

CYBER ALERT OVERLOAD


GAINING THE UPPER HAND

**fed**scoop

UNDERWRITTEN BY  **FORCEPOINT**  
POWERED BY Raytheon

## TABLE OF CONTENTS

The Question . . . . .	<b>1</b>
Survey Results . . . . .	<b>2</b>
Key Findings . . . . .	<b>14</b>
Recommendations . . . . .	<b>15</b>
About FedScoop . . . . .	<b>16</b>

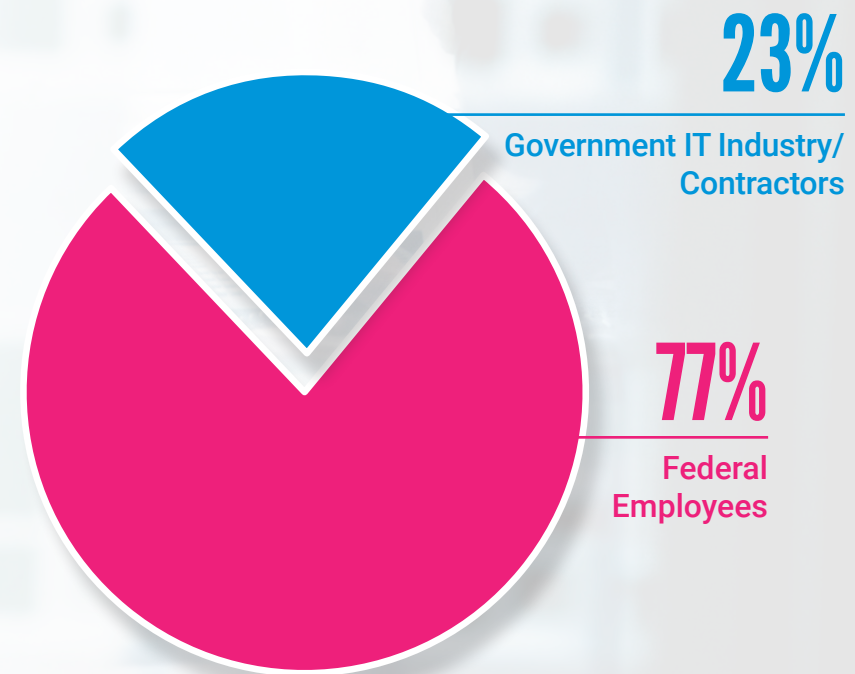
A blurred background image of an office setting. A person is visible in the foreground, leaning over a desk and working on a laptop. The image is faded and serves as a backdrop for the text.

## THE QUESTION

Are federal agencies and government IT firms adequately resourced to keep up with the rising tide of cyber threat alerts? And if not, are the growing array of cyber threat monitoring tools making it easier or harder for agencies to respond to those threats? This survey of government IT decision makers assesses the scope of the challenges IT departments face, their current capabilities and their resource demands in managing cyber threats.

## THE SURVEY

The findings of this survey reflect an audience of executive, senior and mid-level IT professionals either heavily, regularly or somewhat involved with the operation or strategy of security systems. Of those polled, 77% are federal employees, 23% work for government IT industry/contractors. The survey was conducted in March 2016. 100% of the questionnaires were completed online.



## MULTITUDE OF CYBER MONITORING SYSTEMS

The number of cyber threat detection products/systems is becoming a challenge in itself.

# 1 OUT OF 5

respondents have **more than 20 distinct cyber threat detection products/systems** to monitor.

70% have 5 or more systems to monitor.

## TAKE AWAY

The more systems people must monitor, the harder it becomes to coordinate response.

END-TO-END VISIBILITY STILL NEEDED

75%

OF INDUSTRY

respondents have  
“End-to-End Visibility” of  
network and user activity  
in one central location.

vs.

50%

OF GOVERNMENT

respondents have  
“End-to-End Visibility” of  
network and user activity  
in one central location.

## INTEGRATED VIEW STILL LACKING

# ONLY 1 OF 3

government respondents have a single, **integrated view** of threats, compared to half of industry respondents.



## TAKE AWAY

The lack of a single, integrated, end-to-end view of activity creates a significant handicap in detecting—and responding to—cyber threats.

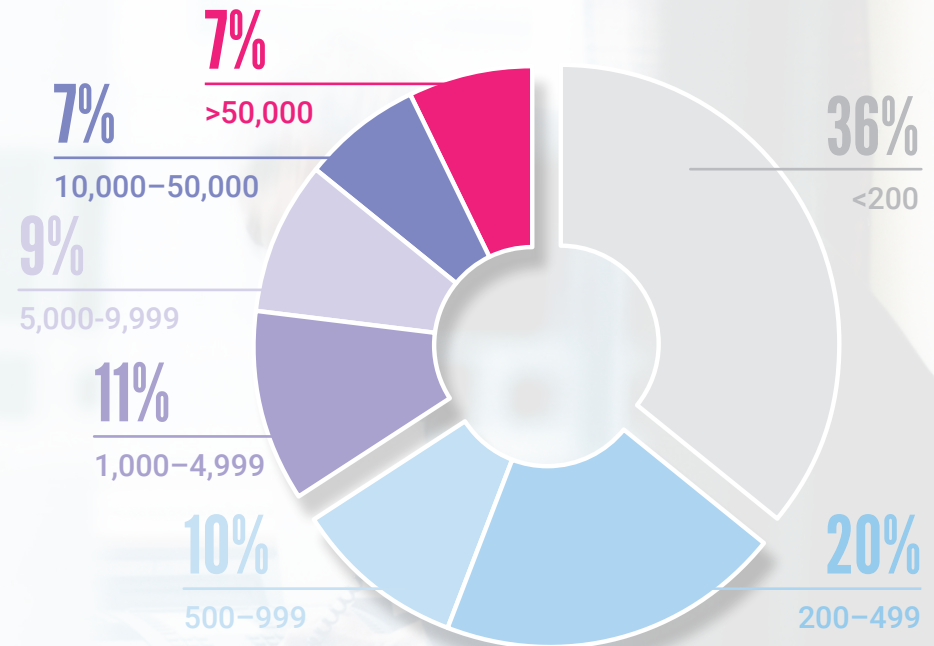
## CYBER ALERT OVERLOAD

# ONE THIRD

of respondents report their IT departments receive more than 1,000 security alerts/day.

# NEARLY 1 IN 10

receive more than **50,000/day**.



## TAKE AWAY

The sheer volume of security alerts demands a comprehensive approach to prioritize response.

## DETECTION CAN TAKE DAYS...WEEKS

**ONLY 15 %**  
OF GOVERNMENT

vs.

**45 %** respondents can identify a threat on their network within 1 hour.  
OF INDUSTRY

**55 %**  
OF GOVERNMENT

vs.

**43 %** said it takes 7+ hours, days, or weeks to detect network threats (or simply weren't sure.)  
OF INDUSTRY

## TAKE AWAY

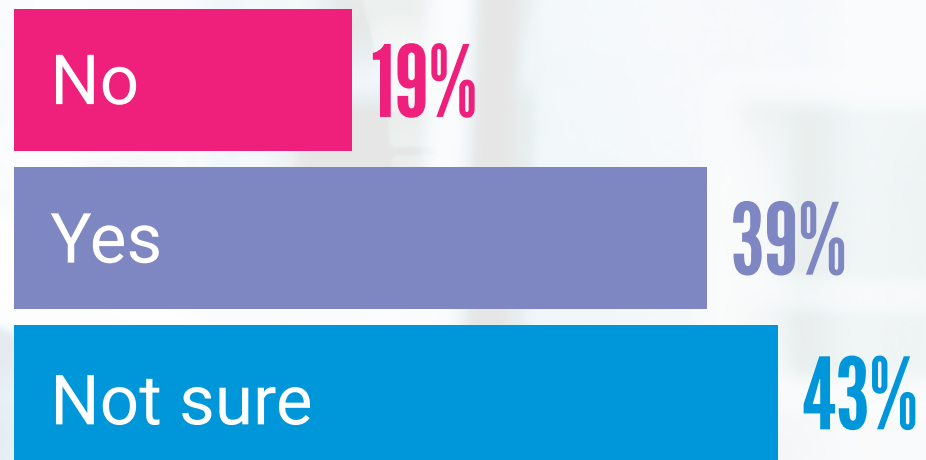
The longer the delay in detecting a threat, the more costly the potential damage.



## TRACKING DWELL TIME

# ONLY 4 OUT OF 10

respondents—in government and in industry—currently track how long attackers were on their networks before they left or were ejected.



## TAKE AWAY

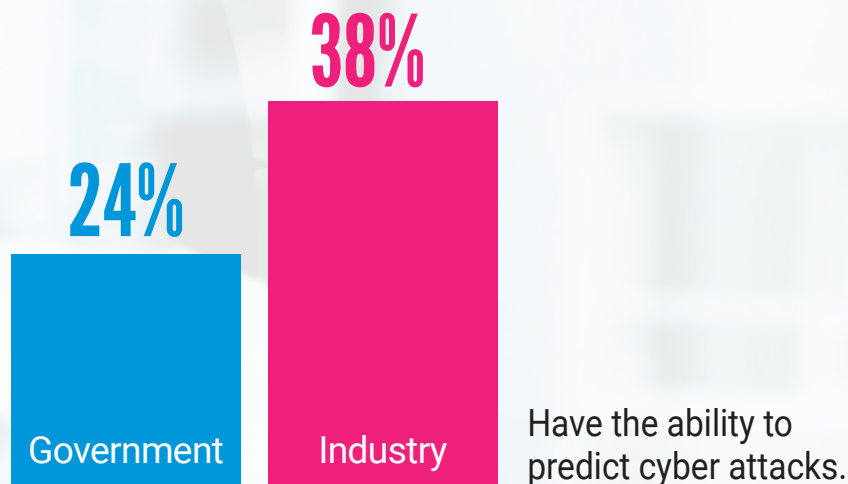
Tracking dwell time can aid understanding the nature of vulnerabilities and compromises.

## ABILITY TO PREDICT ATTACKS

Most IT departments still lack the ability to predict cyber attacks:

**ONLY 1/4**

**government** (and **4 in 10 industry**) respondents say their IT departments can do so.



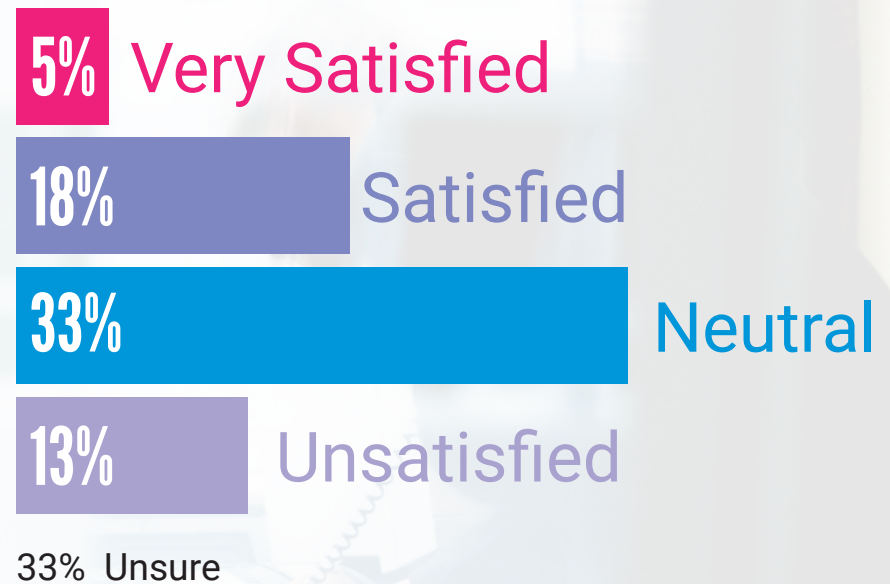
## TAKE AWAY

The lack of prediction tools makes it harder for IT teams to get ahead of potential cyber threats.

## CONTINUOUS MONITORING & DIAGNOSTICS GETS MIXED MARKS

# < 1 OF 4

respondents who use the Department of Homeland Security's CMD program are satisfied with its ability to support cyber threat detection.



### TAKE AWAY

CMD helps but still gets mixed marks for addressing the total threat challenge.

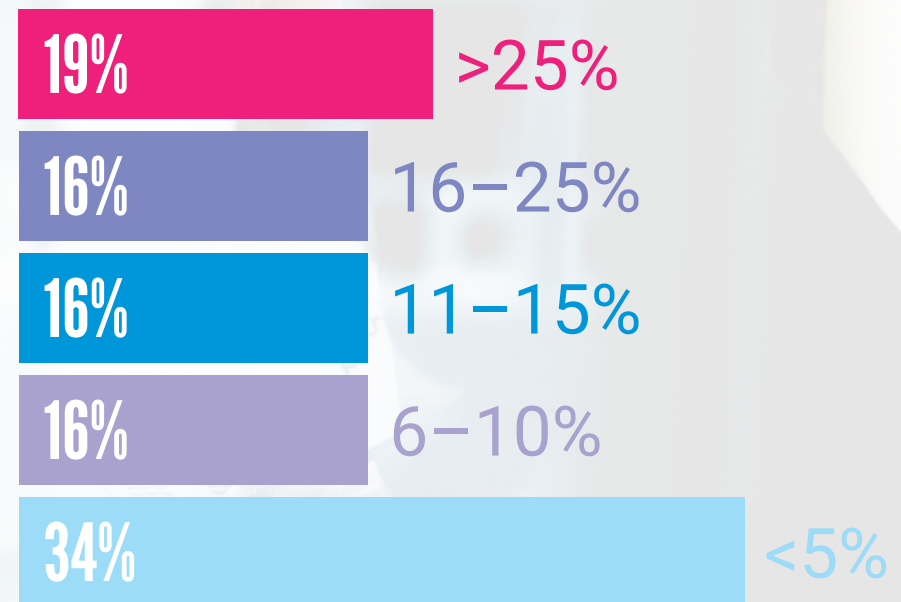
## HELP WANTED—OPEN POSITIONS

# HALF

of all respondents report **over 10%** of budgeted cybersecurity positions are **vacant**.

# 1 IN 4

government respondents say **over 25%** of budgeted cybersecurity positions are currently unfilled.



Percentage of budget cybersecurity positions currently unfilled (all respondents.)

## HELP WANTED— MEETING DEMANDS

**2/3**

of **federal** respondents believe cybersecurity staffs need to expand more than 10% next year to meet enterprise security goals.

vs.

**1/2**

of **industry** respondents believe cybersecurity staffs need to expand more than 10% next year to meet enterprise security goals.

**20%**

of **feds** believe cyber staffs need to grow **over 25%** to meet those goals.

## HELP WANTED—THE RECRUITMENT CHALLENGE

# 2/3 FEDS

say it takes at least 6 months to hire a cybersecurity specialist, compared to about **1/3 industry** respondents.

# OVER HALF

of **both groups** says they can't find qualified cybersecurity specialists for the majority of positions.



# CONCLUSIONS & RECOMMENDATIONS

## CONCLUSIONS

### Key Issues:

- 1** Finding and retaining cybersecurity professionals, particularly in government, remain very challenging.
- 2** The daily volume of cyberthreat alerts across the stack continues to grow to levels that challenge traditional monitoring and mitigation programs.
- 3** Too many alert systems makes it harder to prioritize and respond to an avalanche of threat alerts.



## RECOMMENDATIONS

- 1** Cybersecurity teams need to be better equipped with the right tools in order to be productive, proactive, and predictive.
- 2** Fully deploy end-to-end network monitoring systems that can report real-time situational awareness of users, devices and activities on the network.
- 3** Integrate cyber threat monitoring and mitigation systems to create total visibility and automate response.

# ABOUT FEDSCOOP

FedScoop is a Government IT media company, a one stop news source and the government IT community's platform for education and collaboration. FedScoop gathers top leaders from The White House, federal agencies, academia and the tech industry to discuss ways technology can improve government, and to exchange best practices and identify ways to achieve common goals.

fed scoop