *Threat Intelligence Survey*, October 2022

In describing the benefits of threat intelligence feeds in the June survey, respondents believe the threat data and information they receive is key in helping their organizations secure their environments. This advance notice allows them to benefit from what others are seeing "in the wild" in order to proactively configure their malware defenses.

Real-time detection was another dominant theme in respondents' sentiments about the benefits of threat intelligence feeds. Because threat intelligence feeds deliver threat data in real time, security teams often learn about potential issues as soon as they are discovered, a critical business benefit, since slower threat responses lead to larger data breaches and potentially more significant recovery costs. "It gives you a head start rather than having to start from scratch," according to one senior-level IT manager from the June survey.

Many respondents added that their threat intelligence feeds improve their operational efficiency, enabling them to act fast to stop a perceived

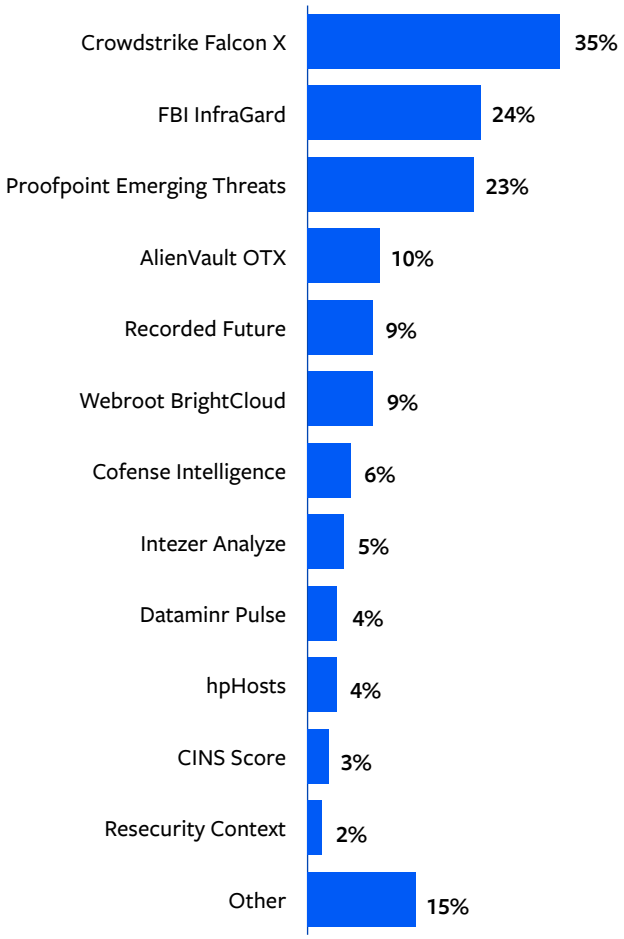
threat — allocating the appropriate resources to increase productivity, and then quickly adapting to the change.

Other comments from the June survey touting the benefits of threat intelligence feeds included improvements in security posture and reducing the risk of compromised data and systems. Several respondents also noted that threat intelligence data feeds their tool investment and selection process.

Organizations typically have multiple sources of data feeds as part of their threat intelligence program. In the October survey, respondents indicated the most common data feed sources are Crowdstrike Falcon X, used by at least one-third of respondents, as well as FBI InfraGard (24%), and Proofpoint Emerging Threats (23%).

Which of the following data feed sources are used as part of your threat intelligence program?

Select all that apply.

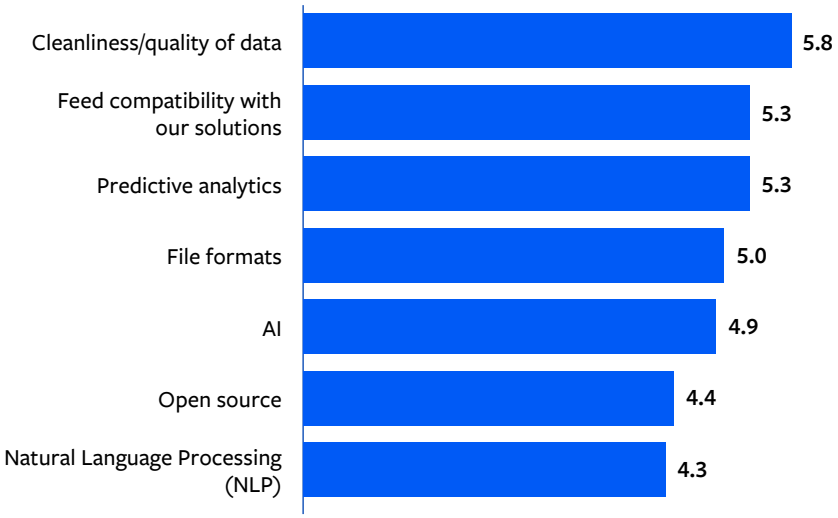


Source: CRA Business Intelligence *Threat Intelligence Survey*, October 2022

In thinking about their organizations' requirements for threat intelligence feed solutions, respondents from the October survey rated cleanliness/quality of data as the most important, with an average score of 5.8 (based on a 7-point scale where 1 is "Not at all important" and 7 is "Extremely important"). Feed compatibility with their organizations' solutions as well as predictive analytics were the next most important with average scores of 5.3 each. Other criteria, such as file formats, AI, open source, and natural language process (NLP) were relatively less important with average scores ranging from 4.3 to 5.0.

In thinking about your organization's requirements for threat intelligence feed solutions, how important are each of the following criteria?

Please rate each on a scale from 1 to 7, where 1 is "Not at all important" and 7 is "Extremely important."



Source: CRA Business Intelligence *Threat Intelligence Survey*, October 2022

Benefits of Threat Intelligence Feeds*

(% of respondents mentioning each benefit)

Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022
*What are the specific benefits of threat intelligence feeds to your organization? Please describe the specific benefits as well as any other relevant information about your threat intelligence feeds.

Buyers seek automated action and response capabilities

As the threat intelligence market matures, vendors continue adding features and functions based on both the changing threat landscape and customer demands. It is noteworthy that respondents, as buyers of these solutions, stressed the importance of having an automated action and response capability as part of their chosen solution now and in the future. Nearly half (46%) of respondents from the June survey indicated they already incorporate automation in their threat intelligence strategies, and almost just as many (41%) said they plan to add that capability, making this the top planned component of their threat intelligence strategies.

> **"Because threat intelligence feeds deliver threat data in real time, security teams will learn about potential issues as soon as they are discovered. This is key because slower threat responses lead to larger data breaches and significant recovery costs."**

Also, according to June survey results, the largest share of respondents (59%) indicated that data integration is currently part of their organizations' strategy, enabling them to connect their systems with other data-generating solutions tied to security information and event management, endpoint detection and response, and firewalls; another 28% noted they are planning to add data integration in the future. Similarly, half of all respondents reported using a threat intelligence platform and an additional 28% said this is also in their future plans.

Threat Intelligence Strategy Components

	Currently included	Planned	Not planned
Data Integration (SIEM, EDR, FW, etc.)	59%	28%	13%
Information Sharing	52%	32%	15%
Threat Intelligence Platform	50%	28%	22%
Automated Action/Response	46%	41%	13%
Internal vs. External Threat Comparison	45%	37%	19%
Threat Modeling	34%	37%	29%
Mitre Att&ck Framework	33%	28%	38%
Statistical Data Analysis	33%	35%	32%
Machine Learning	30%	35%	36%
Cyber Kill Chain Methodology	24%	27%	49%

Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022
Note: Percentages may not sum to 100% due to rounding.

In reviewing respondents' ratings denoting the importance of various threat intelligence capabilities, automated action/response was deemed the most important capability, according to the June survey findings. However, relatively lower satisfaction ratings for this feature indicate security professionals are least satisfied with their current ability to automate and respond to threats and require new solutions or improvements in this area to increase their threat intelligence effectiveness. Respondents also scored their threat intelligence platforms and data integration capabilities high in importance; and relatively high satisfaction scores suggest these capabilities should be considered core requirements in implementing effective threat intelligent solutions.

Importance/Satisfaction for Threat Intelligence Capabilities

Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022

Importance: How important is each of the following technology areas in your organization's threat intelligence strategy? Rate on a scale from 1 to 7, where 1 is "Not at all important" and 7 is "Extremely important."

Satisfaction: How satisfied are you with each of the following technology areas in your organization's threat intelligence strategy? Rate each on a scale from 1 to 7, where 1 is "Not at all satisfied" and 7 is "Extremely satisfied."

Note: Chart shows the relationship of importance vs. satisfaction for threat intelligence capabilities and areas for improvements. Each point in the chart plots importance and satisfaction mean scores. In areas where both importance and satisfaction scores are relatively high (upper right quadrant), organizations are keeping up and should maintain their approach and solutions in these areas. Where importance is high, but satisfaction is relatively low (bottom right quadrant), organizations should make improvements in these areas since they are not as satisfied in these relatively important areas. Low priority areas are those plotted as low satisfaction and low importance (lower left quadrant) as well as high satisfaction for areas of low importance (upper left quadrant).

Conclusion: Limited resources, lack of automation, and actionable intelligence hinder maximum benefits of threat intelligence

Effectively implementing threat intelligence isn't without its challenges — everything from internal obstacles and competing priorities, such as limited resources and lack of skills/qualified staff, and budgeting/financial constraints to issues related to dealing with the evolving threat landscape and expanding attack surface were mentioned in the June survey.

Additionally, the ability to automate the processing of threat intelligence and implement automated security responses to threats in order to immediately detect and remediate the latest types of attacks, remains out of reach for many. Some claim actionable intelligence is hard to find, while others grapple with threat data overload and collating and assembling critical attack data, along with controlling excessive alerts and false positives.

Finding the most efficient solution that enables rapid deployment and the greatest ROI was also considered problematic, as well as intelligence integration and deployment of advanced technologies, such as machine learning models that optimize the use of historical data to predict future events.

> **"[Threat intelligence] is the lifeblood of threat prevention. Especially for zero-day attacks."**

Top Challenges in Effectively Using Threat Intelligence*

(% of respondents mentioning each challenge)

33%
Resources and Skills

"Finding the correct people and building processes to help make this effective."

"I think it's the vast amount of threats that have escalated in the past 3 to 6 months and also keeping up with the massive amount of patching."

30%
Changing Threat Landscape

20%
Budget and Funding

"Budget is always a hot topic and never really gets better. Trying to get the organization to be adaptable to new threats and to be prepared is always challenging."

"... full visibility into the ICS environment. Many of the current tools are not designed to work or integrate with these types of devices. The age of this equipment does not allow for integration or agent type installs, so upgrades to those systems are needed."

19%
Tools and Integration

19%
Data and Intelligence

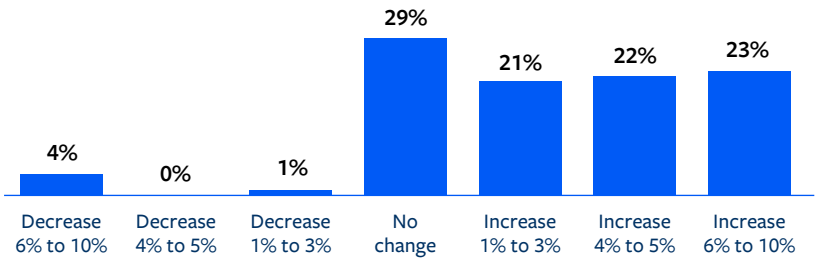
"Assessing the relevance of the intelligence to our type of organization. Much of it is centered on government, defense, or other large corporate targets rather than the smaller organizations. We have a different threat profile."

Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022
*What are your organization's challenges or issues in effectively using threat intelligence to prevent the latest types of cyberattacks in 2022? Please describe any challenges or issues with strategy, technology, solutions, or processes you would like to resolve to improve your organization's threat intelligence.

While respondents from the June survey expressed concerns about their organization's threat intelligence capabilities, many maintained their confidence in their solutions to stop cyberattacks. Almost 70% said they were moderately confident, and another 15% were highly confident in combatting cyberthreats.

In June, about 66% anticipated spending more on threat intelligence in the coming year. This bodes well for security operations centers hoping to boost defense capabilities through improved threat intelligence, particularly as it relates to patching security flaws in current software and responding more quickly to security events.

How will your organization's spending or budget for threat intelligence change in the next 12 months?



Source: CRA Business Intelligence *Threat Intelligence Survey*, June 2022

> **"Knowledge is everything. Knowing exactly how you are being attacked or the type of attacks going on will allow you to build a plan to detect and respond better."**

Related CRA Business Intelligence reports

- **Ransomware Ready: Organizations Fight Back with More Aggressive Strategies and Technology** (November 2022)
- **The Harsh Realities of Cloud Security** (October 2022)
- **Zero Trust Adoption Faces Ongoing Headwinds** (October 2022)
- **Endpoint Security: Security Pros Concerned About the Proliferation of Non-Traditional Devices and Endpoints** (September 2022)
- **Organizations Adopt Aggressive, More Proactive Vulnerability Management Strategies in 2022** (August 2022)
- **Threat Intelligence: The Lifeblood of Threat Prevention** (July 2022)
- **CRA Study: Attackers on High Ground as Organizations Struggle with Email Security** (July 2022)
- **Security Teams Struggle Amid Rapid Shift to Cloud-Based Operations** (June 2022)
- **CRA Study: XDR Poised to Become a Force Multiplier for Threat Detection** (May 2022)
- **CRA Study: Zero trust Interest Surges, But Adoption Lags as Organizations Struggle with Concepts** (April 2022)
- **CRA Study: Managing Third-Party Risk in the Era of Zero trust** (March 2022)
- **CRA Ransomware Study: Invest Now or Pay Later** (February 2022)
- **CRA Research: A Turbulent Outlook on Third-Party Risk** (January 2022)

About CyberRisk Alliance

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, SecurityWeekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. **Click here to learn more**.

About Mimecast

Since 2003, **Mimecast** has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.