Cognyte

2025
Law Enforcement Outlook:
Navigating Security Threats, Investigation Challenges & Technology Innovations

Table of Contents

Introduction

As criminal landscapes evolve in response to geopolitical and technological shifts worldwide, Law Enforcement Agencies (LEAs) must stay a step ahead and continually strengthen their capabilities in order to confront an increasingly complex array of threats and challenges. It's not only the expanding range and variety of crimes being committed — it's also the rapidly advancing techniques of criminals and bad actors, who are quick to adopt cutting-edge technologies to carry out their malicious activities.

With many technologies becoming increasingly commoditized, their ubiquitous use isn't limited to just law-abiding citizens, but also to criminals. From GenAI chatbots and drones to satellite internet, advanced technologies of all types are now increasingly accessible, providing criminals with powerful tools to both expand their criminal activities and more easily avoid detection by authorities. Using these technologies, the crimes they commit can now be executed faster, on a much larger scale, and with more destructive impact.

At the same time, these same technologies hold the potential to do good, by equipping LEAs with more powerful capabilities to fight back against crime.

To carry out their roles effectively, LEAs must broaden their technological readiness in order to successfully combat crime and resolve investigations faster. The purpose of this survey is to offer a unique view of the current state of law enforcement, and to shed light on how LEAs expect technology to impact their strategies and capabilities in the coming year. The report should be of particular interest to law enforcement personnel serving in investigations, intelligence analysis, field operations and other hands-on roles, as well as IT professionals who set the priorities, budgets and technology roadmaps for their organizations.

Methodology

We commissioned a survey of 300 law enforcement stakeholders, both senior decision-makers as well as hands-on practitioners. The survey is based on responses from respondents who are actively working in law enforcement organizations, public safety agencies, financial intelligence units, border police units, maritime police units, as well as SWAT, special forces, and search and rescue units.

This report was administered online by Global Surveyz Research, an independent global research firm. Respondents hail from organizations across a total of 32 countries in North America, Europe, Central and South America, Asia Pacific and the Middle East. The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during July 2024. The answers to most of the non-numerical questions were randomized to prevent order bias in the answers.

Introduction and Key Findings

Key Findings

1 GenAI, group messaging apps and satellite internet are the top technologies fueling crime.

GenAI technologies have made it easier for criminals to produce convincing videos, audio files and textual content such as emails and documents, which is fueling criminal activities. More than half (55%) of LEAs surveyed report that GenAI-powered chatbots are the top technology enabling criminals to accelerate crime (Figure 1), while 38% point to the growing use of deepfake videos and audio produced by GenAI tools.

The increased adoption of group messaging platforms, such as Telegram and Discord, was highlighted by 54% of LEAs, while 40% of LEAs drew attention to satellite communications services such as Starlink, which are increasingly affordable and accessible. Criminals are leveraging these technologies to stay under the radar and more easily evade detection by authorities.

2 LEAs are combatting diverse threats, including terrorism, that extend beyond their traditional mandate.

The top security threats being tackled by LEAs include cybercrime (39%), organized crime (35%) and migrant smuggling and border security (29%), as seen in Figure 3. LEAs are also tackling terror-related threats outside their traditional policing mandate – 28% of LEAs report extremism and radicalization as a top challenge, coupled with 27% of organizations increasingly confronting growing ties between criminal networks and terror groups.

3 39% of LEAs are unable to resolve their investigations in a reasonable timeframe.

A significant portion of LEAs surveyed (39%) admit they are typically unable to effectively resolve their investigations (Figure 4). While the survey highlights several critical factors that contribute to this troubling situation, the ability to access and use relevant data sources is clearly one piece of the puzzle. More than half (53%) of the respondents reported that their inability to access relevant data is the top technological pain point causing delays in resolving investigations (Figure 5).

Key Findings

4 Gathering data isn't enough - 79% of LEAs struggle to unlock the insights they need.

Modern investigations require gathering and analyzing volumes of digital data such as communications records, images, videos, documents, social media and more. 46% of LEAs report challenges with both gathering data for court-admissible evidence as well as then analyzing it to generate intelligence and insights, while an additional 33% of LEAs specifically say that analyzing the data is the most challenging part of the process for them (Figure 7).

We took a closer look at LEAs reporting that generating intelligence and insights is most challenging aspect for them by their ability to successfully resolve investigations in a reasonable time frame (Figure 8). We see that analyzing the data is most challenging for those organizations are never or rarely able to resolve their investigations (48%). Clearly, analyzing data is a key stumbling block, and the more effectively LEAs are able generate intelligence and insights from digital data, the more successfully they succeed in resolving investigations.

5 Lack of cooperation and collaboration top the list of non-tech barriers to effective investigations.

LEAs report that the leading non-technological roadblocks leading to delays in investigations is the lack of cooperation with other agencies (37%), tied closely with the lack of collaboration within organizations (30%), as seen in Figure 6. In today's world, crime knows no limits, with criminal organizations not only committing a wider range of crimes, but also increasingly conducting their illicit schemes across international borders. This is proving challenging for agencies used to operating within fixed borders, both within their own organizations – due to siloed teams and data – and when it comes to sharing information with other domestic and foreign security organizations in a timely manner. The right technology solutions can enable efficient information sharing and collaboration, while ensuring compartmentalization and information security.

LEAs also report that their investigations are delayed due to staffing issues, including lack of staff with relevant skills (33%) and staff shortages in general (32%). These challenges can be alleviated by technology solutions designed to simplify and accelerate complex investigations, without requiring specialized skillsets, and to improve overall effectiveness even with limited staff.

6 LEAs see predictive analytics and GenAI as game-changers for accelerating investigations.

LEAs anticipate that the technologies that will be most impactful in accelerating their investigations in the coming year are AI-powered predictive analytics (48%) and GenAI for data exploration and analysis (47%), as seen in Figure 9. Unsurprisingly, it's the largest organizations that see the most value in AI (Figure 10), because they typically have more data at their disposal, and are generally better equipped to adopt and successfully use advanced technologies.

Survey Report Findings

Top Technologies Enabling Criminals to Accelerate Crime and Evade Detection

GenAI technologies have made it easier for criminals to produce convincing text, video and audio content, significantly fueling fraudulent and criminal activities. **More than half (55%) of LEAs say GenAI-powered chatbots are the top technology enabling criminals,** while 38% point to the growing use of deepfake videos and audio produced by GenAI tools.

LEAs also highlight several technologies that help criminals operate under the radar. 54% cite group messaging apps, such as Telegram and Discord, which criminals are increasingly using both for communications as well as for buying and selling malware, stolen data, illegal goods and illicit services. **40% identify satellite communications as a key enabler allowing criminals to evade detection**, due to increasingly affordable and accessible satellite services such as Starlink. **31% point to the role of** cryptocurrencies, which allow criminals to conduct financial transactions and launder illegal gains with seeming anonymity.

LEAs that are rarely or never able to effectively resolve investigations overwhelmingly view group messaging apps as a significant driver of crime (83%), as seen in Figure 2. This indicates that LEAs lacking the necessary technology solutions to address criminal activities on these platforms face increased challenges in their investigations.

Figure 1

Top Technologies Enabling Criminals

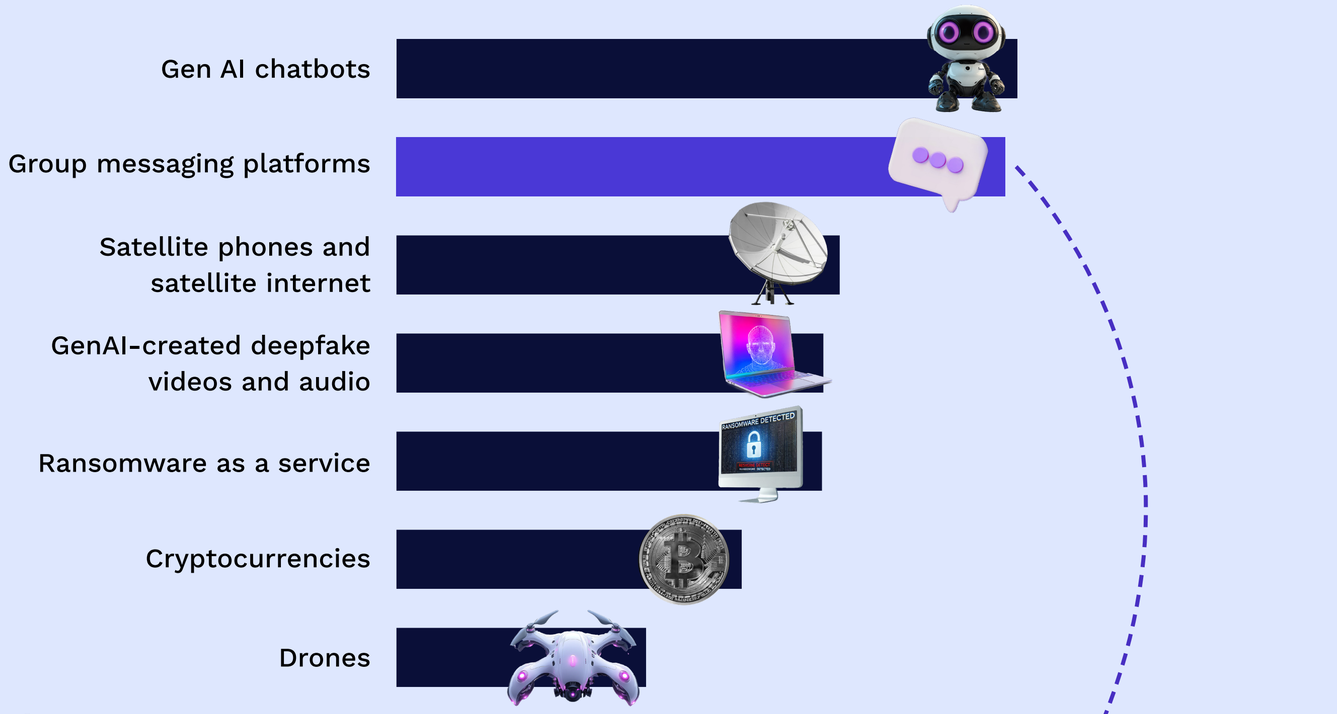


Figure 2

Group Messaging Platforms as a Top Crime Enabler in Relation to Ability of LEAs to Successfully Resolve Investigations

* Question allowed more than one answer and as a result, percentages will add up to more than 100%

Top Threats Tackled by Law Enforcement

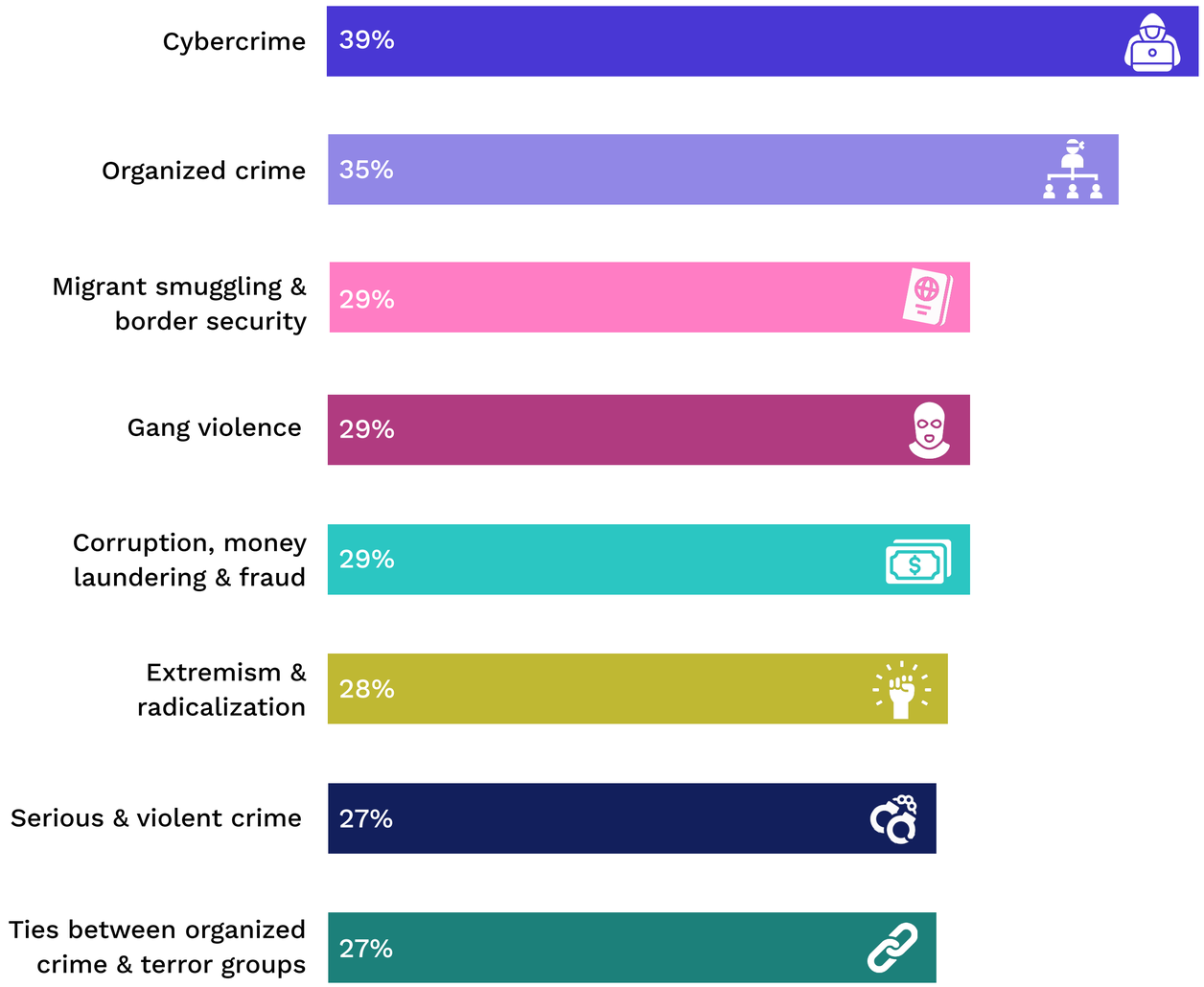
Of the top threats LEAs are combating, cybercrime (39%) and organized crime (35%) stand out as the most significant challenges, followed by migrant smuggling and border security (29%), which is a growing global concern.

While the LEAs surveyed have a range of different mandates, most of the other top threats reported by the respondents are rated almost equally (ranging between 27-29%), reflecting that authorities are tackling multiple threats across the board, and suggesting that many types of investigations require the collaboration of multiple types of law enforcement organizations working in tandem.

Notably, two of the reported threats - extremism and radicalization (28%) and the links between organized crime and terror groups (27%) - highlight that many law enforcement organizations not only must tackle the criminal activities which are traditionally defined in their mandate, but must also increasingly grapple with terror-related challenges.

Figure 3

Top Threats Tackled by Law Enforcement Organizations



* Question allowed more than one answer and as a result, percentages will add up to more than 100%

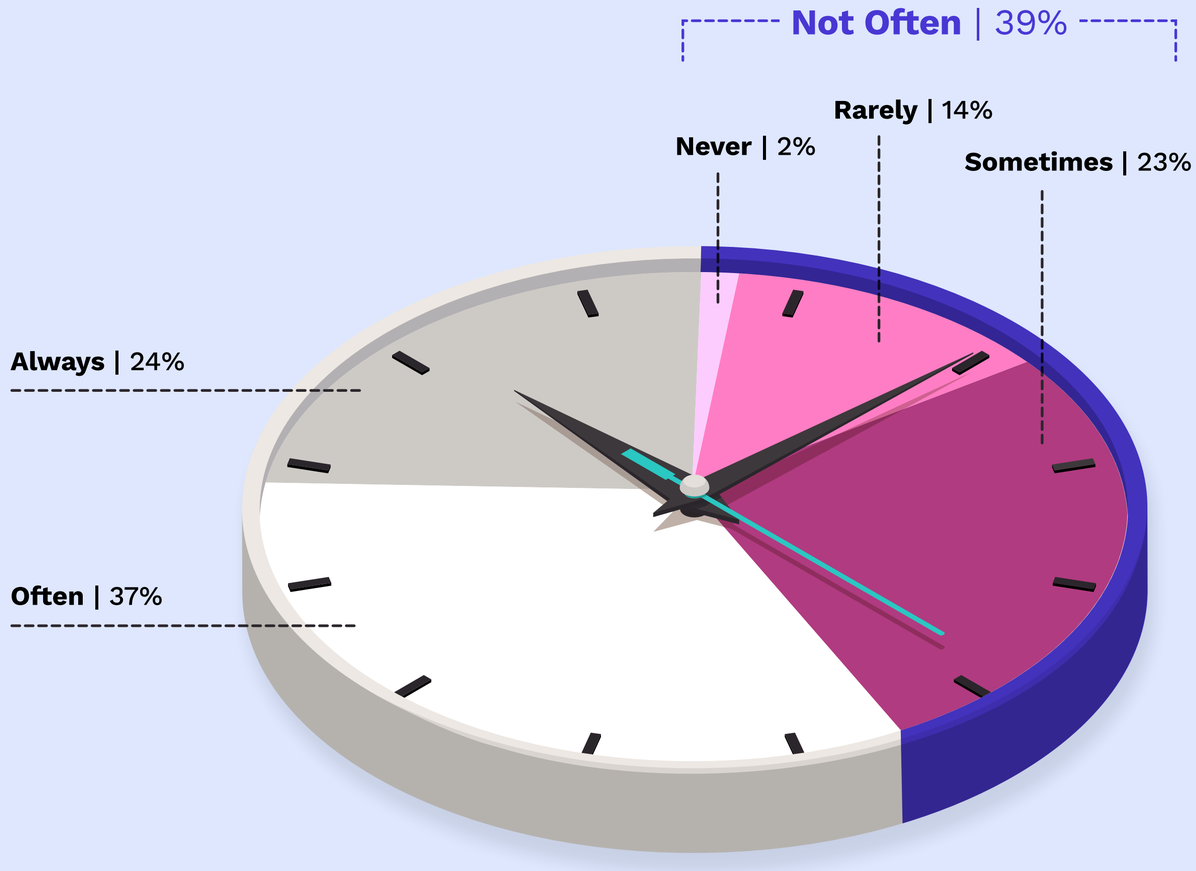
Ability to Successfully Resolve Investigations Within Reasonable Timeframes

A significant portion of LEAs surveyed admit they are typically unable to successfully resolve investigations within a reasonable timeframe: 2% report they never resolve investigations efficiently, 14% rarely achieve efficient resolutions, and 23% are only occasionally successful in doing so.

This highlights a widespread challenge in law enforcement investigations and operations, and as seen in later sections of the survey, technology solutions can play a significant role in helping LEAs to enhance their capabilities and improve their investigation outcomes.

Figure 4

Ability to Successfully Resolve Investigations Within Reasonable Timeframes



Top Technology Pain Points

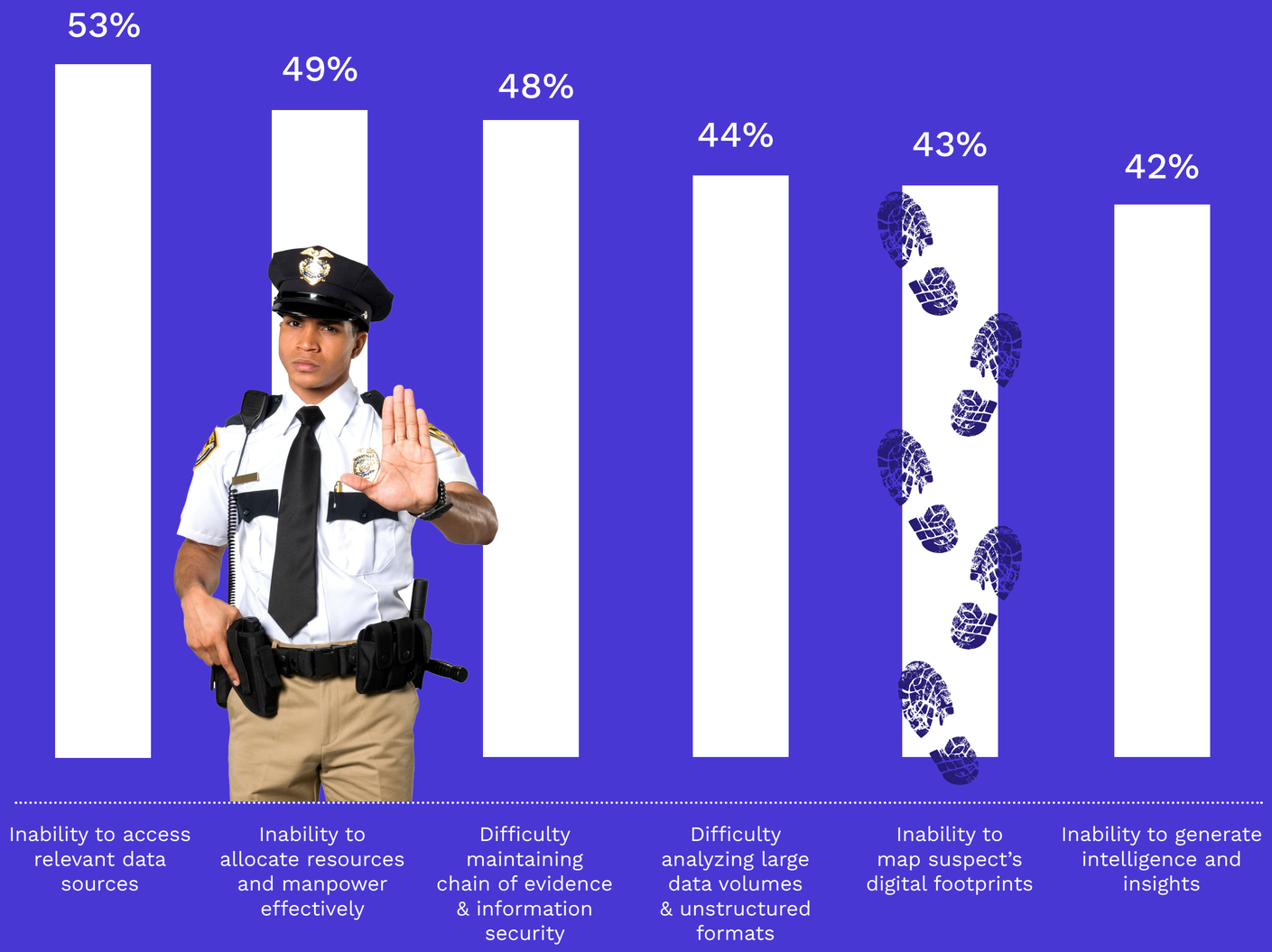
More than half of the law enforcement agencies surveyed (53%) say that their inability to access relevant data sources is the top technological pain point causing delays in resolving investigations.

In today's increasingly digitized world, a diverse and ever-expanding array of data sources are critical for policing work – ranging from criminal records, government databases, cryptocurrency transactions, LPR cameras, social media, financial transactions and more. The survey results indicate that many law enforcement organizations currently lack the right technological solutions or tools to access critical data sources.

Other leading technology pain points that create investigation roadblocks are the inability to plan and allocate resources and manpower effectively (49%), and difficulty in maintaining chain of evidence or ensuring information security (48%). The importance of maintaining chain of evidence is unsurprising, given that law enforcement authorities must abide by strict standards and require evidence that not only must be submissible in court but also compelling enough to enable successful prosecutions.

Figure 5

Top Technological Pain Points



* Question allowed more than one answer and as a result, percentages will add up to more than 100%

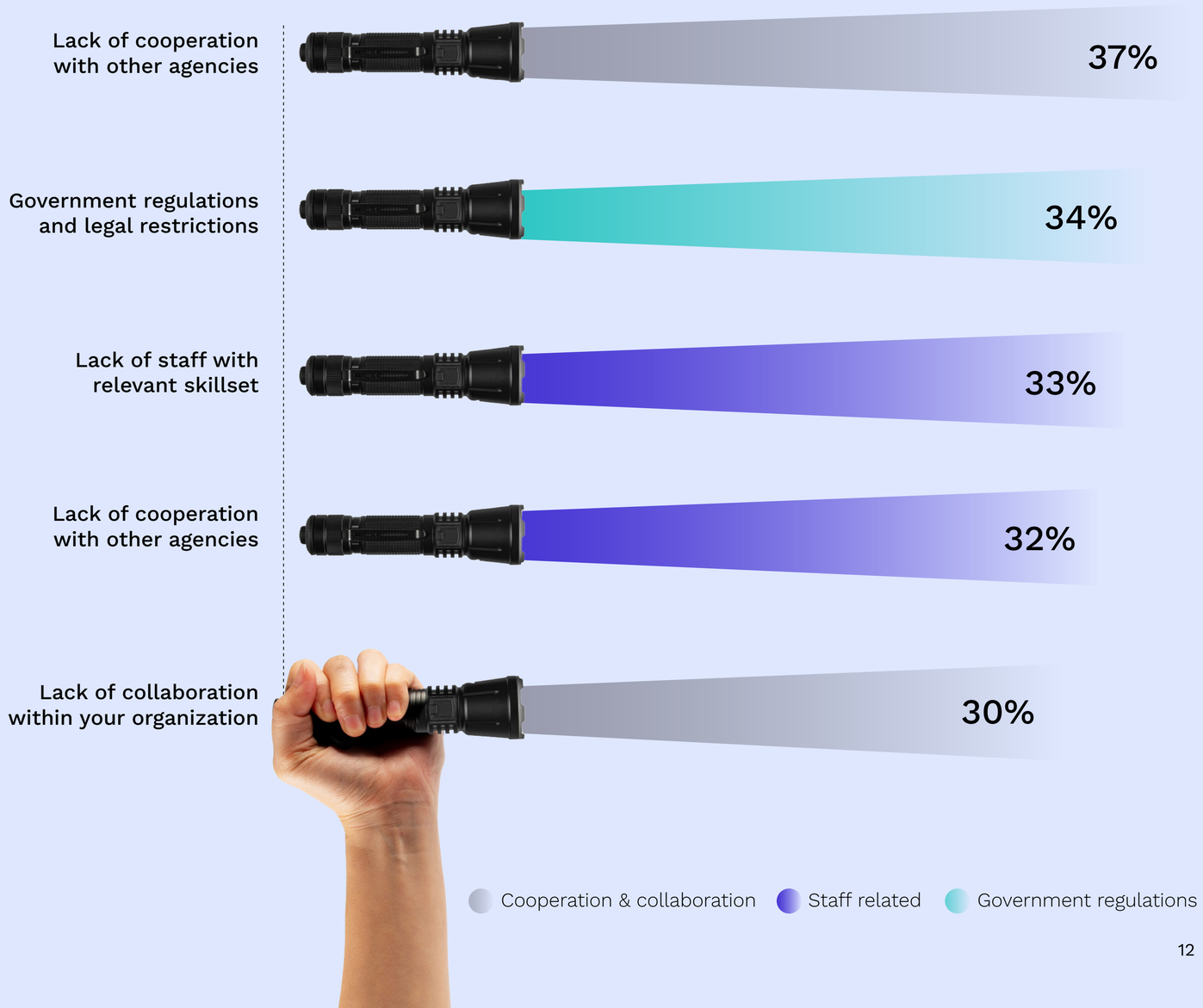
Top Non-Tech Causes for Investigation Delays

In addition to technology-related pain points, the survey surfaced three main roadblocks to successful resolving investigations:

1. **The most painful challenge is the lack of cooperation with other agencies (37%), which is also tied closely with the lack of collaboration within organizations (30%).** Boundaries are blurring in the criminal landscape, with cross-border crime on the rise and criminal organizations branching out to additional types of criminal activities. This new reality is difficult for law enforcement agencies that are used to operating within fixed boundaries, both within their own organizations – due to siloed teams and data, for example – and also when it comes to sharing information and insights with other organizations in a timely manner.
2. The second most cited non-technological cause for stalled investigations relates to the **government regulations and legal restrictions** (34%) which LEAs operate under.
3. **Additionally, staffing issues pose a major stumbling block, with 33% of organizations citing a lack of staff with relevant skills, and 32% suffering from general manpower shortages.** In both cases, these challenges can be alleviated with technology solutions designed to simplify complex investigations, by visualizing key insights and automatically extracting intelligence from data without the need for data scientists, and improving overall efficiency of investigations so that even limited staff can achieve more.

Figure 6

Top Non-Technological Causes for Investigation Delays



* Question allowed more than one answer and as a result, percentages will add up to more than 100%

Challenges in Leveraging Digital Data During Investigations

Digital data has become an integral aspect of modern investigations, with vast quantities of communications records, images, videos, documents, digital forensics and social media routinely needing to be gathered and analyzed to obtain evidence and uncover clues and insights.

When asked what they find more challenging when it comes to working with digital data during investigations – 33% of the respondents say that generating intelligence and insights from digital data is most challenging, 20% say that gathering court-admissible evidence is most challenging, 46% say that both are equally challenging, and only 1% say that they don't find either challenging (Figure 7).

When further examining those respondents who struggle with generating intelligence and insights out of digital data, in relation to their ability to successfully resolve investigations (seen earlier in Figure 4) – we observe that the share of organizations reporting that extracting intelligence and insights is the most challenging aspect for them climbs to 48% (Figure 8). In other words, the ability to generate insights is a critical factor for investigation success.

There is a clear link between the difficulties law enforcement agencies face in generating intelligence and insights from digital data, and their inability to successfully resolve investigations.

Figure 7

Challenges with Digital Data During Investigations

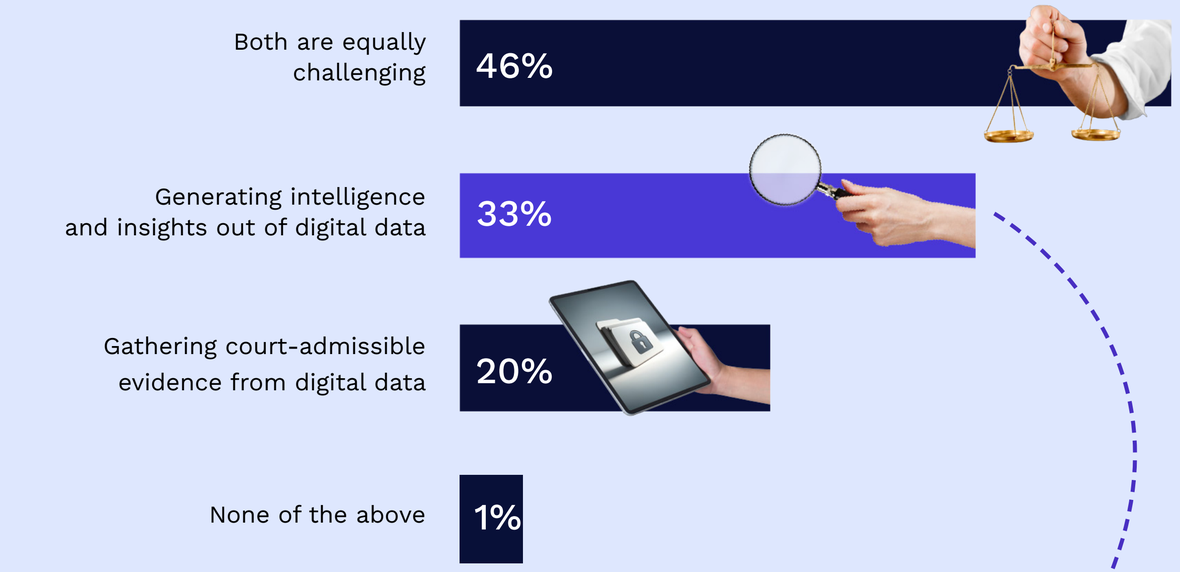


Figure 8

Difficulty in Generating Intelligence and Insights from Digital Data in Relation to Ability to Successfully Resolve Investigations

Top Technologies to Accelerate Investigations

The top technologies that law enforcement organizations believe will have the most impact in accelerating investigations are AI-powered predictive analytics (48%) and GenAI for data exploration and analysis (47%), as seen in Figure 9.

Although GenAI technologies are still evolving, they hold significant promise for addressing the challenge of information overload in investigations. Gen AI has the potential to help investigators and analysts in a myriad of ways, for example by enabling the querying of data using simple questions in natural language, and summarizing large volumes of text to extract key insights with the click of a mouse.

Clearly there is a strong focus currently on GenAI, with GenAI chatbots and tools considered to be the top technologies enabling criminals to accelerate crime and evade detection (Figure 1).

When further examining those who rated AI-powered predictive analytics as the top technology to accelerate investigations, we see that the bigger the organization size, the more they value the potential of AI (Figure 10). This makes sense given that larger law enforcement organizations tend to have access to more data, and since they are generally more technologically advanced, they are also better equipped to put new AI technologies into practice.

Figure 9

Top Technologies to Accelerate Investigations

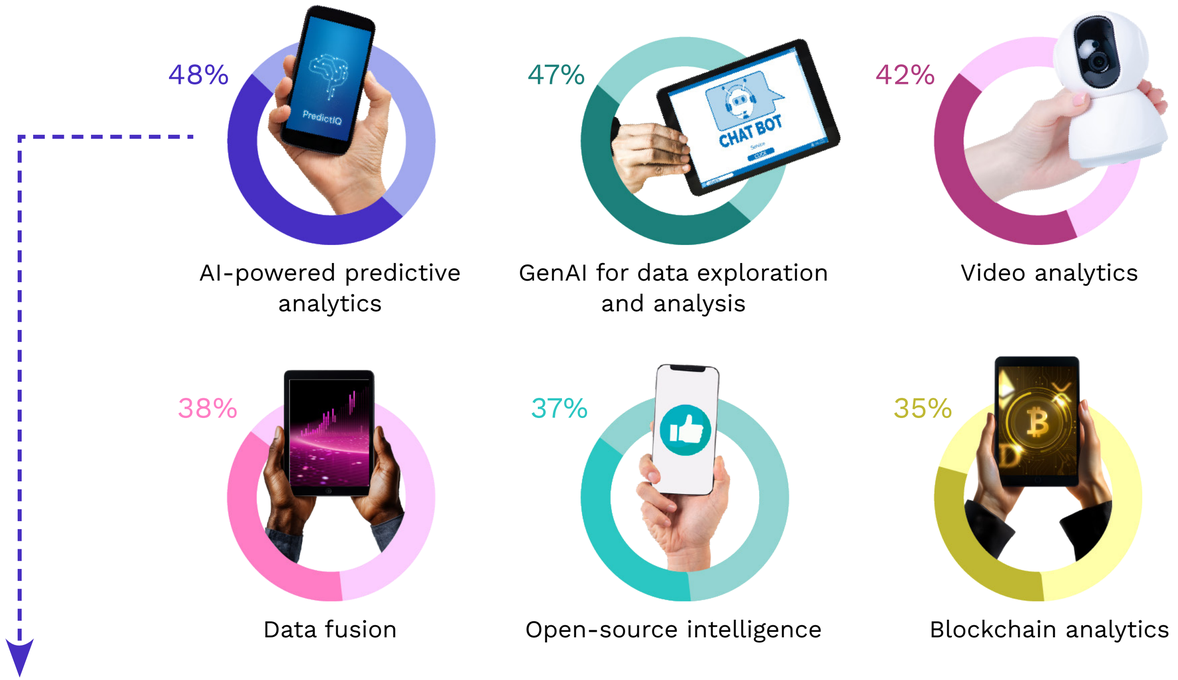


Figure 10

Use of AI-Powered Predictive Analytics by Organization Size

Use of Blockchain Analytics Tools

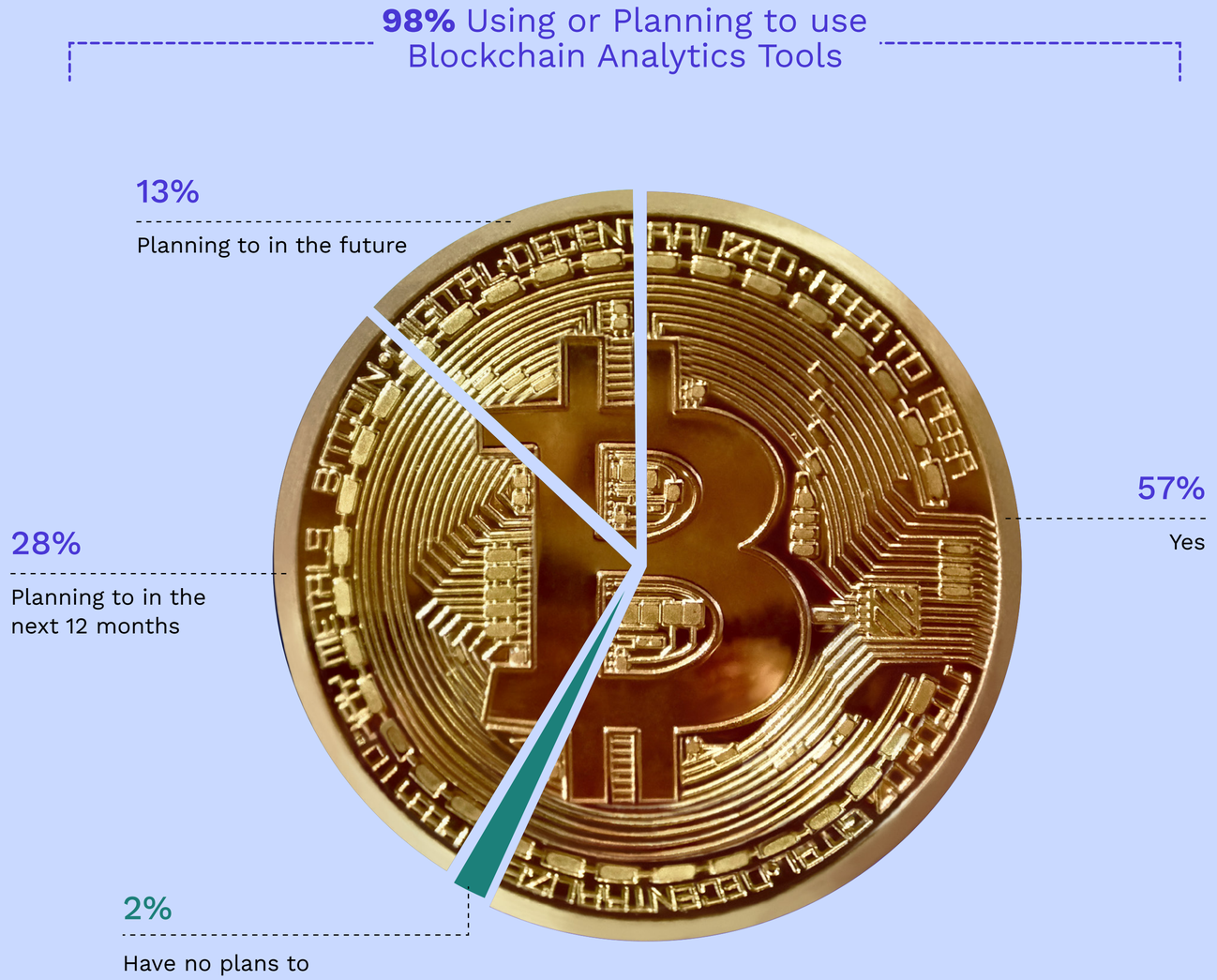
We asked respondents whether their organizations are using blockchain analytics tools to investigate cryptocurrency transactions and wallets suspected of being used for illicit activities.

A resounding 98% of them indicated that their organizations are either already using blockchain analytics tools (57%) or planning to use them (43%) – either as early as the next 12 months (28%) or in the future (13%).

With only 2% of the respondents indicating they have no plans to use blockchain analytics, it is clear that the vast majority of law enforcement organizations see great value in using blockchain analytics for combatting crime. This is unsurprising as cryptocurrencies today are being used to conduct and facilitate many types of crime including fraud, money laundering, terror funding and cybercrime.

Figure 11

Use of Blockchain Analytics Tools



Demographics

Geographical Region, Type of Organization and Organization Size

Figure 12

Geographical Region

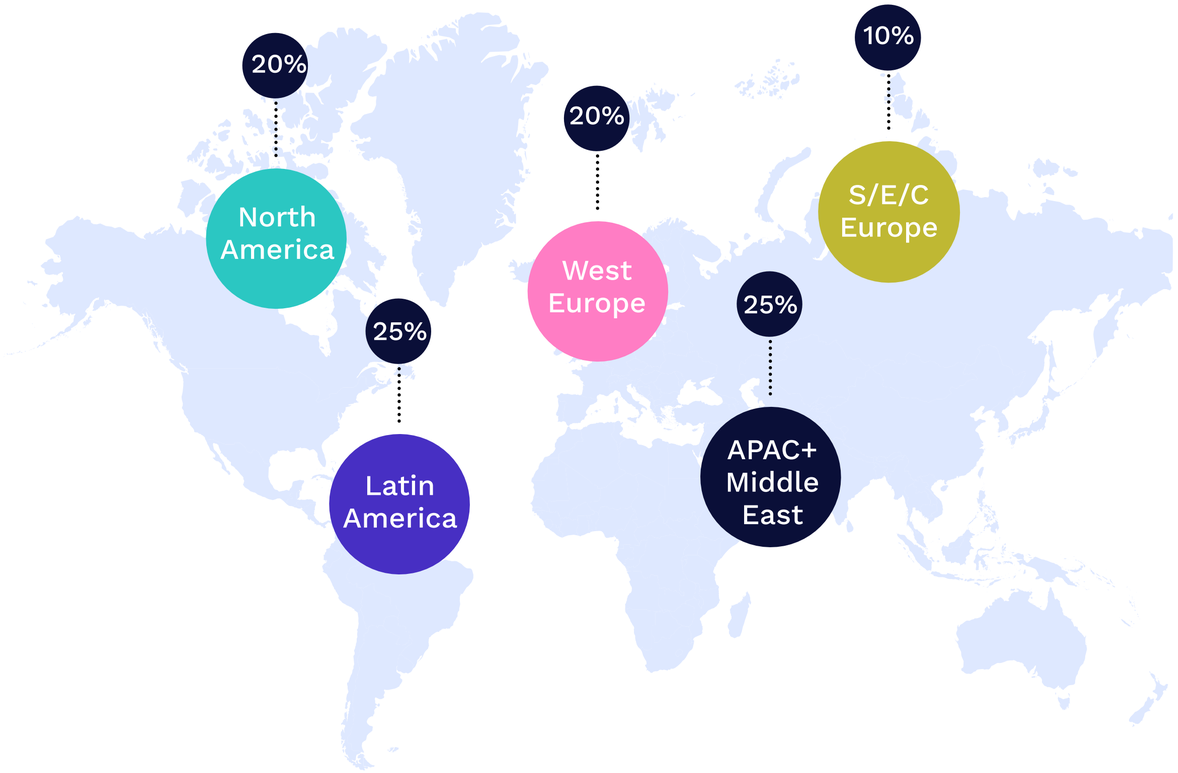


Figure 13

Type of Organizations

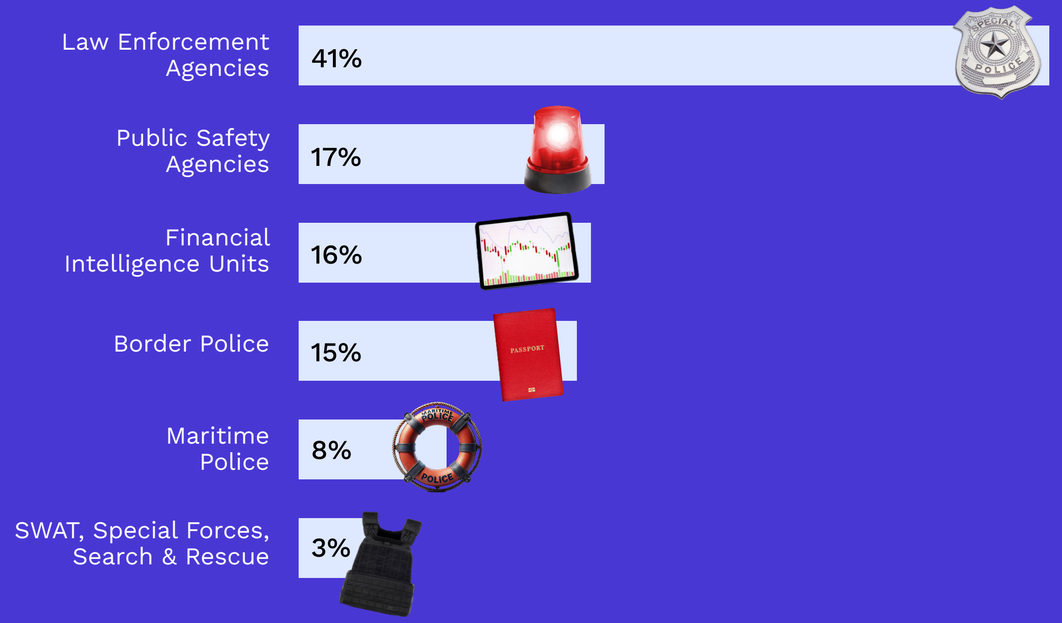
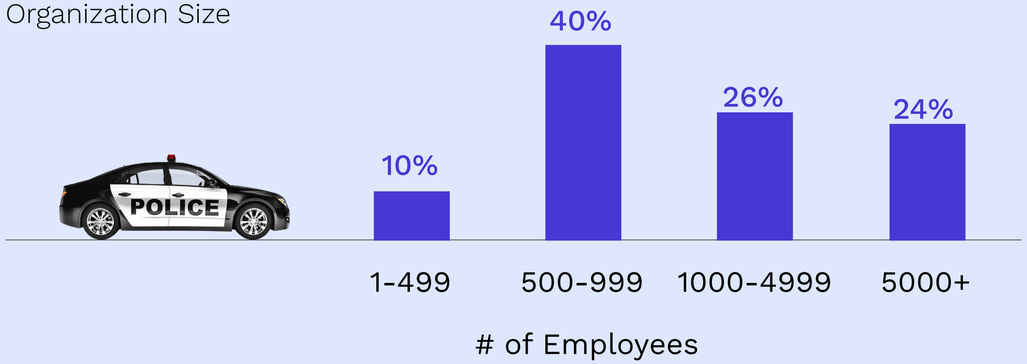


Figure 14

Organization Size



Department Purpose and Seniority

Figure 15

Department Purpose

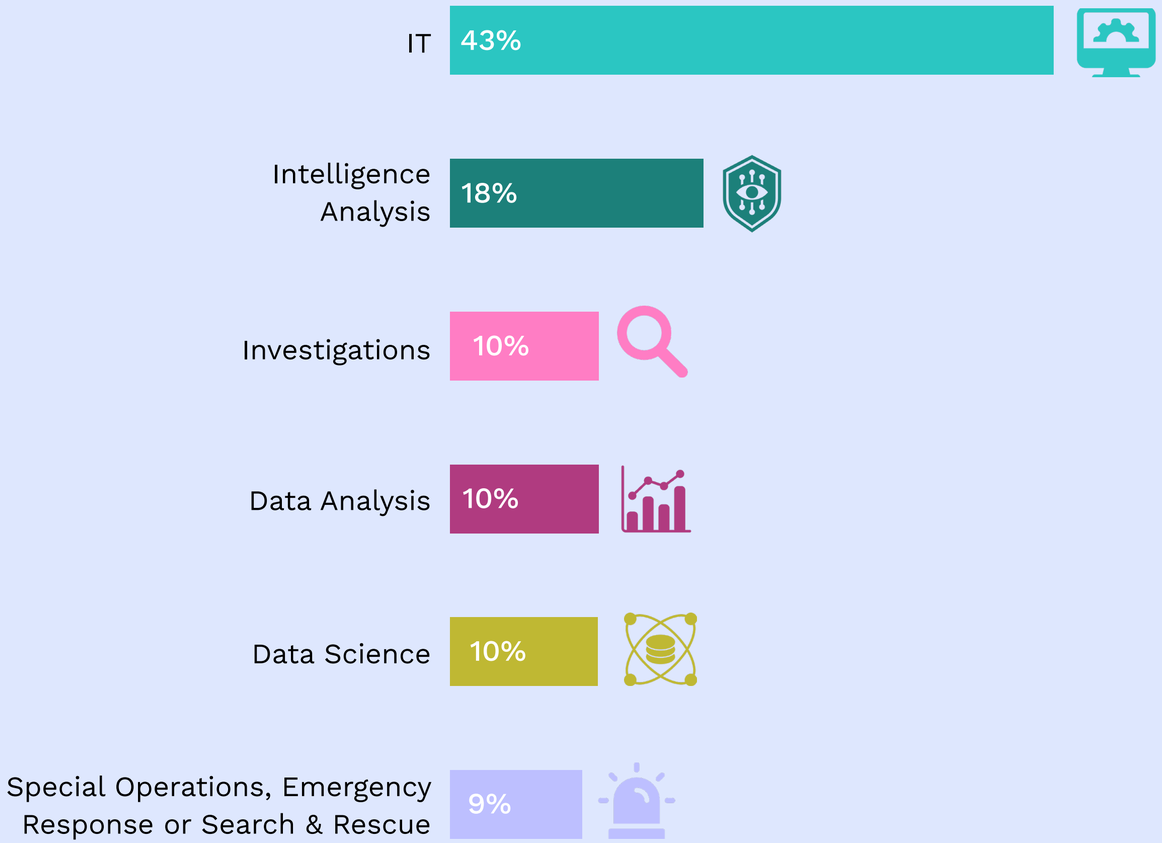
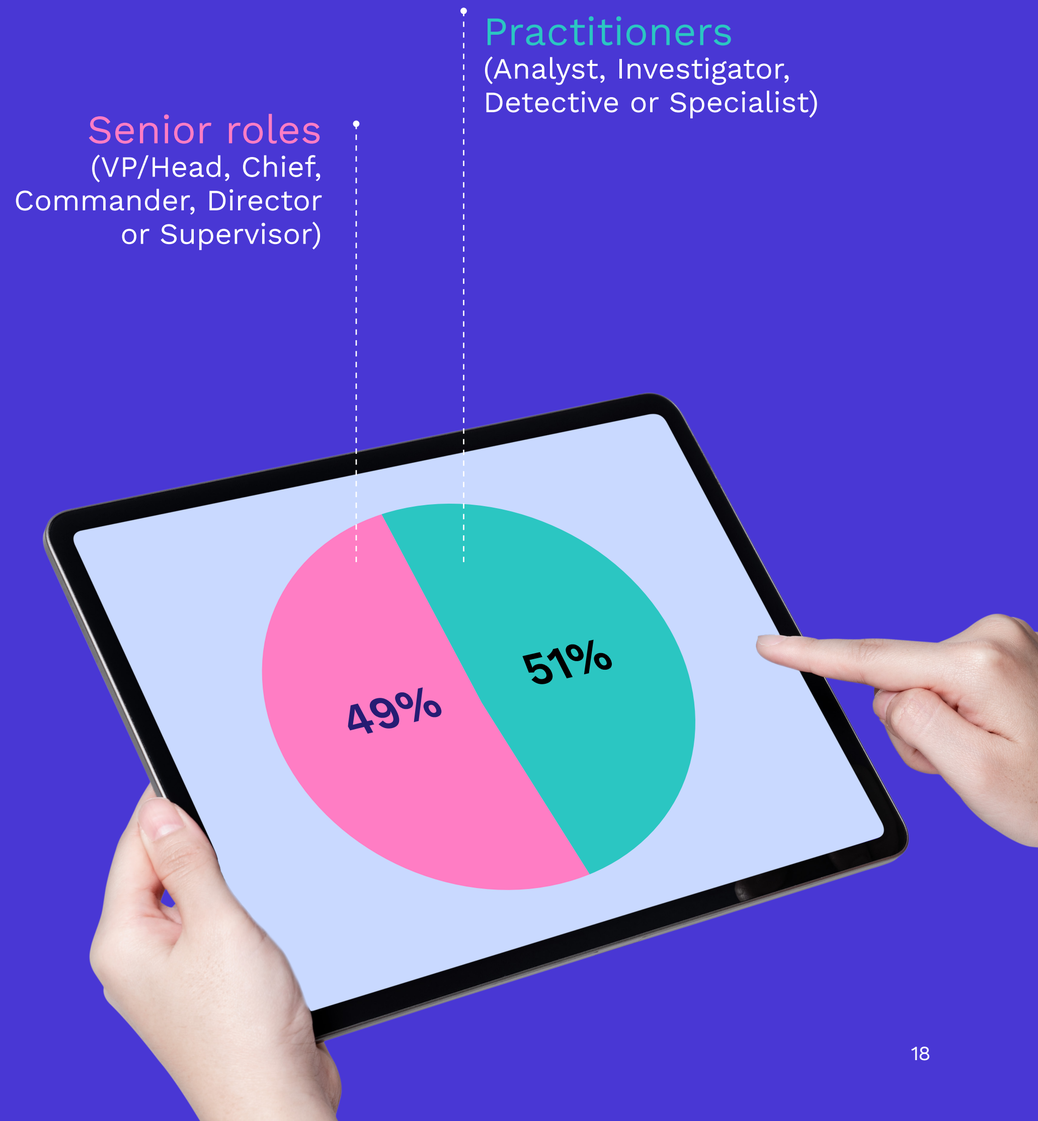


Figure 16

Seniority



Want to learn more?

Top AI Tech Trends for Law Enforcement

Discover the top 5 AI trends empowering law enforcement organizations today

Read Now

ChatGPT & Crime: What Law Enforcement Needs to Know

Explore how GenAI chatbots are fueling crime, yet also equipping authorities with stronger capabilities

Read Now

2024 Threat Intelligence Landscape

Check out the latest developments in cybercrime and learn how threat intelligence can help

Read Now

Financial Investigations in the Crypto Age

Learn how criminals are leveraging cryptocurrencies, and how blockchain analytics can help accelerate investigations

Read Now

About Cognyte

Cognyte is a global leader in investigative analytics software that empowers leading law enforcement, intelligence and government organizations with Actionable Intelligence for a Safer World™. Our portfolio of solutions is designed to help our customers accelerate and conduct investigations, intelligence analysis and field operations, and enable smarter decision-making. Over 400 customers around the world rely on our solutions to detect and combat crime, terror activities, and threats to public safety and national security.

Visit the Cognyte website today!

Cognyte