MSSP Survey

2024

Executive Summary

D3's 2024 MSSP Survey is the first in a series of annual surveys on the state of the managed security service provider industry. Our intention was to capture the definitive snapshot of MSSPs, as told by the people on the front lines. We wanted to know what services today's MSSPs focus on, what they struggle with, and where they see opportunities for growth. As a security automation vendor that works with many MSSPs, we also wanted to drill down on how MSSPs use automation and how they feel about it.

Note: All results are rounded up or down to the nearest percent.

Key Findings

1. Respondents were overwhelmingly positive about automation. 82% used a high or medium amount of automation. 87% said automation had a positive effect on their job satisfaction. 67% said automation had helped their business increase revenue. Only 4% said automation had been used to replace human workers.
2. Artificial intelligence is already used by many MSSPs, but the use cases are not consistent. 80% said they used some AI, but many of the uses they cited were business-focused, rather than enabling security operations.
3. Cybersecurity is still a challenging field to work in. 80% of respondents said stress had a negative impact on the wellbeing of people in the industry.

Who Participated

We had almost 2000 responses to the survey from May to July of 2024. Our dataset comes entirely from active professionals in the managed security services industry. Here's what we learned about the respondents:

71% work for MSSPs headquartered in the USA. 7% are based in Canada. The other countries represented include Brazil, Australia, Denmark, India, and the UK.

44% are cybersecurity practitioners, 29% are non-security executives, and 27% are security leaders, such as CISOs and SOC managers.

44% work a hybrid schedule, 33% primarily work in-office, and 22% are primarily remote.

Of the MSSPs for which our respondents work, 56% have 100+ employees, 22% have 25-100 employees, and 22% have 1-25.

11% have 100+ security analysts, 9% have 25-100 analysts, 44% have 10-25, and 36% have 1-10.

36% of the represented MSSPs have 100+ customers, 40% have 25-100, 24% have 1-25.

13% have more than $100 million in annual revenue, 22% have $25-100 million, 53% have less than $25 million, and 11% were unsure.

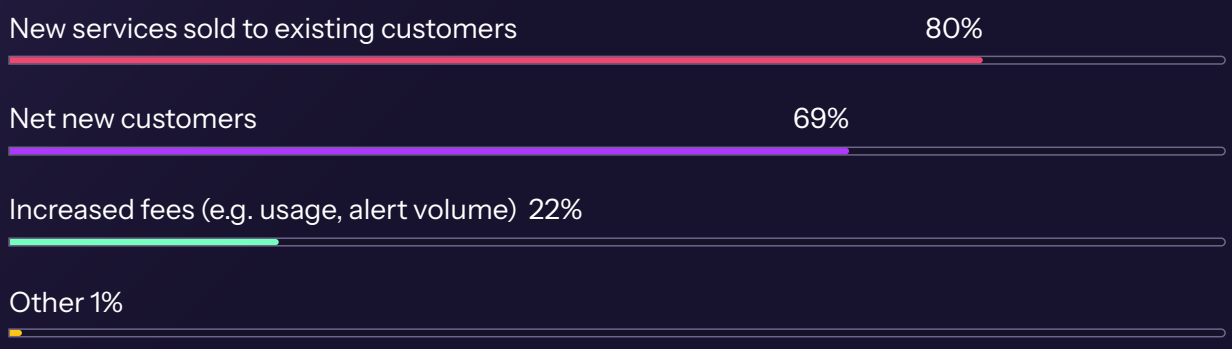
Part One: The MSSP Business

This section of the survey covered the state of the MSSP industry. We wanted to know about if and how MSSPs were growing, the effects of stress on the job, and how hard it was to replace employees.

By how much does your organization expect to grow its number of customers over the next two years?

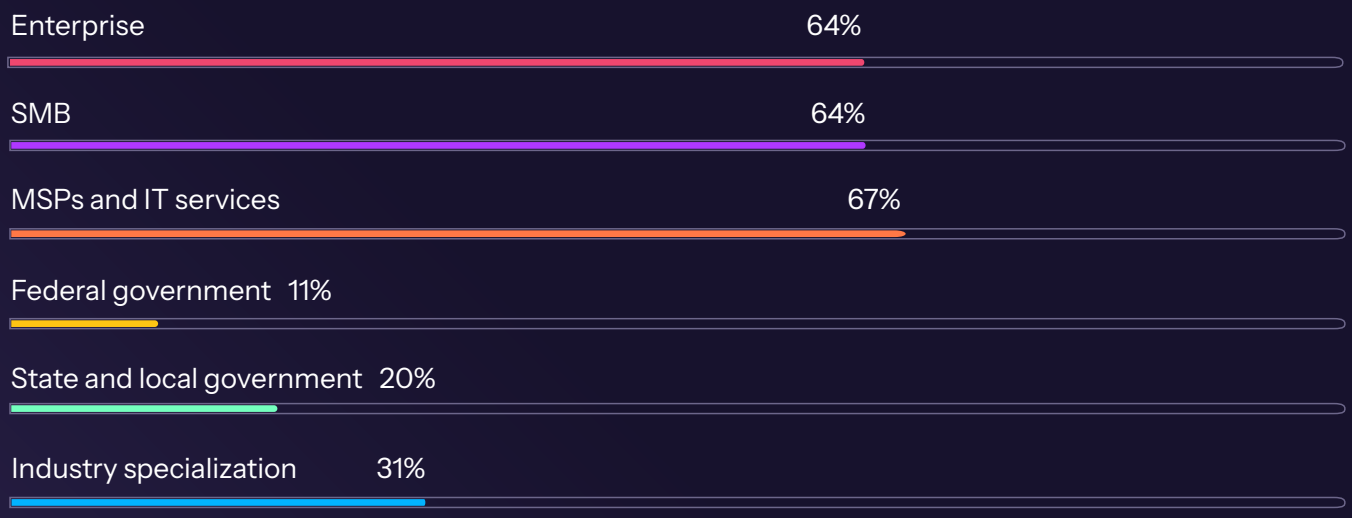
47%	24%	18%	7%	4%
Less than 2X	2X	3X	4X	More than 4X

How does your organization intend to grow its revenue over the next five years? (check all that apply)



Other Answers Included: Developing in-house offerings

From what sectors does your organization intend to drive customer growth over the next few years? (check all that apply)



From your perspective, how does on-the-job stress affect the wellbeing of people working in cybersecurity?

20%
No negative impact

49%
Some negative impact

31%
Considerable negative impact

D3: It is not a surprise, but it is discouraging to see that 80% of respondents said stress had a negative impact on cybersecurity pros.

How long does it generally take for your organization to find and hire a new analyst when a position becomes open?

47% 1-30 days

42% 30-90 days

11% 90-180 days

When a new analyst joins your organization, how long does it take them to become fully productive?

16%
Two weeks or less

44%
Between two weeks and one month

31%
Between one and three months

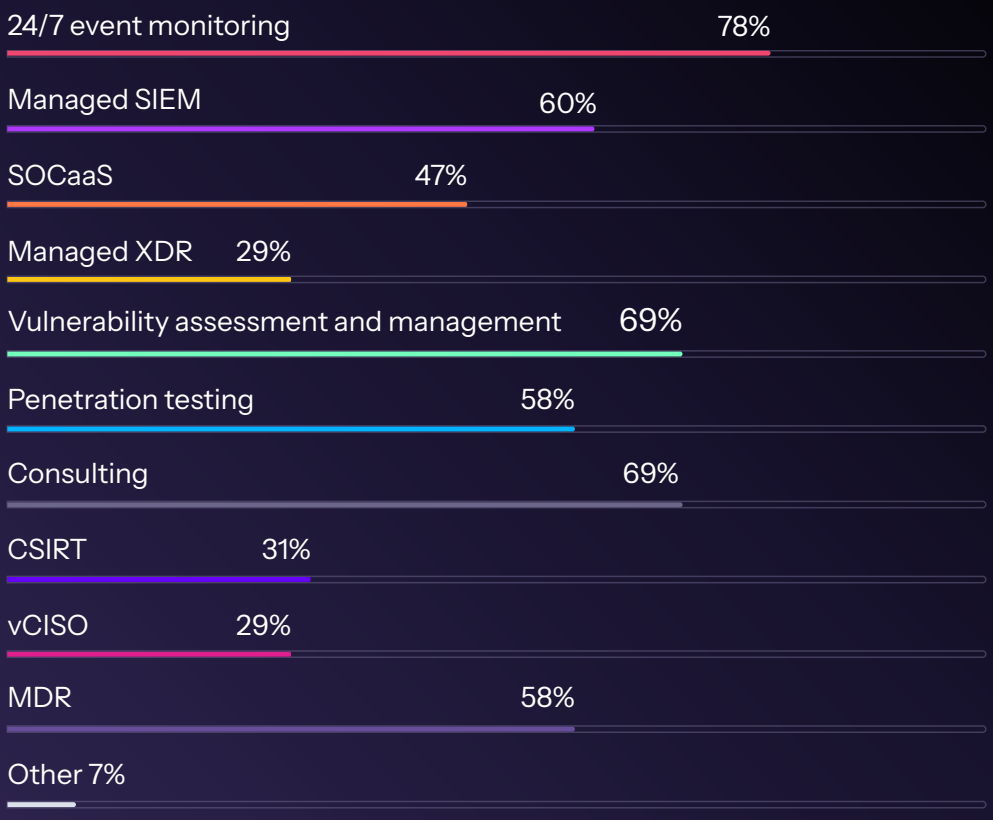
9%
More than three months

D3: Our two questions about hiring and onboarding show that it is taking most MSSPs somewhere between one and four months to hire and fully ramp up an analyst. That could be worse, but it is certainly long enough to underscore the importance of retaining high-performing employees, as well as doing anything possible to streamline the onboarding process.

Part Two: Security Operations

This section got into the specifics of MSSPs' operations. What services do they provide, what do they do to stand out in a crowded market, and what causes the biggest headaches?

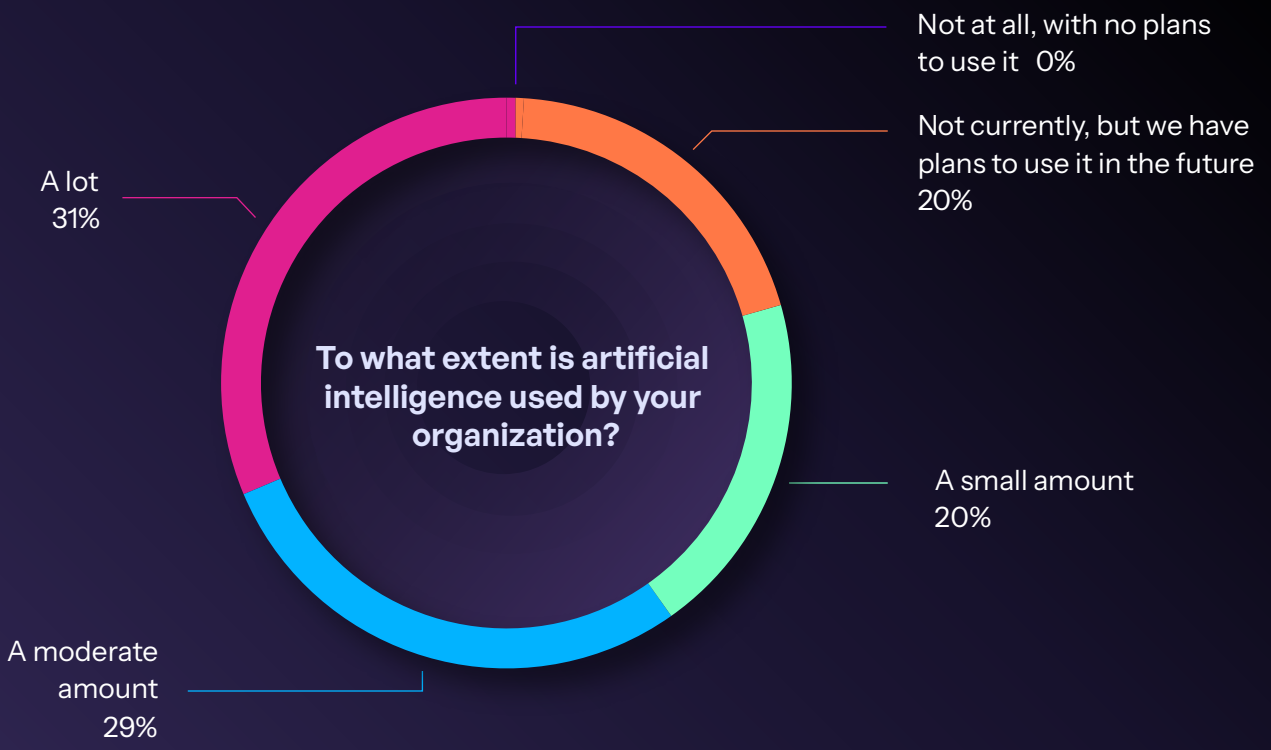
What security services does your organization currently offer? (check all that apply)



Other Answers Included: Edge security, logging as a service, email security

If you were to add one service that you don't currently provide, what would you want it to be?

Answers to this question covered a wide range, with very few repeat answers. Some respondents cited services from the previous question, such as vCISO, managed XDR, and penetration testing. Others were more specific, saying they wanted to offer things like microsegmentation, private TI feeds, and digital forensics. One broad category that came up regularly was consulting services, with answers such as disaster recovery and business continuity planning, personalized awareness planning, and supplier cyber security management.



D3: It was interesting to see how widespread AI already is, with 80% of respondents saying it is used by their companies. Unsurprisingly, not a single respondent said their MSSP had no plans to use AI.

If you use AI, what is the primary thing you use it for?

AI might be prevalent, but there is very little consistency across how it is used. By breaking the responses into loose categories, we found that 15% use AI for non-security tasks—like supporting sales and marketing—13% use it for analysis and threat detection, and 13% use it for automation and orchestration.

Which of the following is your organization more focused on?

33%

Consolidation on a major vendor's tools (e.g. Microsoft or Palo Alto Networks)

60%

Working across diverse tech stacks

7%

Neither

How does your organization differentiate its services to stand out against competitors?

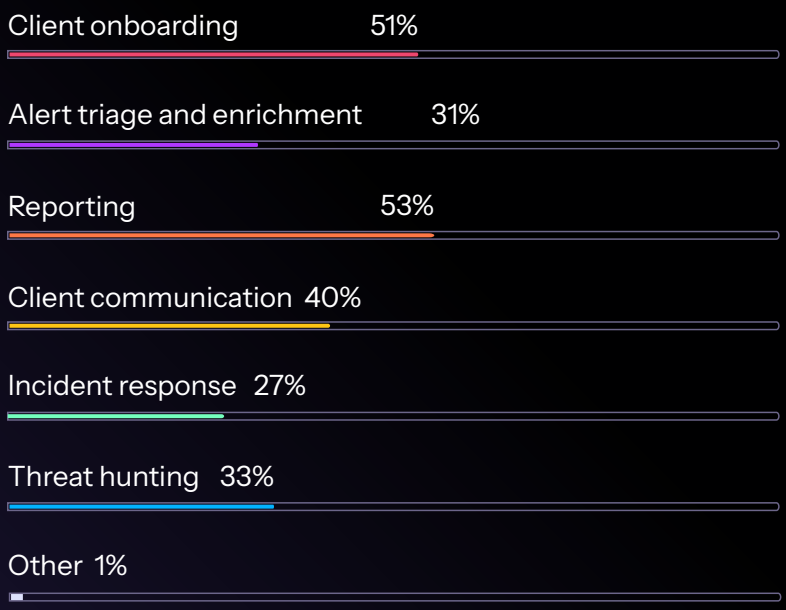
In our responses, there was no one clear way for MSSPs to differentiate their services. Some respondents relied on third-party certifications, specific technologies, or an emphasis on regional presence. The most common categories of responses were along the lines of the basics: quality of service (24%) and an emphasis on being a good, reliable partner to customers (15%).

"We provide services and consulting services to businesses in a language they understand."

"Quarterly security assessments/reports with implementation recommendations and road mapping."

"All services are based in country, Real SOC with 'eyes on glass.'"

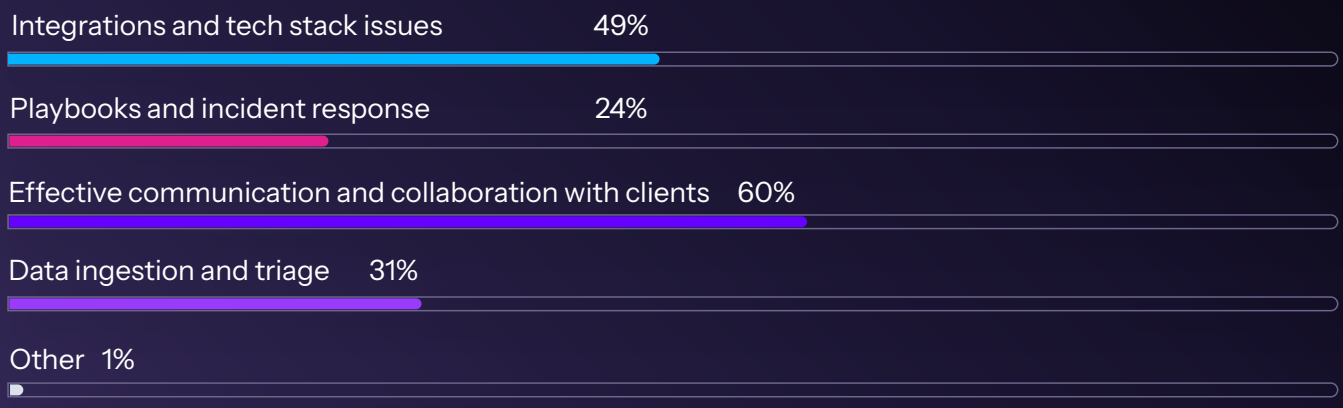
What tasks currently tie up too much time in your organization? (check all that apply)



Other Answers Included: Monitoring of false alerts

D3: It was interesting to see that the top three timewasters were all administrative, not security activities.

What security operations and processes pose the biggest challenges for your organization? (check all that apply)



Other Answers Included: All of the above

D3: Once again, the administrative task of working with clients was the most frequently cited challenge, underscoring the fact that running a successful MSSP business is about more than just providing great security services

Part Three: Automation in MSSPs

In the third and final section of the survey, we wanted to cover a topic that is dear to us: automation. We provide security automation software to MSSPs around the world, so we were interested to learn the general perspectives MSSP pros have on automation. How extensively do they use it, what does it help them achieve, and what is its impact on their business?

To what extent are security automation tools used by your organization?

0%

None: no significant processes are automated

18%

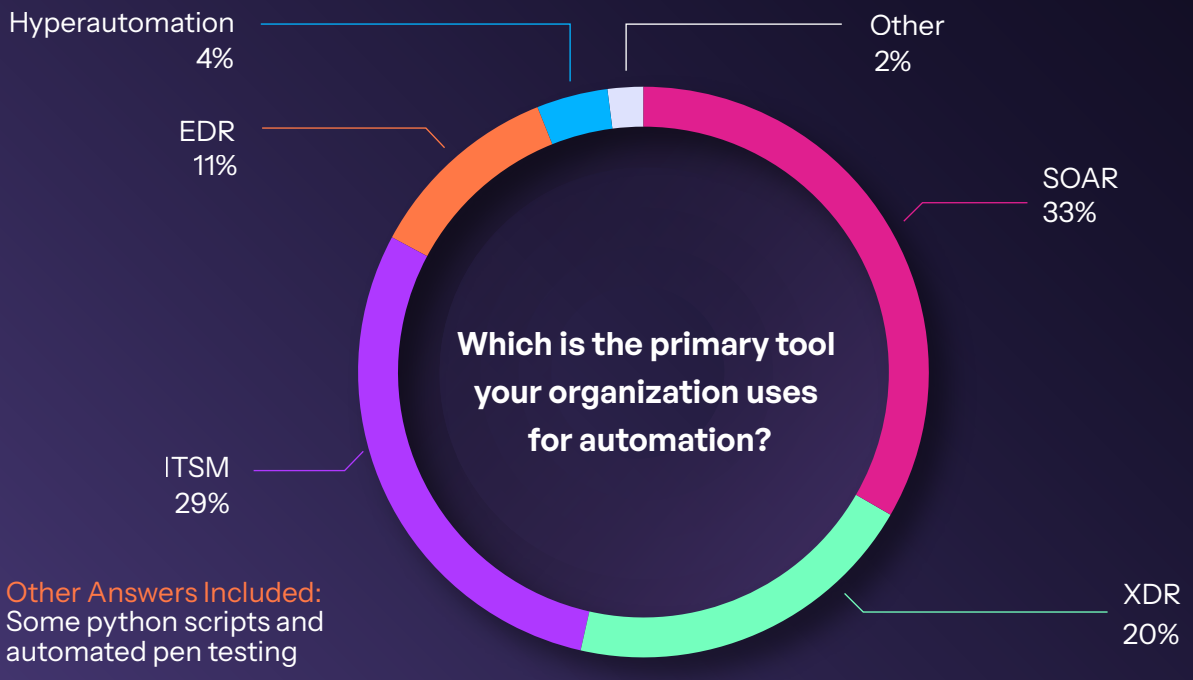
Low: minimal processes are automated

51%

Medium: automation is used for a range of tasks and is an important part of our processes

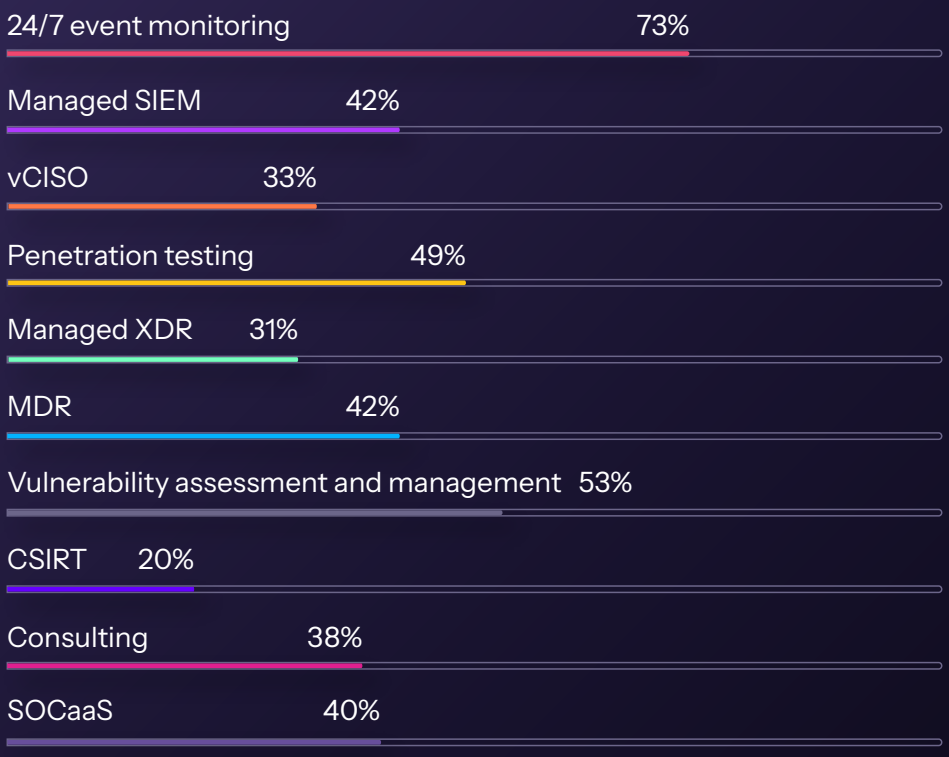
31%

High: automation is used throughout the business, with some processes entirely automated



Other Answers Included:
Some python scripts and automated pen testing

Which services does automation help your organization deliver? (check all that apply)



D3: By comparing this question to the question in part one about what services respondents offer, we can see which services are most and least likely to involve automation. Most respondents that offer 24/7 event monitoring (78% of respondents) use automation to deliver it (73%). Conversely, the services that were less likely to be automated include managed SIEM (60% offer it, 42% automate it), vulnerability assessment and management (69%/53%), and MDR (58%/42%).

If your organization could automate one thing that it currently doesn't automate, what would it be?

Respondents were interested in automating a wide range of things that they don't currently. Incident response (13%), reporting (11%) and a range of specific security functions like vulnerability management and penetration testing were all represented in the answers.

D3: It was great to confirm what we have heard from our customers at MSSPs and enterprises: almost no one uses automation in place of human employees. Automation is a way to augment the output of people, not replace it.

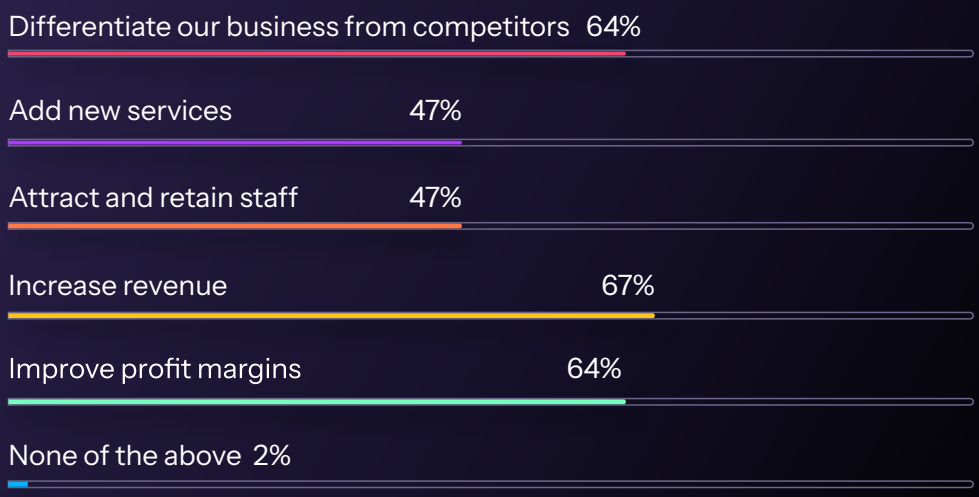
What effect has automation had on your job satisfaction?

87%
Positive

11%
Not much difference

2%
Negative

Automation has helped my organization... (check all that apply)



In your opinion, what is the primary reason that your organization has not utilized *more* automation?

24%

Decision-makers don't think it will have good ROI

20%

Don't have the people and expertise to assess, implement, and operate automation software

9%

Not enough budget available

24%

Intend to add automation, but haven't found the right solution yet

2%

Customers are not comfortable with automation

18%

We believe we already use the optimal amount of automation

About D3

We are an independent security orchestration, automation, and response (SOAR) vendor. Our platform, Smart SOAR, is the preferred choice of MSSPs like High Wire Networks, Trifork Security, and VerSprite, thanks to its ability to filter out the noise, enable high-value services, and improve efficiency, leading to better business outcomes.

Learn More About D3 Smart SOAR for MSSPs

No More Noise:
Make Your SOC Your Sanctum

Smart SOAR for MSSPs:
Helping MSSPs Deliver
Higher-Value Services

High Wire Networks Eliminates
99% Of Noise & Triples Client
Capacity with Smart SOAR

D3 Smart SOAR Helps
Trifork Security Scale Up
Its MSSP Offering

Read More Original Research from D3 Labs

In the Wild 2024

D3Security.com

1-800-608-0081

sales@D3Security.com