Government Business Council

Threat Hunting in the Federal Government

A Candid Survey of Public Sector Leaders on Cybersecurity and Preemptive Tactics

Underwritten by

elastic

May 2019

Table of Contents

Overview

Purpose

The best cybersecurity programs today aren't defensive, but offensive. It's no longer sufficient security to react when an alert identifies adversaries entering a network. The next frontier of cybersecurity employs professional threat hunters, skilled human analysts capable of studying a range of threat intelligence to pursue and eliminate potential threats *before* they emerge. These human analysts are skilled at using not just one, but a combination of tools to automate anomaly detection and follow hunches in real time by running ad hoc queries on massive amounts of data. While threat hunters have seen growing popularity in the private sector, their recognition and deployment in government still remains largely unknown.

To understand if government agencies are transitioning to a proactive security mindset grounded in threat hunting best practices and technologies, Government Business Council (GBC) conducted an in-depth research study of federal employees on the subject of threat hunting and preemptive cybersecurity tactics.

Research Methodology

In January 2019, GBC released a survey exploring perceptions of cybersecurity, data requirements, and threat hunting within the federal workforce. More than 930 respondents from the federal government participated in the survey; among this cohort, approximately 200 respondents were qualified to finish the survey after acknowledging threat hunting capabilities at their organization. 54% of respondents self-identified as GS/GM-13 rank or higher, and 90% claimed some degree of familiarity with their organization's cybersecurity programs.

Executive Summary

Respondents understand that increased data needs will demand new solutions

Successful navigation of cybersecurity challenges in 2019 will hinge on how agencies harness the rapid influx of large amounts of data from disparate sources. 3 in 4 respondents anticipate their data needs will increase to accommodate requirements for retaining and reporting ever greater amounts of data. While 75% believe data quantity and data quality are equally important considerations for effective cybersecurity, others place more emphasis on quality (24%) and making sure that detection and response procedures are executed based on reliable, unbiased sources.

More see cybersecurity in proactive terms, but formalized threat hunting programs remain the exception rather than the rule

Although more respondents see their organization's cybersecurity posture as proactive (44%) than reactive (29%), less than a third say their organization actually hunts for threats. When it comes to cybersecurity in general, a significant majority of respondents (85%) stress the need for human input and oversight while downplaying the ability of automated software to tackle these challenges on its own. A majority of organizations plan to devote more skilled workers and acquire new technology to address growing data requirements in 2019.

Even among threat hunting practitioners, intrusion detection is seen as the most reliable tool

When asked about tools they need to conduct threat hunting operations, respondents place greatest emphasis on intrusion detection and prevention systems, which does not by itself entail proactive hunting for threats. By comparison, just 30% identify threat intelligence as a tool required to initiate successful threat hunting.

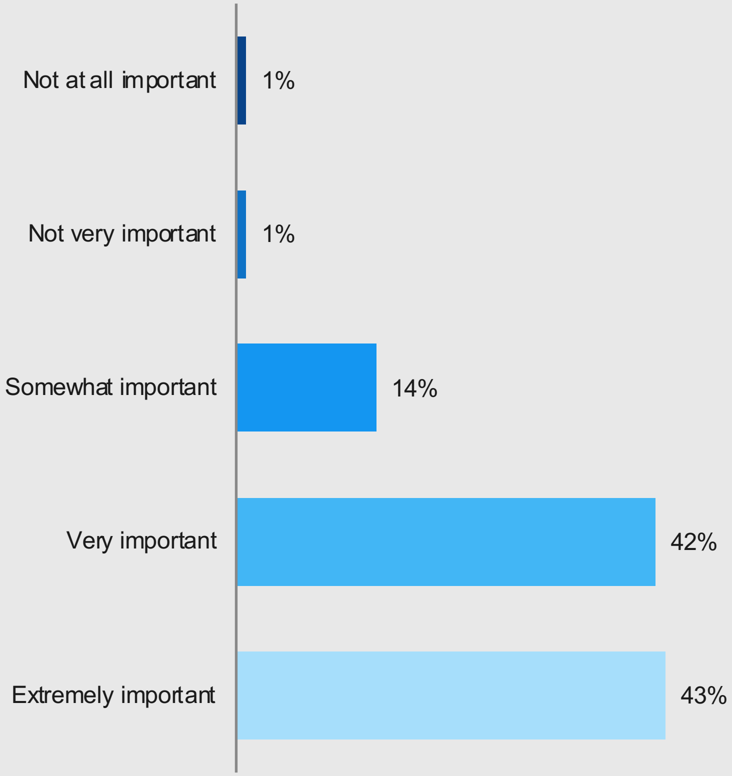
Agencies plan to invest in threat hunting technologies to increase confidence in their organization's security. When considering ways to prioritize threat hunting in 2019, respondents value 'better detection' and 'more automated tools' over recruiting more human workers with investigative skill sets. 66% of respondents anticipate an increase in investments to threat hunting this year, not surprising given that a significant majority feel threat hunting has increased confidence in their organization's security.

Research Findings

By a significant margin, respondents see human involvement as critical to good cybersecurity

As cyber technology and autonomous systems have advanced, to what extent should humans maintain an active role in cybersecurity measures? Government respondents show a clear consensus: 85% believe human input/oversight is very or extremely important to effective cybersecurity, in that it is 'inadequate to defend against threats without benefiting from human curation of threat information'.

How important is having human input/oversight when it comes to maintaining effective cybersecurity?



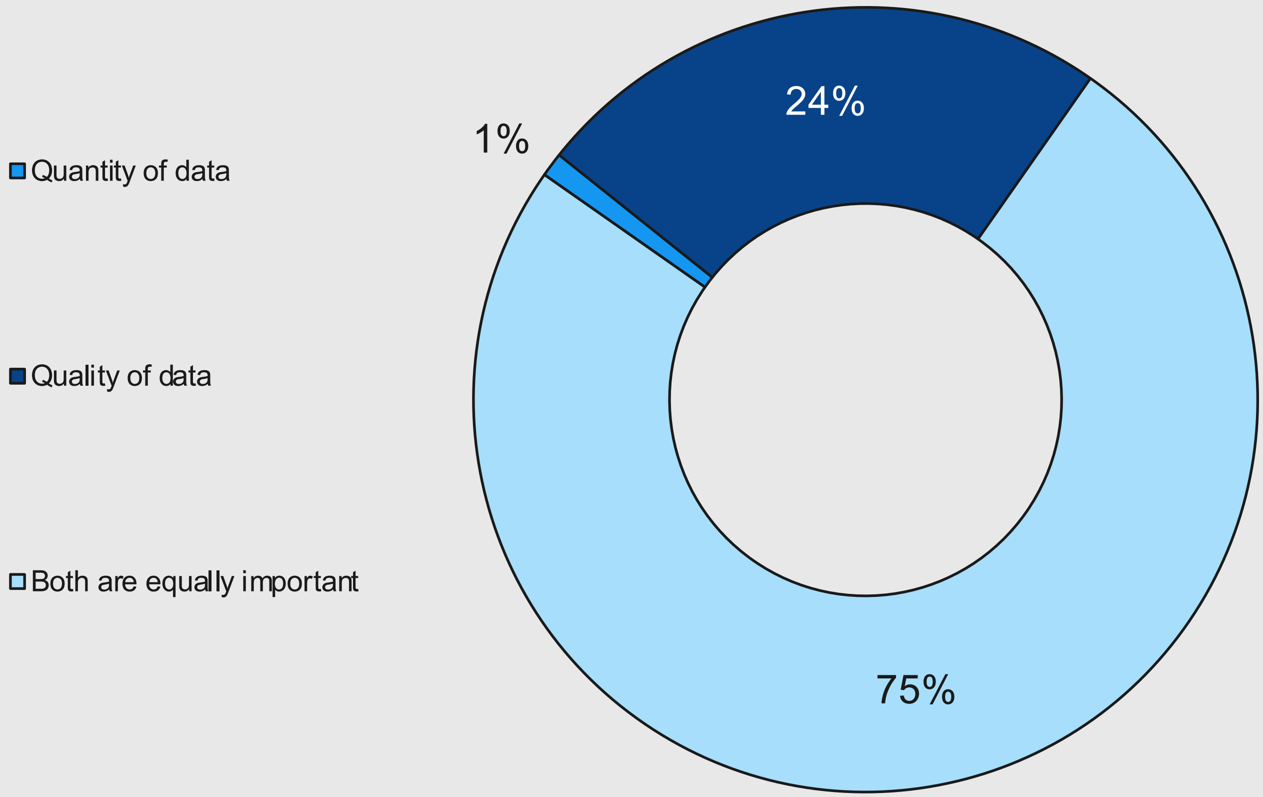
Percentage of respondents, n=797
Note: Percentages may not add up to 100% due to rounding

85%
of respondents believe human oversight is a very or extremely important contributor to effective cybersecurity.

3 in 4 respondents say quality and quantity of data are equally important to effective cybersecurity

Cybersecurity hinges on having available, actionable access to data, but is it quality or quantity of data that matters more? Most respondents place a premium on both aspects, insisting that each have their value; however, 24% feel that quality is a more effective determinant: for cybersecurity to make accurate conclusions, it must be able to interpret data that is accurate and devoid of bias.

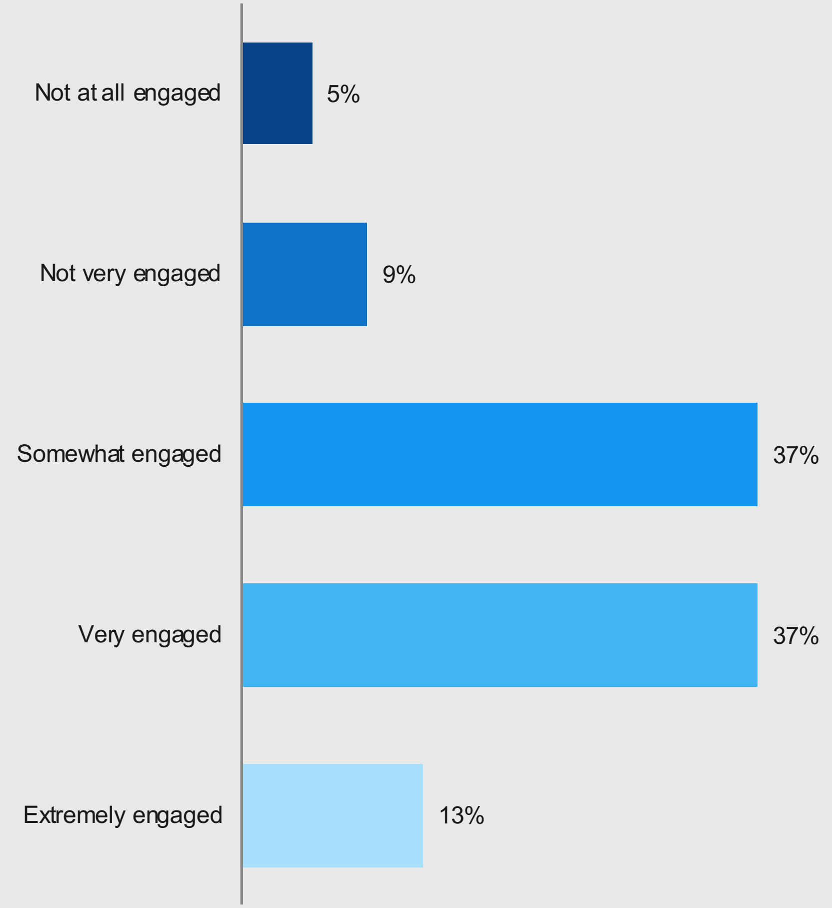
Which is a more important determinant for effective cybersecurity operations?



Percentage of all respondents, n=797
Note: Percentages may not add up to 100% due to rounding

A majority of respondents feel their organization takes cybersecurity seriously, but others point to continued room for growth

How engaged are your organization's employees when it comes to taking cybersecurity and cyber hygiene seriously?



Percentage of respondents, n=936
Note: Percentages may not add up to 100% due to rounding

1 in 2

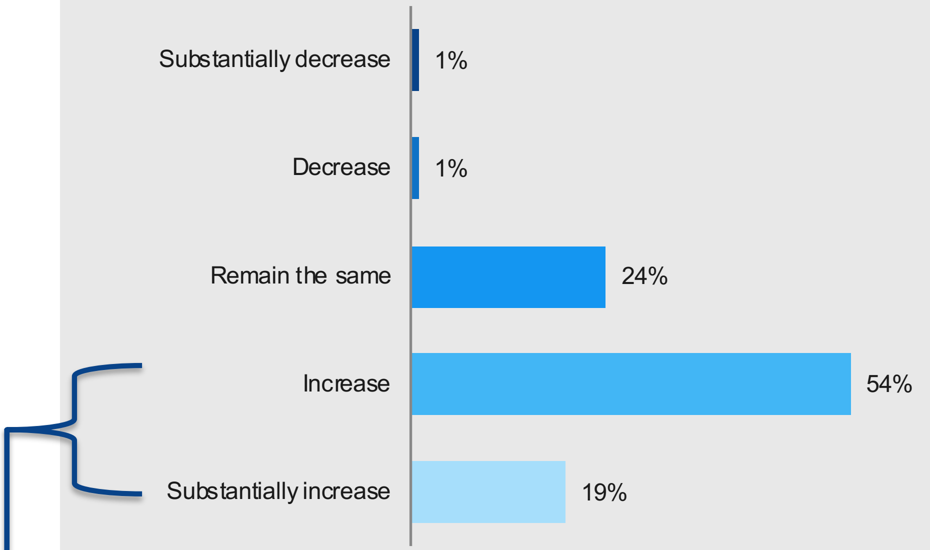
respondents feel their organization's employees are 'very' or 'extremely' engaged when it comes to cybersecurity and cyber hygiene.

> "DoD CIO, working in concert with DISA, is evaluating emerging architectures to **shift** the way the Department's networks are protected. This requires rethinking how we implement protections so that our ability to conduct operations is unimpeded but ensures that the network resists unauthorized activity and **makes it easier to detect bad actors**."

DoD CIO Dana Deasy

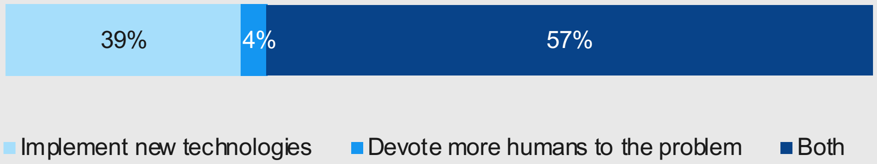
Growing data volumes escalate needs for more effective technologies and more skilled workers

"I anticipate my organization's data needs (e.g., volume, retention) will ______ in 2019 relative to the previous year."



Percentage of respondents, n=878
Note: Percentages may not add up to 100% due to rounding

How does your organization plan to address its growing data needs (e.g., volume, retention) in 2019?



Percentage of respondents, n=600
Note: Percentages may not add up to 100% due to rounding

73%
of respondents anticipate their organization's data requirements will increase or substantially increase in 2019.

39%
of those who indicated their data needs will increase in 2019, say they will address the growth *solely* through acquisition and implementation of new technology.

Government Perspective

Brian DeWyngaert Jr.
INFOSEC Specialist
U.S. Department of Homeland Security

"What forces do you think are responsible for the 73% of respondents who say their data needs will increase generally or substantially in 2019 relative to previous years?"

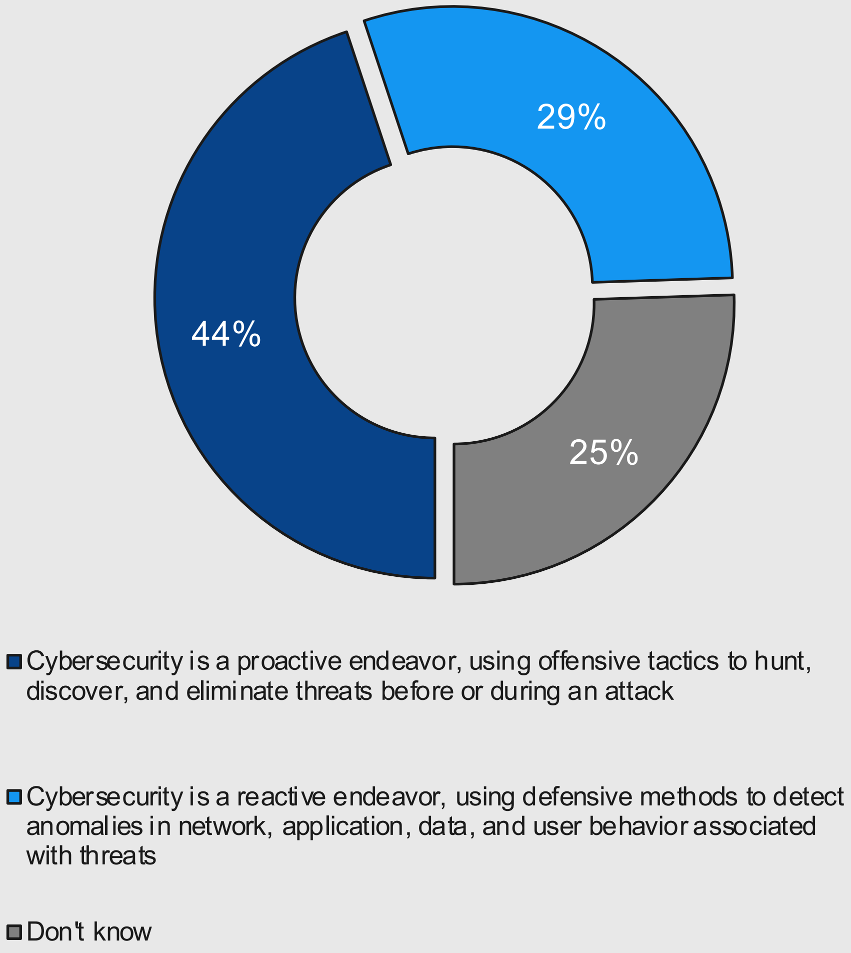
DeWyngaert: In our daily lives, our culture has driven to this information saturated society. Everyone wants to know everything about everything. We look at our enterprises and we're starting to be able to know more about our enterprises to a level of detail that we just couldn't get to before. With the cloud making the expansion so much easier, I think that from a technology perspective it's more prolific. Maybe now there is a possibility for a digital medium to last longer…with the way that storage is becoming so cheap. [The cloud] just makes it more accessible.

"What does that mean for holding up an effective cybersecurity program? How does the increase in data requirements complicate things?"

DeWyngaert: Oh I mean it absolutely complicates the [landscape]. As a CIO, you've got to try and get your arms around where all of your information is, who has access to it. You want to try to be protective of the information but still enable the mission for whoever's mission that is that requires that information. That gets complicated really fast because a lot of times we don't have really good processes in place for tracking when people onboard or when they leave. These requirements are there such that a lot of times people may have access to things they actually shouldn't. Or in the converse, sometimes our processes for onboarding are pretty poor and it takes a lot longer for us to be able to share information that could be critical for somebody else's job with them because they haven't been able to make it through the process.

Proactive cybersecurity tactics are on the rise, but reactive measures remain the norm for many

Which statement more accurately describes your organization's cybersecurity posture?



Percentage of respondents, n=936
Note: Percentages may not add up to 100% due to rounding

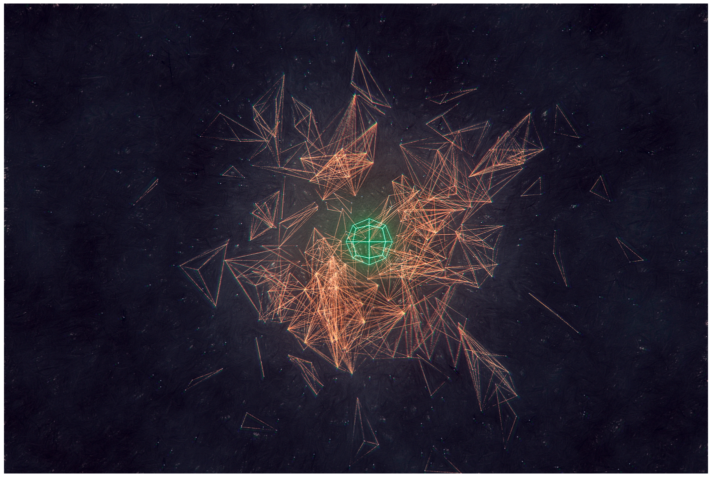
44%
of respondents say their agency uses proactive tactics to eliminate cybersecurity threats before or during an attack.

> "It's critical to stay ahead and not abreast. I don't really think we all understand the absolute danger and threat that cyberwar, spying, and stealing pose [to our networks]."

Anonymous Survey Respondent

Threat Hunting In Action

As threat hunting capabilities gain steam, government agencies must grapple with blind spots



Scenario: A series of home burglaries have occurred in your neighborhood, and you know the perpetrator's approach consists of entering through the garage. Instead of simply locking all the potential entry points into the house, you might also consider installing a camera in your garage to anticipate such an incident and snag the intruder in the act.

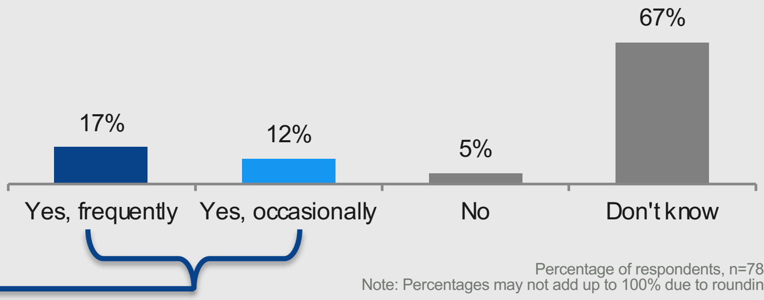
Threat hunting operates by the same principle: based on available threat intelligence – indicators of compromise (IOCs), as well as tools, techniques, or procedures (TTP) used by an attacker -- a human analyst creates a **hypothesis** about how the intruder may enter and takes **proactive measures** to eliminate or reduce the likelihood of infiltration *before* it takes place.

More government agencies claim to be employing threat hunt teams, but are they leveraging the right tools, human expertise, and strategic consideration of risks to execute successful hunts?

Less than a third of respondents acknowledge threat hunting operations in their agency

It is not uncommon for agencies to keep knowledge of threat hunting programs and practices to limited personnel. As would be expected, nearly two-thirds of respondents are not familiar with their organization's threat hunting practices.

Does your organization use proactive security practices like threat hunting?

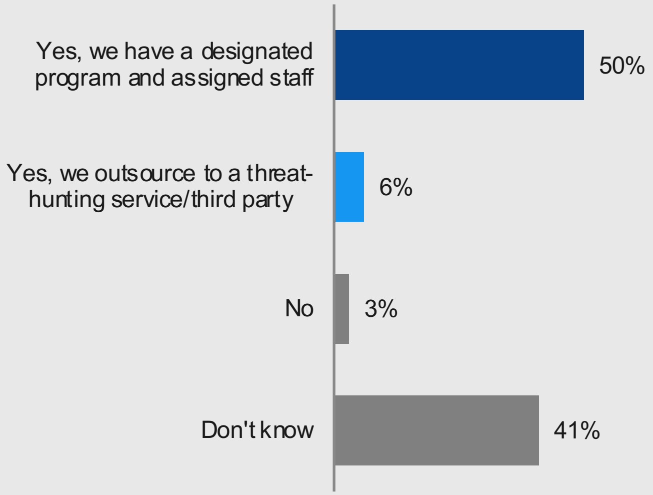


Percentage of respondents, n=782
Note: Percentages may not add up to 100% due to rounding

29%
of respondents say their organization deploys proactive measures like threat hunting to remove threats before they manifest as attacks.

At this point, ***only*** respondents who acknowledged 'frequent' or 'occasional' threat hunting practices at their agency were allowed to continue taking the survey in order to ensure qualified responses.

Does your organization have a formal threat hunting methodology with dedicated personnel assigned to that mission?



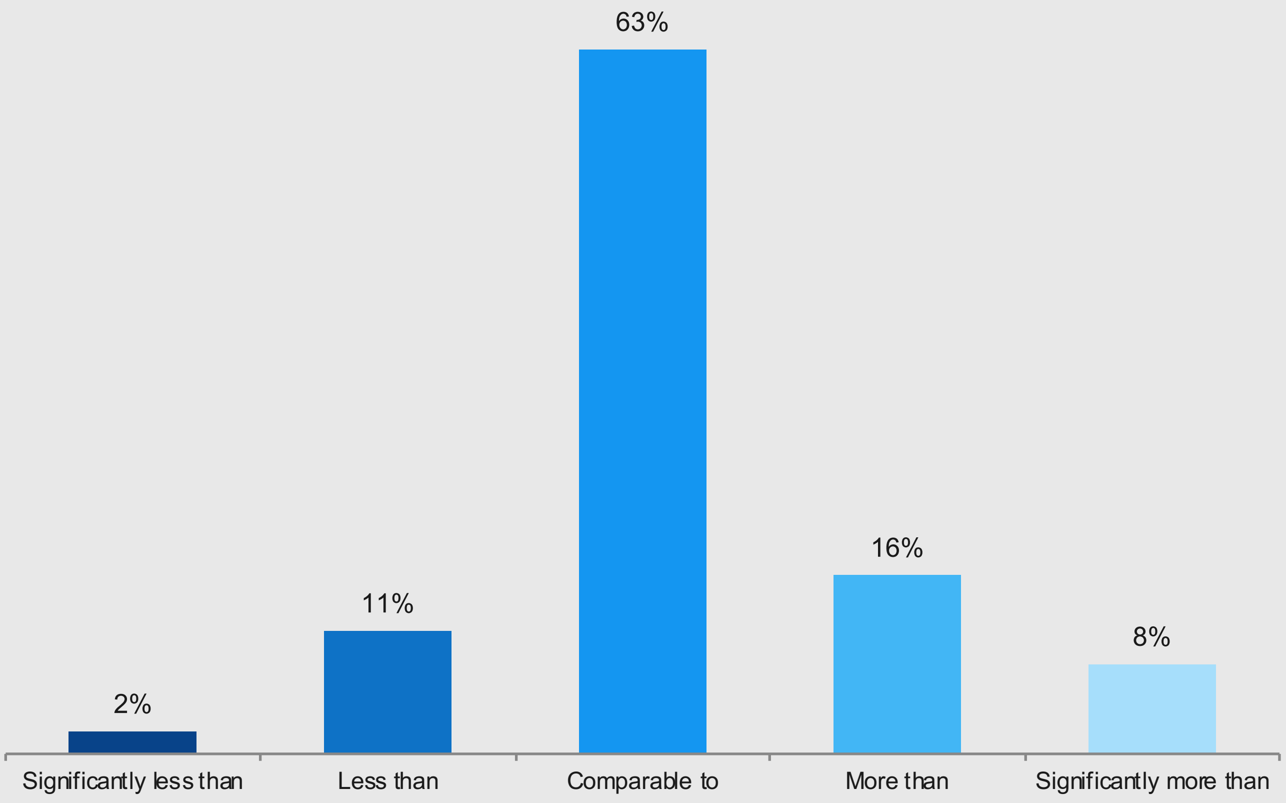
Percentage of respondents, n=201
Note: Percentages may not add up to 100% due to rounding

1 in 2
respondents say their organization's threat hunting methodology is supported by the expertise of in-house threat hunting personnel. At the same time, 41% are unsure if a methodology even exists and who supports its execution.

1 in 4 feels that investments in threat hunting technology outweigh investments in staffing

While a clear majority (63%) believe their organization is investing equally in technology and personnel to take care of threat hunting needs, those who feel greater attention is paid to technology than training new analysts (24%) outnumber those holding the opposite opinion (13%).

"My organization's investment in threat hunting technology is ______________ its investment in people responsible for that task (i.e., training threat hunters/analysts)."

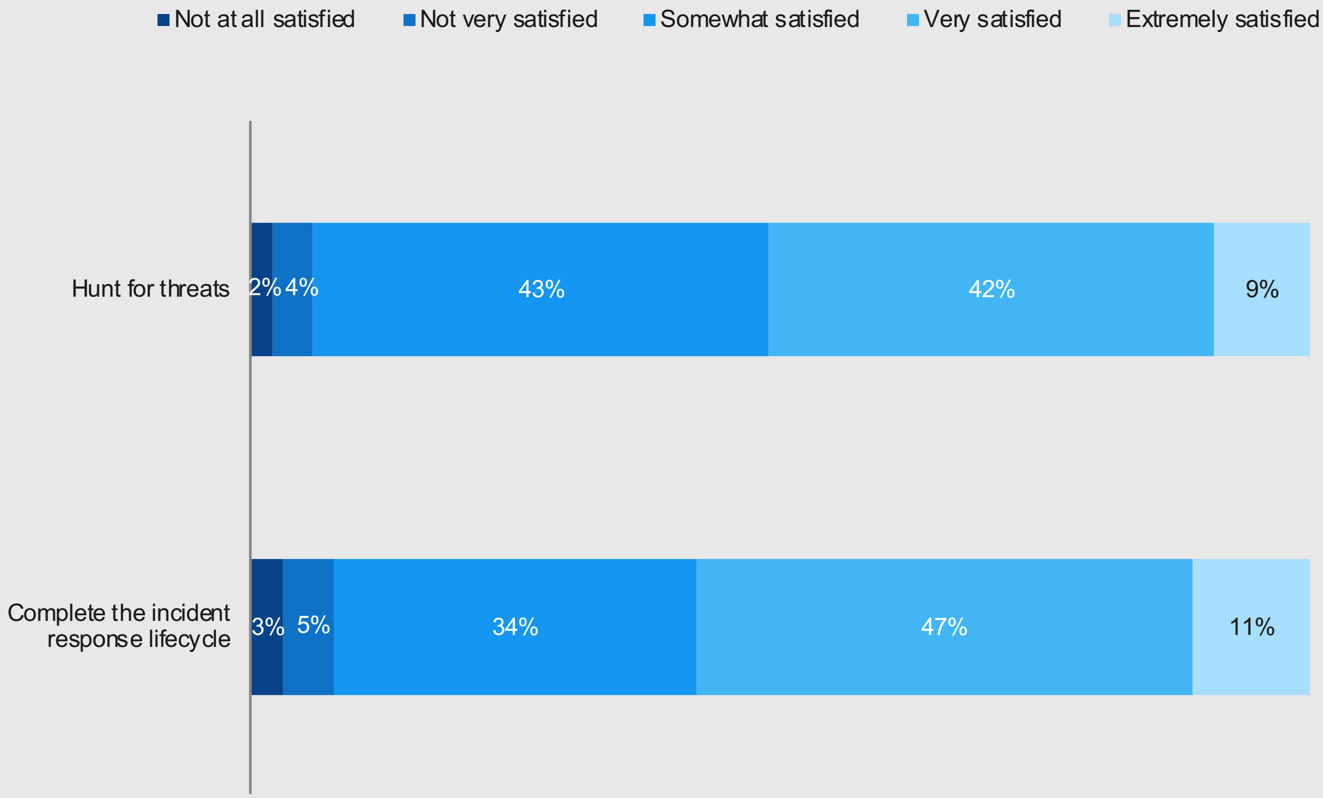


Percentage of respondents, n=189
Note: Percentages may not add up to 100% due to rounding

Respondents show moderate to high levels of satisfaction with threat hunt and response lifecycles

Unlike threat hunting, which aims to diagnose vulnerabilities *before* they manifest in an attack, incident response only takes place *following* the discovery of an intrusion. On the whole, respondents show general to high satisfaction with the length of time it takes their organization to hunt for threats and complete incident response: at least half are very or extremely satisfied with duration of both operations.

How satisfied are you with the length of time it takes your organization to _______________?

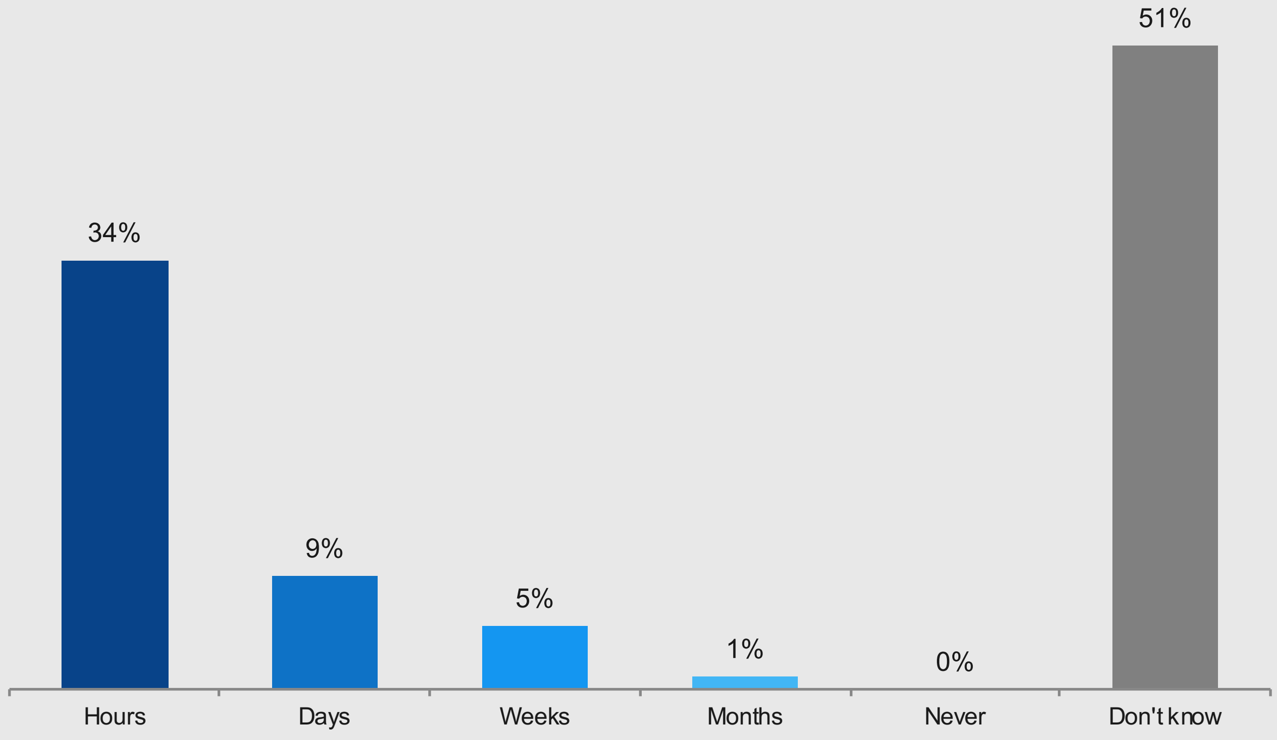


Percentage of respondents, n=116 and 131, respectively
Note: Percentages may not add up to 100% due to rounding

A majority of respondents are unable to say how long it takes to detect active network threat

Alarmingly, 51% of respondents do not know how long it takes for their organization to detect an active attacker to the network, despite having familiarity with cybersecurity programs. While one-third say it takes only a few hours to detect threats, another 14% say identifying a threat can take a matter of days to several weeks on average.

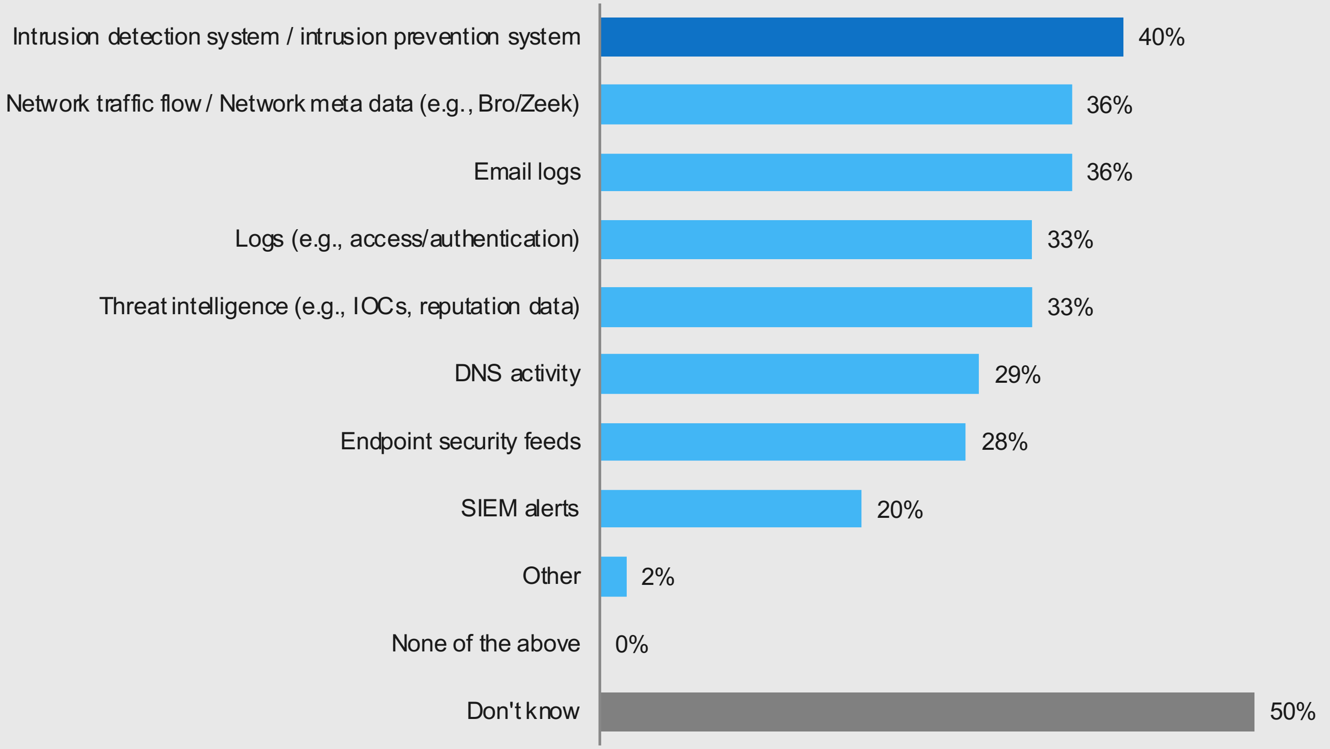
How long does it generally take for your organization to detect an active attacker to the network?



Percentage of respondents, n=490
Note: Percentages may not add up to 100% due to rounding

Intrusion detection and prevention systems are most required data sources for threat hunts

Which of the following data sources/feeds does your organization need to conduct its hunts? Select all that apply.



Percentage of respondents, n=181
Respondents were asked to select all that apply

While half of respondents do not know what sources are needed to ensure effective threat hunts, those who do know signal greatest need for intrusion detection and prevention systems (40%), as well as network traffic monitoring tools (36%) and email logs (36%).

While intrusion detection is important, cybersecurity experts say true threat hunting hinges on having accurate threat intelligence of a cyber actor’s tools, techniques, and procedures (TTP) and studying these conditions to create hypothesis-driven playbooks for proactive mitigation.

1 in 3

respondents point to the need for threat intelligence, such as indicators-of-compromise and reputation data, to ensure effective threat hunts.

Government Perspective

Brian DeWyngaert Jr.

INFOSEC Specialist
U.S. Department of Homeland Security

"Cybersecurity is generally understood through a defensive lens, but threat hunting goes a step further. Can you speak to the nature of threat hunting and what falls under that mindset?"

DeWyngaert: I think a lot of that starts with being able to look at your system through the lens of an adversary. How would they try to gain access? What do you have that would be valuable to them? So that you can try and find your way through manipulation or abuse of trust privileges to get to the things the adversary might be useful for. I think for me that means asking 'what do we need to protect?' What could the adversaries come after?' From there, it's stepping back and asking 'how can I look for the anomalies?'

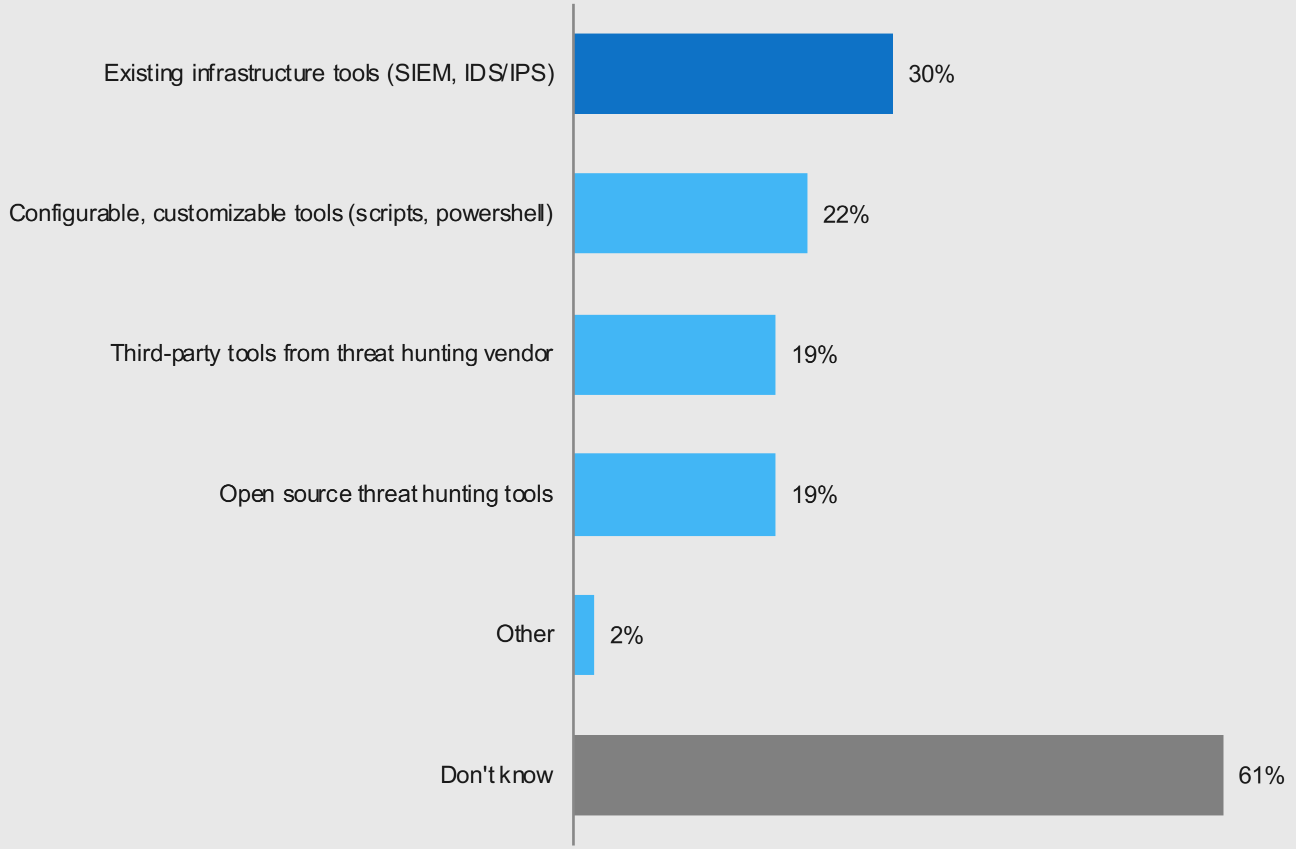
"Anomalies?"

DeWyngaert: We call them atomic indicators, the value of the string that I have that somebody else has seen as the bad thing. It has a limited life span. Quite frankly, we know that those are always useful because adversaries can go find new domains, it can wreck botnets really easily. So changing your avenue of attack is fairly simple or easier than it has been in the past. So I have to start looking at behavioral techniques to find these. That comes down to baselining systems and knowing what's running when, who's talking to whom, and then be able to automate the detection of those variations when it comes out of the baseline.

61% lack awareness into the types of tools needed to perform threat hunting

A majority of respondents are unable to say what types of tools they need to perform successful threat hunts. Among those who know, existing infrastructure tools like security information and event management (SIEM) products are a popular option. Only 19% of respondents see value in open source threat hunting tools, an approach increasingly recommended by cyber professionals.

What tools does your organization need to perform threat hunting? Select all that apply.

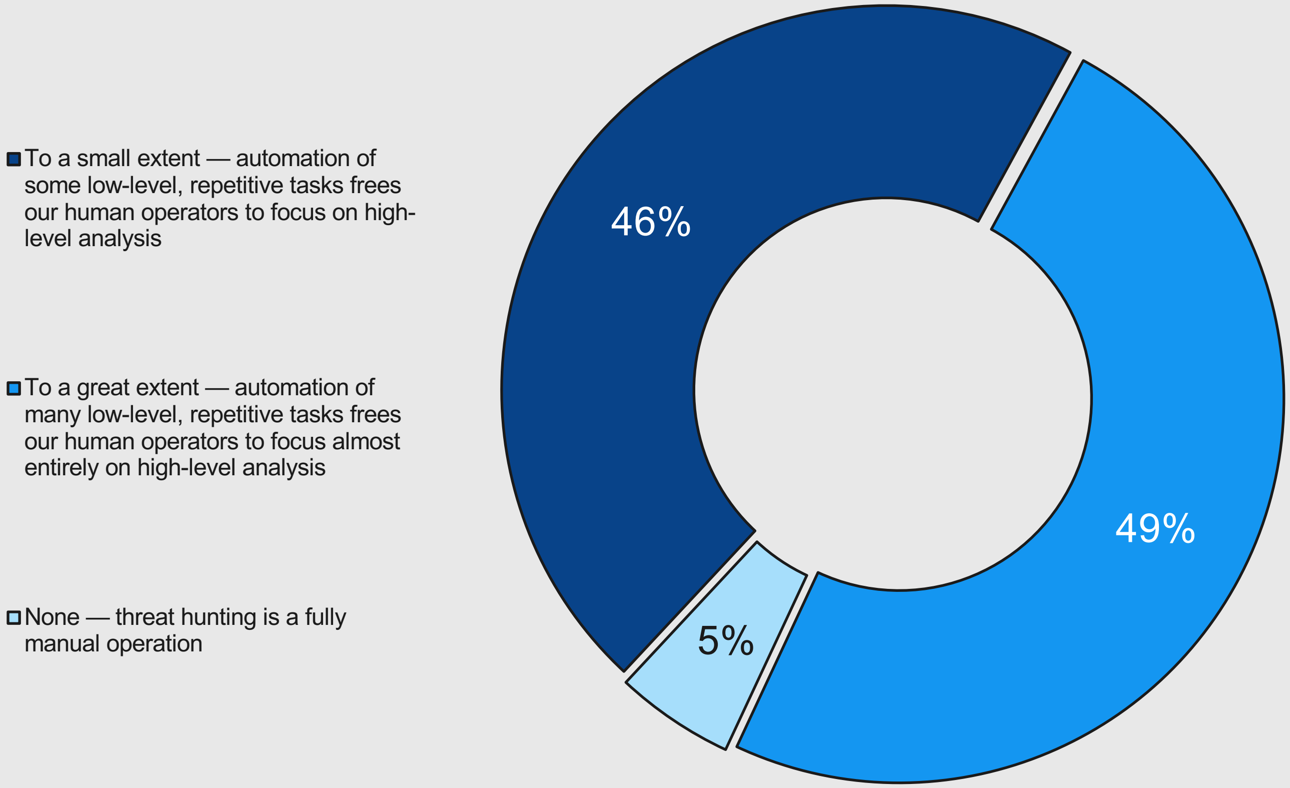


Percentage of respondents, n=167
Respondents were asked to select all that apply

Most organizations have automated at least some portion of their threat hunt operations

Organizations are increasingly automating threat hunting capabilities, and government agencies are no different. 46% have begun automating threat hunts to a small extent, and 49% have gone even further – automating much of the repetitive, routine work so their human operators can focus almost entirely on high-level analysis.

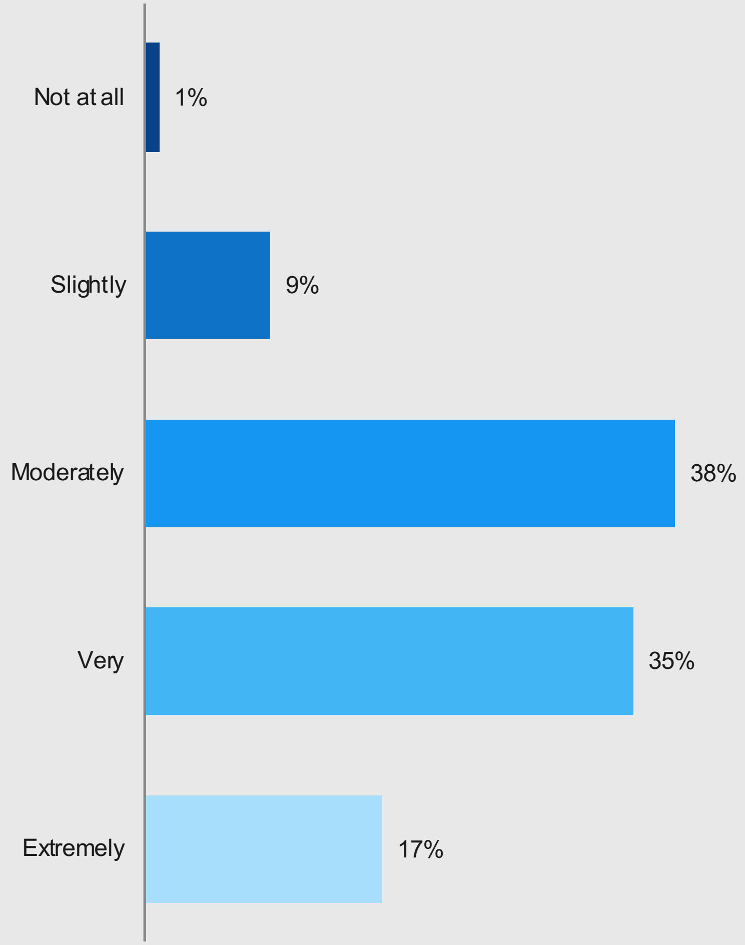
To what extent does your organization automate threat hunting capabilities?



Percentage of all respondents, n=146
Note: Percentages may not add up to 100% due to rounding

Threat hunting operations have increased overall confidence in organizational cybersecurity

How much has threat hunting increased confidence in your organization's security posture?



Percentage of respondents, n=104
Note: Percentages may not add up to 100% due to rounding

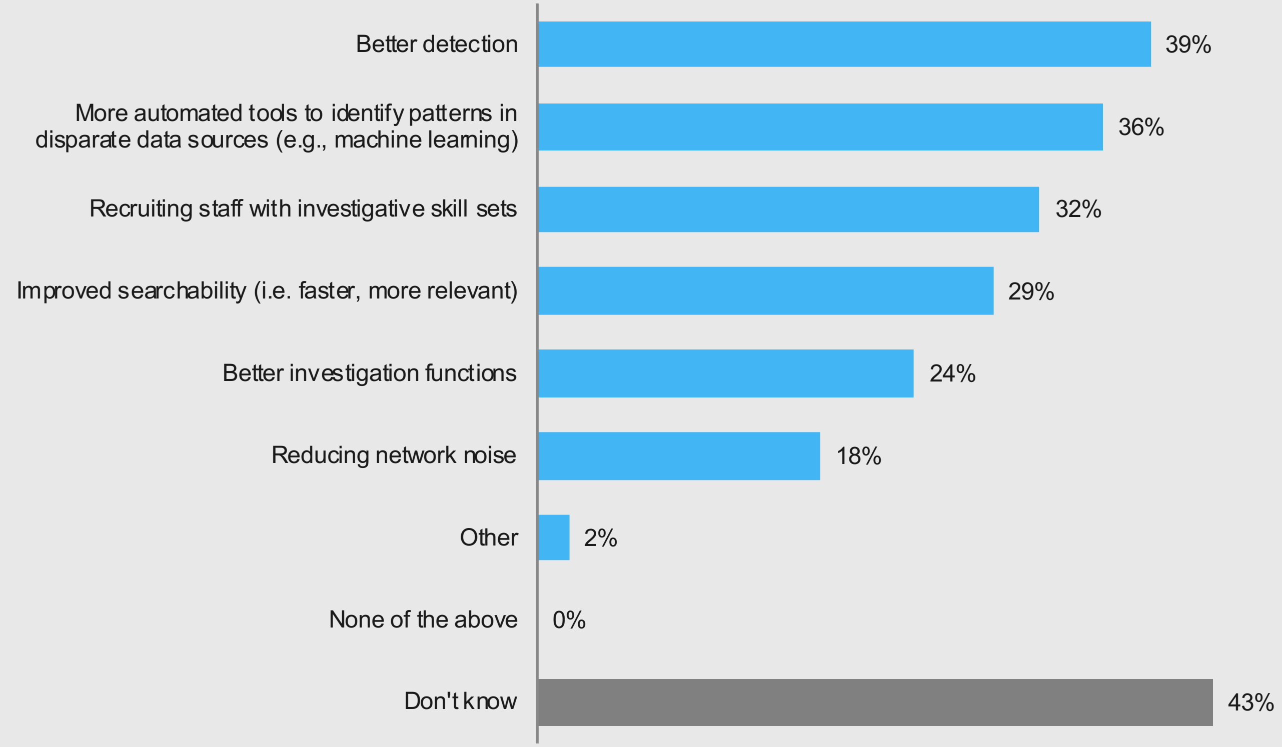
90%
of respondents feel that threat hunting has moderately, very, or extremely increased confidence in their organization's cybersecurity posture since its inception.

> "I think my agency does a pretty good job at threat hunting activities and engaging all of us on being vigilant and providing training."

Anonymous Survey Respondent

Improved detection and greater variety of automated tools are seen as top priorities

In your opinion, what areas can your organization prioritize to improve threat hunting capabilities? Select all that apply.



Percentage of respondents, n=152
Respondents were asked to select all that apply

40% of respondents believe in prioritizing better detection when considering ways to improve threat hunting capacity. Interestingly, more respondents (36%) highlight the need for expanding automated tools than for recruiting staff who can provide investigative oversight (32%).

32%

of respondents favor prioritizing the recruitment of skilled staff as a way to improve threat hunting capability.

Government Perspective

Brian DeWyngaert Jr.

INFOSEC Specialist
U.S. Department of Homeland Security

"When it comes to threat hunting, can you speak more about the roles that the human plays versus the technology? To what extent do they both play an important part?"

DeWyngaert: So orchestration automation has been getting a lot of attention recently from a security perspective. I think folks are starting to realize that we have a lot of data sources at our disposal. There's just no way for humans to enrich and fuse this information in a timely manner that can keep up with the adversary. So we are using things like clustering and graph analysis and link analysis to be able to find data sets or data points, connections that we would've just never seen before. The automation of being able to reach multiple data sources, we're talking in the scheme of like four thousand to five thousand data sources almost instantaneously… or within the span of five minutes — which doesn't seem instant but when you're talking about human time trying to do that it's pretty instant.

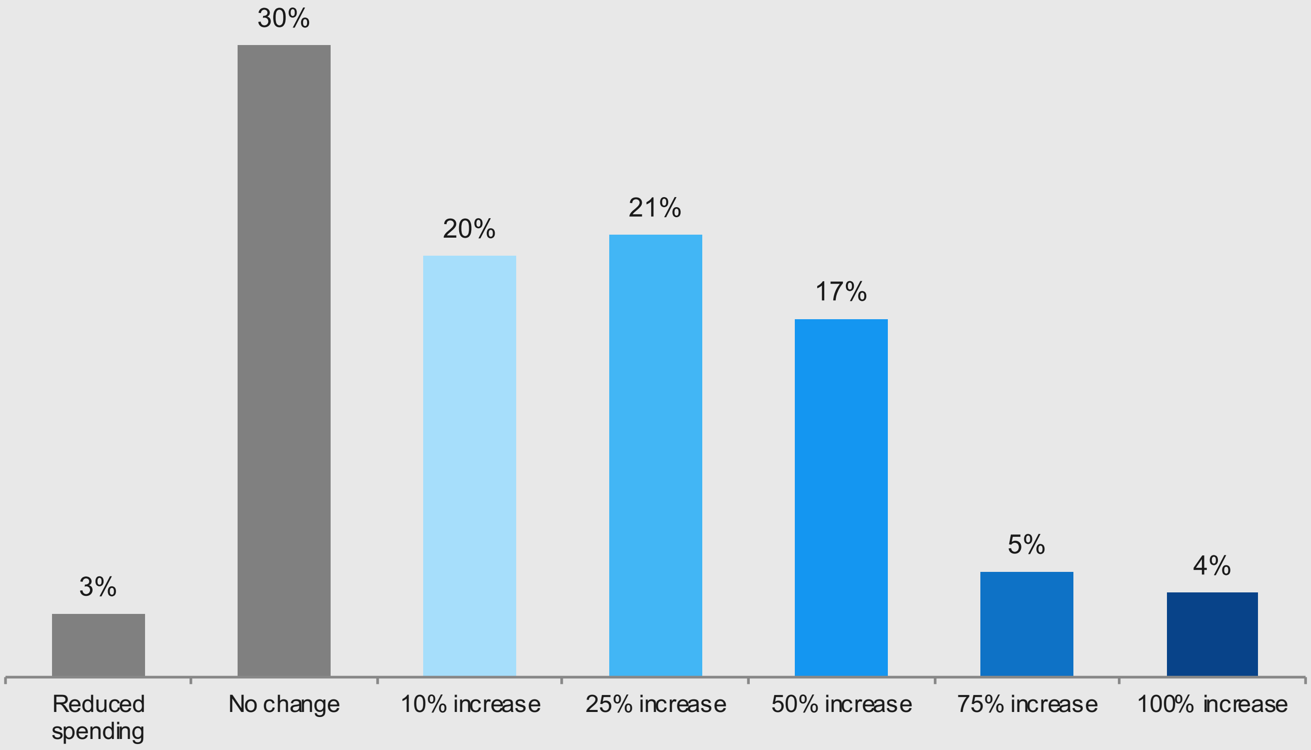
"So, in terms of looking at in the near immediate future this year what do agencies need to do to get onboard here? What is the risk if they don't?"

DeWyngaert: First they need to evaluate whether they have a sufficient program or not. If they're just relying on their SOC to do this and they don't have a proactive, dedicated hunt team they're probably not in the right place. They need to look at how mature their processes are and reach out for help. I think ultimately it's about taking advantage of the data that they have in house and really starting to build a system that understands the baselines and can incorporate in an automated process a way to find the deviations, the baseline, and tie that to available threat intelligence. If they don't, the chances of them recovering are… I mean you talk about the effectiveness of stealing passwords out of memory now and getting domain controllers. The reality is that once you have those for a domain you own the domain. You almost literally have to burn the domain down and start over. I don't know that there are a lot of agencies that could do that.

Two-thirds of respondents expect threat hunting investments will increase in 2019

Threat hunting is poised to get substantial financial boosting in 2019. 1 in 4 respondents anticipate funding will increase by 50% or more from previous levels, and another 41% expect increases of 10-25% overall. This is a positive development for agencies who have seen tighter budgets in recent years and are looking to course correct their security posture for a new wave of threats.

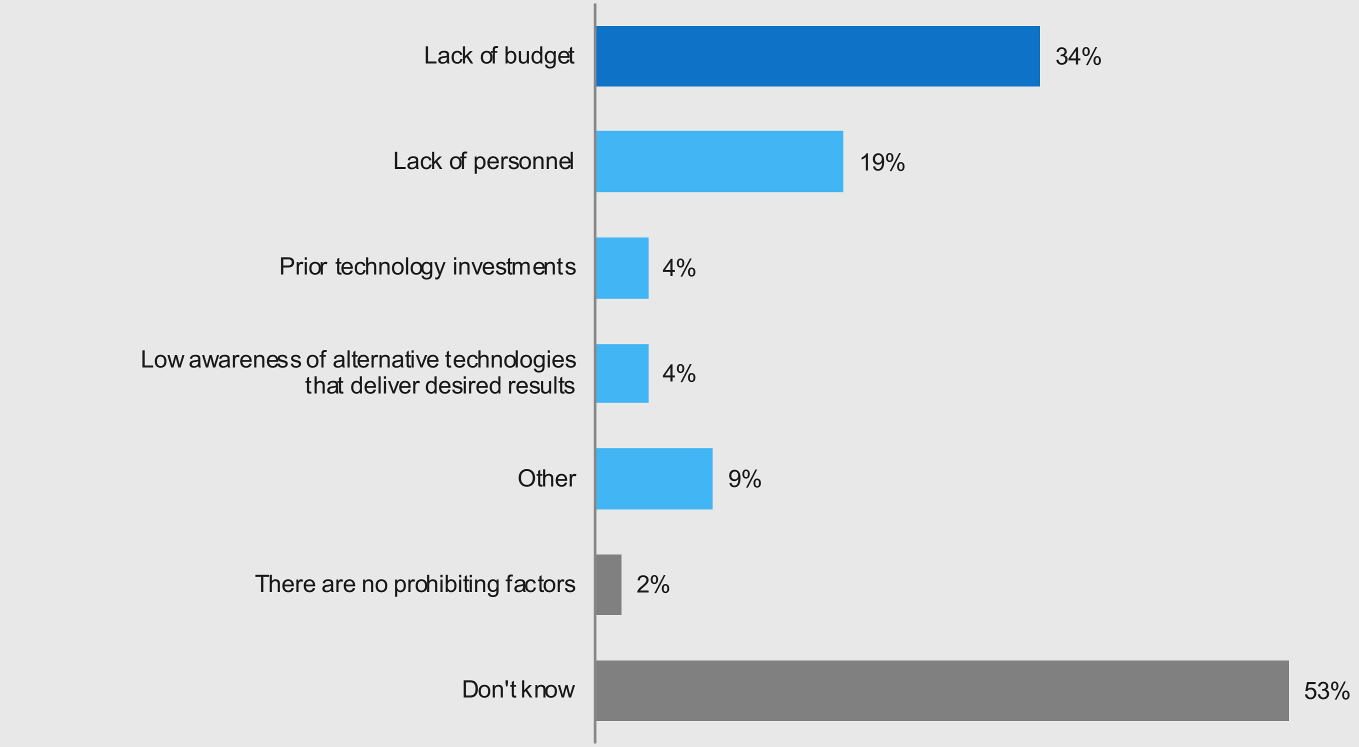
Compared to current levels, how much do you anticipate your organization will invest in threat hunting personnel and/or technologies in 2019?



Percentage of respondents, n=143
Note: Percentages may not add up to 100% due to rounding

Those who anticipate no change or less funding for threat hunting in 2019 attribute the decision to tighter budgets and limited personnel

What are the prohibiting factors (if any) keeping your organization from implementing desired threat-hunting strategies? Select all that apply.



Percentage of respondents, n=47
Respondents were asked to select all that apply

For respondents who said their agency would see no change or even less funding in 2019 for threat hunting operations, the most common reason is lack of budget. While threat hunting investments can reap extensive benefits down the line, demonstrating the benefits upfront to those holding the purse strings remains an uphill battle for these agencies.

50%
of respondents say genuine interest in learning new subject matter would be sufficient motivation to develop skills.

What Respondents Say…

"Is there anything else related to your agency's threat hunting capabilities that you can share?"

- **"It's critical to stay ahead and not abreast. I don't really think we all understand the absolute danger and threat that cyberwar/spying and stealing pose."**
- **"Government employees are low-hanging fruit. My government PII [personally identifiable information] has been stolen 4 times that I know of. It's so common it doesn't even raise an eyebrow anymore."**
- **"I believe the IT security measures vary from unit to unit. Some people take it very seriously and others don't at all and 'wing it.' The level of fluctuation of accountability and enforcement concerns me."**
- **"We desperately need more OI&T HUMAN support, for everything, including cybersecurity. The current cybersecurity technology alone seems only to keep us from doing our jobs. If a secure system is one that nobody can access, well, I guess we're on the right track."**
- **"We take cybersecurity training annually. The training helps employees to identify as well as report activity that is a potential threat to the agency in my opinion."**
- **"Awareness needs to be raised even higher to all leadership levels that additional staff are required to maintain and onboard technologies. It doesn't just magically get plugged in and work."**
- **"Our greatest threat is the patchwork networks that we have and can't protect."**
- **"I do not believe, from my vantage point, that adequate funds are available to deal with the rapidly growing threat. Our opponents have beat us to the punch, and most commercial resources we use know that more needs to be done, but they are tied up with just keeping the equipment running."**
- **"We have been operating short-staffed and short-budgeted for training people that have the correct skills to set up, manage, and maintain IT systems for quantity and quality of data and records. People don't understand IT security and records management is everyone's duty."**
- **"I think my agency does a pretty good job at threat hunting activities and engaging all of us on being vigilant and providing training."**

Looking Forward

Agencies can prioritize threat hunting by:

Shifting focus to the threat hunter

While technology can aid threat hunting operations, it is crucial that agencies understand threat hunting success hinges on finding and equipping skilled specialists to track adversaries proactively. This requires organizations to shift their mindset from reactive defense to aggressive offense: close to one-third of those surveyed believe their agency's cybersecurity posture is reactive, largely dependent on defensive tactics to detect anomalies in the network. And 24% also feel that their organization devotes more resources to technology than skilled human labor when it comes to threat hunting investments. At the end of the day, cybersecurity is a very human problem and requires trained human specialists to root out adversaries who understand how to exploit gaps in intrusion detection and alert systems.

Eliminating data silos

Successful threat hunts will require greater visibility into network data, threat intelligence, and systems than respondents indicate is currently provided. Even among those who acknowledge threat hunting as a practice, an alarming number are unsure how long it takes to detect an attacker to the network or what tools are required to access the necessary data for launching threat hunts in the first place. Agencies can address this by eliminating unnecessary silos and treating data sharing as a top priority. With 3 in 4 respondents signaling that their data needs will increase in 2019, it's imperative that IT leaders and threat hunters deploy tactics across the enterprise instead of succumbing to system-specific restraints and locked endpoints.

Elastic's Perspective

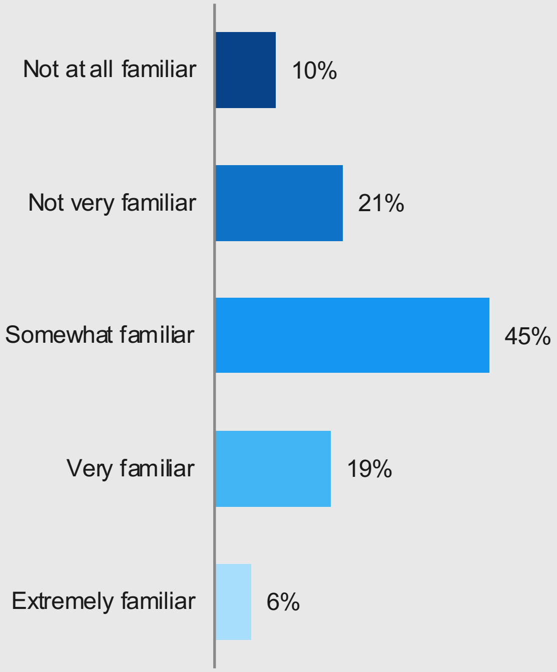
Federal CIO Suzanne Kent recently spoke to the need to analyze data fast enough for it to be usable. "If one of us tried to process a terabyte of data, we would have to watch the equivalent of 400 90-minute videos. Using technology, and with the right discipline around data, we can process that in seconds. But it has to be structured, and we have to understand it."

While enterprise search tools date back to the days of the mainframe, agency search needs are much more complex now. Today's distributed systems need high-volume, deep-dive searches that can happen in real time and continually update indexes as new data is added. Elastic's search capabilities can yield the insights you need at lightning speed to empower your agency to make critical mission decisions. Combining human intelligence with the best automated detection and search tools is our best chance for staying one step ahead.

Respondent Profile

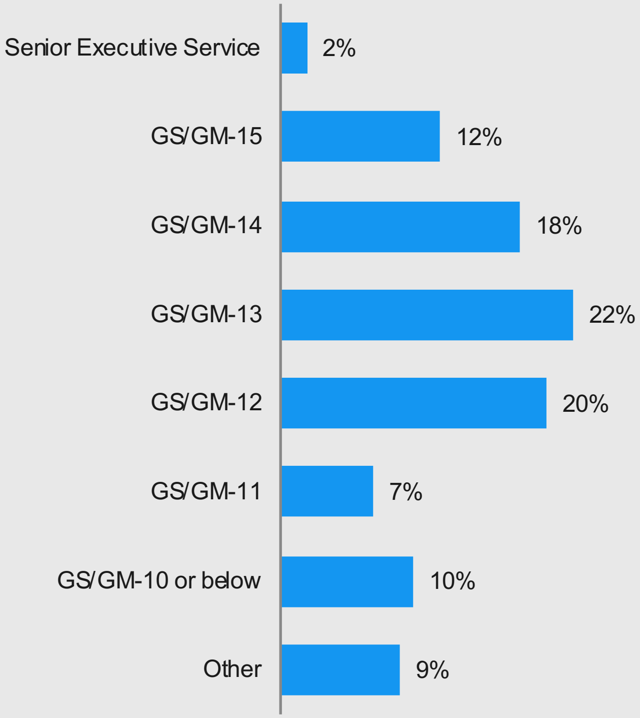
Majority of respondents are senior-level decision makers with familiarity over cyber programs

How would you rate your familiarity with your organization's cybersecurity programs?



Percentage of respondents, n=484
Note: Percentages may not add up to 100% due to rounding

Job Grade/Rank



Percentage of respondents, n=465
Note: Percentages may not add up to 100% due to rounding

90%

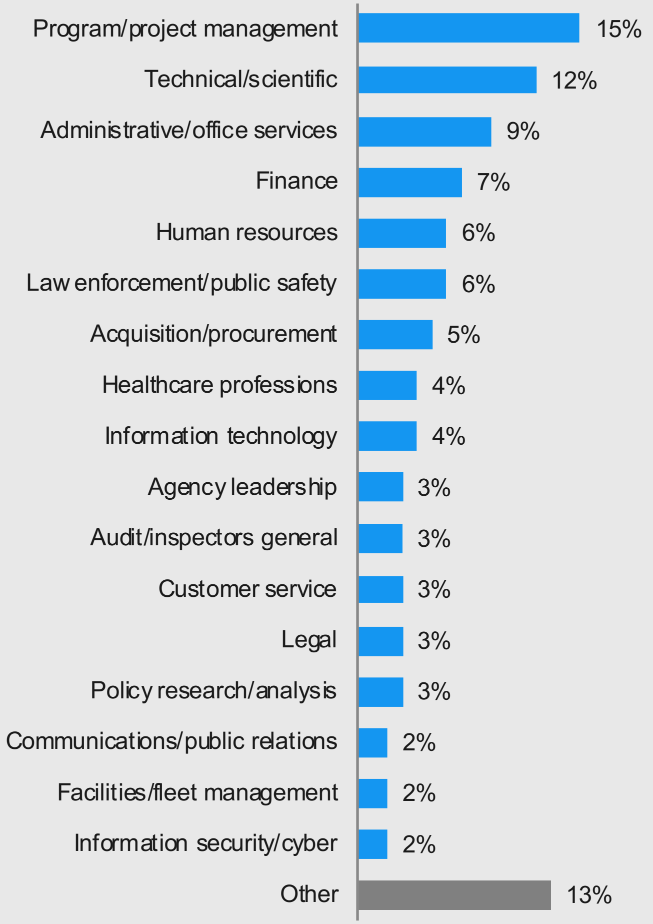
of respondents acknowledge at least some degree of familiarity with their organization's cybersecurity programs.

54%

of respondents hold senior positions at the GS/GM-13 rank or above, which include Senior Executive Service personnel.

Most widely represented are program managers, technical specialists, and administrative officers

Job function



Percentage of respondents, n=704
Note: Percentages may not add up to 100% due to rounding

Departments and agencies represented

- Homeland Security
- Agriculture
- Veterans Affairs
- Air Force
- Army
- Interior
- Treasury
- Navy
- Health & Human Services
- Justice
- Transportation
- Commerce
- Office of the Secretary of Defense
- General Services Administration
- Housing & Urban Development
- NASA
- Social Security Administration
- Energy
- Environmental Protection Agency
- State
- Small Business Administration
- Congress/Legislative Branch
- Government Accountability Office
- Intelligence Community/ODNI
- Agency for International Development
- Labor
- Nuclear Regulatory Commission
- Office of Personnel Management
- Education
- Marine Corps
- Combatant Commands
- Other independent agency

Respondents, n=1014

Respondents were asked to choose which single response best describes their job function.

Departments and agencies are listed in order of frequency.

About

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive*'s 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights

Report Author: Daniel Thomas

Contact

Daniel Thomas
Manager, Research & Strategic Insights
Government Business Council
Tel: 202.266.7905
Email: dthomas@govexec.com

govexec.com/insights
@GovExecInsights

About Elastic

Elastic is a search company. As the creators of the Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash), Elastic builds self-managed and SaaS offerings that make data usable in real time and at scale for search, logging, security, and analytics use cases.

Learn more at elastic.co.