exabeam®

The State of Threat Detection, Investigation, and Response 2023

Research insights by

IDC

Exabeam Report

Executive Summary

Examining enterprises' spending trends reveals that cybersecurity is one of the main worries of CEOs. IDC estimates that in 2022, the spending on cybersecurity solutions was more than US$92 billion. This figure is expected to almost double to over US$170 billion by 2027. With all these investments, how do enterprises feel about their threat detection, investigation, and response (TDIR) capabilities today? Are they better equipped and prepared? Are there areas where they still need help?

To find out the answers to these questions, Exabeam commissioned IDC to conduct a study on the state of TDIR. In the study, IDC surveyed over 1,100 senior security and IT professionals across eight countries on their organizations' perception of TDIR capabilities and processes. The study revealed compelling results about TDIR's capabilities, challenges, and future intentions:

High confidence and good progress on TDIR

The overwhelming majority of organizations (over 90%) believe they have good or excellent ability to detect cyberthreats today. 78% also believe that their organizations have a very effective process for investigating and mitigating threats. Over 70% of organizations reported better performance on cybersecurity key performance indicators (KPIs) such as mean time to detect, investigate, respond, and remediate for 2023 as compared to 2022.

TDIR platforms enhance security through automation

Investments in TDIR platforms have helped enterprises automate and streamline TDIR workflows. Just under half of the organizations IDC surveyed said that more than 50% of their TDIR workflow is automated. They also reported benefits such as operational efficiency, reduction in repeat attacks, increased visibility, and improved security posture from their TDIR investment.

Automation tops TDIR wish list

Incident mitigation/remediation and incident investigation automation top organizations' wish list for their TDIR platforms — having seen the benefits of automation, they want to go further. It is really the only way to keep up with threat actors. 60% of respondents consider the ability to access data for forensic investigation an important feature of a TDIR platform. Prepackaged use case support and the depth of content were also high on the list.

Challenges remain, visibility and timely processes are top concerns

Despite their confidence and process improvements, many organizations still face challenges. While over 70% of respondents reported year over year improvement, almost 57% of organizations surveyed said they experienced significant security incidents in the last 12 months that required extra resources to remediate. And an issue that is extremely concerning is that they are only seeing, on average, 66% of their IT environments. Limited visibility and time-consuming investigation processes top the list of challenges in TDIR.

Ongoing efforts needed in TDIR

Over a third of the organizations surveyed need more assistance in understanding normal user and entity behavior in their IT environment and finding expertise to manage TDIR.

Organizations have come a long way in improving their TDIR. However, the study shows CISOs and their security teams must invest in more automation, internal training to combat knowledge gaps, and improving the visibility of their environment.

Key Stats

- **Over 70% reported better performance** on TDIR versus the prior year.
- Half claimed **over 50% of TDIR workflow is now automate**d.
- **Despite confidence and improvement**, 57% experienced significant security incidents in the past 12 months.
- **Limited visibility and time-consuming investigation are top TDIR challenges**. Organizations claimed to only be able to see 66% of their IT environment.

High Confidence and Good Progress in TDIR

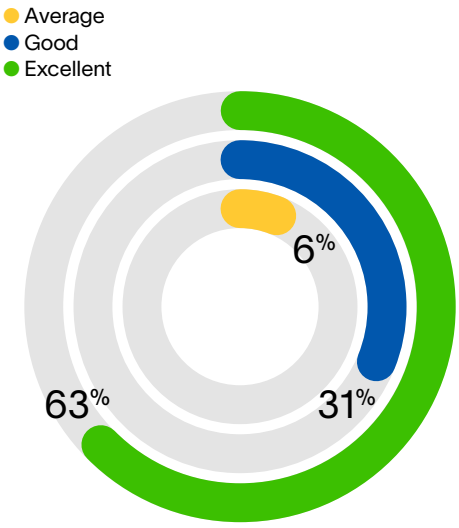
IDC's *CEO Sentiment Survey*, 2023, placed cybersecurity among the top three CEO or boardroom concerns. With an avalanche of news about breaches, such concerns are warranted and have driven significant investments in cybersecurity solutions in recent years. In 2022, IDC estimated spending of over US$92 billion on cybersecurity solutions. This figure is expected to almost double to US$170 billion by 2027. These investments have certainly brought more confidence and process improvements to enterprise security teams in combating cyberthreats.

In fact, IDC's survey with over 1,100 senior security and IT professionals revealed that the majority of organizations (over 90%) believe they have good or excellent ability to detect cyberthreats today. 78% also believe that their organizations now have a very effective process for investigating and mitigating cyberthreats. The level of confidence is quite high across the regions surveyed, with the Asia/Pacific including Japan (APJ) region showing slightly less confidence. Lower spending levels in cybersecurity in the APJ region might contribute to the region's lower confidence.

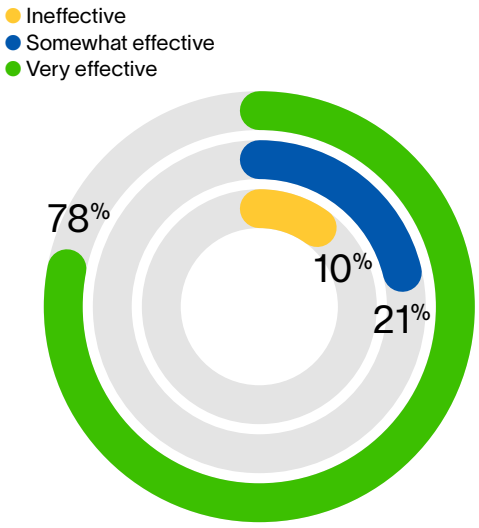
Such high confidence is supported with perceptions of better performance. Over 70% of organizations reported better performance on cybersecurity KPIs such as mean time to detect, investigate, respond, and subsequently remediate. A relatively lower percentage of organizations reported better performance on remediation time, especially in the APJ region. Improvements in analyst time spent per incident and IT infrastructure visibility were also reported across surveyed organizations.

Over 70% of organizations reported better performance on TDIR KPIs versus the prior year.

Q Please rate your organization's ability to detect cyberthreats.



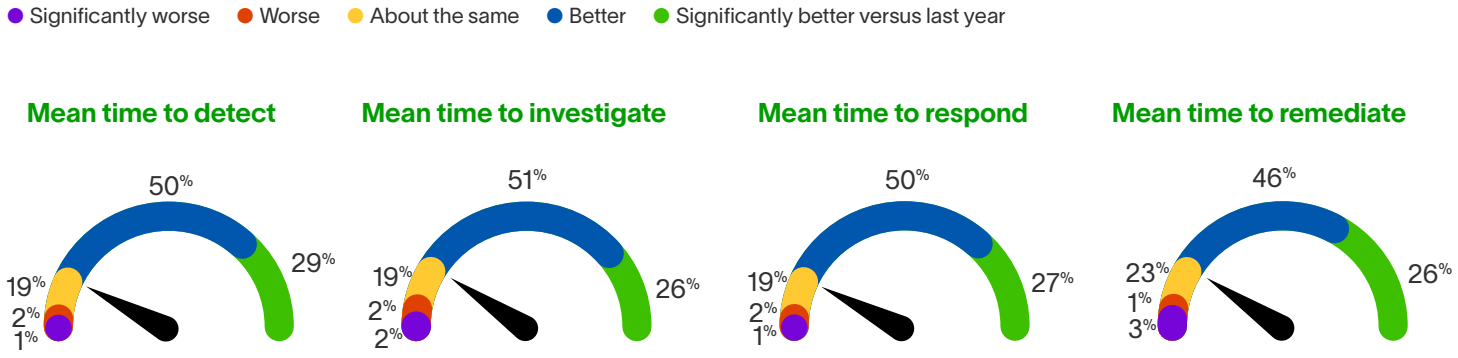
Q How effective do you consider your organization's process in investigating and mitigating cyberthreats?



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 1. **High Confidence in TDIR**

Q Please rate your organization's performance on cybersecurity in 2023 thus far, compared to 2022.



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 2. **Security Performance KPI — 2023 versus 2022**

But Challenges Remain — TDIR Pain Points

Despite the high confidence and progress, many organizations IDC surveyed admitted that they are still struggling. About 57% of organizations surveyed said they have experienced significant security incidents in the last 12 months that required extra resources to remediate. This high incident percentage is consistent with findings from another IDC survey. The IDC *Future of Enterprise Resiliency and Spending (FERS) Survey*, March 2023, shows that 65% of respondents had experienced a ransomware attack or breach that blocked access to systems and data in the last 12 months. Interestingly, APJ reported a lower percentage of security incidents than other regions. IDC hypothesizes this lower percentage doesn't reflect the actual incident level in the region, which it believes to be as high as other regions, but may instead reflect the reluctance of the respondents IDC surveyed to openly admit security incidents or breaches.

The study also revealed that CISOs are more likely to admit security incidents publicly than mid-level management. This makes sense, as CISOs will have a better perspective of the overall enterprise security operation and also function as the public face/spokesperson of the team. Moreover, in many countries, organizations are now required by law to report cybersecurity breaches or else face hefty fines.

57% experienced significant security incidents that required extra resources to remediate in the last 12 months.

Q Has your organization had a significant security incident that required extra resources to remediate in the last 12 months?

All
(n = 1,101)
57%

North America
(n = 526)
66%

Western Europe
(n = 283)
65%

Asia/Pacific
(n = 292)
34%

Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,101

Figure 3. **Significant Security Incidents**

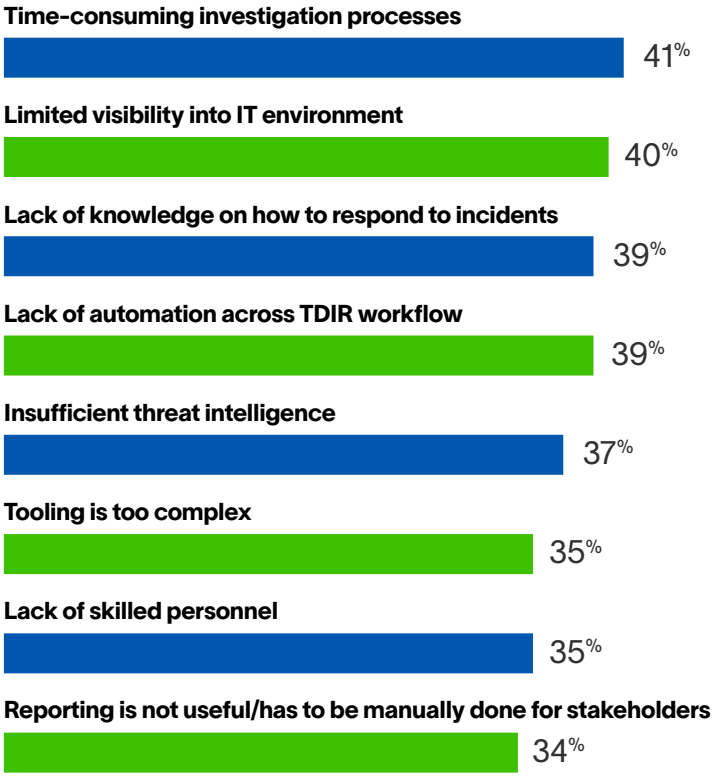
What's even more interesting is that organizations that claimed better TDIR performance reported experiencing security incidents at a higher percentage than ones that reported less effective TDIR. While it might appear counterintuitive, it makes sense that as an organization improves its average time to detect, investigate and respond, the more security issues it will likely uncover and resolve.

Regardless, the fact remains that despite all their TDIR efforts, organizations are still experiencing cybersecurity breaches. Threats will continue and will be challenging to evade when visibility is limited. Organizations surveyed estimate that they can "see" or monitor only 66% of their IT environments; this is a real concern when there are blind spots. This percentage is fairly consistent across the different regions, with the APJ region reporting even lower visibility of their IT environment at 62%. With business transformation initiatives moving operations to the cloud, combined with an ever-increasing number of edge connections, lack of visibility will likely continue to be a major pain point for most security teams. Hence, it is not a surprise that visibility was ranked among the top challenges for TDIR.

Time-consuming investigation processes, lack of knowledge to respond to incidents, and lack of automation round out the top challenges in TDIR delivery. When asked about time spent in TDIR, respondents estimated an average 57% of their security time is spent on TDIR each week. Obviously, that is a significant amount of time that the team will want to reduce through automated tools and processes. C-level respondents also ranked complexity of tooling at the top of their list of challenges, possibly because they have to oversee/manage everything, not just a portion of security tools. Security information and event management (SIEM) is particularly complicated due to the need to manage its analytics and storage capacity; customers have welcomed the opportunity to use a cloud SIEM instead of maintaining their own SIEM infrastructure.

> **"As your TDIR processes improve,** your security metrics will likely look worse before they get better."
>
> **Steve Moore**
> Exabeam Chief Security Strategist

Q What are the three greatest challenges in delivering your organization's threat detection, investigation, and response?



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 4. **Top TDIR Delivery Challenges**

Automation Accelerates TDIR Platform Response

A TDIR platform analyzes data to identify anomalous events, potential attacks, intrusions, misuse, or failure. Event correlation in a TDIR platform simplifies and speeds the monitoring of security events, packaging related alerts with threat intelligence to present to a security operations center (SOC) analyst. How fast the cyberattack unfolds, its sequence of steps, and its sophistication and uniqueness are factors that affect the elapsed time in detection and response. Automation with playbooks and predefined workflows, along with user and entity behavior analytics (UEBA) to identify anomalous activities, assists in reducing the elapsed time. Products can also consolidate and store the log and event data that was processed for future investigations and threat hunts.

Overall, 46% of organizations claimed that more than 50% of their TDIR workflow is automated. Automation has greatly streamlined threat monitoring, detection, and investigation, but it varies by region. While North America (NA) is similar to the total, in Western Europe (WE), only 36% of organizations have automated their TDIR workflow, while the APJ region is at 56%. VPs and C-level executives also say less of the workflow is automated than what department heads and directors claim, so they may not know the full scope of automation.

46% of organizations claimed that over 50% of their TDIR workflow is automated.

Topping respondents' wish list for their TDIR platform is investigation and remediation automation, which is expected given the challenges in finding enough security personnel and the complexity of using TDIR tools.

Threat detection and monitoring are more automated than threat investigation. Threat remediation is less automated than those three; there is often concern over what might happen without a human approving the process. As attackers increase their pace, enterprises will have to overcome their reluctance to automate remediation.

While this is a positive development, on the flip side, the other 53% of respondents have automated 50% or less of their TDIR workflow, which contributes to the amount of time spent on TDIR. As mentioned earlier,

> **57% of security teams' time is spent on TDIR.** The time spent is highest in NA at 65% and lowest in APJ at 41%.

organizations estimated 57% of their security teams' time is spent on TDIR, so greater automation can cut the amount of time required, particularly for investigations where an analyst needs to move in and out of systems to research the information they need. The time spent is highest in NA at 65% and lowest in APJ at 41%.

Despite more automation, organizations still need all the help they can find. 35% of respondents need more assistance understanding normal user and entity behavior in their IT environment. Training UEBA models is not simple, and the data used must be of good quality. Therefore, TDIR solutions that offer UEBA that requires less customization and provides automated timelines and prioritization will aid security teams in identifying normal behavior. About the same percentage needs help looking for a third party or specialists that understand their industries to manage their threat detection and response because they have concluded they cannot do it all themselves.

TDIR is a team sport

In this study, IDC surveyed organizations' security and IT senior leadership (CISOs and department heads), as well as mid-level management (Directors) to gain multiple perspectives of TDIR progress and challenges.

Overall, CISOs appear to be more confident and bullish on TDIR progress than their direct reports. 67% of CISOs surveyed had high confidence in their threat detection capability versus only 58% of Directors of Security.

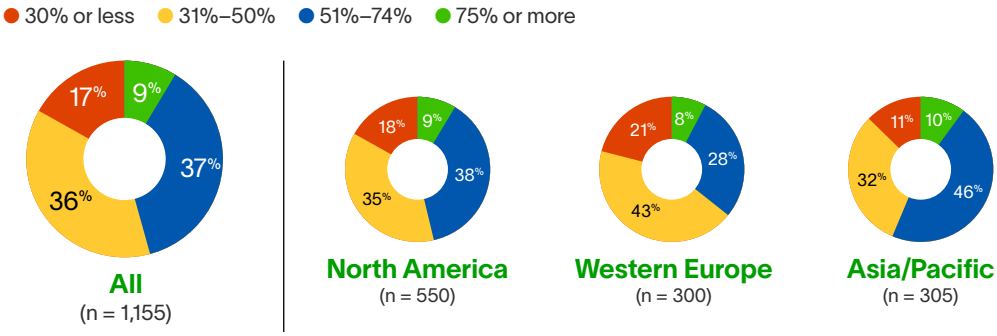
However, interestingly, CISOs are more likely to admit having a significant security incident in the last 12 months (76%) versus only 45% of Directors. This could be due to CISOs having a broader purview of their organization.

Despite the differences of opinion on TDIR progress, CISOs and their direct reports are mostly in agreement on the challenges they face. All placed time-consuming investigation processes and lack of automation, knowledge, and visibility into the IT environment as their top pain points when it comes to delivering TDIR. In fact, CISOs are more likely to say their TDIR workflows are less automated, and their security teams are spending a higher percentage of their time in TDIR.

When it comes to TDIR platform considerations, CISOs prioritize vendor reputation and implementation support capability, while Directors put more weight on ease of use. Depth of content is a higher priority for CISOs, while a simple user interface ranks higher with Directors. Investigation and remediation automation are at the top of organizations' TDIR platform wish list. CISOs and their direct reports also share similar sentiments about the difficulties in finding third-party or industry-aligned specialists that can assist them with TDIR. About 40% of organizations IDC surveyed used a combination of internal and external third-party services providers to manage their TDIR workflow.

Close to 80% of organizations IDC surveyed have more than five employees on their security team. It does require a team effort to improve an organization's TDIR workflow. Despite differences of opinion within the team, leadership, collaboration, and a similar drive toward common goals will be critical success factors in TDIR.

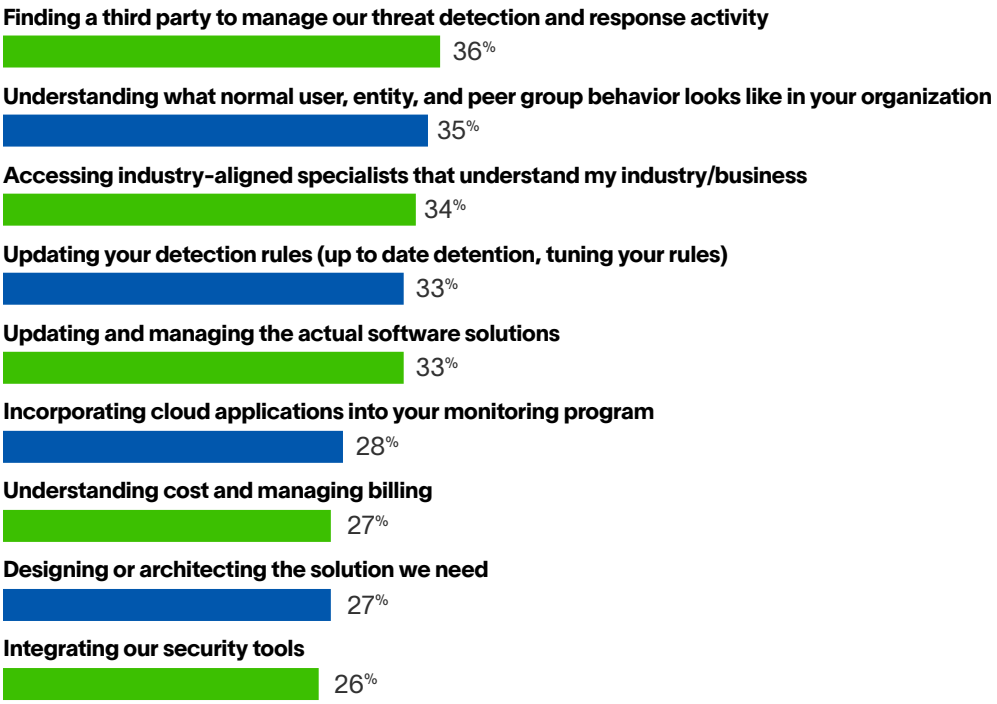
Q How much of your threat detection, investigation, and response workflow is automated?



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 5. **TDIR Workflow Automation**

Q When it comes to managing cyberthreat detection, investigation, and response, in which areas does your organization need the most assistance?



Organizations need assistance in finding third parties to help manage TDIR and understanding normal user and entity behavior.

Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 6. **Areas Needing the Most Assistance in TDIR**

What They Want: Enterprise TDIR Considerations

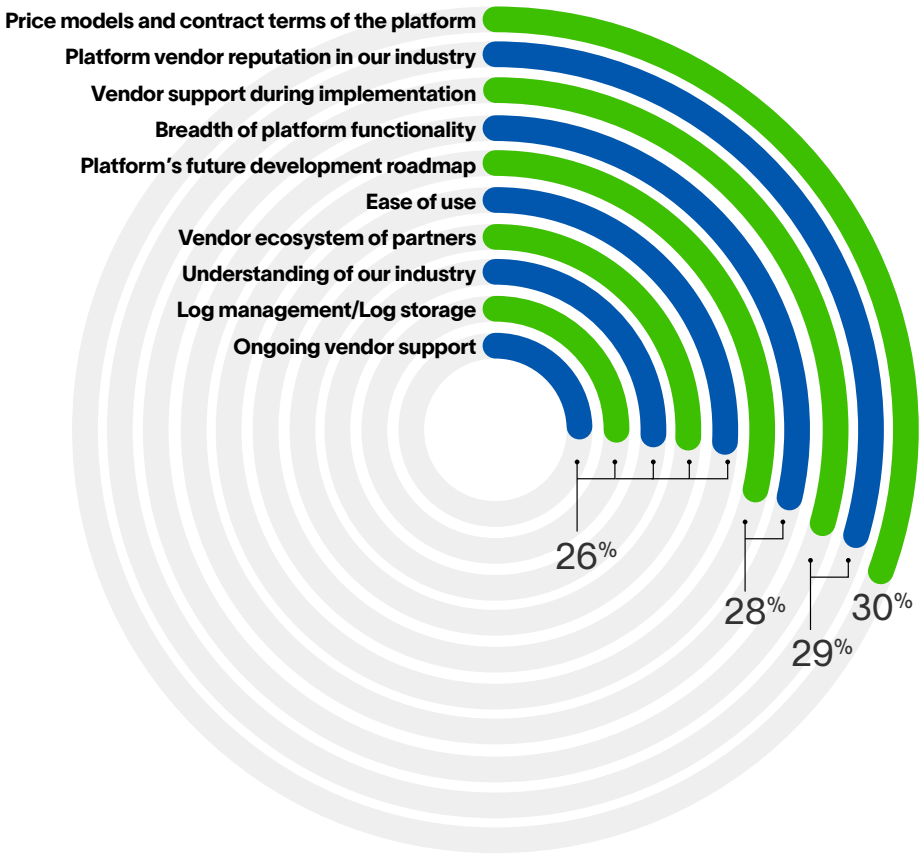
Organizations have invested in a range of TDIR-related capabilities: endpoint detection and response (EDR), managed detection and response (MDR), extended detection and response (XDR), network detection and response (NDR), and SIEM. This correlates with the amount of spending on TDIR solutions that is expected to reach US$33 billion in 2023 and forecasted to double to US$65 billion in 2027 (source: IDC's 2023 Security Product Tracker and Security Services Forecast).

When considering these TDIR solutions, organizations prioritize the price of the platform as well as implementation support, the vendor reputation, its platform's roadmap, breadth of integration (openness), and the breadth of functionality.

The complexity of TDIR solutions means they are not "set it and forget it" tools; they require care and feeding with constant updates and health checks to ensure they are performing as expected.

Beyond price, implementation support, vendor reputation, and platform roadmap top TDIR solution considerations.

Q What are your top 3 priorities when considering a platform solution for your organization's cyberthreat detection, investigation, and response?



Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 7. **Top TDIR Platform Considerations**

Log management/storage and ongoing vendor support are ranked higher in WE than in other regions. There is also variation by role, with the C-level and VP more concerned about the vendor reputation in the organization's industry than lower-level respondents. Perhaps it is because they take more heat for making the wrong vendor choice.

The most important features for respondents are the ability to access data for forensic investigation, prepackaged use case support, and the depth of content offered. TDIR tools are often the place to start a query once something happens, so the ability to search historical data to figure out what exactly happened is critical. Content, consisting of detection rules, dashboards, and threat hunts, is related to specific use cases. Many organizations do not have enough staff to write everything needed themselves and will benefit from the assistance of a TDIR platform vendor that can identify new threats. Respondents in APJ see working with data stored in many locations as having greater importance than prepackaged use case support. Those in Western Europe said log ingestion and UEBA were more important than content.

The most important TDIR platform feature that organizations look for is the ability to access data for forensic investigation.

Q What are the 5 most important features when considering a solution that allows your organization to improve its cyberthreat detection, investigation, and response?

Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 8. **Important TDIR Features to Consider**

IDC Essential Guidance

Organizations have come a long way in improving their TDIR processes, but CISOs and their security teams know they cannot stop; there is no end to the fight.

Investment in a TDIR platform brings a range of benefits to the enterprise. Better defense from repeat attacks, lower insurance premiums, and operational efficiency are the top business benefits for enterprises investing in TDIR.

However, there are many challenges. The lack of workflow automation and visibility greatly increases the security team's time spent on TDIR. Security leaders need to encourage teams to automate. Start with the simplest, most painful tasks; once those are done, work toward the more complex ones.

In addition to investment in a TDIR platform, enterprises still need assistance in setting up processes and finding industry-specific expertise in managing TDIR. Invest in training the team and seek external service providers who can help mature processes. The depth of content available also matters, so look for vendors who have internal research teams that are constantly adding new detections, threat hunts, and playbooks that can easily be downloaded to the TDIR platform.

Best practices in information security include:

Know your organization's business and how it makes money.

Partner with internal stakeholders to understand their needs for confidentiality, integrity, and availability of data and systems.

Communicate risk in a language understood by non-technical business leaders.

Prioritize risk reduction in critical assets to cut down on the amount of reactive work required later.

Innovate in security just as the threat actors do.

Stay up to date on the latest threats and tools designed to stop them. Have plans in place and practice them so you are ready to execute them when needed.

Better defense from repeat attacks, lower insurance premiums, and operational efficiency are top business benefits for TDIR platforms.

TDIR — Regional Perspectives

North America

In 2022, IDC estimated spending of over US$50 billion on cybersecurity solutions in North America. This figure is expected to grow to over US$92 billion by 2027.

IDC's survey with 550 senior security and IT professionals across US, Canada, and Mexico revealed that over 70% of organizations reported better performance on cybersecurity key performance indicators such as mean time to detect, investigate, respond, and remediate. Improvements in analyst time spent per incident and IT infrastructure visibility were also reported across surveyed organizations.

Despite the progress, challenges remain. 66% of organizations surveyed said they have experienced significant security incidents in the last 12 months that required extra resources to remediate. These threats are still coming through and will continue to be challenging to fend off when visibility is limited. Organizations surveyed estimate that they can "see" or monitor about 68% of their IT environments — that's a serious problem. Hence, it is not a surprise that visibility was ranked the top challenge for TDIR. Time-consuming investigation processes, lack of knowledge to respond to incidents, and lack of automation compound the challenges facing organizations in TDIR delivery for the region.

Just under half of organizations claimed that over 50% of their TDIR workflow is automated. Automation has greatly streamlined threat monitoring, detection, and investigation. While this is a positive development, on the flip side, the other half of the respondents have automated less than 50% of their TDIR workflow, which contributes to the amount of time spent on TDIR. Organizations estimated 65% of their security teams' time is spent on TDIR, so greater automation can cut the amount of time required, particularly for investigations where an analyst needs to move in and out of systems to research the information they need. Another capability, UEBA, used to establish a baseline of normal behavior to improve detection accuracy, can be leveraged to expedite investigations.

Despite more automation, organizations still need all the help they can find. 37% of respondents need more assistance understanding normal user and entity behavior in their IT environment. Training UEBA models is not simple and the data used must be of good quality, so using UEBA that does not require significant customization will aid security teams. About the same percentages need help in looking for third parties or specialists that understand their industries to manage their threat detection and response because they have concluded they cannot do it all themselves.

Organizations have invested in a range of TDIR-related capabilities: EDR, MDR, SIEM, XDR, and NDR. This correlates with the amount of spending on TDIR solutions that is expected to reach US$18 billion in 2023 and forecasted to almost double to US$34 billion in 2027 (source: IDC's 2023 Security Product Tracker and Security Services Forecast).

When considering these TDIR solutions, organizations in the region prioritize the price of the platform as well as the vendor reputation, its platform's roadmap, and the breadth of functionality. The most important features for respondents in the region are the ability to access data for forensic investigation, prepackaged use case support, and UEBA.

In 2022, IDC estimated spending of over US$50 billion on cybersecurity solutions in North America.

TDIR — Regional Perspectives

Western Europe

In 2022, IDC estimated spending of over US$17 billion on cybersecurity solutions in Western Europe. This figure is expected to grow to over US$32 billion by 2027.

IDC's survey with 300 senior security and IT professionals across the UK and Germany revealed that over 80% of organizations reported better performance on cybersecurity key performance indicators such as mean time to detect, investigate, respond, and remediate. Improvements in analyst time spent per incident and IT infrastructure visibility were also reported across surveyed organizations.

Despite the progress, challenges remain. 65% of organizations surveyed said they have experienced significant security incidents that required extra resources to remediate in the last 12 months. These threats are still coming through and will continue to be challenging to repulse when visibility is limited. Organizations surveyed in the region estimate that they can "see" or monitor about 65% of their IT environments — that's a serious issue. Hence, it is not a surprise that visibility was cited as a challenge for TDIR by 35% of the respondents.

Time-consuming investigation processes, insufficient threat intelligence, tooling complexity, and lack of knowledge to respond to incidents are top challenges in TDIR delivery for the region.

About 36% of organizations claimed that over 50% of their TDIR workflow is automated. Automation has greatly streamlined threat monitoring, detection, and investigation. But on the flip side, 64% have only automated less than 50% of their TDIR workflow, which contributes to the amount of time spent on TDIR. Organizations estimated 62% of their security teams' time is spent on TDIR. Greater automation can cut the amount of time required, particularly for investigations where an analyst needs to move in and out of systems to research the information they need. AI-based alert triage helps save time on investigations.

Despite more automation, organizations still need all the help they can find. 39% of respondents need more assistance understanding normal user and entity behavior in their IT environment. Training UEBA models is not simple and the data used must be of good quality. Using a UEBA model that requires less customization improves its usefulness. 37% need help in looking for third parties or specialists that understand their industries to manage their threat detection and response because they have concluded they cannot do it all themselves.

Organizations have invested in a range of TDIR-related capabilities: EDR, MDR, SIEM, XDR, and NDR. This correlates with the amount of spending on TDIR solutions that is expected to reach US$6 billion in 2023 and forecasted to double to US$13 billion in 2027 (source: IDC's 2023 Security Product Tracker and Security Services Forecast).

When considering these TDIR solutions, organizations in the region prioritize the price of the platform as well as the log management capability, ongoing vendor support, and vendor implementation support. The most important features for respondents in the region are the ability to access data for forensic investigation, log parsing or ingestion rate, and UEBA.

In 2022, IDC estimated spending of over US$17 billion on cybersecurity solutions in Western Europe.

TDIR — Regional Perspectives

Asia/Pacific Including Japan

In 2022, IDC estimated spending of over US$17 billion on cybersecurity solutions in APJ. This figure is expected to grow to over US$32 billion by 2027.

IDC's survey with 305 senior security and IT professionals across Australia, New Zealand, and Japan showed that over 60% of organizations reported better performance on cybersecurity key performance indicators such as mean time to detect, investigate, respond, and remediate. Improvements in analyst time spent per incident and IT infrastructure visibility were also reported across surveyed organizations.

Despite the progress, there are challenges. 34% of organizations surveyed said they have experienced significant security incidents that required extra resources to remediate in the last 12 months. IDC believes this percentage is higher, as some Japanese respondents were reluctant to admit incidents in a survey. Regardless, the threats are still coming through and will continue to be challenging to fend off when visibility is limited. Organizations surveyed in the region estimate that they can "see" or monitor about 62% of their IT environments — that's a major problem. Hence, it is not a surprise that visibility was cited as a challenge for TDIR by 36% of the respondents. Lack of automation, time-consuming investigation processes, and lack of knowledge to respond to incidents are top challenges in TDIR delivery for the region.

About 56% of organizations claimed that over 50% of their TDIR workflow is automated. Automation has greatly streamlined threat monitoring, detection, and investigation. However, there are still 44% that have only automated less than 50% of their TDIR workflow, which contributes to the amount of time spent on TDIR. Organizations estimated 41% of their security teams' time is spent on TDIR, so greater automation can cut the amount of time required, particularly for investigations where an analyst needs to move in and out of systems to research the information they need. There is an opportunity to seek out TDIR platforms that leverage AI algorithms to triage alerts to reduce time required for investigation.

Despite more automation, organizations still need all the help they can find. About 35% need help in looking for third parties or specialists that understand their industries to manage their threat detection and response because they have concluded they cannot do it all themselves.

Organizations have invested in a range of TDIR-related capabilities: EDR, MDR, SIEM, XDR, and NDR. This correlates with the amount of spending on TDIR solutions that is expected to reach US$5 billion in 2023 and forecasted to double to US$10 billion in 2027 (source: IDC's 2023 Security Product Tracker and Security Services Forecast).

When considering these TDIR solutions, organizations in the region prioritize the vendor reputation, price of the platform, ease of use, and vendor implementation support. The most important features for respondents in the region are the ability to access data for forensic investigation, work with data stored in many locations, and content depth.

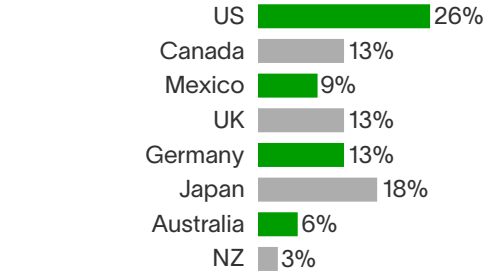
In 2022, IDC estimated spending of over US$17 billion on cybersecurity solutions in APJ.

Appendix: IDC Methodology

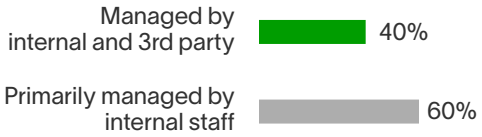
IDC's *Global Threat Detection, Investigation, and Response (TDIR) Survey*

The information presented in this report is sourced from IDC's *Global Threat Detection, Investigation, and Response Survey*, commissioned by Exabeam, August–September 2023. IDC surveyed 1,155 senior and mid-level security and IT professionals across industries in eight countries. Survey respondents were asked about their organizations' perception, challenges, and TDIR requirements.

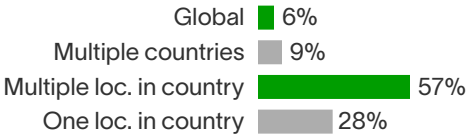
Countries



Security: Internal versus third-party management



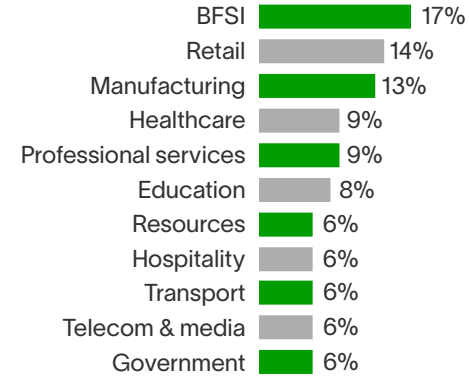
Primary & number of locations



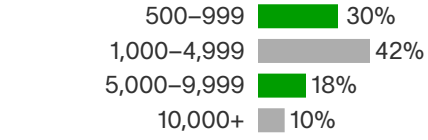
Security team

Length of operation

Industry/sector (self-described)



Employee size



CY22 Revenue range (US$)

Note: percentages might not add exactly to 100% due to rounding.
Source: IDC's *Global TDIR Survey*, commissioned by Exabeam, August–September 2023, n = 1,155

Figure 9. **Survey Respondents' Profile**
Respondents are familiar with their organizations' cyberthreat detection, investigation, and response practices or processes.

About the Analyst

Michelle Abraham Research Director, Security and Trust

Michelle Abraham is Research Director in IDC's Security and Trust Group responsible for the Security Information and Event Management (SIEM) & Vulnerability Management practice. Michelle's core research coverage includes SIEM platforms, attack surface management, breach and attack simulation, cybersecurity asset management, device and application vulnerability management alongside related topics.

About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.