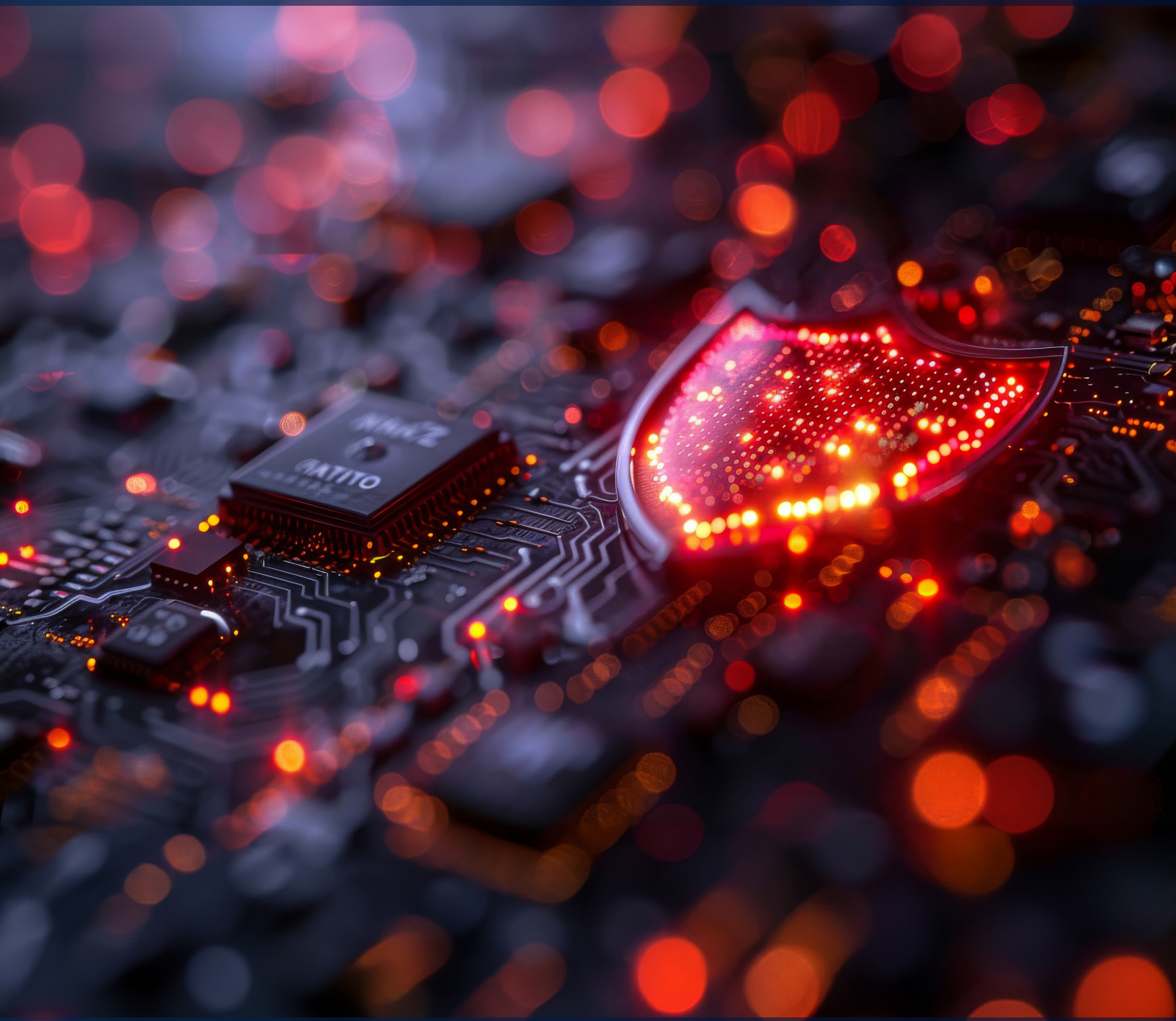
Dataminr Real-Time External Threat Detection Report



biz tech INSIGHTS | Dataminr®

Dataminr Real-Time External Threat Detection Report

Contents

The Case for Real-Time Data Analytics in Cybersecurity

In an era when cyber threats are increasingly sophisticated and persistent, the ability to detect and respond to threats in real-time has become a critical differentiator for cybersecurity resilience.

Organizations face an overwhelming volume of external threat signals, necessitating advanced tools and strategies to process, analyze, and act on this data efficiently. While many organizations recognize the importance of real-time analytics, adoption remains inconsistent, leaving significant gaps in cybersecurity postures.

To better understand current trends in cyber resiliency, Dataminr sponsored this survey, fielded by BizTech Insights from November 2024 until early February 2025. 200 IT and IT security professionals representing a range of industries and organizations participated in the study.

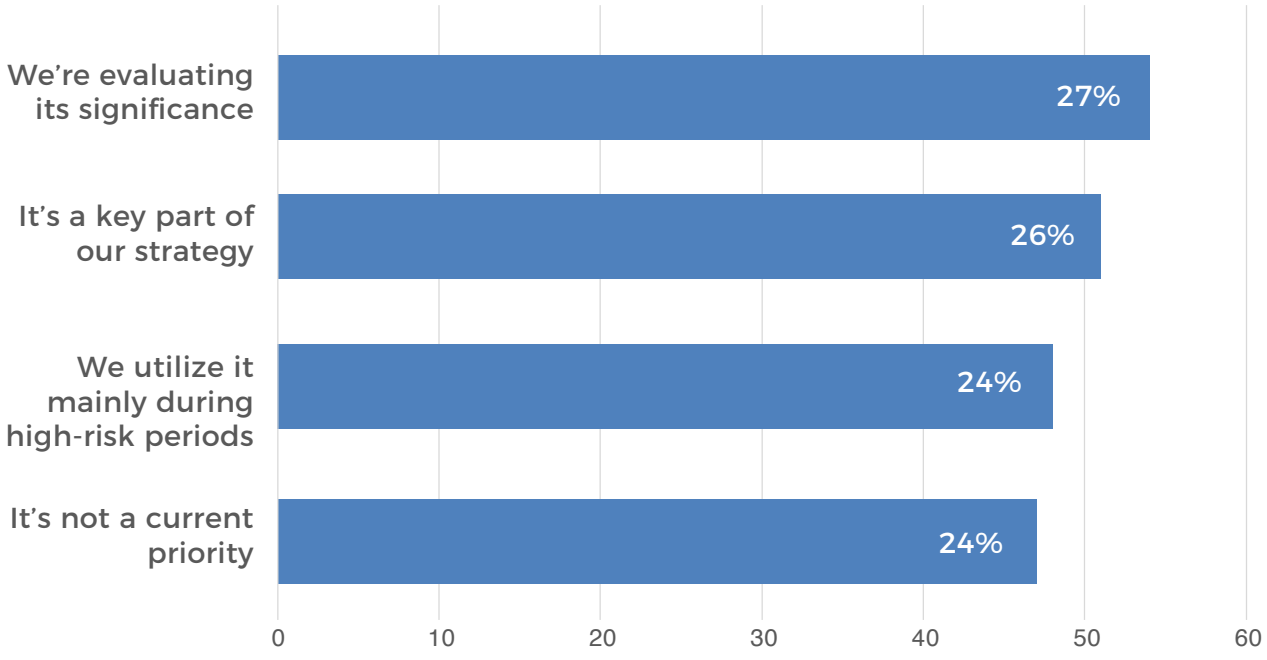
This report examines the survey findings to highlight the current state of real-time data analytics in cybersecurity. Key insights include the varying degrees of reliance on real-time threat detection, the challenges organizations face in integrating external intelligence sources, and the evolving role of automation and AI in streamlining risk response.

What's top of mind when considering your organization's data storage, IT infrastructure, and cyber resiliency?

There are several reasons why real-time threat detection is essential: Cyber threats can escalate within minutes, delayed detection often results in prolonged downtime, the number of false positives can be reduced, and the volume of threat signals can be managed more effectively.

Only 24% of the respondent firms said that real-time threat detection was not a priority for their organization. The largest number, 27%, are currently evaluating the significance of real-time detection, and a nearly equal number (26%) said it is a key part of their strategy.

The remaining 24% of respondents stated they only utilize real-time detection during high-risk periods.

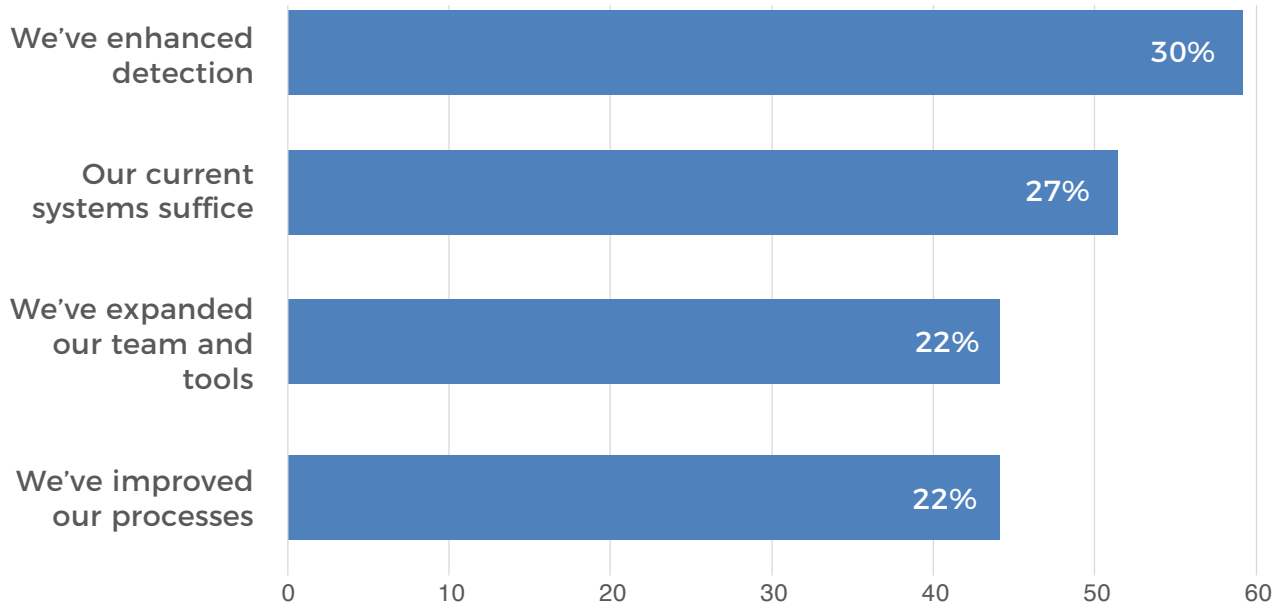


How are you addressing the volume of external threat signals?

According to the "2024 Attack Surface Threat Intelligence Report" produced by Cybersecurity Insiders, 80% of all breaches result from external threats. Rapid detection is critical to safeguarding the organization's assets and customer data.

Nearly a third (30%) of respondents have reacted by enhancing the detection of external threat signals. An additional 22% have expanded their teams and tools to handle the growing volume of threat signals better, and the same amount said they have improved their processes to better deal with threats.

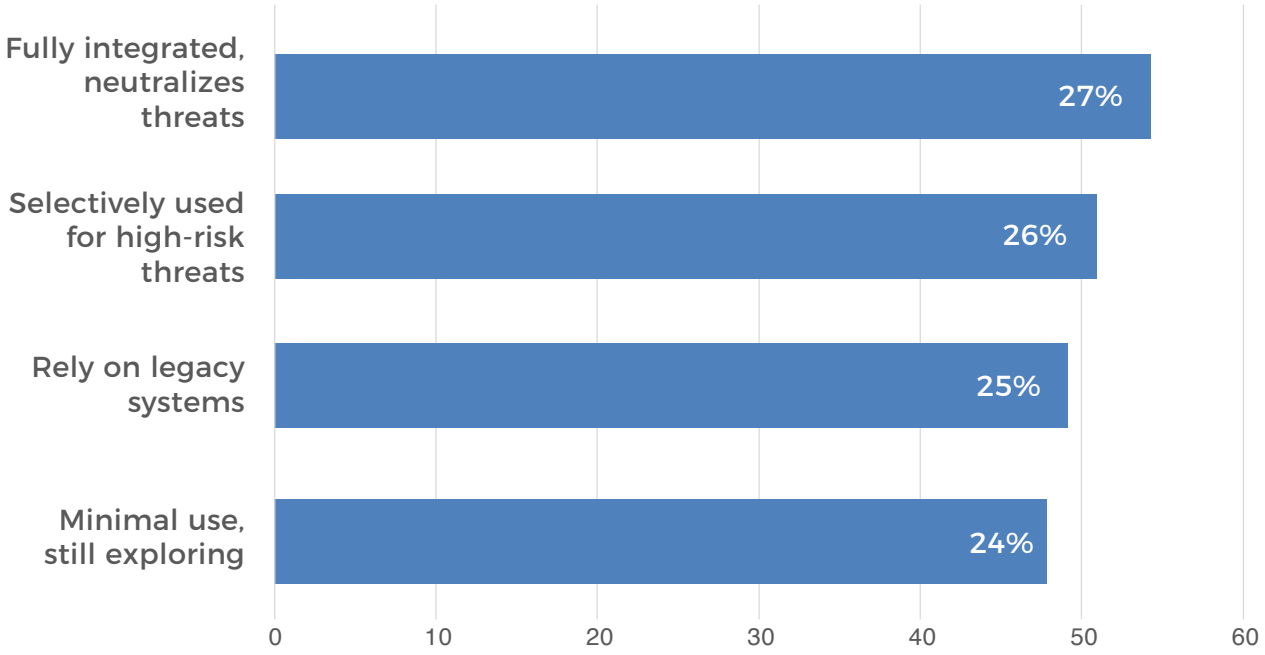
However, more than a quarter (27%) of respondents believe that their current systems are sufficient to handle the volume of threat signals today.



Which best describes your approach to using real-time analytics to identify and handle external threats?

There is a bifurcation of responses on the approach to real-time analytics. Just over half (53%) have either fully integrated real-time analytics to neutralize threats (27%) or are selectively using real-time analytics to address high-risk threats (26%).

The remaining 49% who are not utilizing real-time analytics are either relying on legacy systems (25%) or are in the process of exploring and thus have only minimal use of real-time analytics in their external threat detection processes (24%).



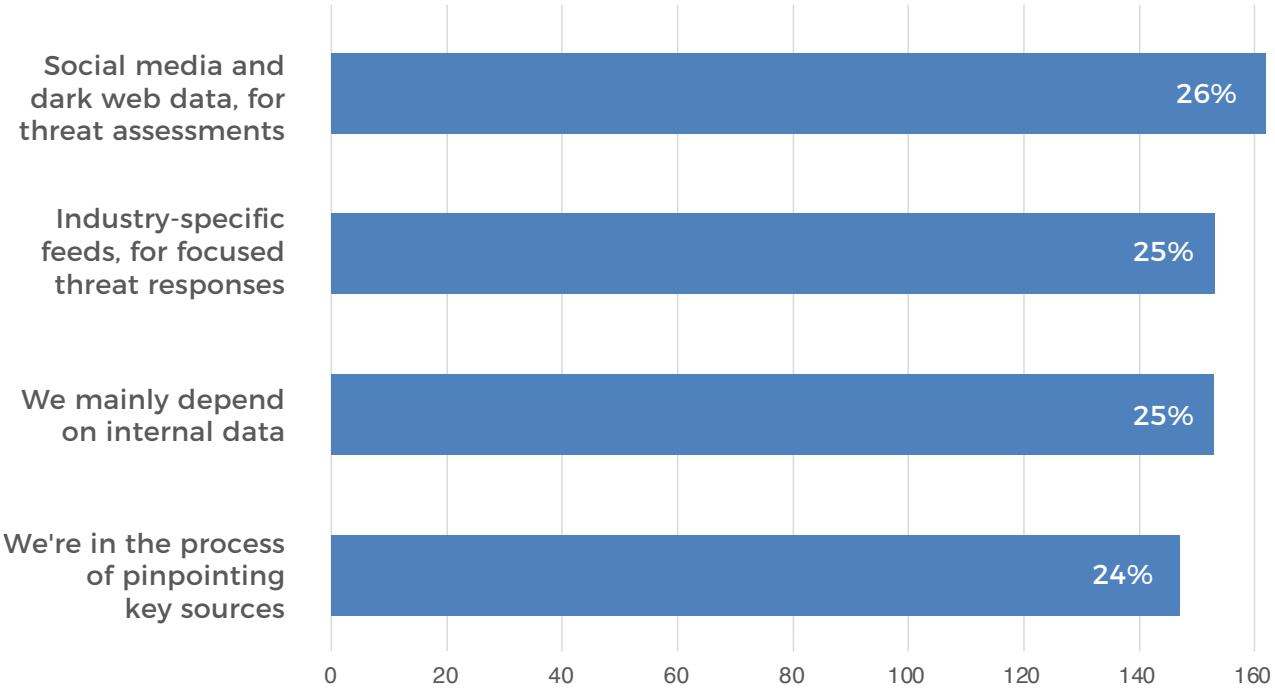
What data sources have become crucial for your cybersecurity operations? (Select all that apply)

Effective real-time cybersecurity threat detection relies on a diverse set of data sources that provide visibility into emerging threats, attack patterns, and vulnerabilities. Security teams can quickly identify, analyze, and respond to cyber threats by integrating multiple external and internal data feeds.

The largest number of responses (26%) indicated that social media and dark web data were used for threat assessments. Nearly as many responses indicated that the organization relied on industry-specific feeds for focused threat responses.

While 24% of responses said their organizations were in the process of pinpointing key sources, it should be noted that 25% of responses from 150 of the 200 organizations indicated that their organization was still relying mainly on internal data for threat detection.

Base: 612 responses



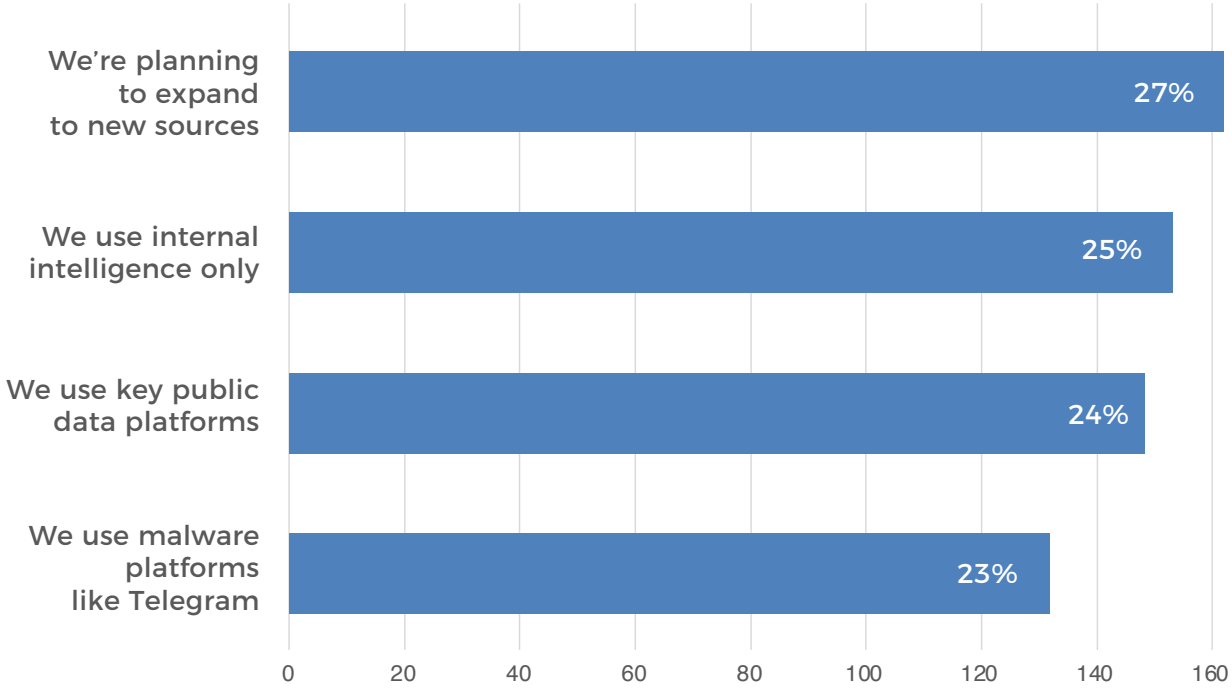
Which public data sources are you actively using for external threat detection? (Select all that apply)

Survey results indicate that while some organizations actively use key public data platforms, others rely primarily on internal intelligence or plan to expand their external threat monitoring capabilities.

The greatest number of responses (27%) indicated their organization is planning to expand to new sources. Another 24% of respondents said organizations were using key public data platforms, while just under a quarter (23%) of responses representing 132 respondents said their organizations were using malware platforms like Telegram.

However, 1 in 4 responses (representing 145 respondents) indicated that they currently use only internal intelligence data for threat detection.

Base: 570 responses



What do you want to achieve by enhancing your third-party risk detection program? (Select all that apply)

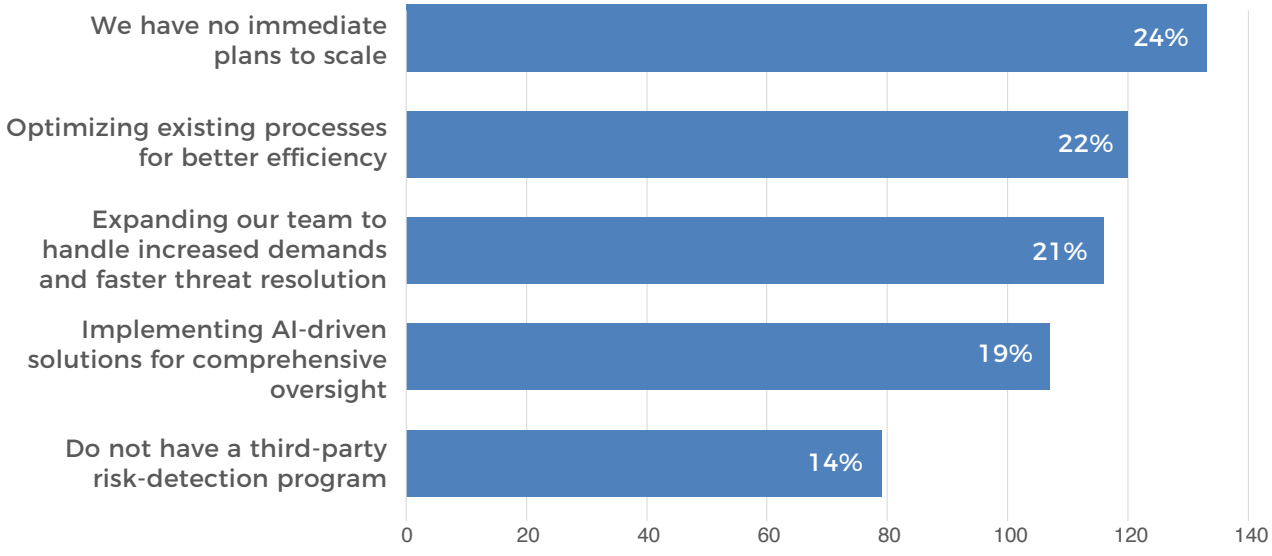
Third-party vendors, suppliers, and partners often have access to an organization's systems and data, making them a critical attack vector for cyber threats. Enhancing third-party risk detection programs improves security, compliance, and overall business resilience.

However, the greatest number of responses (24%) indicated their organization has no immediate plans to scale their third-party risk detection plans. In comparison, another 14% of responses said the organization did not have a third-party risk-detection plan.

Of those with plans to enhance their security, 22% of respondents said they were optimizing the existing processes for better efficiency. In comparison, nearly as many (21%) of respondents said they are expanding their team to handle increased demands and faster threat resolution to manage the growing number of signals.

Just 19% of responses from 107 respondents said their organization was implementing AI-driven solutions for comprehensive oversight.

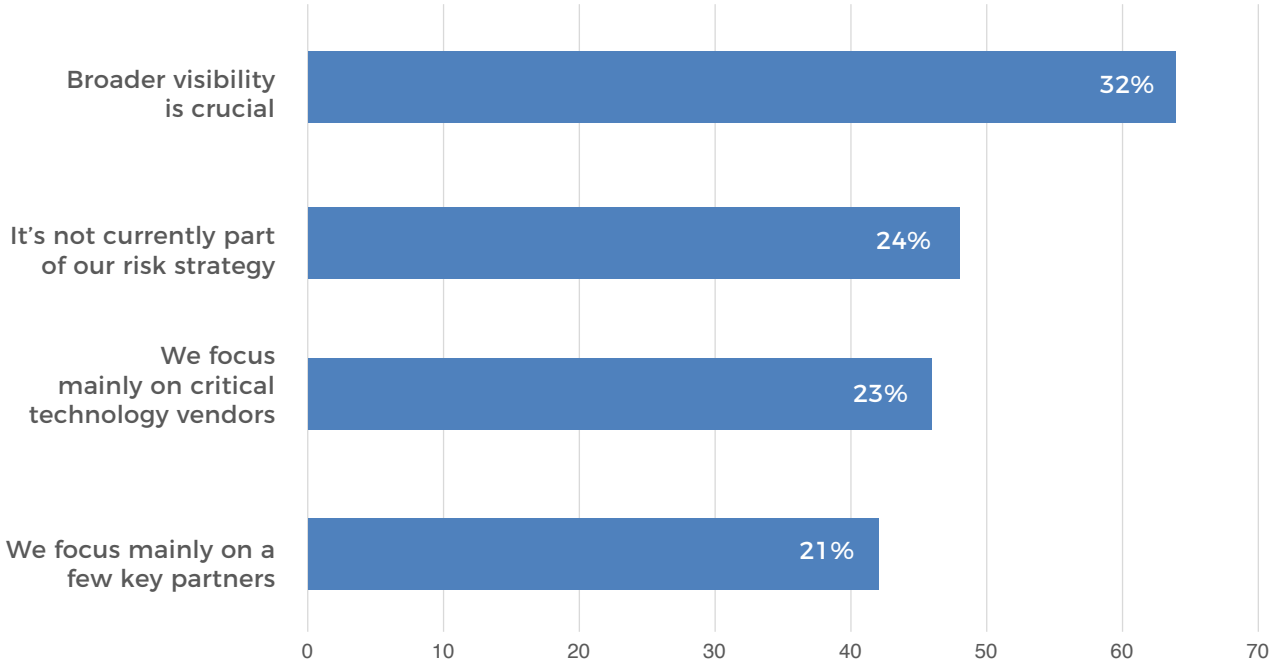
Base: 555 responses



How important is having broader visibility into your smaller vendors and suppliers?

Only 24% of respondents said that broader visibility into third-party partners was not currently part of their risk prevention strategy.

The greatest percentage of the remaining respondents (32%), however, believe that broader visibility is crucial. Another 23% of respondents are focused mainly on their critical technology vendors, while 21% said they focus only on a few key third-party partners.



How does visibility into kinetic events and physical threats support your cybersecurity objectives?

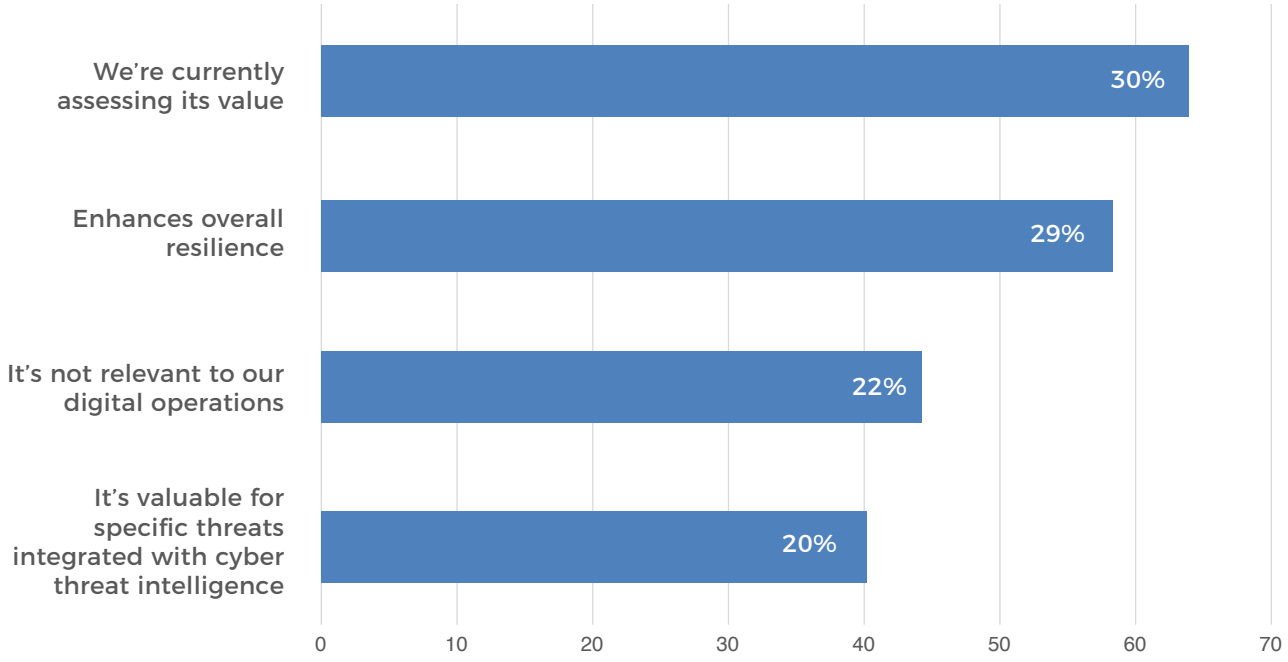
Cybersecurity is no longer limited to digital threats. Physical security events and kinetic threats (such as geopolitical conflicts, infrastructure attacks, and natural disasters) can directly impact an organization's cyber risk. Enhanced visibility into these events enables security teams to proactively adjust defenses, mitigate risks, and maintain operational continuity.

All but 22% of respondents either see the value or are assessing the value of this type of security data.

Currently, the greatest number (30%) of respondents are assessing the value of visibility into these events and threats. In comparison, nearly as many (29%) of respondents believe that this visibility enhances overall resilience to threats.

One in 5 respondents said this visibility is valuable for specific threats when integrated with cyber threat intelligence.

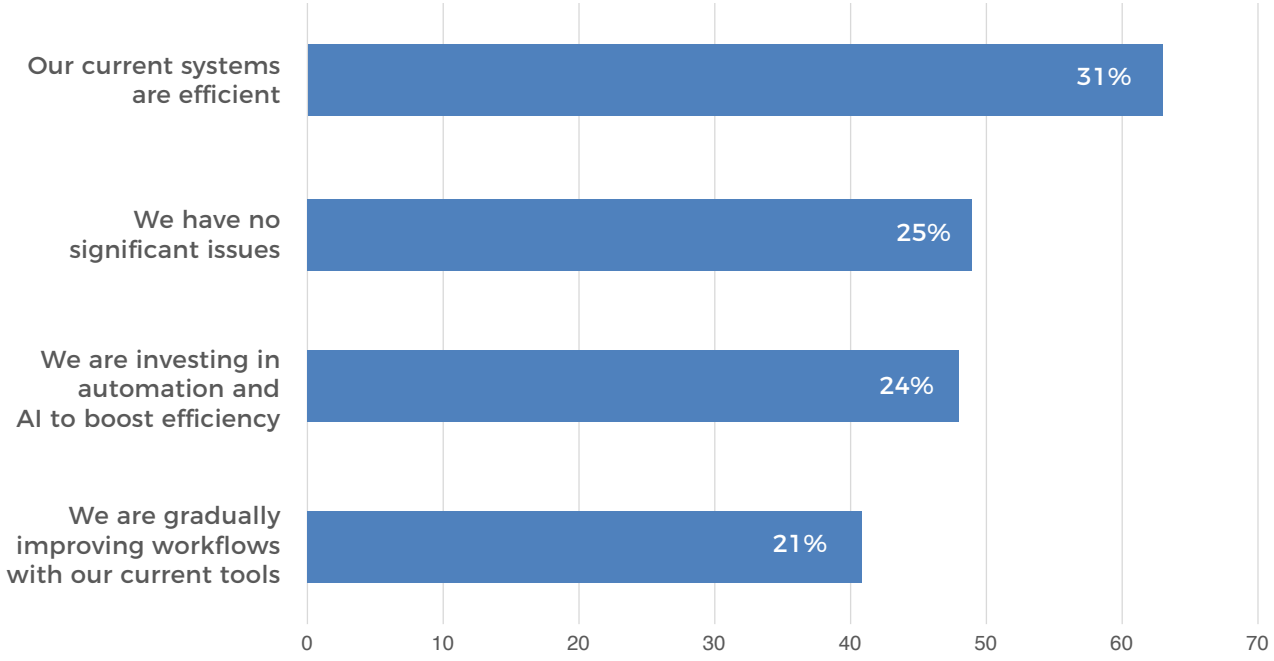
As previously mentioned, 22% of respondents said that visibility into kinetic events and physical threats is irrelevant to their digital operations.



What solutions are you exploring to meet challenges in streamlining workflows and automating risk responses?

Surprisingly, the greatest number of respondents (31%) indicated that their current systems were sufficient for streamlining workflows and automating risk response, while another 25% believe they have no significant issues to improve.

Of those who are taking action. 21% of respondents said they are gradually improving workflows with their current tools, while 24% indicated that they were making investments in automation and AI to boost efficiency.

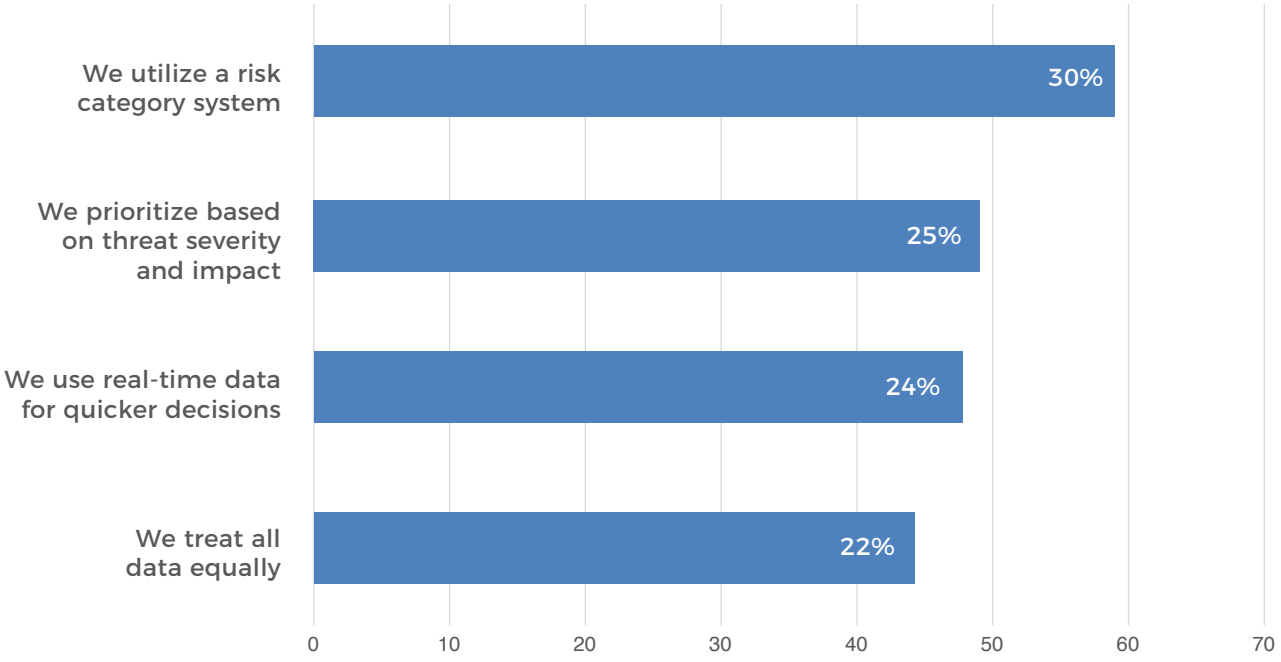


How do you prioritize workflows using various data sources ad threat intel feeds?

Respondents were split as to what methods of prioritization—if any—are used to assess threats.

The largest number (30%) of respondents noted they utilize a risk category system, while an additional 25% prioritize based on the threat severity and impact.

Just under a quarter of respondents (24%) stated they currently use real-time data for quicker decision-making, while the remaining 22% said they treat all data equally.



Conclusion

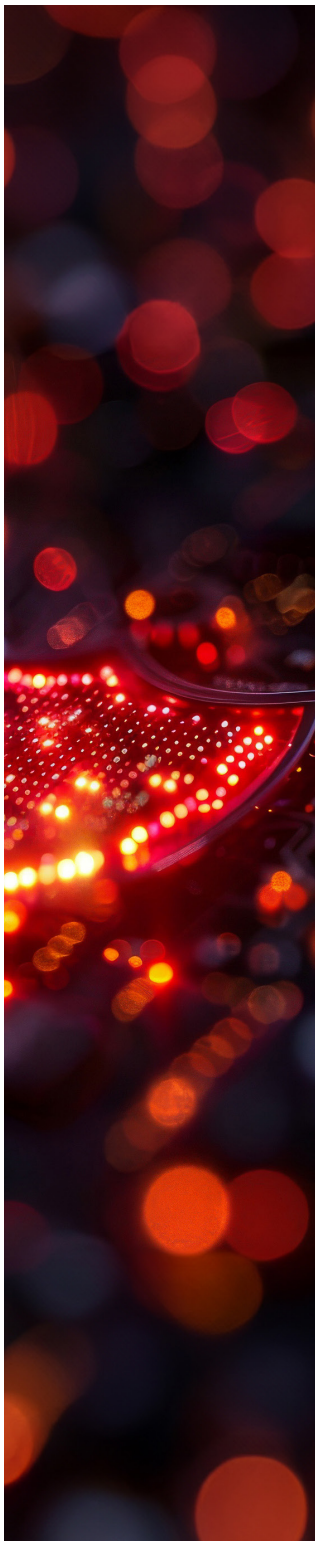
The findings highlight a clear but uneven adoption of real-time data analytics in cybersecurity. While many organizations acknowledge the importance of rapid threat detection and response, significant gaps remain in execution, strategy, and investment.

A key takeaway is that cyber resilience depends on an organization's ability to efficiently process vast volumes of external threat signals. The survey shows that while some companies are enhancing their detection capabilities through automation, AI-driven analytics, and expanded security teams, a notable portion still relies on legacy systems or internal intelligence alone, leaving them vulnerable to external threats.

Additionally, third-party risk remains an under-addressed challenge, with many organizations lacking a comprehensive program for monitoring vendors and suppliers. Given that supply chain vulnerabilities are a leading cause of cyber breaches, the need for broader visibility into third-party risks cannot be overstated.

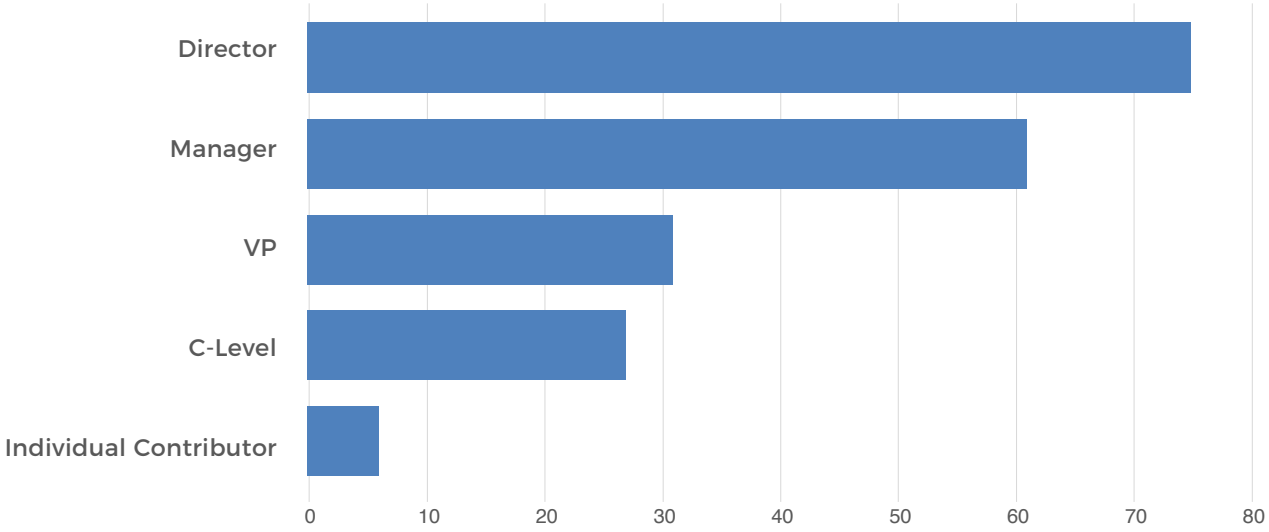
Another emerging priority is integrating kinetic event monitoring with cybersecurity strategies. As geopolitical instability, infrastructure attacks, and natural disasters increasingly impact digital security, organizations must expand their threat intelligence beyond traditional cyber threats to build a truly resilient security posture.

As the threat landscape evolves, those who fail to embrace real-time cybersecurity strategies will face increased exposure to breaches, regulatory penalties, and reputational damage. Organizations that prioritize real-time threat intelligence, automation, and external data integration will be better positioned to defend against today's increasingly sophisticated cyber threats. ■

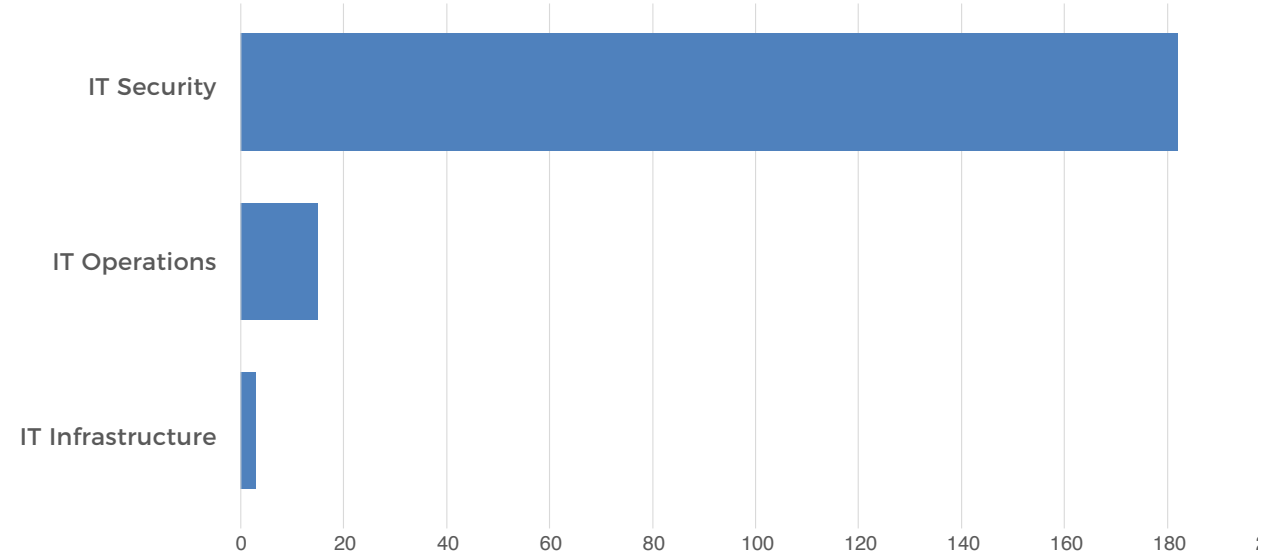


Survey Demographics

PERSONAS by Job Level

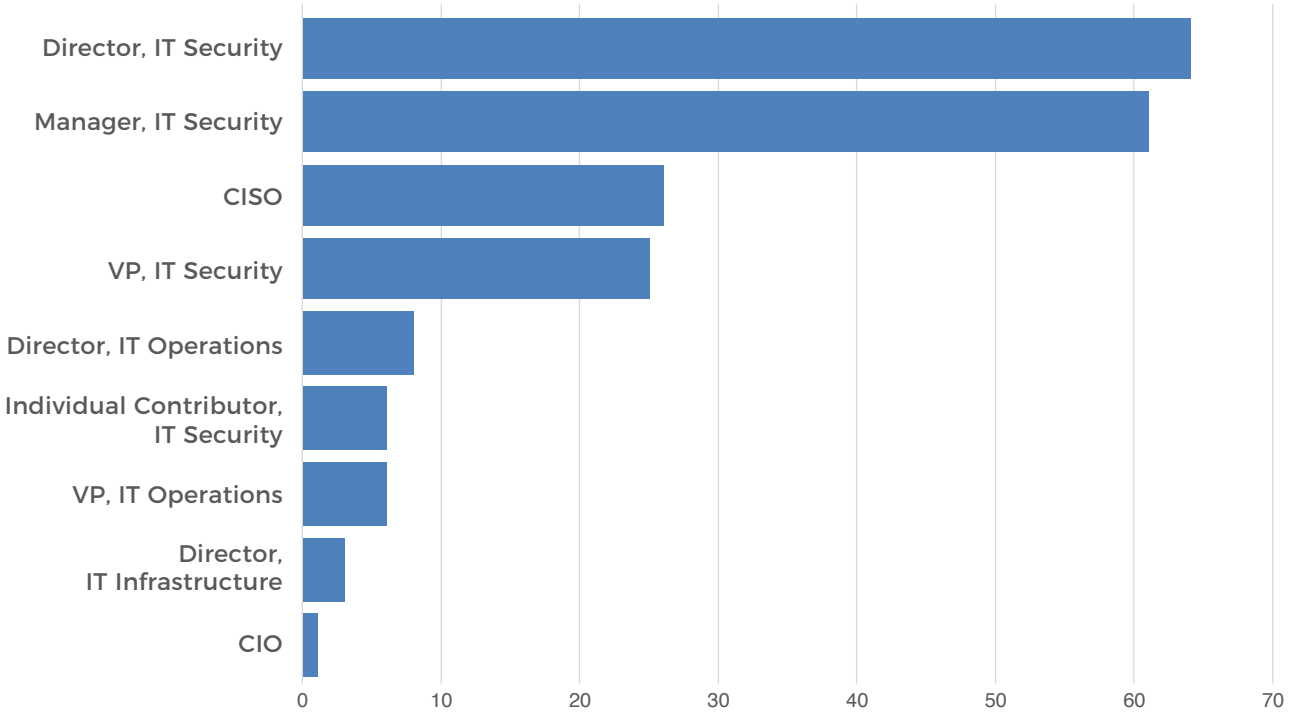


PERSONAS by Job Function



Survey Demographics

PERSONAS by Job Title



PERSONAS by Country