2021 Devo SOC Performance Report™:

Federal Edition

Survey independently conducted by Ponemon INSTITUTE

2021 Devo SOC Performance Report™:
Federal Edition

TABLE OF CONTENTS

For the past three years, Devo has published a report, based on independent survey results, capturing the perspectives of cybersecurity professionals who work in security operations centers. The 2021 Devo SOC Performance Report™ shows that SOCs — and the people who work in them — face several significant challenges. In 2021, for the first time, Devo expanded the reach of the survey to include more than 100 professionals who lead or work in SOCs for federal agencies, bureaus and departments.

The overall 2021 survey results show a continuation of the pain of SOC work that has been reflected in all of the survey results Devo has published since 2019. This federal edition of the 2021 report delves into the specific responses from federal SOC workers and shines a spotlight on their opinions, concerns and ideas for alleviating the pain of pressure-packed SOC jobs.

To put that pain into perspective, federal survey respondents were asked to rate — on a 10-point scale — the pain their organization's SOC personnel experience in meeting their daily job requirements. The majority of respondents rated SOC workers' pain in their organizations as being at a very high level. That's a problem organizations and SOC leaders need to address. This federal-centric report delves into the survey results to identify the pain points, frustrations and other challenges federal SOC workers face.

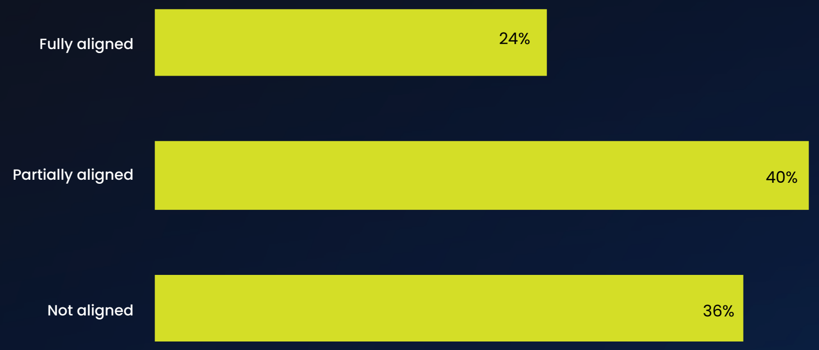
Getting Federal Organizations — and Their SOCs — on the Same Page

For a security operations center to function optimally, there needs to be a collaborative alignment between SOC objectives and the business needs of the organization. Let's start our examination of these survey results by looking at whether federal survey respondents feel their SOC is in sync with the needs of the agency, bureau or department they serve.

First, the good news. Nearly one-quarter of respondents feel their SOC's objectives are aligned with the overall needs of the organization they serve. Now the not-so-good news. That means nearly three-quarters of respondents see partial or no alignment between business needs and the SOC. Less than half feel their SOC is partially aligned with business needs. Even worse, more than one-third feel their SOC is not at all aligned with the business needs of their organization.

Figure 1.

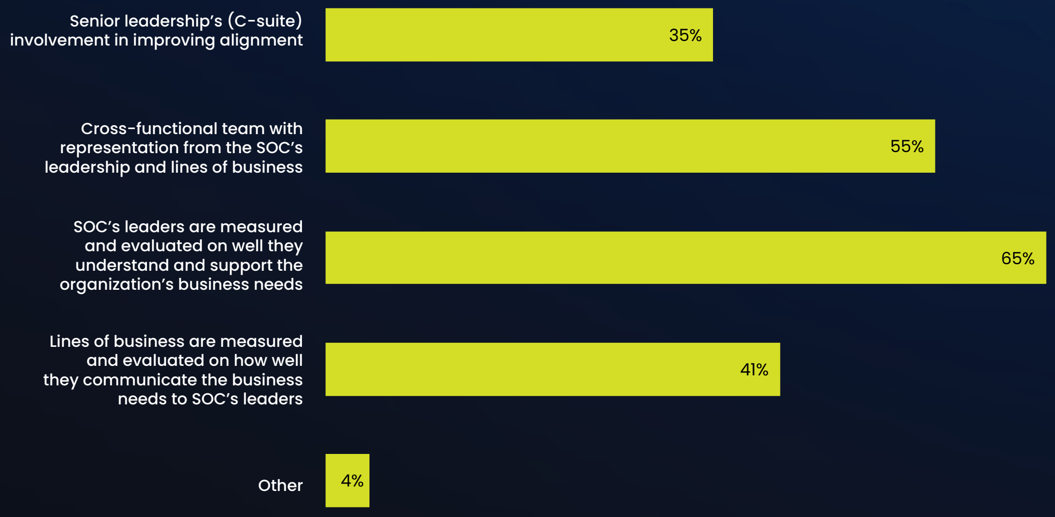
Within your organization, are SOC objectives aligned with business needs?



What can be done about this issue? Those federal SOC workers who felt their SOC's objectives were only somewhat or not at all aligned with business goals were asked to choose two ways to improve the situation. The majority of respondents felt the responsibility lies with SOC leadership, with more than two-thirds saying SOC leaders should be evaluated on how well they understand and support business needs. The next highest-ranked response, chosen by more than half of respondents, was to have SOC leaders work more closely with the organization's lines of business.

Figure 2.

If alignment between the SOC's objectives and your organization's business needs is only partially or not aligned, what would improve alignment? Please select your top **two** choices.



Barriers to SOC Success

By now, the theme of this survey's results is clear: There are problems in federal SOCs that range from painful working conditions to disconnects between the SOC and lines of business as well as shortcomings with SOC leadership. Let's dig deeper to gain insights into what is preventing SOCs from achieving greater success.

When asked to identify the top three barriers to successful SOC operation, 61% of federal respondents cited turf or silo issues between the organization's IT security operations and the SOC. A close second is a lack of visibility into the IT security infrastructure, chosen by 60% of respondents. Those two issues are closely related and also reflect responses to the previous question about how to improve alignment between the SOC and business needs.

The third most popular response is a bit of a departure from internal disconnects or turf battles. 55% of respondents said that the lack of available analyst talent is a major impediment to the successful operation of federal SOCs. This is a huge barrier to success that is not unique to the federal government. In the overall survey of more than 1,000 cybersecurity professionals, the issue of not being able to find, hire and retain SOC analysts has consistently been among the top annual challenges. A similar number of overall 2021 survey respondents from a wide range of industries cited this as a continuing obstacle to SOC success.

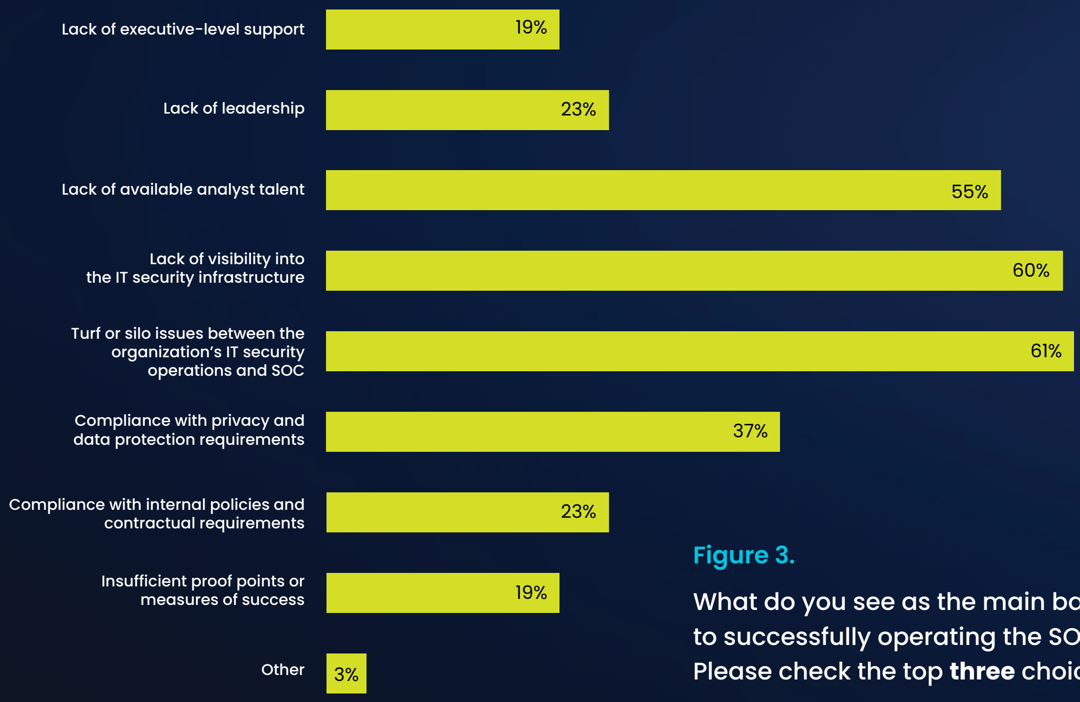


Figure 3.

What do you see as the main barriers to successfully operating the SOC? Please check the top **three** choices.

Given the challenges already identified by federal SOC practitioners, it should come as no surprise that most respondents do not feel their SOC is operating with high effectiveness. The survey asked participants to rate the effectiveness of their SOC on a 10-point scale. At the high end, 46% of respondents rated their SOC a 7 or above, which translates to being highly effective. However, the majority of respondents — 54% — rated their SOC as being somewhat effective to ineffective, giving it a rating of 6 or lower.

Figure 4.

Using the following 10-point scale, please rate the effectiveness of your organization's SOC.
On a scale from 1 = Ineffective to 10 + Very effective

1 or 2	9%
3 or 4	11%
5 or 6	34%
7 or 8	26%
9 or 10	20%

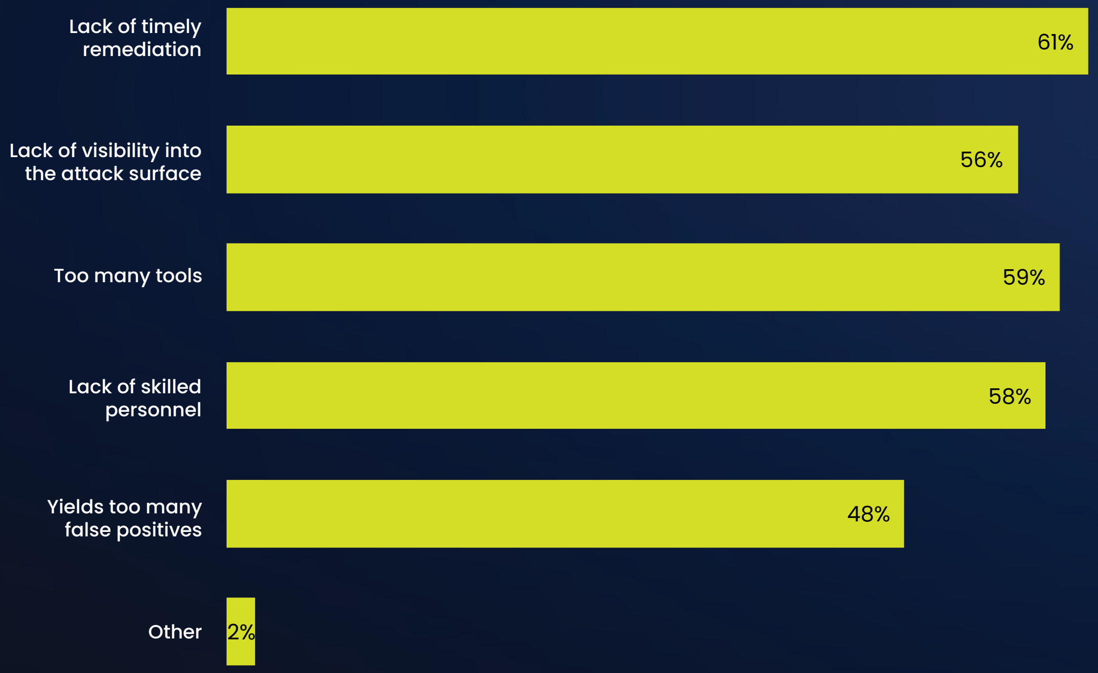
What's Causing These Pain Points?

After taking the pulse of SOC professionals to measure how effective — or ineffective — they feel their SOC is, let's look at the reasons behind these less-than-stellar opinions.

When asked to identify the causes of SOC ineffectiveness (respondents could choose all responses they felt applied to their situation), the answers spanned a wide range, from lack of timely remediation capabilities to lack of visibility into the attack surface. 59% of respondents cited "too many tools" as a reason their SOC is ineffective. This may be the most interesting response because very often when a business problem is identified the response is to find the budget to buy new tools in the hope that will remedy the situation. But these survey results throw cold water on that concept. It would appear that it's not a case of adding *more* tools but rather providing the *right* tools that is likely to deliver the desired performance improvements.

Figure 5.

What makes your organization's SOC ineffective (responses 1 to 4 on the scale above)? Please select all that apply.



The Importance of Effective Communication

With SOC professionals' opinions about what makes their SOC ineffective, let's look at the people who are contributing to the problem.

In a high-pressure work environment such as a federal SOC, it is vitally important that everyone on the team knows what's expected of them, what they need to focus their efforts on, and how they need to work together as a team — and with other organizational departments and lines of business. To make any or all of those objectives possible requires one foundational element: good communication.

Survey respondents were asked to rate the ability of SOC leaders to communicate the SOC's strategy to the entire team. A small minority — 12% — felt leadership does a very good job of communicating. Nearly as many respondents — 10% — said their leaders are not good communicators. Only 29% of respondents rated their leaders a 7 or 8 on the 10-point scale. There is much work to be done in this area at most federal SOCs.

Figure 6.

Using the following 10-point scale, please rate how well SOC leaders communicate the SOC’s strategy to staff members from 1 = not well at all to 10 = exceptionally well.	
1 or 2	10%
3 or 4	23%
5 or 6	26%
7 or 8	29%
9 or 10	12%

The ability to articulate the SOC’s strategy, along with other vital information, is just one part of the communication equation.

The other ability survey respondents were asked about is how well SOC leaders listen to and understand what team members need to perform their jobs as effectively as possible. Not surprisingly, respondents’ scores about the listening and comprehension skills of their leaders were in line with their assessment of those leaders’ communication skills.

30% of respondents rated their leaders as a 4 or below out of 10 for how well they listen and understand. Only 46 percent of respondents said their leaders did a very good or better job when it comes to comprehending the needs of SOC team members.

Again, this is another area that needs attention in the effort to reduce analysts’ pain and make federal SOCs operate more efficiently and effectively.

Figure 7.

Using the following 10-point scale, please rate how well SOC leaders listen to and understand the needs and priorities of staff from 1 = not well at all to 10 = exceptionally well.	
1 or 2	10%
3 or 4	20%
5 or 6	24%
7 or 8	30%
9 or 10	16%

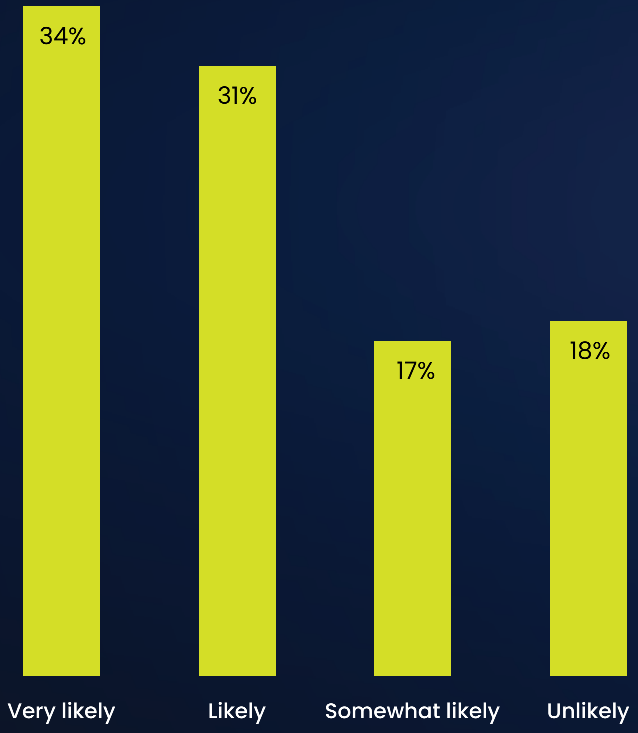
The Right Tools for the Job

We've already seen how nearly 60% of SOC professionals feel there are too many tools for them to learn, master and use as they work to identify, hunt and remediate the barrage of threats common to every SOC. But as noted above, it's important to provide SOC analysts with the right tools to do their jobs, including emerging technologies that incorporate artificial intelligence and machine learning, particularly when it comes to sifting through and prioritizing the relentless threat stream. 65% of respondents said their organization is likely or very likely to deploy new or different technologies to try and improve SOC performance. Only 18% of respondents said such technological enhancements were unlikely in their organizations.

It's a positive development to see that SOC workers believe their leaders are willing to embrace new technologies to help make their jobs easier and improve productivity.

Figure 8.

How likely is your organization to add new technologies or change technologies to improve the operation of the SOC?



The Pain Remains

Throughout this report, the topic of SOC analyst pain has been a consistent theme. Even without taking a survey, anyone who works in or adjacent to a security operations center, particularly in the federal government, should be well aware that the work is difficult, and the pressure is high. Relentless, sophisticated and clever threat actors from around the world are fixated on disrupting government (and non-government) entities, stealing or destroying data, and generally putting a continuous high level of pressure on SOCs.

The next question directly addresses the elephant in the SOC, so to speak. Survey respondents from federal SOCs were asked to assess how much pain SOC workers experience in performing their work.

We may as well start with the bad news first: 39% of respondents said the pain experienced by SOC workers is 9 or 10 on a 10-point scale. Right behind that came 36% of respondents who put the pain level at 7 or 8. That means 75% of survey respondents feel that working in a federal SOC is painful. Not surprisingly, only 10% of respondents rated workers' pain at 4 or below.

Figure 9.

Using the following 10-point scale, please rate the "pain" your organization's SOC security personnel experience in meeting their daily job requirements.

From 1 = low pain to 10 = very painful

1 or 2	2%
3 or 4	8%
5 or 6	15%
7 or 8	36%
9 or 10	39%

Sources of SOC Analyst Pain

Now that we know how strongly respondents feel about painful working conditions in the SOC, let's delve into the causes of that chronic discomfort.

Survey respondents were presented with more than a dozen reasons for SOC workers' pain and asked to select all they felt applied to their own experience. 72% of respondents cited burnout due to increasing workloads.

Other responses chosen by more than half of respondents include information overload (69%), lack of visibility into the attack surface (66%), and lack of resources (56%). While the level of pain and its causes likely vary from federal SOC to federal SOC, the following chart presents a harrowing picture of myriad problems that need to be addressed and remediated as quickly and effectively as possible. It's a situation not unlike every SOC needing to respond promptly and efficiently to the threats that fill their screens all day, every day.

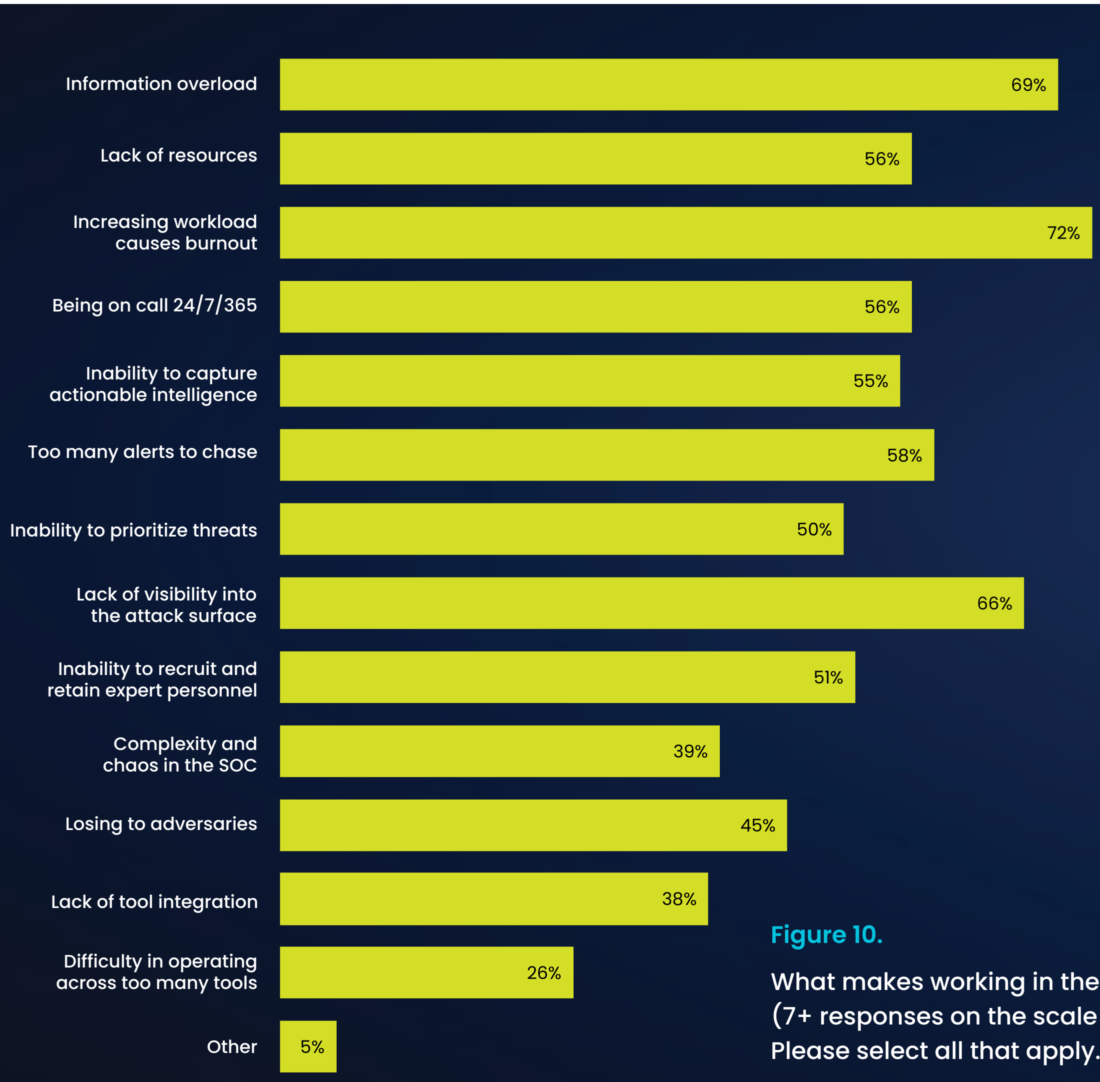


Figure 10.

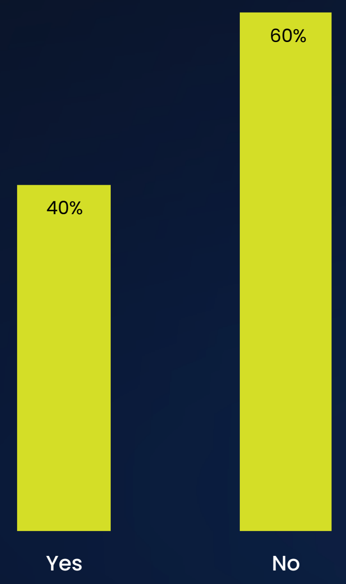
What makes working in the SOC painful (7+ responses on the scale above)? Please select all that apply.

Pain Prevents Gain

To determine a benchmark, survey respondents were asked if their SOC tracks performance based on mean time to remediate (MTTR). More than one-third of respondents said that is a metric used in their SOC.

Figure 11.

Does your organization track Mean Time to Remediate (MTTR)?

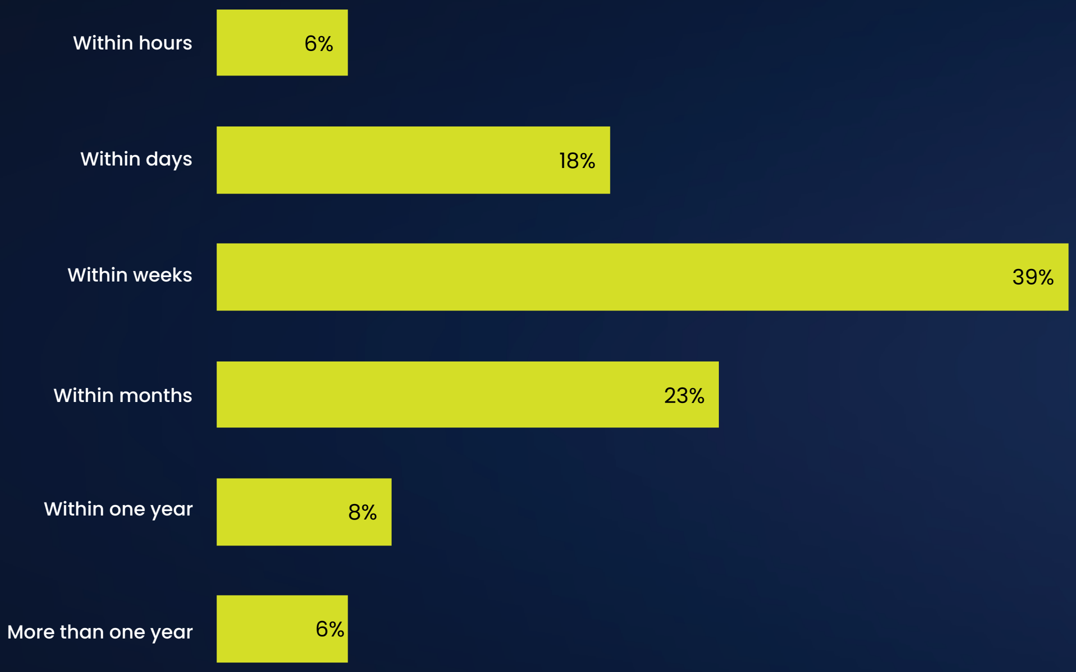


Given the pain experienced by SOC analysts and its numerous causes, it is not surprising the MTTR numbers are not good, especially when you put them in perspective against the undeniable quantity and quality of cyberthreats that hit SOCs daily, especially those that are working to protect government data, as all federal SOCs do.

Only 6% of respondents said the average MTTR for their SOC is to stop a threat within hours of identifying it. Another 18% said their MTTR is within days. The single largest response cited an MTTR of within weeks (39%), while 37% said the average MTTR is *months to a year or more*. Clearly, SOC analyst pain, poor communication and listening skills by SOC leaders, and not having the right training and tools for analysts to perform their jobs successfully is putting SOCs at a great disadvantage against the onslaught of threat actors seeking to breach federal agency, bureau and department defenses.

Figure 12.

If yes, on average what is the MTTR for a security incident in your SOC?



Summary

This survey-based examination of the thoughts and concerns of professionals who work in federal SOCs provides clear-cut evidence that there is significant pain and poor communications affecting the majority of SOC teams.

Given that these findings were largely consistent with the overall results in the broader survey reflected in the 2021 Devo SOC Performance Report™ lends additional weight to the theory that the challenges faced by federal SOCs are universal in SOCs throughout the United States and Europe. However, while "misery loves company" according to the cliché, no SOC team should face such significant obstacles to success.

Perhaps shining a light on the problems and their causes will lead to better results the next time this poll is conducted.

SURVEY CONDUCTED BY PONEMON INSTITUTE

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

ABOUT DEVO

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass.

Learn more at **www.devo.com**.