Detecting Threats in the Federal Government

RESEARCH BRIEF

Executive Summary

Twenty two thousand, seven hundred and eighty eight.

That's the number of confirmed cyberthreat incidents – suspicious or threatening acts that are an attempt to compromise a system – that took place against the public sector in 2017. And of those 22,788 incidents, over 300 resulted in actual data breaches that violated public-sector information. That's not all. The National Institute of Standards and Technology (NIST) identified 94,901 publicly known cybersecurity vulnerabilities and exposures as of Sept. 19, 2017, with more being added each day.

It's clear that, particularly at the federal level, government IT, networks and systems are under attack by persistent, sophisticated and resourceful adversaries. The government is also facing significant insider threats and other bad actors who want to gain citizens' personal data and exploit it for nefarious use.

In response, the government has been doubling down on threat detection. In May 2017, the President issued an executive order titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Additionally, in early 2018, Congress passed the implementation of the Modernizing Government Technology Act, which established a centralized Technology Modernization Fund to give agencies dedicated funding to modernize their networks and provide more robust cybersecurity.

This all takes place against the backdrop of the 2014 creation of the NIST Cybersecurity Framework (CSF). NIST developed the CSF in collaboration with the private sector and government agencies to set frameworks, guidelines and best practices to promote the protection of critical infrastructure and improve government security. The core of the CSF consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond and Recover. It is now required under the current administration.

We've previously discussed the state of overall adoption of the CSF in government, as well as the perception and use of the Identify and Protect functions. But how is the federal government using the Detect function? Is it adequately discovering threats in a timely manner, or are challenges holding it back from rapid detection, and thereby response?

To learn more about the CSF's Detect function usage, perception and outcomes in the government, GovLoop teamed with Symantec and DLT Solutions to survey 117 federal employees engaged in cyber activities.

In this research brief, we'll discuss those results, as well as explain why the Detect function is so critical. We'll also share additional insights from Ken Durbin, CISSP Senior Strategist of Global Government Affairs and Cybersecurity at Symantec, and Don Maclean, Chief Cybersecurity Technologist at DLT Solutions.

Threat Detection: Why It's So Critical to the Public Sector

To best understand the critical functions of the NIST Cybersecurity Framework, it is helpful to think about the framework as just that – a foundation or blueprint to build a very secure environment for your data. Each of the five functions is a critical component to building that safe environment. For example, Identify is the foundation of the house you are building – knowing what you want and what you already have. The Protect function gives you plans for how you want to give yourself protection – with walls, a roof, etc.

Once your house is built and sturdy, you want tools to make sure you're keeping it protected. That's where the Detect function comes into play. You wouldn't build a house without installing an alarm system or smoke alarms. Those sort of tools alert you to potential dangers that are trying to harm your house. The Detect function does the same for your cybersecurity posture. This function detects cybersecurity events and problems that might be occurring on your network that you need to investigate further. And according to NIST, the true definition of the function is to "develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

In the Detect function, there are only three categories, but they are especially critical for the public sector, which may lag in detection capabilities or the ability to quickly respond to identified threats.

1. **Anomalies and Events:** Anomalous activity is detected in a timely manner and the potential impact of events is understood.

2. **Security Continuous Monitoring:** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

3. **Detection Processes:** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

It's clear why the Detect function of the NIST CSF is critical for the public sector to take seriously. So, is the federal government taking threat detection seriously?

> **"People are finally getting the idea that threat detection is a really important activity and does require time and attention."**
>
> Don Maclean, Chief Cybersecurity Technologist at DLT Solutions

Is Threat Detection Being Taken Seriously in Government?

To better understand the perception and implementation of threat detection in government, GovLoop surveyed 117 federal respondents on everything about threat detection, including whether agencies are adhering to it, how they're funding it and what challenges they face in achieving it.

Generally, results showed there is more awareness and focus than ever on the ability to detect threats.

"People are finally getting the idea that threat detection is a really important activity and does require time and attention," said Maclean. "People see breaches, they see outside interference, and it starts to take on a level of importance that we may not have had in the past."

Maclean added that the focus on mandates and executive orders from administrations has had a real effect. "You had executive orders from both Presidents Obama and Trump," he said. "Nearly everyone agrees that agency heads need to be responsible for security."

The GovLoop survey results reflect this growth in awareness around the Detect function. When asked if they believe their agency is able to detect threats in a timely manner, 67 percent of respondents said "yes" *(Figure 1)*.

Additionally, when asked if their agency complies with or follows the Detect function, nearly 80 percent of respondents said yes *(Figure 2)*. That is a startlingly high number and a positive trend in terms of compliance.

For the minority of respondents who do not believe their agencies are able to detect threats proactively and/or are not following the NIST Detect function, prioritization and labor resources seem to be an issue. "We don't currently have the tools or the manpower to fully implement the Detect function. We are part of the way there, working on a solution," said one respondent. Another respondent noted that, "We are still prioritizing cyber issues to be tackled, working within manpower available."

Durbin and Maclean were heartened by these results, but cautioned the public sector might have some more work to do. "Mandates, compliance, general awareness and Federal Information Security Management Act (FISMA) reporting have all helped with adherence and threat detection," Durbin said. But, he noted, thinking your agency is great at detecting threats is different from actually being great. There's still work to be done, and agencies must see how reporting plays out before claiming threat detection victory.

To understand other aspects of threat detection in the public sector, GovLoop also asked our community about four other main areas: how the Continuous Diagnostics and Mitigation (CDM) program is affecting their threat detection abilities; how agencies feel they are doing detecting internal threats vs. external threats; how the cloud vector is playing into threat detection; and what agencies' top priorities in a threat detection solution are.

FIGURE 1

The CSF Detect function enables timely discovery of cybersecurity events. Do you believe your agency is able to detect threats in a timely manner?

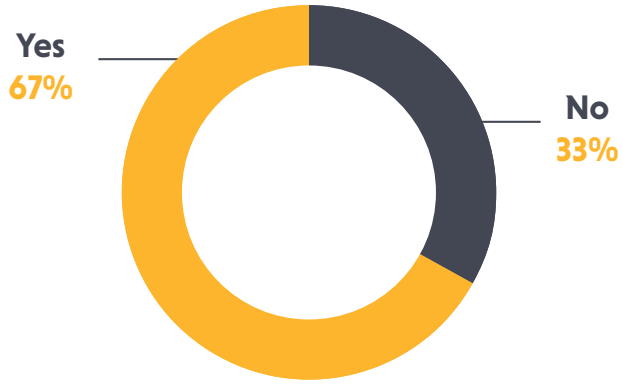
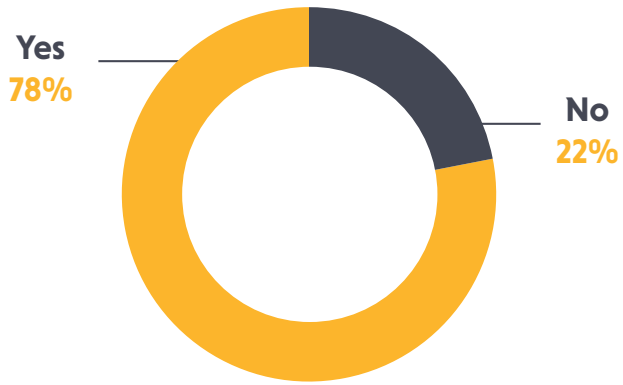


FIGURE 2

Does your agency comply with or follow the Detect function of the CSF?



CDM and Threat Detection

In addition to the core functions set up by the NIST Cybersecurity Framework, the CDM program set up by the Department of Homeland Security in 2012 provides insight, standards and guidance into cybersecurity efforts in civilian federal agencies. CDM encourages agencies to identify who's on the network, what's on the network and what's happening on the network, and to establish a baseline approach to improve their end-to-end security posture.

"The overarching goal of CDM is to move the federal government from a check-the-box mentality around cybersecurity to deploying tools to satisfy FISMA controls. But they still need to continuously monitor those tools to make sure they are in place, working and still relevant," said Durbin.

So how is the public sector doing when it comes to CDM and threat detection? According to our survey, adoption of CDM is not as high as the NIST CSF. Only 46 percent of respondents' agencies have deployed CDM *(Figure 3)*, and 55 percent are still in Phase 1, the earliest phase of the program *(Figure 4)*.

One potential reason for the lower adoption rate? Maclean stated: "CDM is picking up steam but I think there is a certain amount of confusion over how to implement it. I think there is also confusion about the nature of the program and a perception that it could be a burden over the long term."

Of the survey respondents whose agencies had implemented CDM, however, 71 percent found the program helpful for threat detection capabilities *(Figure 5)*.

But Maclean may have been on to something with his observation about CDM and confusion. For those who did not find CDM useful for threat detection or only somewhat useful, respondents cited that "No one has explained how CDM addresses the Detect function," at nearly 38 percent *(Figure 6)*. In an era of limited resources, employees understanding the "why" behind a program or mandate is essential to adoption. Otherwise, as Maclean noted, employees may view additional programs as simply more work with no real ROI.

FIGURE 3

Has CDM been deployed at your agency?

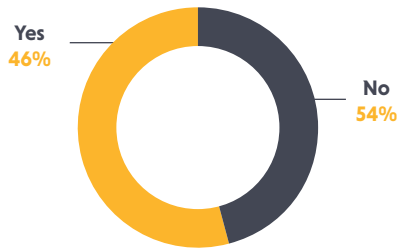


FIGURE 4

If yes, what phase?

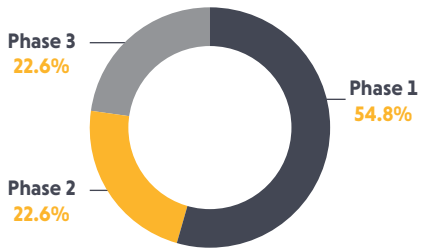


FIGURE 5

If yes, do you find CDM helpful for threat detection capabilities?

FIGURE 6

If no, why not?

37.8%	No one has explained how CDM addresses the Detect function
26.7%	Other
11.1%	CDM not fully deployed
6.7%	It is not comprehensive enough
6.7%	It is too complex to implement
6.7%	It does not help address threats in the cloud vector
4.4%	It does not detect threats in real time

External vs. Internal Threats

Government agencies understand the risk of external threats to their cybersecurity posture, but are they aiming to detect potential internal and insider threats as clearly? Some internal threats or data breaches happen because of a careless mistake, while other attacks are carried out with malicious intent. It is the government's job to put policy and controls in place to ensure that cyberthreats, including insider threats, are detected and mitigated as soon as possible.

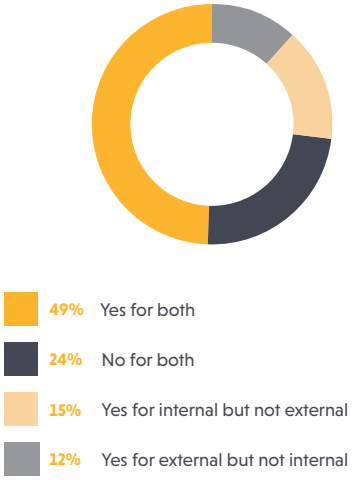
To that end, GovLoop asked members of our federal cyber community if they felt their agency's current detection capabilities are adequate for both external and internal threats. Forty-nine percent believed their detection capabilities are adequate for both *(Figure 7)*. Those who struggle with threat detections cite a number of challenges.

"Users are not complying with best or mandatory practices for internal device use – internal threats are most insidious," wrote one respondent.

"External threats are too varied and changing all the time – sometimes we can handle it, as those external threats get into the internal network via users," pointed out another.

FIGURE 7

Do you feel that your agency's current detection capabilities are adequate for both external and internal threats?



Threats from the Cloud Vector

As cloud usage by government has become more and more common over the years, its appeal to attackers has naturally increased. Thus, threat detection efforts by agencies must be considering potential threats from the cloud vector. When we asked survey respondents, "Do you feel your agency's current detection solutions are adequate for detecting threats from the cloud vector?" the majority – 69 percent – said they did believe their solutions were adequate *(Figure 8)*.

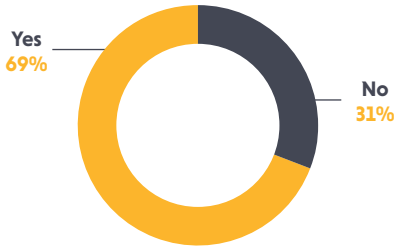
But Durbin and Maclean cautioned government IT leaders that this may not actually be the case. In fact, widespread adoption of cloud applications in government, coupled with risky user behavior that the agency may not even be aware of, is widening the scope for cloud-based attacks.

"Organizations are using many more cloud apps than what is typically assumed," said Durbin. "A Symantec survey showed IT professionals believed the average number of different cloud apps in use at an enterprise was 40. The actual number of cloud apps in use averaged 1,232."

Even if IT leaders and government employees feel that they are doing due diligence or using FedRAMP-certified cloud applications, they must still stay vigilant when it comes to threats from the cloud vector. They're increasing and can come from anywhere.

FIGURE 8

Do you feel your agency's current detection solutions are adequate for detecting threats from the cloud vector?



What's a Priority in a Detection Solution?

Finally, we asked our community what they found most critical in a threat detection solution. Far and away, the most popular answer was "rapid response time," with 84 percent of the respondents citing that as their most important need *(Figure 9)*. Ease of use was also a cited component.

Durbin agreed that this factor in a detection solution is imperative, but also needs to be looked at from a few different angles.

"The public sector must be clear on the difference between detection time and response time," he said. "Fast detection has to do with what's called dwell time. In other words, how long was that threat resident in your network before you detected it?"

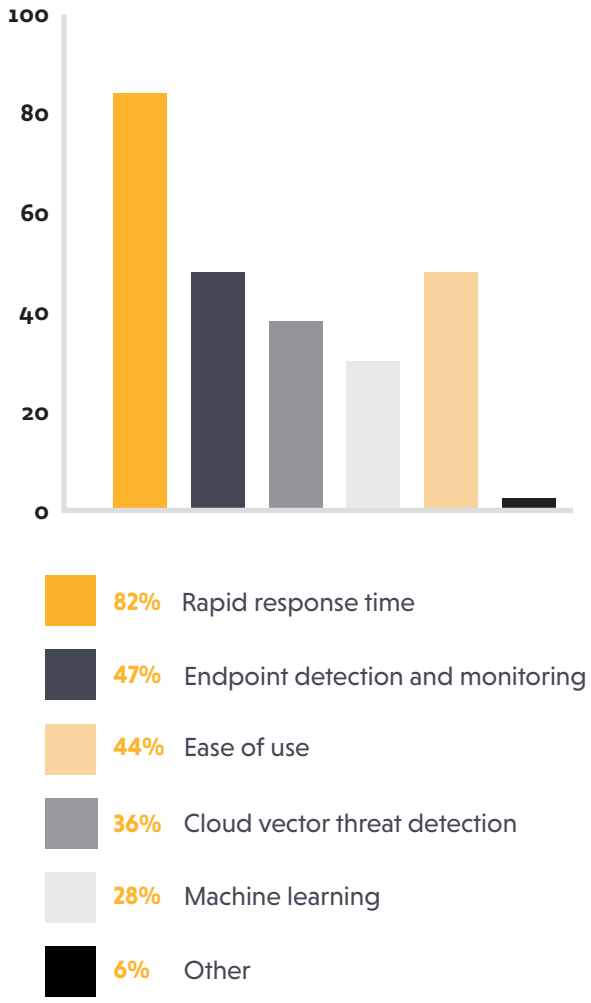
In addition to dwell time, the public sector must also be measuring its response time.

"Of course you want your response to be rapid," said Maclean. "But my experience in security programs is that rapid response typically means making sure that you report it to the people on time and that fixing it, you do at your leisure. So just 'responding' quickly is not enough."

A positive note that Maclean pointed out is that dwell times in the public sector are trending downward, indicating a better detection and response time in government agencies.

FIGURE 9

What abilities are most critical to you in a detection solution? Check your top 3.



Rapid response time is the #1 priority in threat detection. But what about "dwell time"?

Finding, Funding and Purchasing the Right Detection Solution

As with many areas of the public sector, it can be a challenge to get dedicated funds to spend on increasing cybersecurity solutions. Funding and purchasing detection solutions are no different.

There is, however, good news on the horizon: The Modernizing Government Technology (MGT) Act, which established a centralized Technology Modernization Fund (TMF), became law in 2018. The TMF gives agencies dedicated funding to modernize their networks and enable better cybersecurity solutions.

The MGT Act will provide federal agencies with $500 million over the next two years to update legacy systems. The act calls on agencies to use new technologies, such as cloud computing, to replace older systems that impose an increased security risk.

And according to responses from the survey, the federal government plans to take full advantage of that money. When asked, "Does your agency plan to use IT Modernization funding for detection solutions?" 67 percent of respondents said yes *(Figure 10)*.

Additionally, 51 percent of respondents plan on using the Detect function of the NIST CSF to guide and inform their purchasing choices or solutions around threat detection, showing a solid awareness and adherence to the overall Cybersecurity Framework *(Figure 11)*.

But clearly there is always more to be done, particularly on the education and awareness front about what the NIST Cybersecurity Framework Detect function can offer and how it can guide agencies. Those who are not planning to use those dedicated funds to purchase detection solutions cited lack of buy-in from leadership, a general lack of awareness about the importance of detection and too many other cybersecurity issues to address as the reasons *(Figure 12)*.

That's why proving a strong ROI and getting leadership buy-in ahead of time is so important when spending discretionary funds. Finding the right vendor and solution for threat detection can help with this.

FIGURE 10

Does your agency plan to use IT Modernization funding for detection solutions?

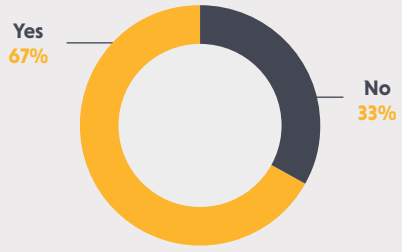


FIGURE 11

Are you using the Detect function of the CSF to guide and inform your purchasing choices or solutions around threat detection?

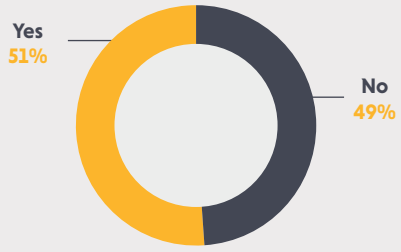
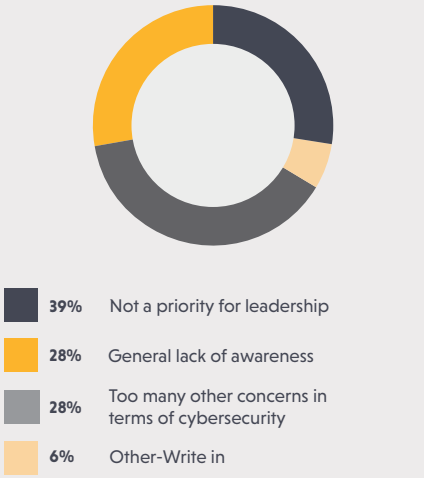


FIGURE 12

If you don't plan on using dedicated funds for detection solutions, why not?



How Symantec and DLT Can Help

Symantec and DLT are uniquely positioned in the public-sector arena to help agencies take a more proactive stance against cybersecurity incidents, and to help government detect threats in a timely manner.

"We understand the existing architecture, the move to the NIST Cybersecurity Framework and how cloud-enabled solutions can help," Durbin said. "We can position our solutions to fill technology gaps identified by the CSF."

Symantec and DLT can help their federal customers understand and manage the latest threats to better identify, protect, detect, respond to and recover from advanced attacks. Symantec's tools and comprehensive solutions make it easy for government agencies to discover what is in their network and continuously access and manage their security posture.

In particular, Symantec's Advanced Threat Protection Platform helps agencies detect, prioritize, investigate and remediate threats across multiple control points in a single console. It can automatically prioritize threats based on various attributes, including the type, scope and complexity of a threat.

"The solution is automated," Durbin said, "but it also keeps an accurate record of everything that was going on so that you can go back and triage any event and learn from it. You can improve your security posture based upon what you learned, as well."

Additionally, Symantec offers its Cloud Access Security Broker, which lets agencies leverage cloud applications and services while staying safe, secure and compliant and providing visibility into shadow IT, governance over data in cloud apps and protection against threats targeting cloud accounts.

"The Cloud Broker addresses shadow IT by making sure that whether it's inside or outside your perimeter, everything is being funneled through this solution so it's properly protected before it hits the cloud," Durbin said.

"We understand the existing architecture, the move to the NIST Cybersecurity Framework and how cloud-enabled solutions can help. We can position our solutions to fill technology gaps identified by the CSF."

Ken Durbin, CISSP Senior Strategist of Global Government Affairs and Cybersecurity at Symantec

Conclusion

To best protect your agency's most critical assets while ensuring that your data is safe, you will need to continue investing in data loss prevention and identity and access management in addition to training and educating the cyber workforce of tomorrow. These efforts can be enhanced with the right solutions, encompassing DLP and a way to automate the protection of your agency's most valuable information.

Symantec and DLT can help you effectively discover what is on your network and continuously assess and manage your cyber posture, all while making the most out of the NIST Cybersecurity Framework.

About Symantec

Symantec Corporation, the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.
Learn more at: www.symantec.com.

About DLT

Established in 1991, DLT accelerates public sector growth for technology companies in the federal, state and local, education, utilities and healthcare markets. As a premier governmentag-gregator, DLT creates value for tech-nology companies by enabling their public sector customers to make smarter technology choices by providing access to a robust network of channel partners and through a broad portfolio of over 40 in-house contract vehicles. DLT's go-to-market expertise is focused on six core technology domains; Big Data & Analytics, Cybersecurity, Cloud Computing, Ap-plication Lifecycle, Business Applications, and IT Infrastructure which are strategic-ally crafted around how our technology partners, customers, and vendors go to market. **Learn more at: www.dlt.com.**

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector prof-essionals by serving as the know-ledge network for government. GovLoop connects more than 270,000 members, fostering cross-government collaboration, solving common prob-lems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to **info@govloop.com.**

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop