CLOSING THE GAPS IN CYBERSECURITY RESILIENCE

AT U.S. GOVERNMENT AGENCIES

Two-thirds of federal IT executives in a new survey say their agency's ability to withstand a cyber event, and continue to function, is moderately to highly mature.

But a number of gaps in cybersecurity resilience remain, with 6 in 10 defense or intelligence agency IT executives — and 55% at civilian agencies — saying their agencies "don't have all the tools and resources needed to detect and respond to cyberthreats."

This new survey of IT leaders at civilian, defense and intelligence agencies explores how prepared agencies are to continue operating during an attack, the tools they're using and their top concerns and priorities.

PRESENTED BY
cyberscoop | fedscoop

UNDERWRITTEN BY
REDSEAL

In a new survey of federal civilian, defense and intelligence agency IT decision makers, CyberScoop & FedScoop identify:

1. The overall resilience and preparedness of civilian and defense/intelligence agencies to recover from cyber incidents
2. How long it takes their organizations to detect and respond to security incidents
3. What cybersecurity tools, activities and metrics they rely on most
4. How frequently they conduct Blue Team / Red Team testing
5. Their top cybersecurity investment priorities

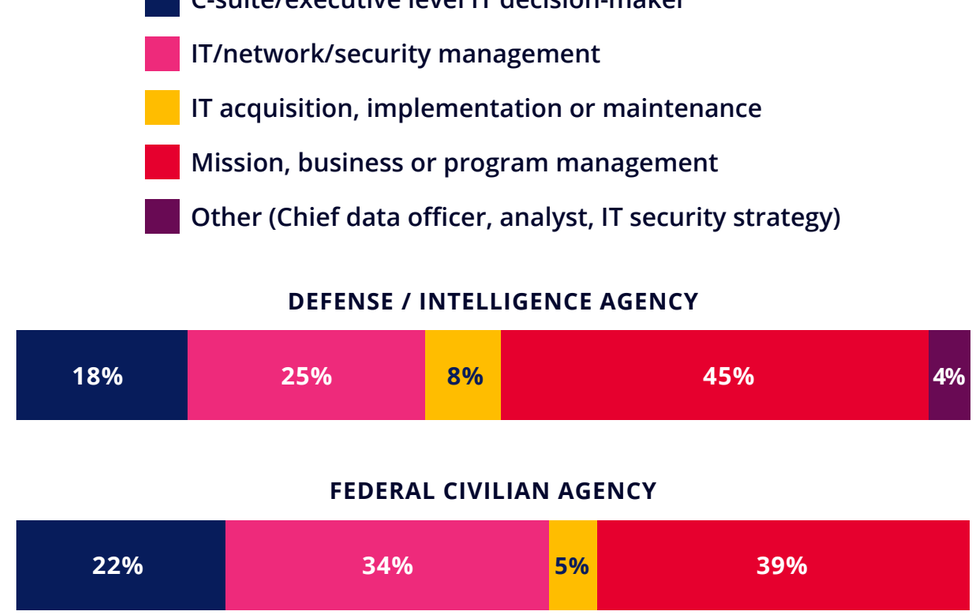
cyberscoop | fedscoop

WHO WE SURVEYED

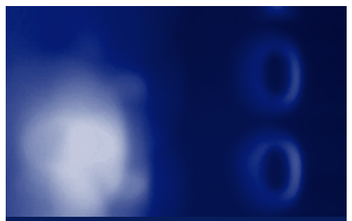
FedScoop and CyberScoop conducted an online survey of qualified federal government IT, cybersecurity and mission, business or program executives. A total of 64 IT officials working for civilian agencies and 51 IT officials working for defense or intelligence agencies completed the survey.

All respondents are involved either in identifying IT and network security requirements, evaluating or deciding on solutions and contractors, allocating budgets, or implementing or maintaining cybersecurity solutions. The study was completed in the first quarter of 2018.

GOVERNMENT RESPONDENTS BY JOB ROLE



The state of cybersecurity resilience and preparedness in federal agencies:

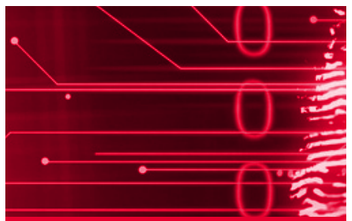


2 IN 3

... federal IT executives surveyed rate their agency's cybersecurity resilience — the ability to withstand a cyber event and continue to function — as moderately to highly mature.

9 IN 10

... IT executives surveyed say they are "very or somewhat confident" that their agency will continue running as usual in the midst of a cyberattack or IT security incident.

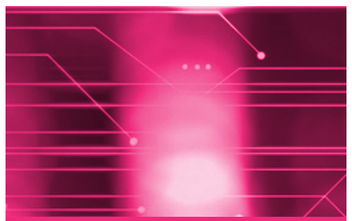


MORE THAN HALF

... of respondents say their organizations can respond to security incidents within 12 hours after detection.

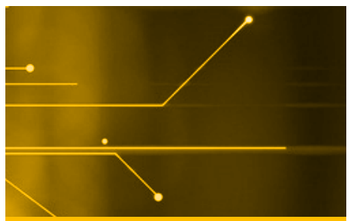
6 IN 10

... defense or intelligence executives — and half at civilian agencies — say their organizations "don't have all the tools and resources" needed in place to meet their security objectives.



HALF OF

... civilian executives — and 45% at defense/intelligence agencies — say their agencies lack the network context to prioritize responses to vulnerabilities.

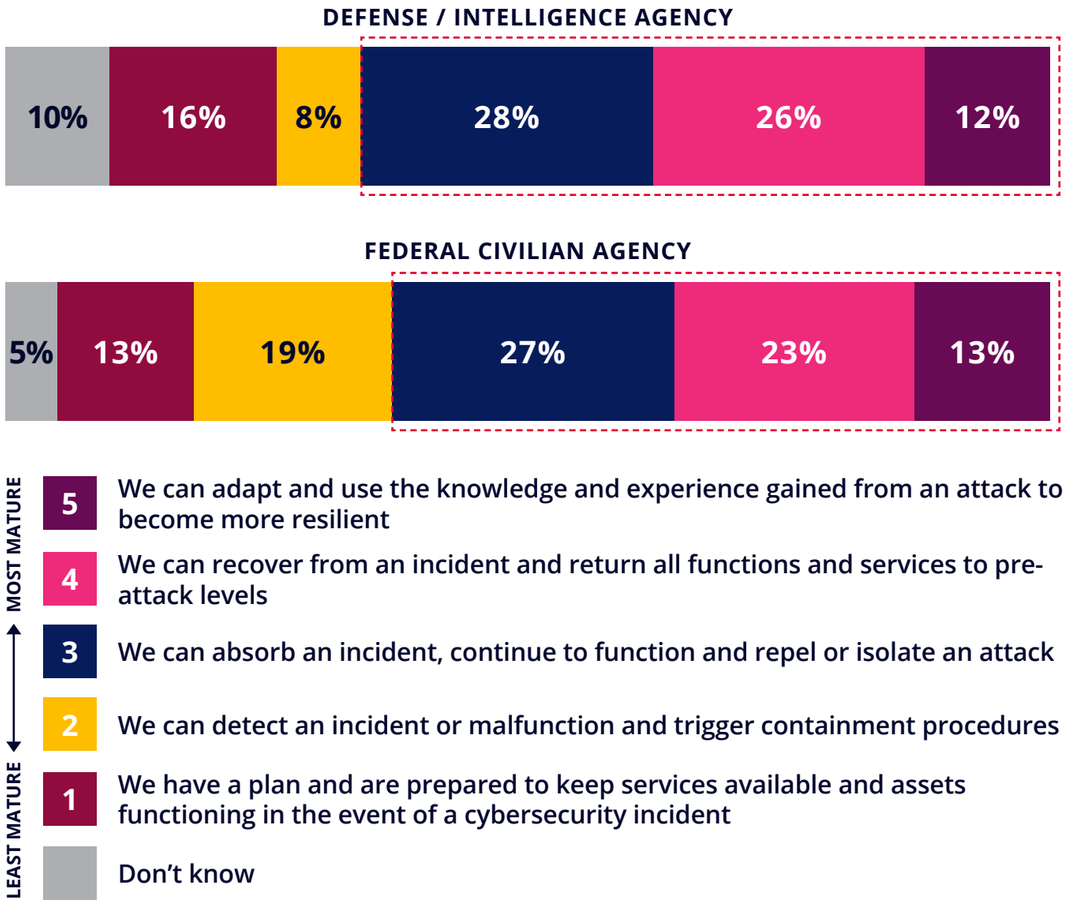


7 IN 10

... civilian executives and 55% at defense/intelligence agencies — believe the threat landscape is evolving quicker than their agency can respond.

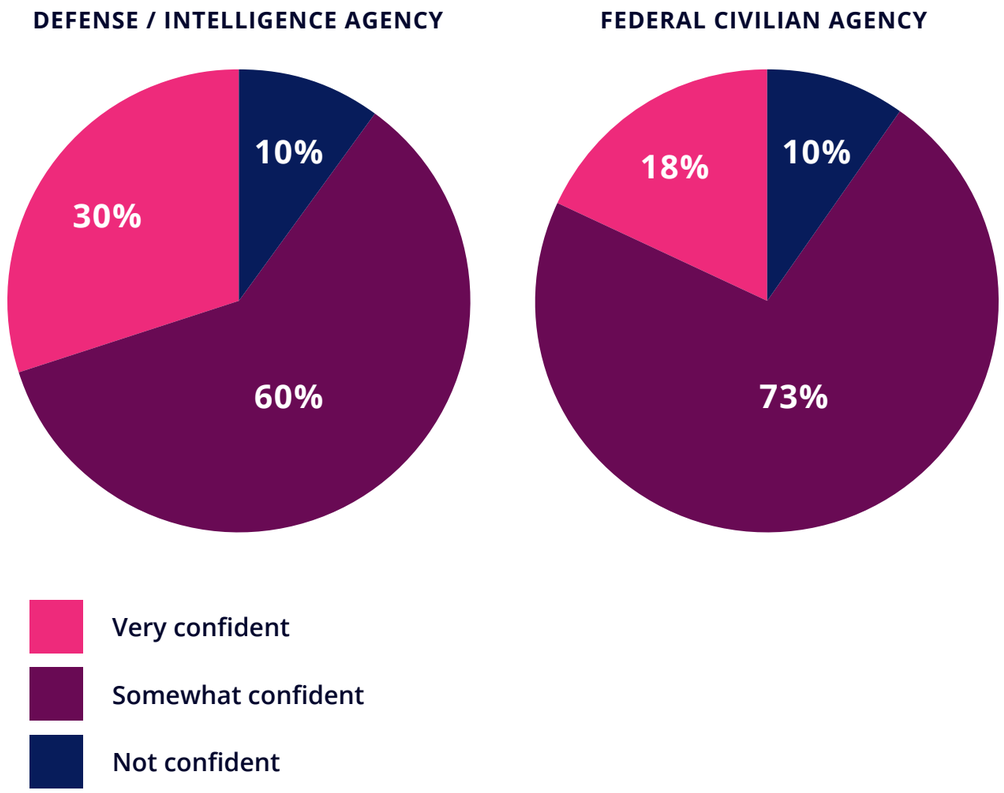
About **2 in 3** federal IT executives surveyed rated their agency's **cybersecurity resilience maturity** — the ability to absorb, recover or adapt to an attack — as **moderate to high**.

CYBER RESILIENCE MATURITY
(1=LEAST MATURE 5=MOST MATURE)

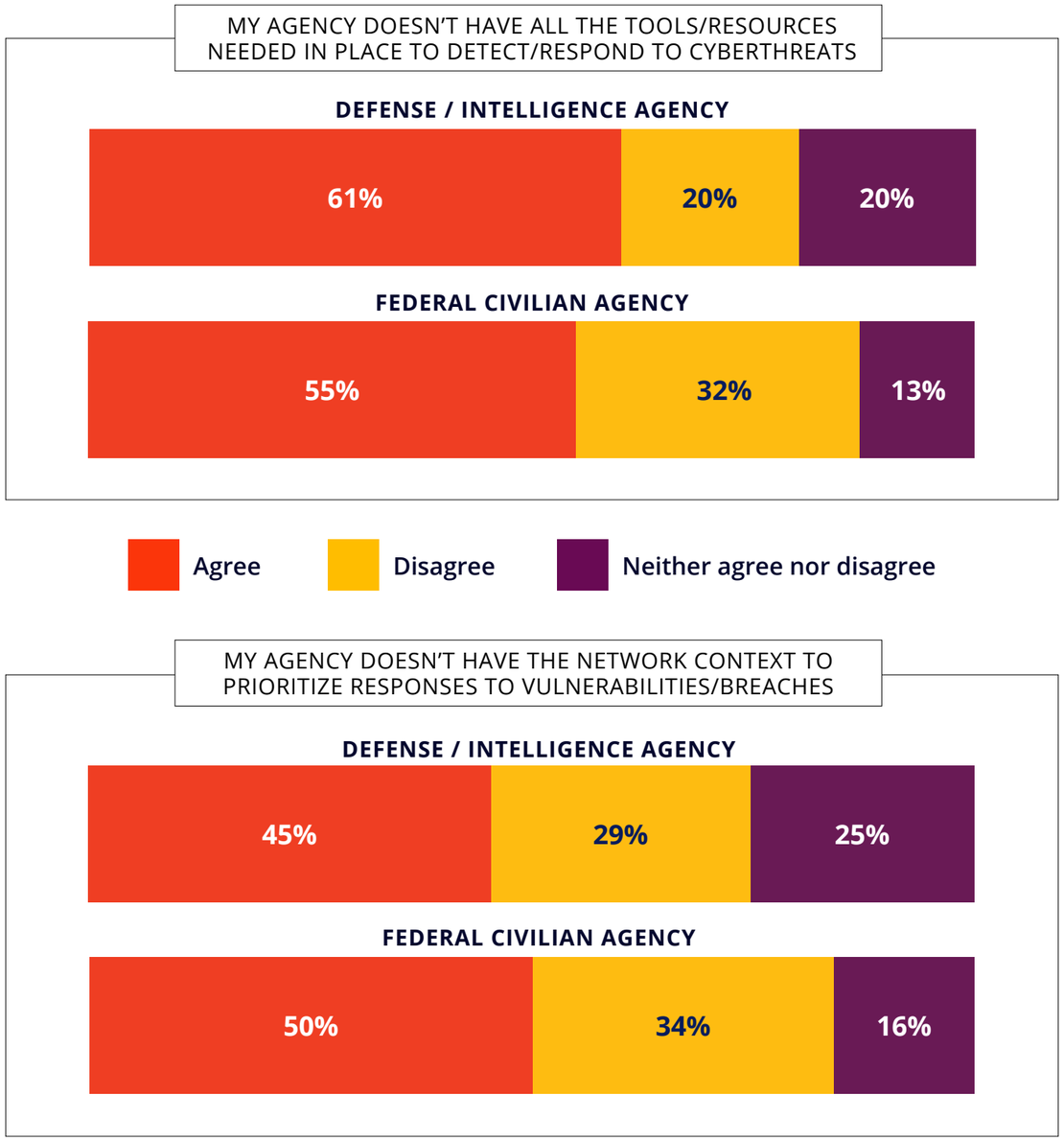


Nine in 10 federal IT executives are **confident** their agencies will "continue running as usual" in the face of a cyberattack. But a **majority** are only "**somewhat confident**."

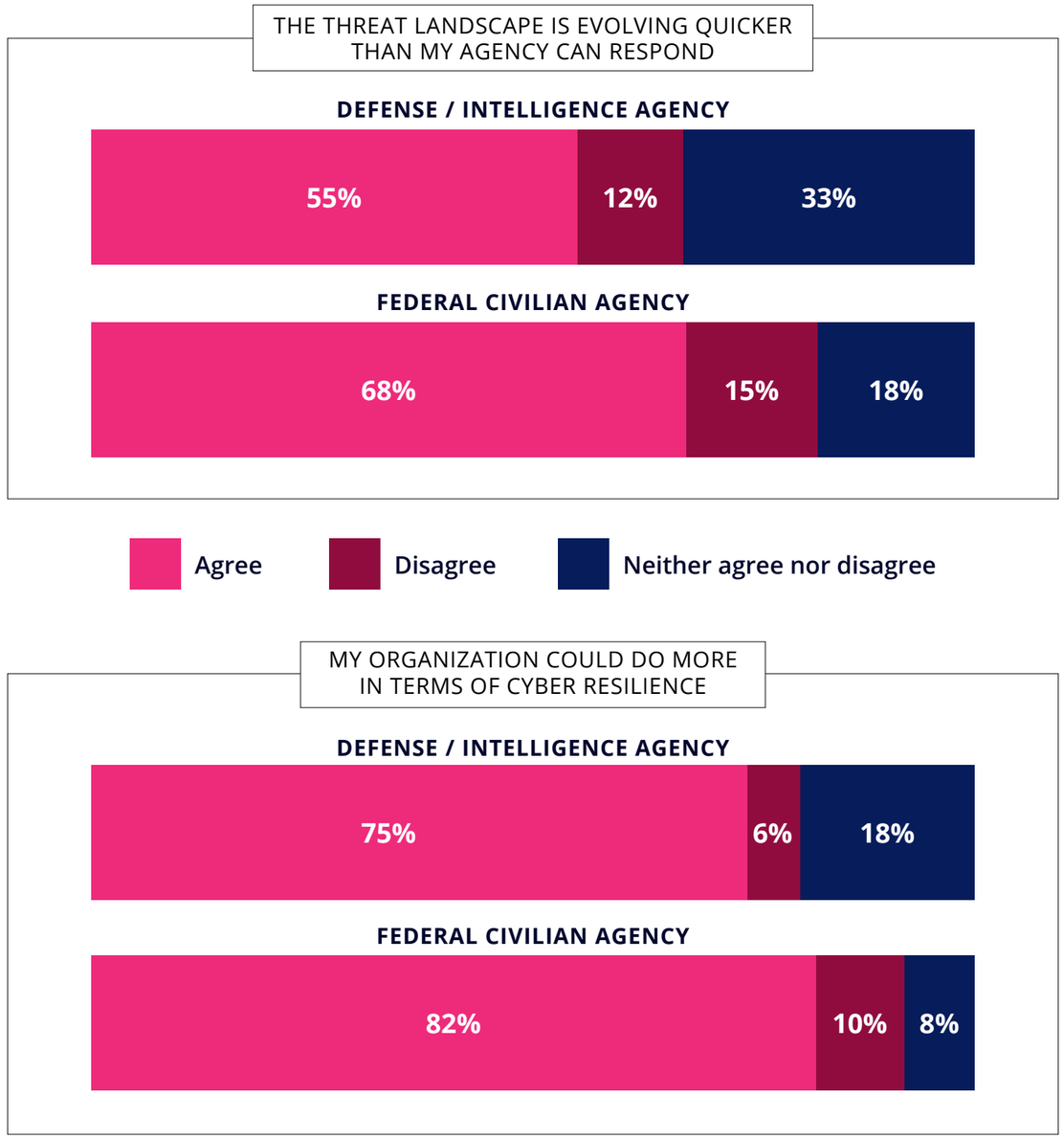
CONFIDENCE THAT THEIR ORGANIZATION WILL CONTINUE RUNNING AS USUAL UPON THE DISCOVERY OF A CYBERATTACK OR IT SECURITY INCIDENT



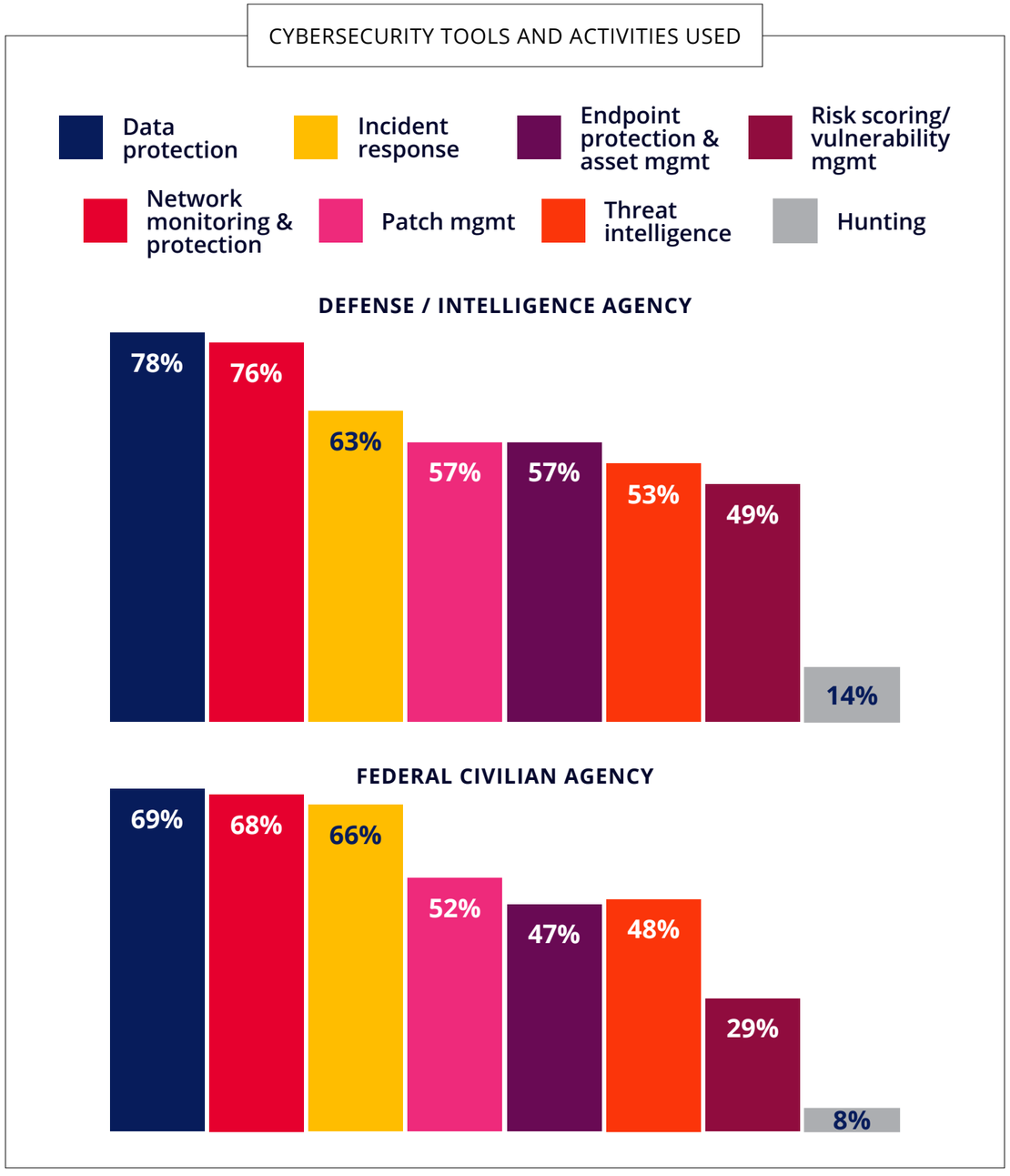
Though **2 in 3** respondents say their agency **"has sufficient tools and resources** to identify cyberthreats," roughly **half or more** agree that their agencies don't have all the **tools**...or **network context** they need.



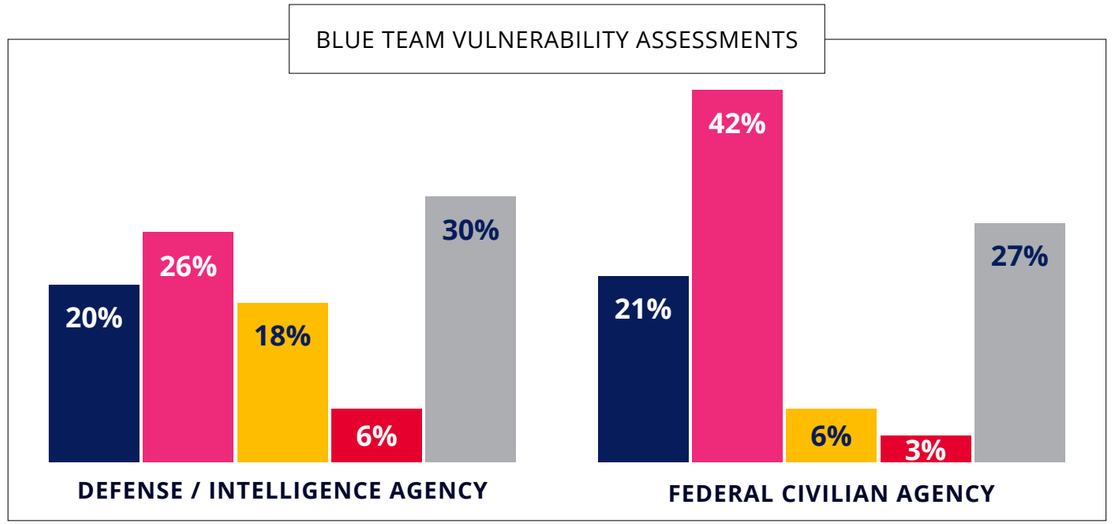
A **majority** of federal IT respondents believe that their **agency isn't keeping pace with evolving threats**...and could do more to ensure cyber resilience.

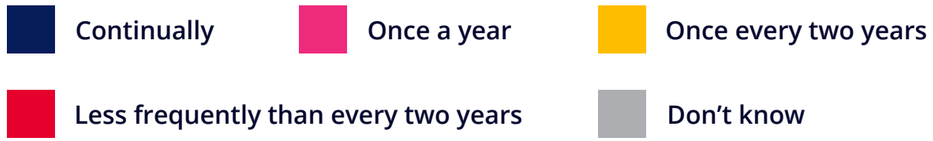


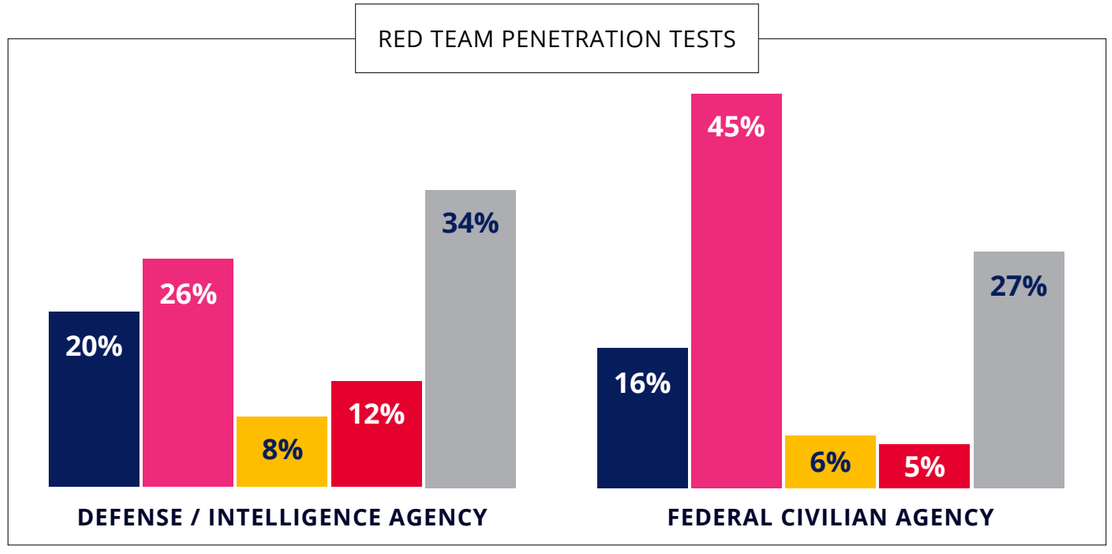
Agencies currently rely on various tools and tactics to guard against cyberthreats:



Only about **1 in 5** federal IT executives say their agencies conduct **Blue Team** / **Red Team** cybersecurity tests on a **continuous basis**.

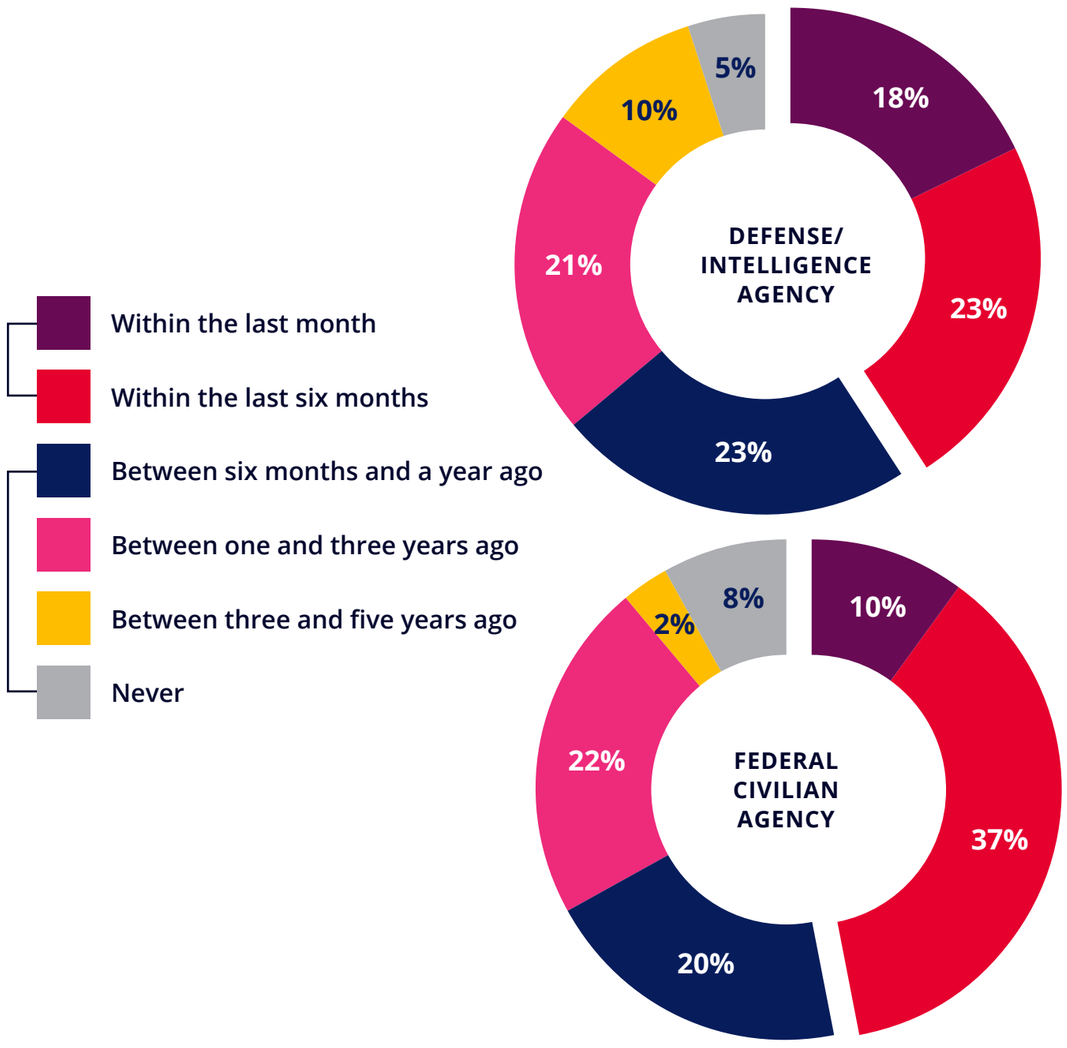






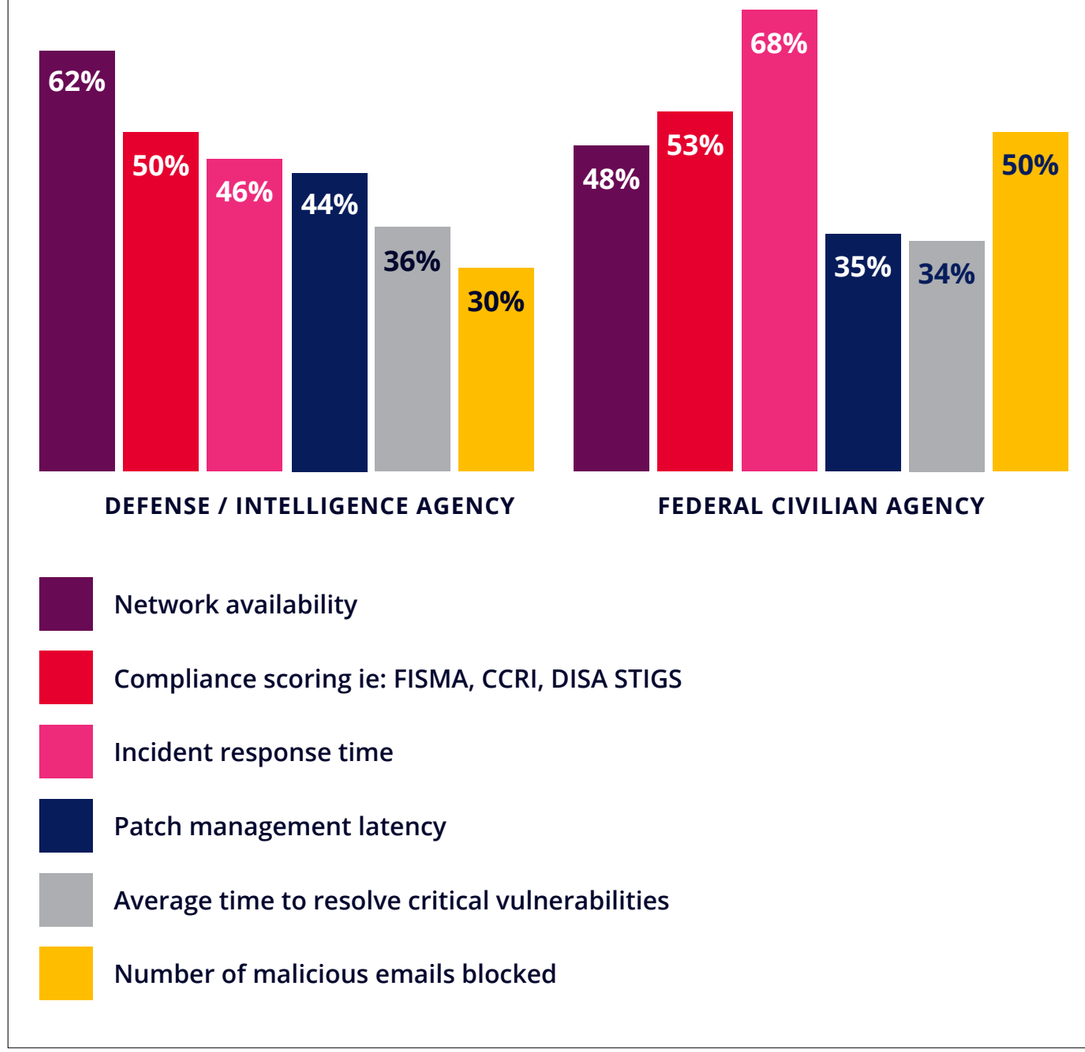
About **6 in 10 defense / intelligence** agency executives — and **over half at civilian agencies** — say their organizations **have not completed a map** or blueprint of their entire network **within the last six months.** Most respondents say they don't have the time, budget or resources.

THE LAST TIME THEIR ORGANIZATION CREATED A COMPLETE BLUEPRINT, MODEL OR MAP OF ITS ENTIRE NETWORK

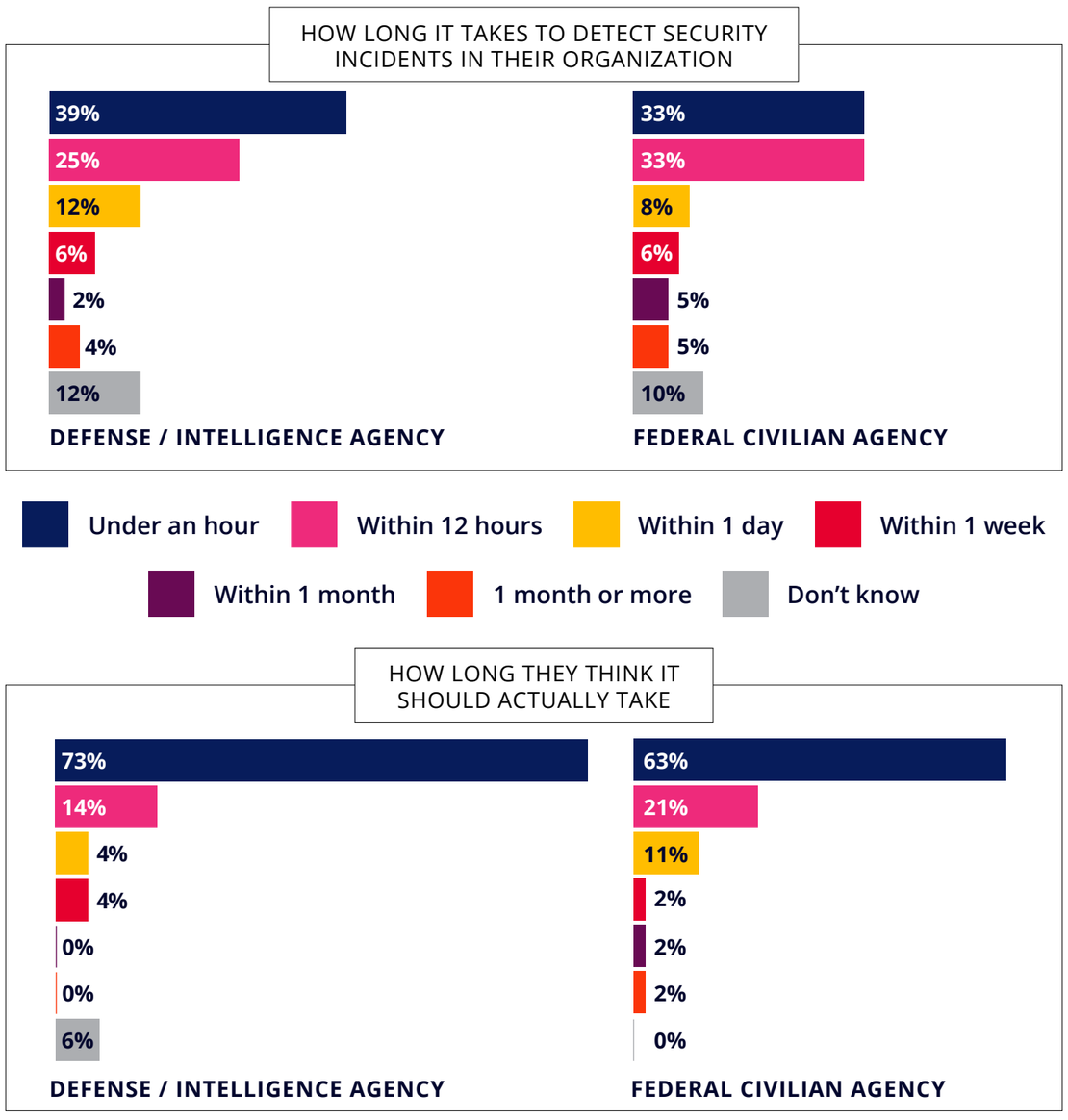


Agencies use multiple metrics to gauge the security of their networks. **Network availability** is cited most by defense/ intelligence IT executives; **incident response** is cited most by civilian agency executives.

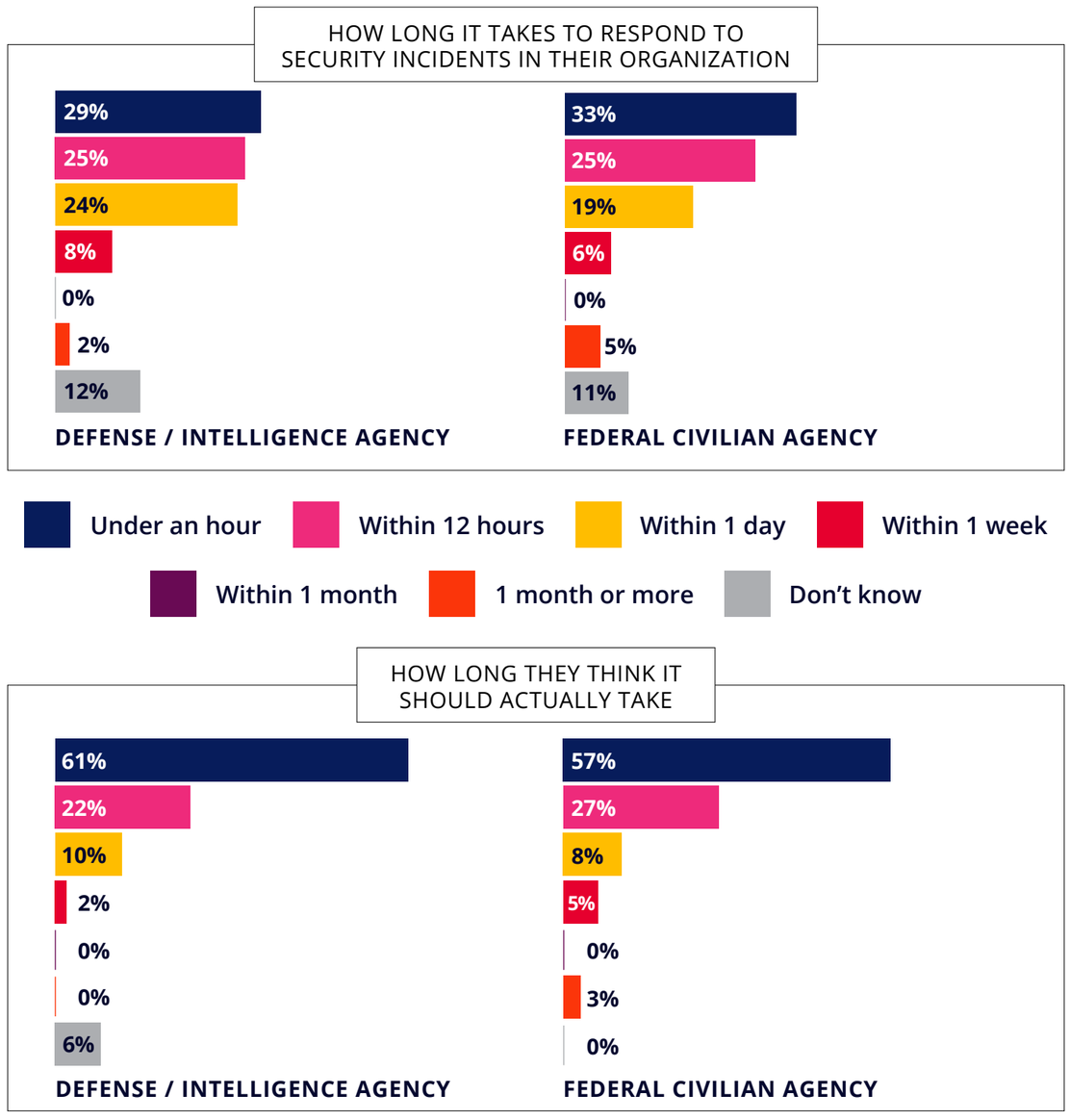
WHAT METRICS ARE CURRENTLY BEING USED TO MEASURE NETWORK SECURITY?



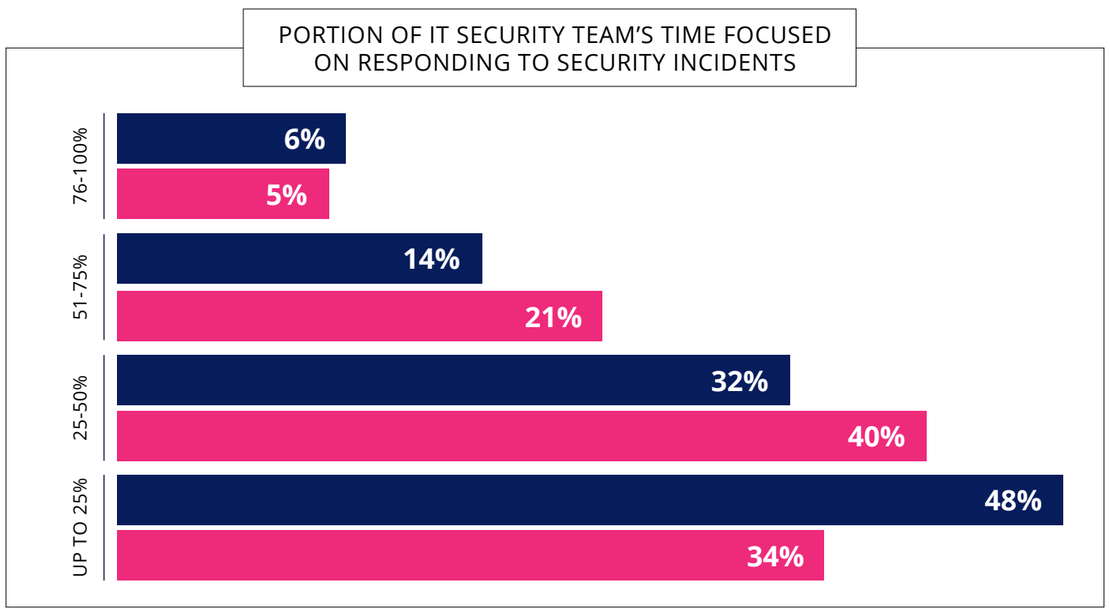
One-third of federal IT respondents say their agency can ***detect*** security incidents in **under one hour**; and more than two-thirds can do so within 12 hours. But nearly **2 in 3 civilian** — and nearly **3 in 4 defense/intelligence** — agency respondents say their agency ***should detect*** incidents in **under one hour**.



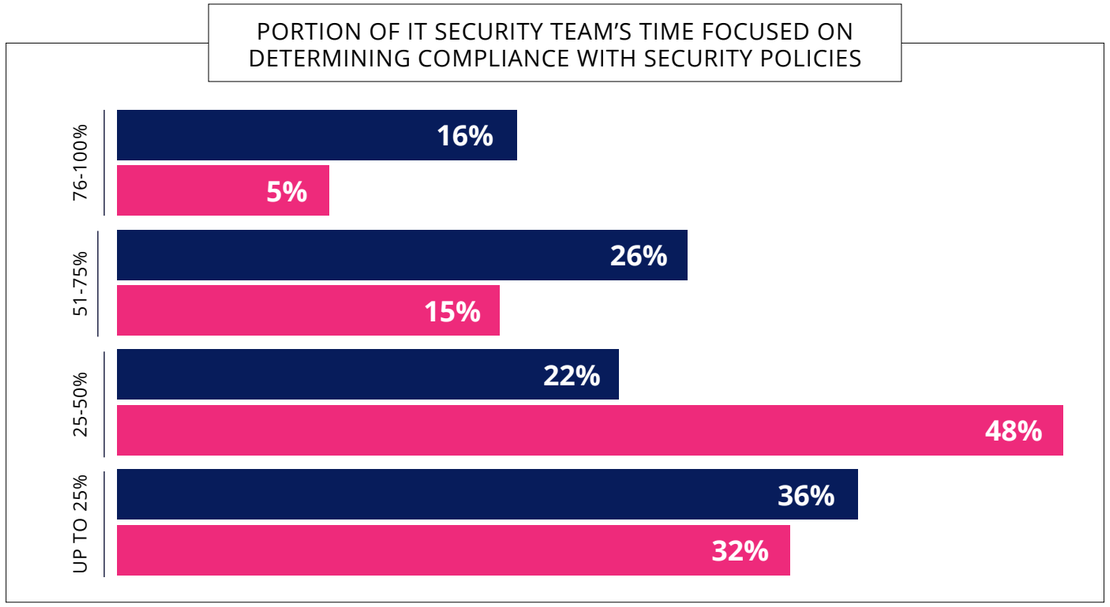
More than half of federal IT respondents say their agency can ***respond*** to security incidents **within 12 hours**. But the majority believe their agency ***should respond*** to security incidents in **under one hour**.

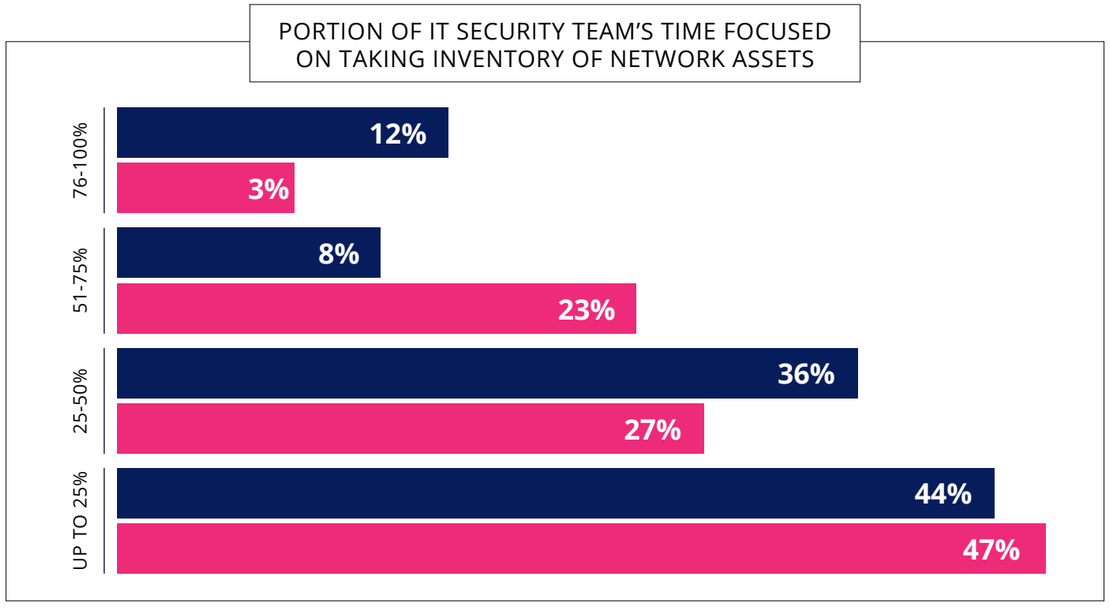


3 in 4 IT executives say their IT security teams focus **up to half** of their time **responding to security incidents**.

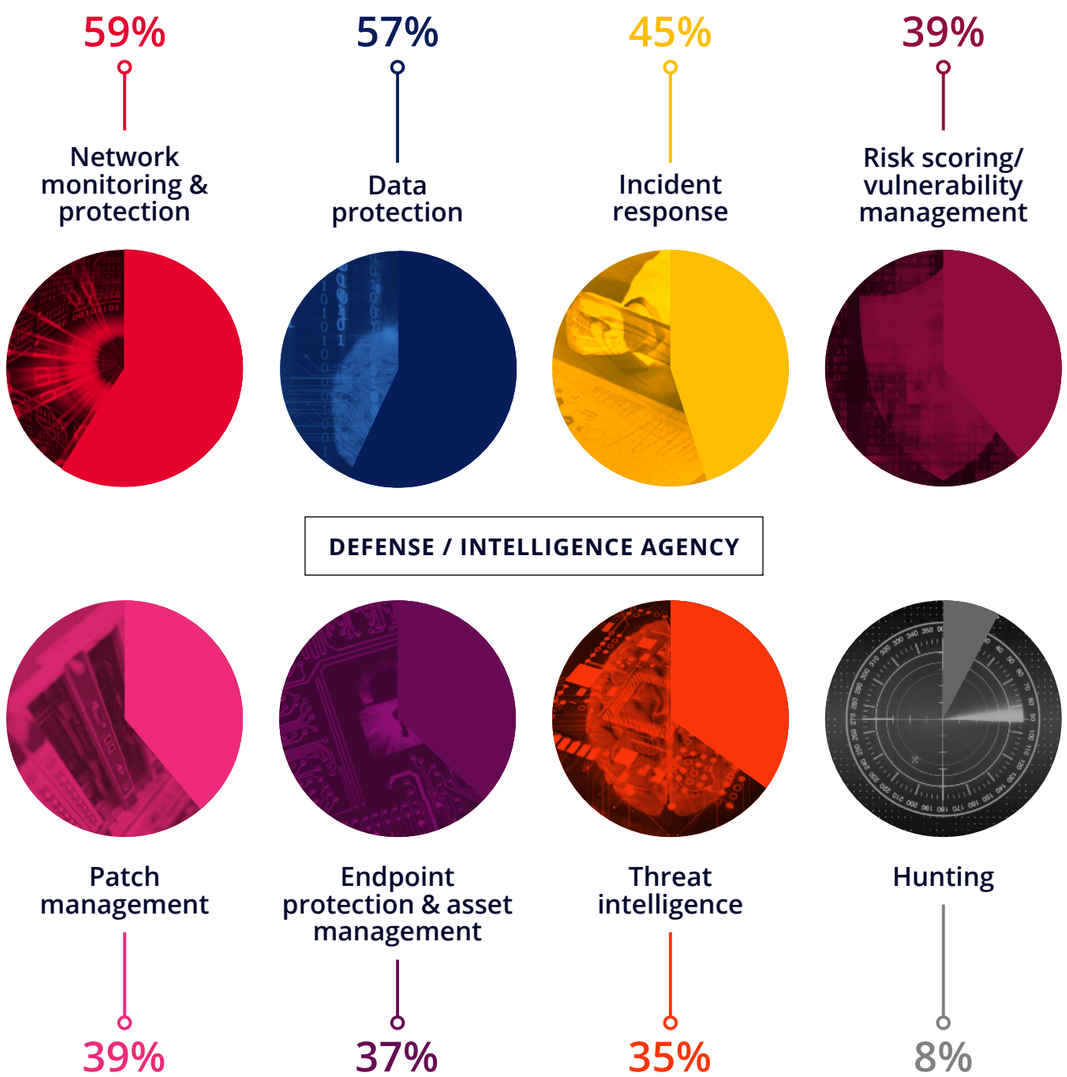


Determining compliance with security polices and **taking inventory of network assets** also consume a significant shares of the security teams' time.

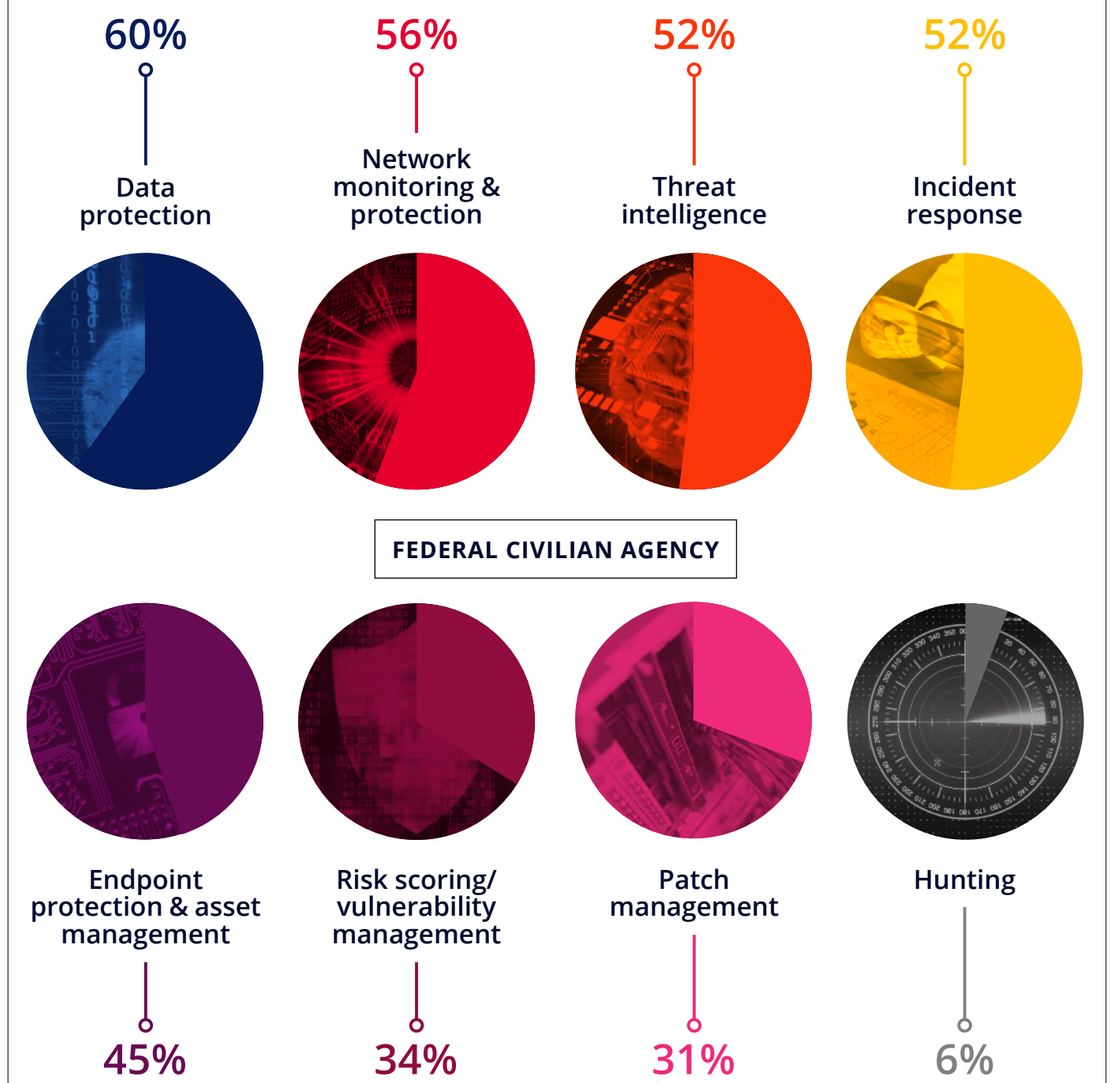




Looking ahead: **Data and network protection top the list of investment priorities** for civilian and defense/intelligence agency executives.

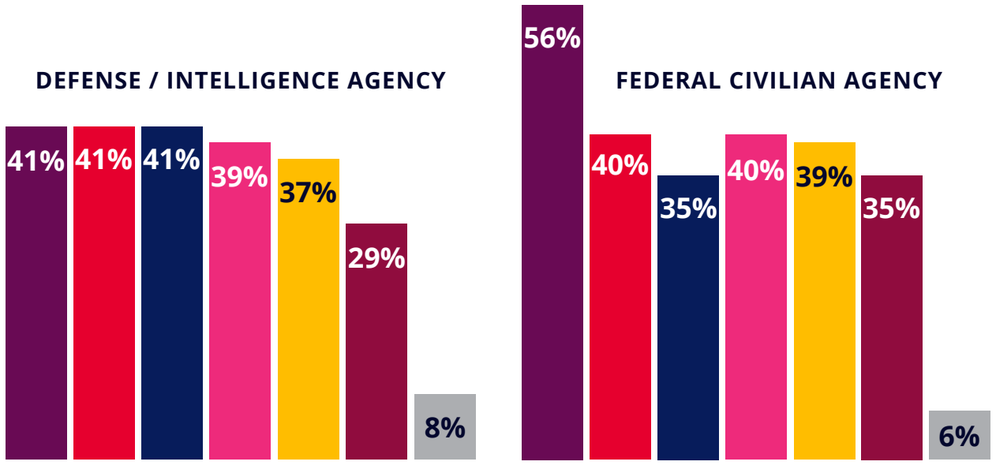


Civilian agency executives are giving **threat intelligence and endpoint/asset management investments higher priority** than their defense/intelligence counterparts.



Executives rank **competing IT priorities**, **a lack of cross-system visibility**, extensive **security requirements** and **inadequate automation** among their top obstacles to detecting and responding to cybersecurity incidents.

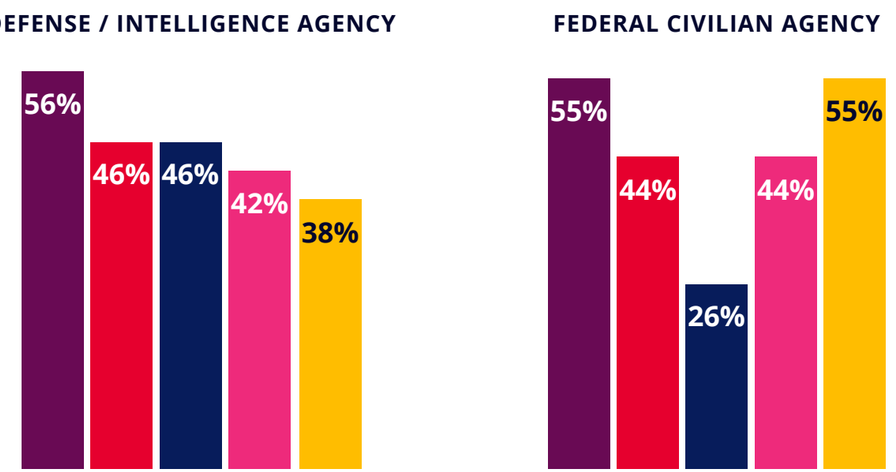
TOP OBSTACLES THAT PREVENT ADEQUATE DETECTION AND RESPONSE TO CYBERSECURITY INCIDENTS IN THEIR ORGANIZATION



- We have too many IT priorities competing for funding
- Cybersecurity requirements such as FISMA compliance, NIST guidelines, DOD STIG configuration or commercial security standards take a long time to implement and check
- Lack of integrated visibility across all IT security systems
- Incomplete real-time visibility of network configuration and potential risk points
- Cybersecurity activities are not adequately automated
- Cybersecurity tools do not prioritize threats to help us focus attention on the areas of highest risk
- Other (Lack of staff/trained personnel/understanding app behavior)

A **shortage of skilled cybersecurity professionals**, a lack of **training or understanding of existing capabilities** and **insufficient automation** continue to hinder cybersecurity efforts.

TOP PERSONNEL OBSTACLES TO CYBERSECURITY IN THEIR ORGANIZATION



- Not enough skilled cybersecurity professionals in our organization
- Staff lack training to use and optimize the cybersecurity tools we have
- Difficulty retaining skilled cybersecurity professionals
- Insufficient automation slows down productivity
- Staff do not fully understand the capabilities and benefits of the tools we have

1

CYBER INCIDENT RESPONSE

While about 2 in 3 federal IT officials claim their agency can detect cybersecurity incidents — and more than half claim they can respond — within 12 hours, officials stress the need for more skilled cybersecurity help to confirm there aren't deeper, undiscovered threats lurking in networks.

2

CYBERSECURITY RESILIENCE

Federal IT executives are very or somewhat confident that their agencies can absorb a cyberattack and continue to function. But more than half of civilian executives — and 6 in 10 at defense/intelligence agencies — say their agencies don't have all the tools and resources needed to meet their security objectives.

3

EVOLVING THREAT LANDSCAPE

The majority of IT executives believe the threat landscape is evolving quicker than their agencies can respond. More than 6 in 10 agreed if their agency could automate more monitoring and mitigation activities, it would be more secure.

4

OBSTACLES AND PRIORITIES

Executives are investing most heavily in fiscal 2019 into data and network protection tools and threat intelligence. But more than 3 in 4 agree there's more that their agency could do to fortify their cyber resilience.

cyberscoop

CyberScoop is the leading media brand in the cybersecurity market. With more than 350,000 unique monthly visitors and 240,000 daily newsletter subscribers, CyberScoop reports on news and events impacting technology and security. CyberScoop reaches top cybersecurity leaders both online and in-person through our website, newsletter, events, radio and TV to engage a highly targeted audience of cybersecurity decision makers and influencers.

fedscoop

FedScoop is the leading tech media brand in the federal government market. With more than 210,000 unique monthly visitors and 120,000 daily newsletter subscribers, FedScoop gathers top leaders from the White House, federal agencies, academia and the tech industry to discuss ways technology can improve government and identify ways to achieve common goals. With our website, newsletter and events, we've become the community's go-to platform for education and collaboration.

Learn more about RedSeal

Contact:

Wyatt Kash

Sr. Vice President, Content Strategy

Scoop News Group

Wyatt.Kash@FedScoop.com

202.887.8001

PRESENTED BY

cyberscoop | fedscoop

UNDERWRITTEN BY

REDSEAL