2021

Cybersecurity INSIDERS

MANAGED SERVICES REPORT

No Rest for the Wary.

MITRE ENGENUITY™ | ATT&CK® Evaluations

TABLE OF CONTENTS

LETTER FROM THE SPONSOR

Organizations are increasingly relying on external support from managed services. In order to gain a better understanding of the state of affairs in managed services security, MITRE Engenuity, MITRE's tech foundation for the public good, commissioned Cybersecurity Insiders to run an extensive industry survey to answer essential questions:

- Are organizations adopting a threat-informed defense?
- How are organizations doing? Are they doing the right things?
- What are teams doing to improve who watches the environment?
- What are the confidence levels of in-house teams?
- How does the confidence compare to managed services?

The survey of 311 IT security professionals unearthed many surprising results. Some insights that stand out include:

- Most organizations (65%) confirm they utilize a threat-informed defense approach to their security efforts, while an alarming 28% validate performance with a "no news is good news" approach.
- When asked whether teams conduct offensive testing before the selection process, 59% of respondents claim to conduct offensive testing on products while 53% conduct testing on services.
- Most respondents (68%) use MSSP/MDR, yet nearly half (47%) are not confident in managed services technology or people.

The results from the 2021 Managed Services Report: No Rest for the Wary highlights the substantial low level of confidence organizations have in their managed services support than their in-house technology, people, and processes. MITRE Engenuity ATT&CK® Evaluations for Managed Services provide the community with open, transparent, and threat-informed evaluations in hopes of achieving a similar level of confidence in their managed services as they have in their in-house SOC and allow for the wary to rest.

Enjoy the report,

Frank Duff

FRANK DUFF
Director of ATT&CK Evaluations
MITRE Engenuity

Frank Duff is the General Manager for MITRE Engenuity's ATT&CK Evaluations. Frank has spent over 15 years at the MITRE Corporation, starting in radar signal analysis and then transitioning to cyber security. He was on the forefront of early endpoint detection and response research, before leading a team responsible for developing and executing test methodologies. He now leverages this experience to foster public-private partnerships to drive organizational security and product improvement.

ARE ORGANIZATIONS ADOPTING A THREAT-INFORMED DEFENSE?

THREAT-INFORMED DEFENSE APROACHES

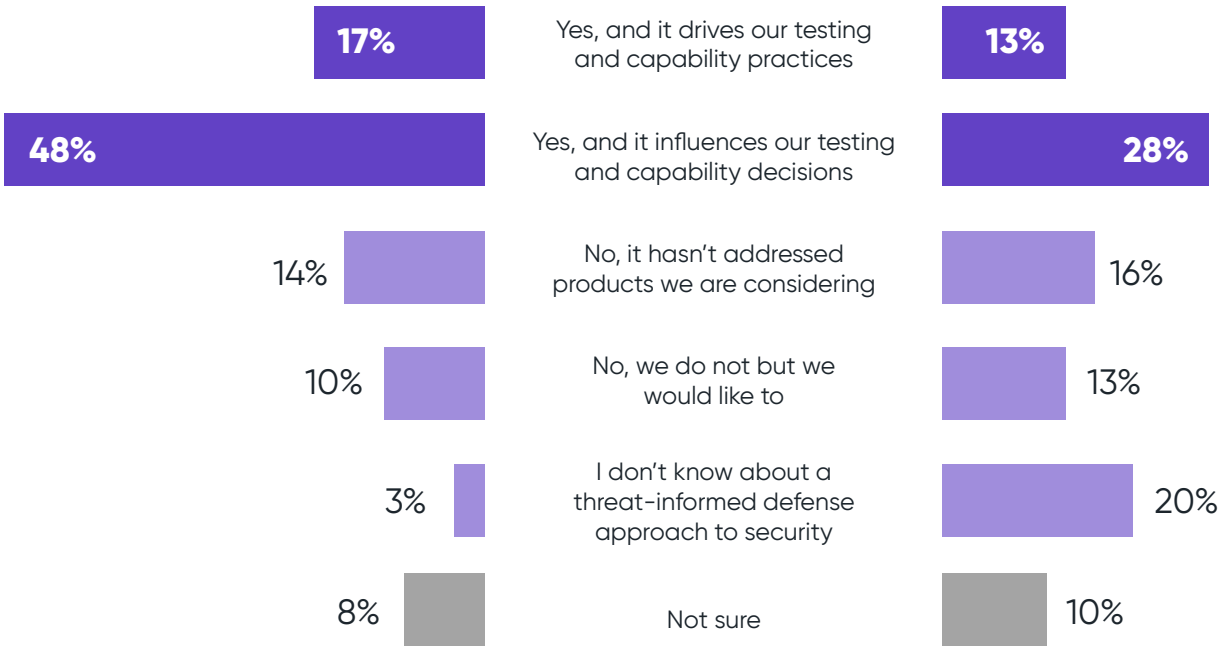
A majority of organizations (65%) confirm they utilize a threat-informed defense approach to their security efforts, driving their testing and capability practices and decisions. Forty-one percent (41%) use the freely available MITRE Engenuity ATT&CK® Evaluations to assess endpoint vendor decisions.

Do you utilize threat-informed defense approaches to your security efforts?

Do you use the freely available ATT&CK Evaluations to assess endpoint vendor decisions you make?

65%
utilize a threat-informed defense approach to security

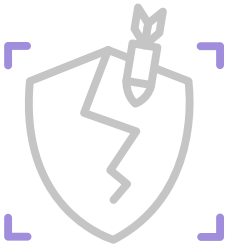
41%
use ATT&CK Evaluations to assess endpoint vendor decisions



OFFENSIVE TESTING

Organizations are increasingly adopting offensive testing approaches, including breach and attack simulation tools (39%), external red team services (34%), and in-house red teaming (30%).

Do you conduct offensive testing (i.e., red teaming) using any of the following approaches?



39%

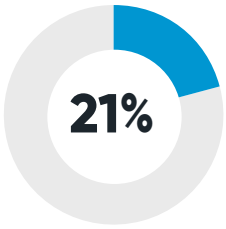
Breach and attack simulation tools

34%

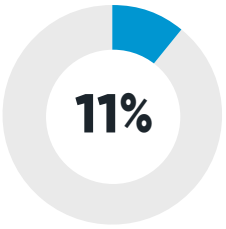
External red teaming service providers

30%

In-house red teaming



None of the above



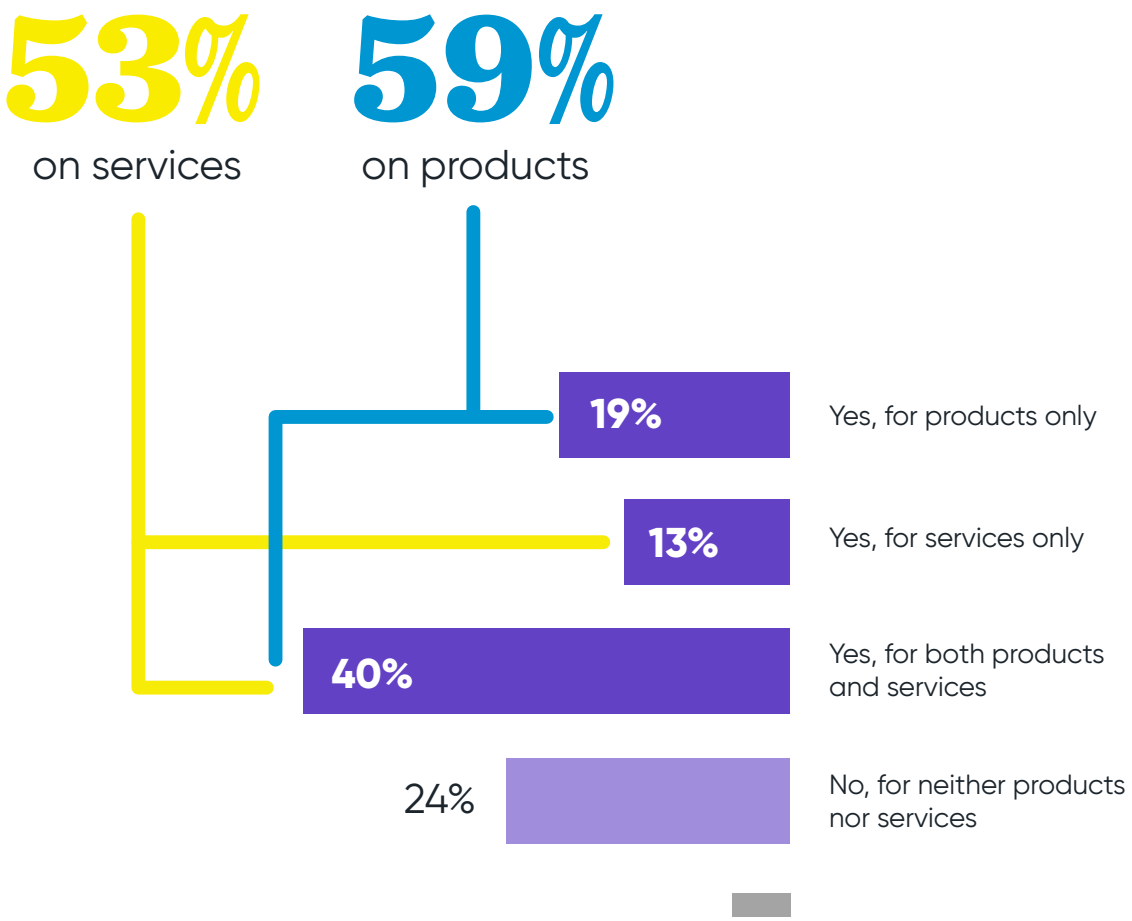
Not sure

Other 6%

OFFENSIVE TESTING DURING SELECTION PROCESS

When asked whether they conduct offensive testing before the selection process, 59% of respondents conduct offensive testing on products while 53% conduct testing on services before investing in a new solution.

Do you conduct offensive testing (i.e., red teaming) during your selection process?

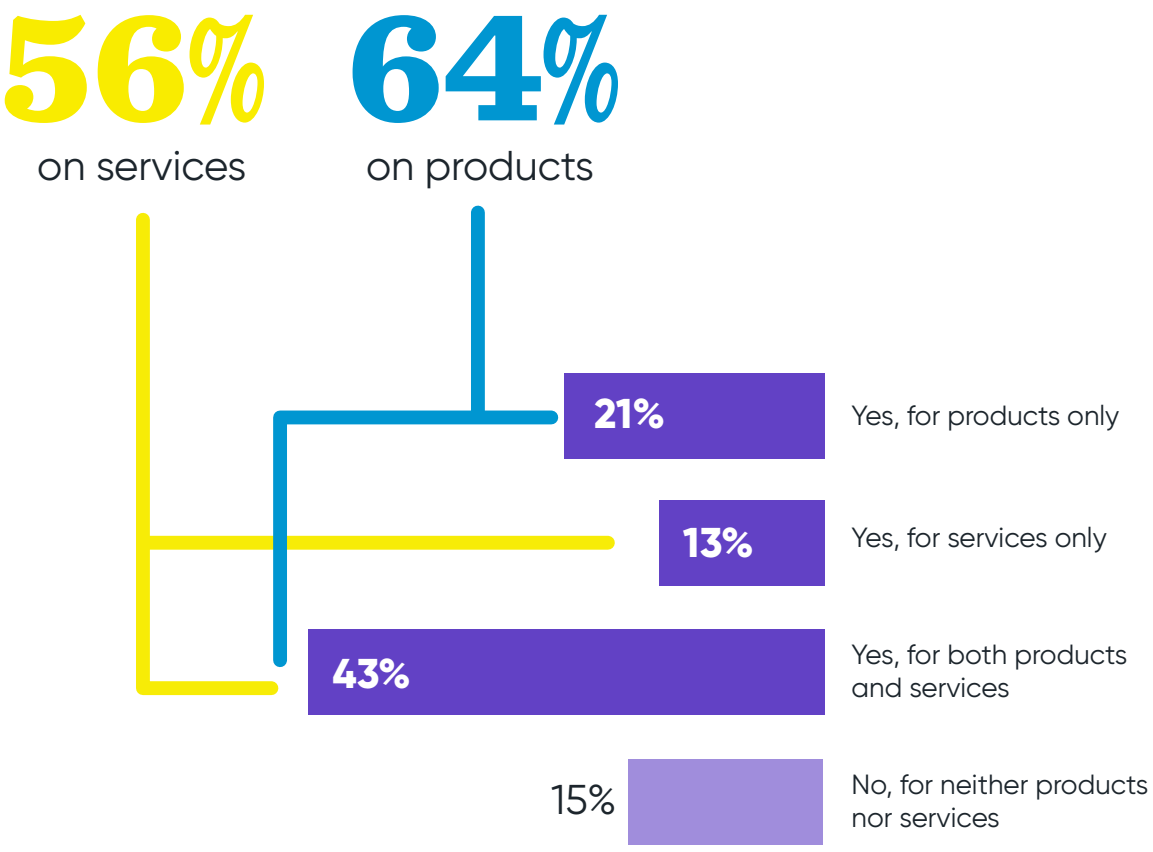


Not sure 4%

OFFENSIVE TESTING AFTER SELECTION PROCESS

More organizations perform offensive testing only after the selection process. Sixty-four percent (64%) of respondents conduct offensive testing on products while 56% of respondents conduct offensive testing on services after investing in the new solution.

Do you conduct offensive testing (i.e., red teaming) after your selection process?



Not sure 7%

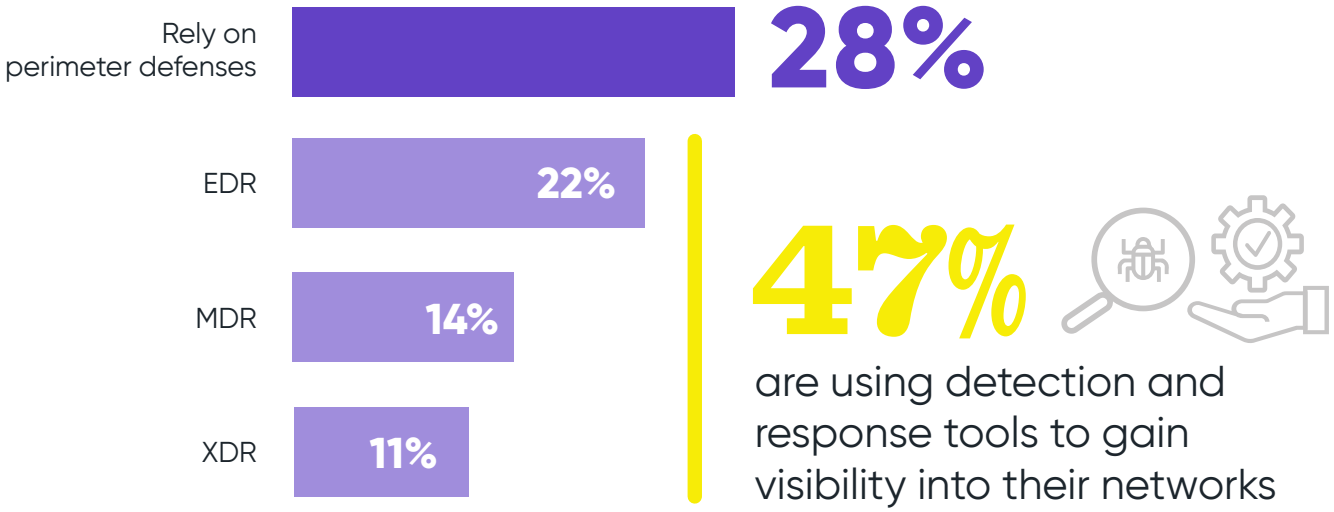
The data shows that organizations are doing all the right things, but...

HOW ARE ORGANIZATIONS ACTUALLY DOING?

ENDPOINT VISIBILITY

When asked how organizations manage visibility into their endpoint management processes, more than 28% still rely on perimeter defenses. Additionally, only about half (47%) are using detection and response tools to gain visibility into their networks.

Regarding your organization's endpoint management processes, how do you address visibility?



Not sure/other 25%

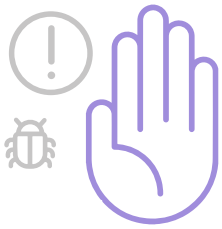
SECURITY PERFORMANCE VALIDATION

We asked how organizations would characterize their current security performance validation processes. While a majority of cybersecurity professionals perform offensive testing (58%) to validate security performance or measure how many breaches have been stopped (40%), an alarming 28% take a "no news is good news" approach.

How would you characterize your current validation processes regarding your organization's security performance?

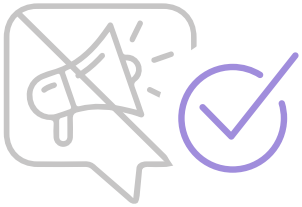
58%

Offensive testing
(e.g., pen tests, red team, adversary simulation/emulation)



40%

Breaches stopped



28%

No news is good news

Not sure/other 31%

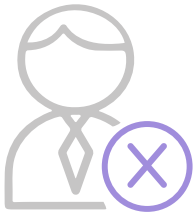
SECURITY LIMITATIONS

Security training remains the biggest barrier to improving organizations' security posture (42%). This is followed by hiring problems, not having the right security skills (38%), and not enough people (31%), as the greatest limiting factors.

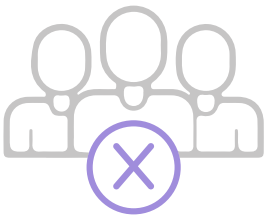
What would you say are the major limiting factors to your ability to have high confidence in your organization's security?

42% Training
(have the people yet not the right skills)

Hiring



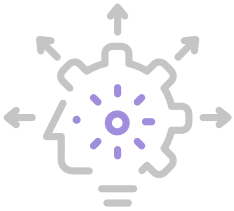
38%
Don't have the right people



31%
Don't have enough people

Technology

35%
Cost



28%
Capabilty

Not sure/other 14%

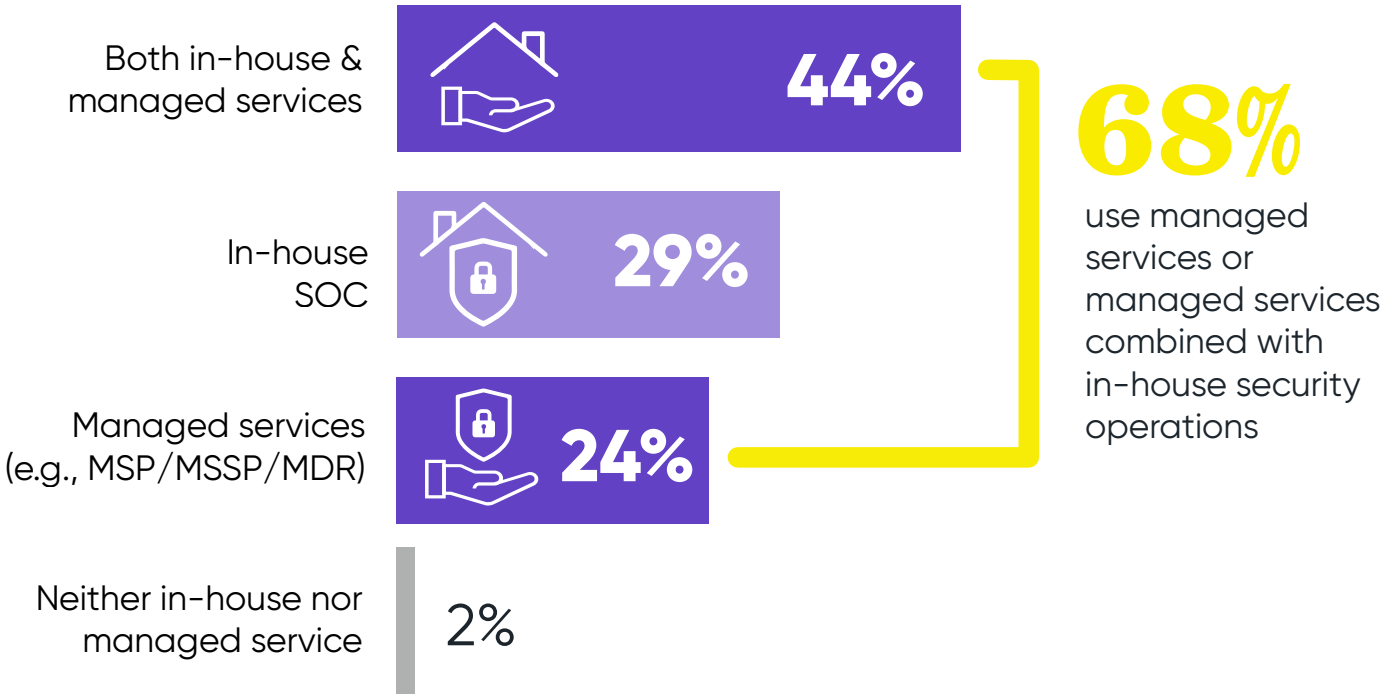
WHAT ARE ORGANIZATIONS DOING TO IMPROVE?

Despite identifying as threat-informed and doing the right things, there are a significant number of organizations that aren't leveraging the data ATT&CK recommends. The data shows an over-reliance on keeping the adversary out, as well as limitations on hiring and training.

ENVIRONMENT

A majority of organizations are exclusively using managed services or a hybrid of managed services combined with in-house security operations (68%). Only a third solely use their in-house security operations (29%).

Who watches your environment?



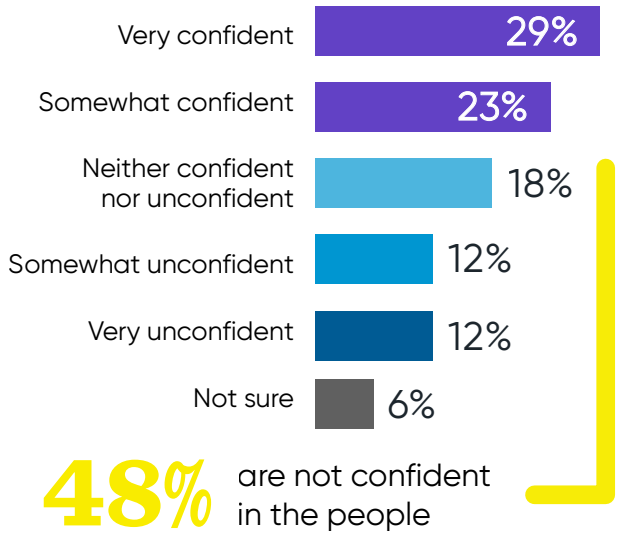
Not sure 1%

IS THERE CONFIDENCE IN MANAGED SERVICES?

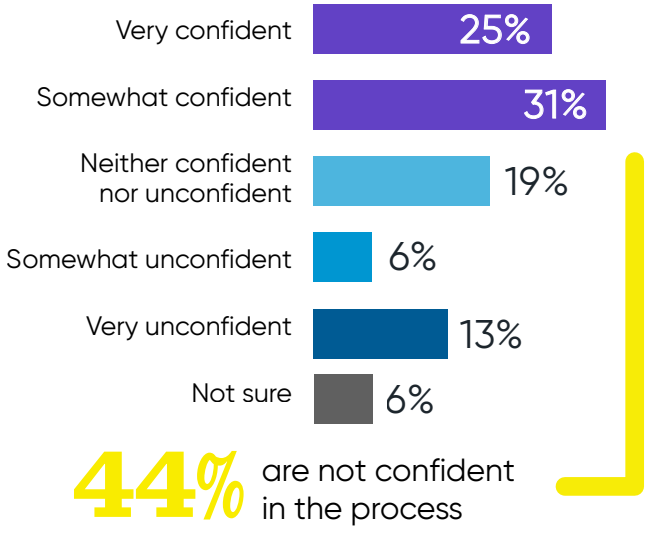
CONFIDENCE IN MANAGED SERVICES

We asked organizations about their confidence in the protection provided by managed services security, in terms of confidence in people, technology, and process. Forty-eight percent (48%) of organizations are not confident in people and technology providing security services. Forty-four percent (44%) expressed lack of confidence in the process component of managed services.

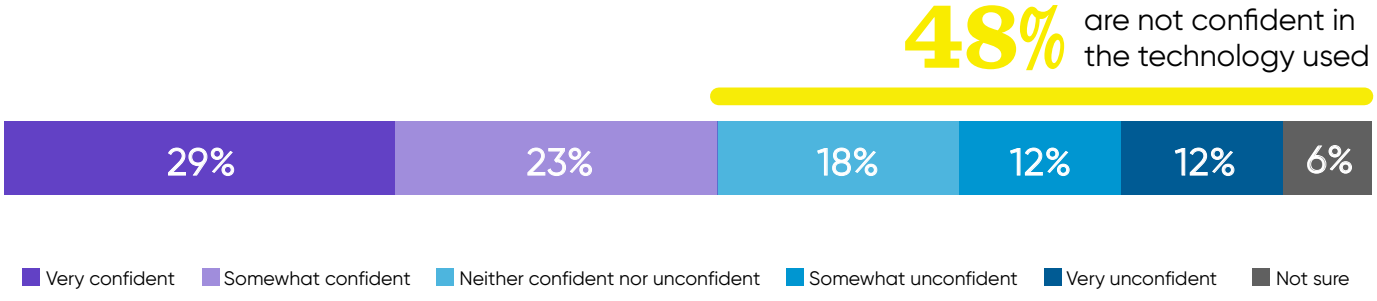
How would you rate your current level of confidence in your managed services security **people**?



How would you rate your current level of confidence in your managed services security **processes**?



How would you rate your current level of confidence in your managed services security **technology**?



HOW DO CONFIDENCE LEVELS COMPARE WITH IN-HOUSE SECURITY?

CONFIDENCE IN PEOPLE

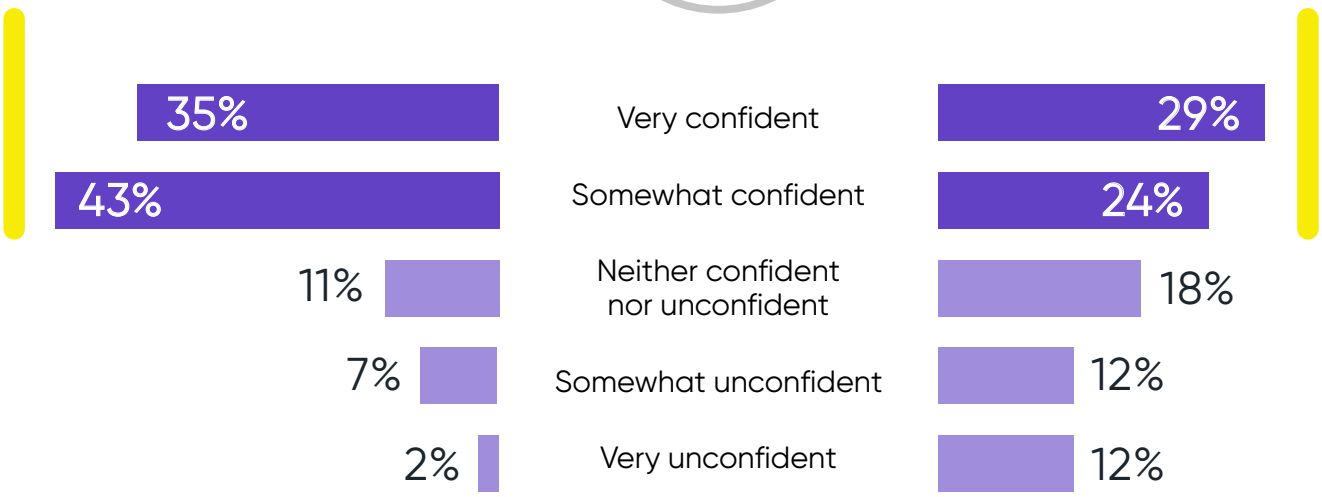
Seventy-eight percent (78%) of respondents have confidence in the people of their in-house SOC, while only 53% have confidence in the people within their managed services providers.

How would you rate your current level of confidence in your **in-house SOC** security people?

How would you rate your current level of confidence in your **managed services** security people?

78%
have confidence in the people of their in-house SOC

53%
have confidence in the people within their MSP



Not sure 2%

Not sure 5%

CONFIDENCE IN PROCESSES

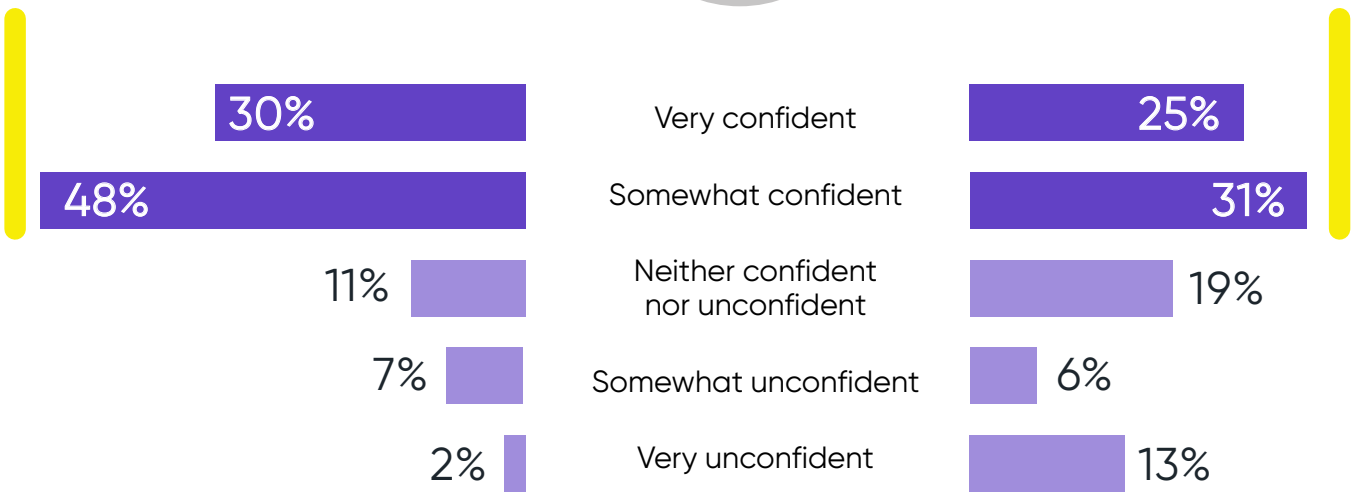
Seventy-eight percent (78%) of respondents have confidence in their in-house processes, while only 56% have confidence in managed services processes.

How would you rate your current level of confidence in your **in-house SOC** processes?

How would you rate your current level of confidence in your **managed services** security processes?

78%
have confidence in their in-house SOC processes

56%
have confidence in managed services processes



Not sure 2%

Not sure 6%

CONFIDENCE IN TECHNOLOGY

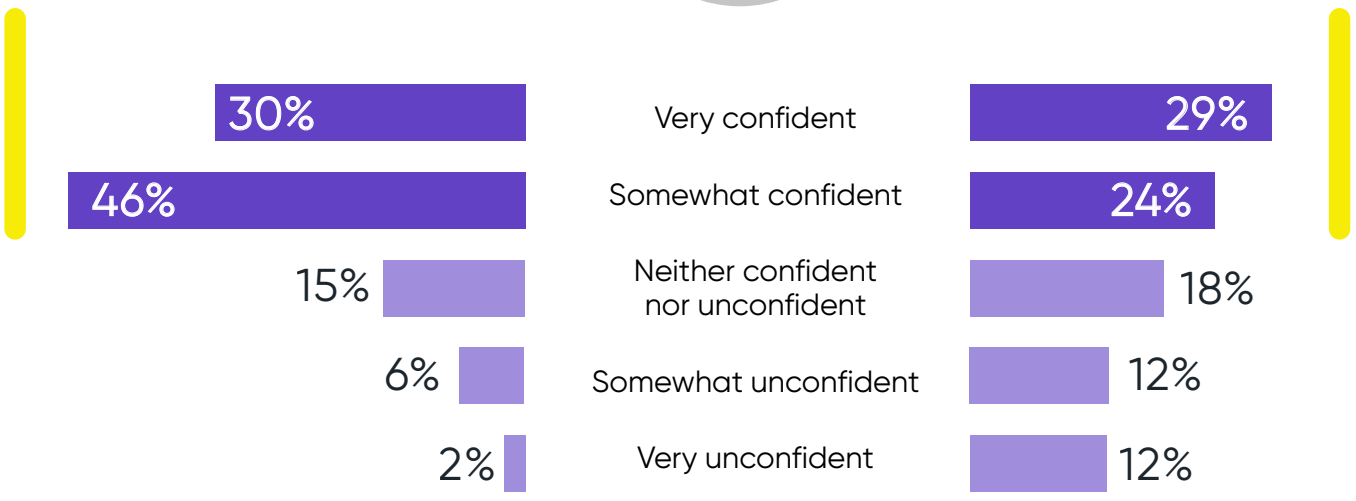
Seventy-six percent (76%) of respondents have confidence in their in-house SOC technology, while only 53% have confidence in managed services security technology.

How would you rate your current level of confidence in your **in-house SOC** technology?

How would you rate your current level of confidence in your **managed services** security technology?

76%
have confidence in their in-house SOC technology

53%
have confidence in managed services security technology



Not sure 1%

Not sure 5%

How can organizations achieve a similar level of confidence in their managed services as in their in-house SOC?

WITH OPEN, TRANSPARENT AND THREAT-INFORMED EVALUATIONS

About MITRE Engenuity ATT&CK Evaluations for Managed Services

ATT&CK Evaluations for Managed Services assess vendor participant capabilities (e.g., MDR and MSSP) in their ability to analyze and describe adversary behavior. Adversary activity emulated by the MITRE Engenuity red team, and correlating context provided by the participants will be mapped to the ATT&CK knowledge base. Managed services participants will leverage a self-supplied toolset to enable their detection capabilities and provide the relevant analysis in the same format they provide to their customers. Examples include—but are not limited to—real-time alerts, daily roll-up reports, dashboard access, etc.

Managed services evaluations employ a closed book version of adversary emulation. Vendor participants do not know the emulated adversary until after the execution is complete, though they are based upon publicly available threat intelligence. Emulations are conducted in the Microsoft Azure Cloud. MITRE Engenuity will execute the emulation, and participants will provide their analysis as if MITRE Engenuity was a standard customer.

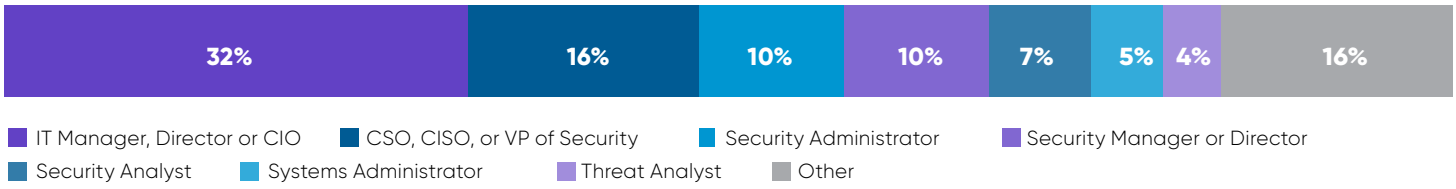
The evaluation focuses entirely on understanding adversary activity, and remediation/prevention is prohibited. During a post-mortem purple team, MITRE Engenuity will disclose the adversary emulated, all behavior performed, and disclose how MITRE Engenuity mapped participant-provided analysis to that behavior. MITRE Engenuity works with participants to enhance their detection capability during this period, as participants are encouraged to ask questions regarding the execution.

For a complete overview of the evaluation process, to learn more, or to contact the ATT&CK Evaluations team, visit https://attackevals.mitre-engenuity.org.

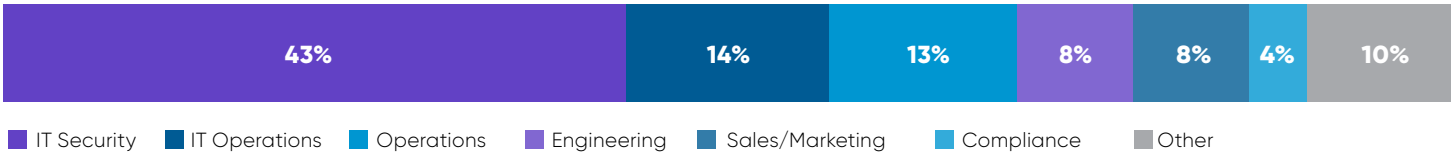
DEMOGRAPHICS

The Managed Services Report is based on the results of a comprehensive online survey of 311 cybersecurity professionals, conducted in November 2021, to gain deep insight into the latest trends, key challenges, and solutions for MITRE Engenuity ATT&CK® Evaluations. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

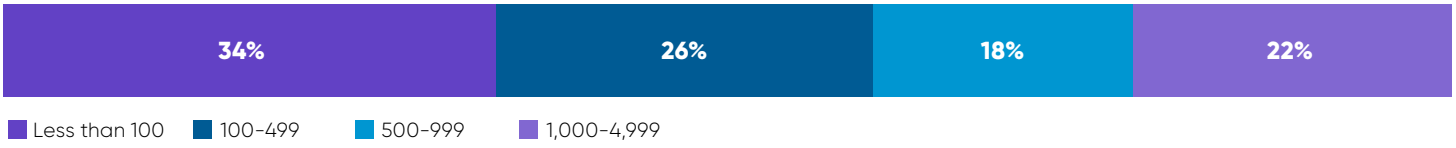
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



INDUSTRY