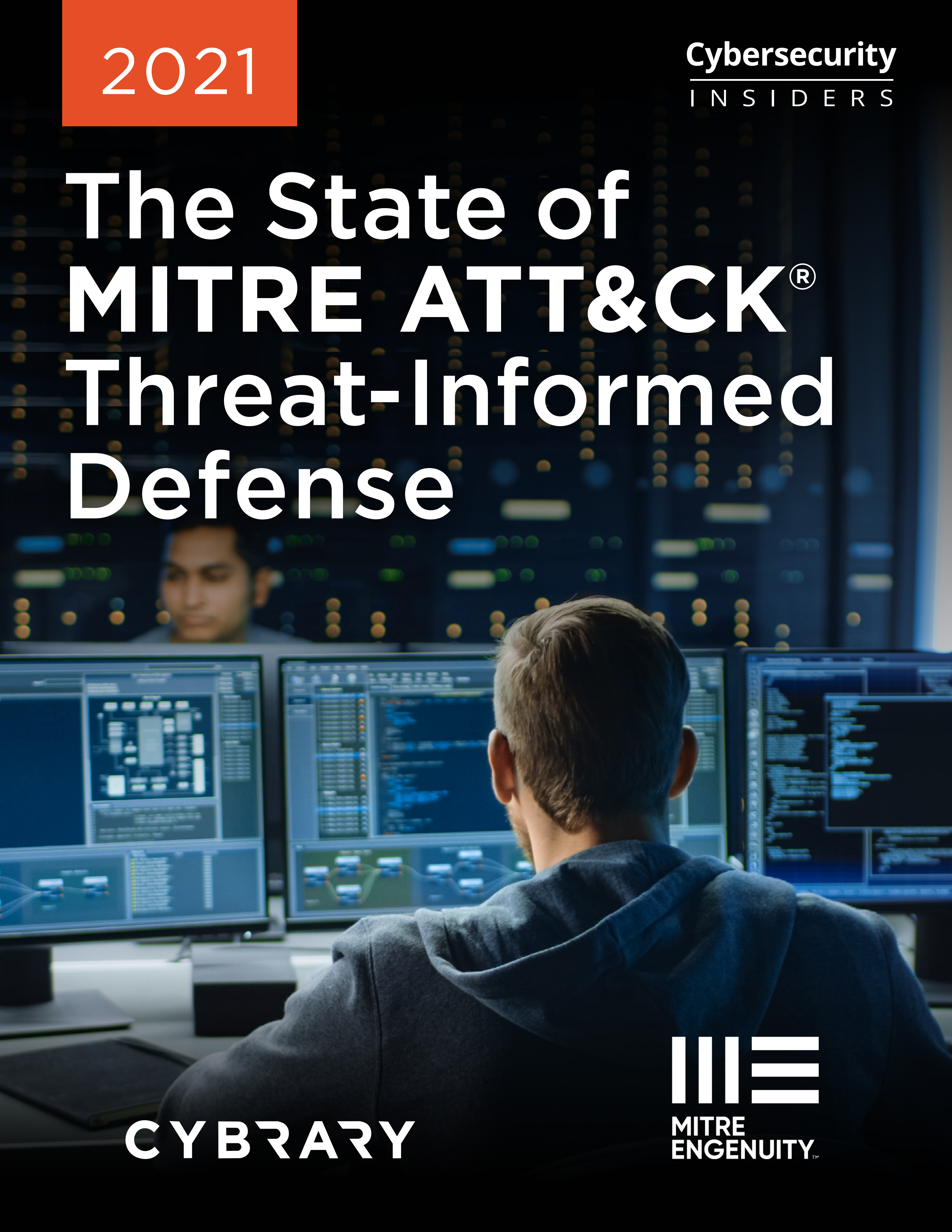
2021

Cybersecurity INSIDERS

The State of MITRE ATT&CK® Threat-Informed Defense



CYBRARY

MITRE ENGENUITY™

INTRODUCTION

Cyber adversaries and threats are becoming increasingly sophisticated and more frequent. In order to gain deeper insights into cybersecurity organizational readiness and help close the cybersecurity community's skills gap, MITRE Engenuity, MITRE's tech foundation for public good, conducted a comprehensive survey to answer important questions:

- What can we do to help close the skills gap with MITRE ATT&CK®?
- What is the state of the knowledge of ATT&CK vs. the ability to apply ATT&CK in 2021?
- Are practitioners gaining the advantage over the adversary with ATT&CK, or playing catch, chasing traditional IOCs?
- Does the community have an interest in learning more about how to apply ATT&CK?
- How are organizations utilizing ATT&CK?

MITRE Engenuity commissioned Cybersecurity Insiders for a comprehensive survey "The State of MITRE ATT&CK Threat-Informed Defense in 2021." The survey of 297 IT security professionals found that:

- Although 82 percent of respondents said they know about the MITRE ATT&CK framework, only 8 percent reported that they are using the ATT&CK framework regularly;
- 84 percent noted they do not have a thorough mapping to ATT&CK techniques;
- 48 percent of respondents said they feel very confident that they could utilize ATT&CK, but only 8 percent use it regularly.
- 73 percent of respondents found it valuable to have credentials validating mastery in applying ATT&CK and 70 percent of hiring managers seek out employees who have the skill to apply it.

We would like to thank MITRE Engenuity and Cybrary for supporting this unique research.

We hope you enjoy the report.

Thank you,

Chriss Knisley

Chriss Knisley

General Manager,
MITRE ATT&ACK Defender ™

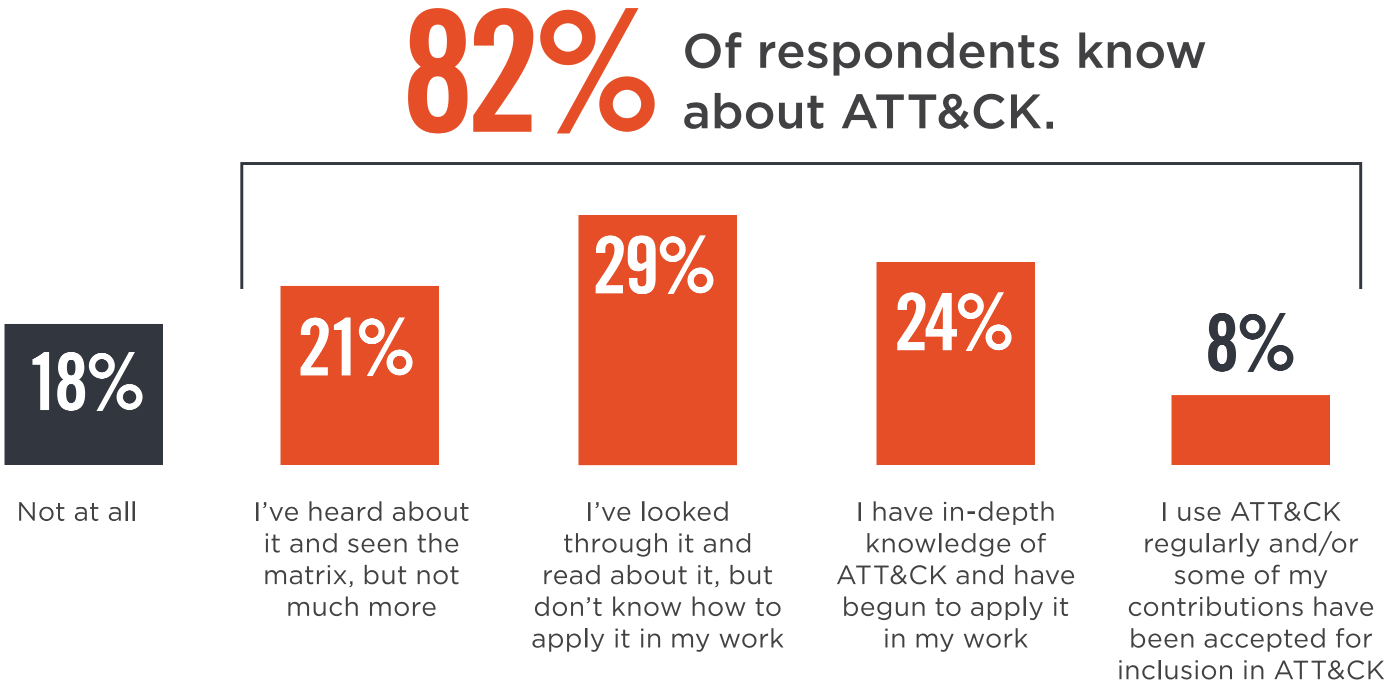
MITRE ENGENUITY™

Use of ATT&CK in the Industry

USE OF ATT&CK TODAY

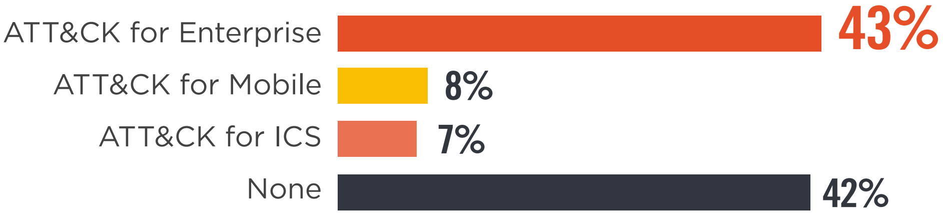
Although 82% of respondents know about ATT&CK, only 8% are using ATT&CK regularly. Twenty -four percent have in-depth knowledge of ATT&CK and have started to apply it in their work.

How knowledgeable are you of the MITRE ATT&CK framework?



Please identify the ATT&CK matrices that you use today.

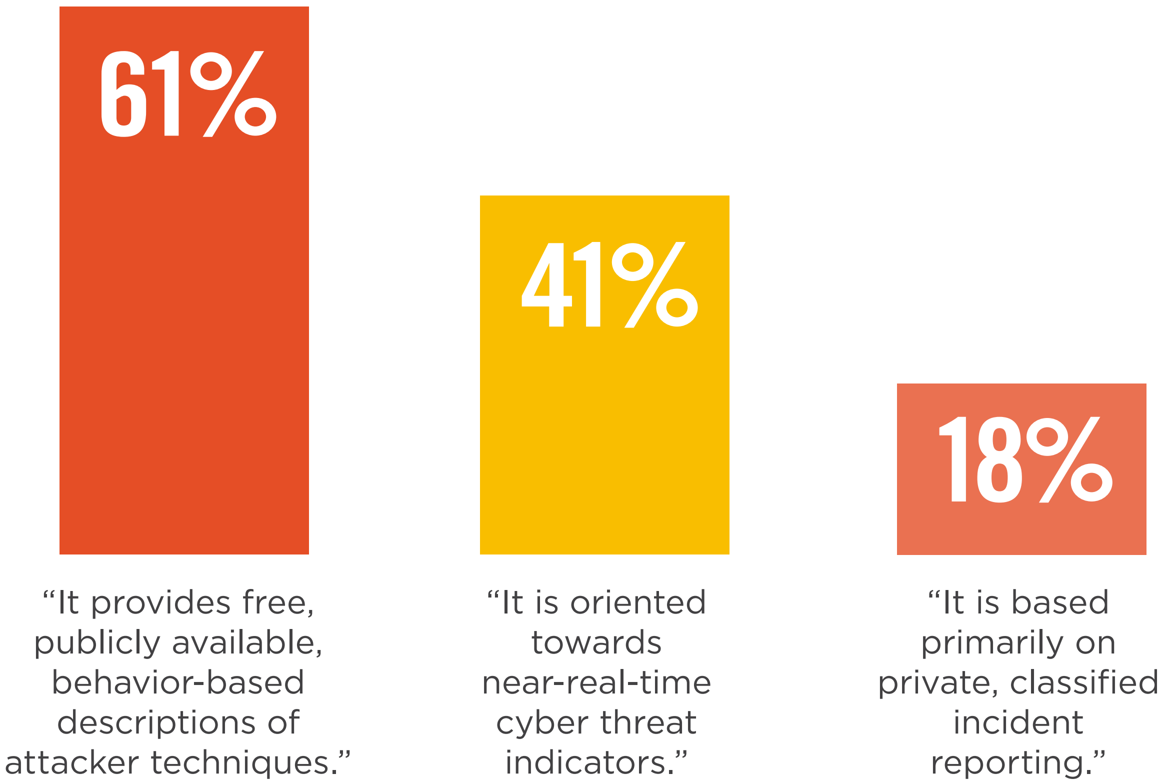
The most commonly used ATT&CK matrix is ATT&CK for Enterprise (43%).



ATT&CK AWARENESS

While a majority of 61% know the value of ATT&CK, a significant number of respondents have misconceptions.

Which statements are factual about ATT&CK?



Not sure/Other 19%

PRIMARY ATT&CK USE CASES

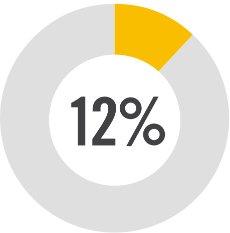
We asked about the primary use cases for ATT&CK in user organizations. The most common need for ATT&CK is Cyber Threat Intelligence (CTI) (35%), and many CTI analysts utilize ATT&CK on a daily basis. This is followed by defense analysis (21%) and threat hunting (20%).

Given your experience, what is your primary need for ATT&CK?

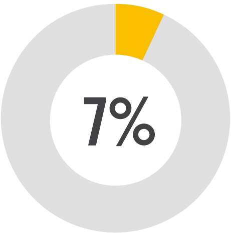
35%
Threat intelligence

21%
Defense analysis

20%
Threat hunting



Defense evaluations



Adversary emulation

Other 5%

TECHNOLOGIES LEVERAGING ATT&CK

ATT&CK is utilized by a variety of cybersecurity technologies to maximize their effectiveness and value. Endpoint Detection and Response (EDR) is the most commonly used technology (44%), followed by cyber threat intelligence platforms (41%), incident reporting (41%) and SIEM (40%).

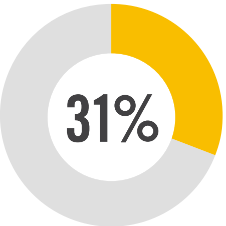
Which of the following technologies at your organization utilize ATT&CK?

44%
Endpoint detection and response (EDR)

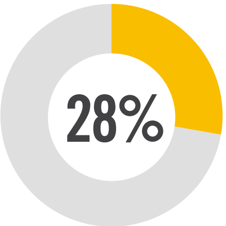
41%
Cyber threat intelligence platform

41%
Incident reporting

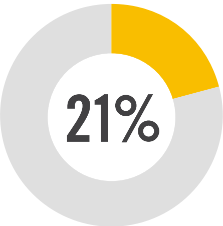
40%
SIEM



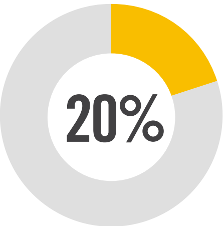
Cyber threat intelligence feeds



Network sensor

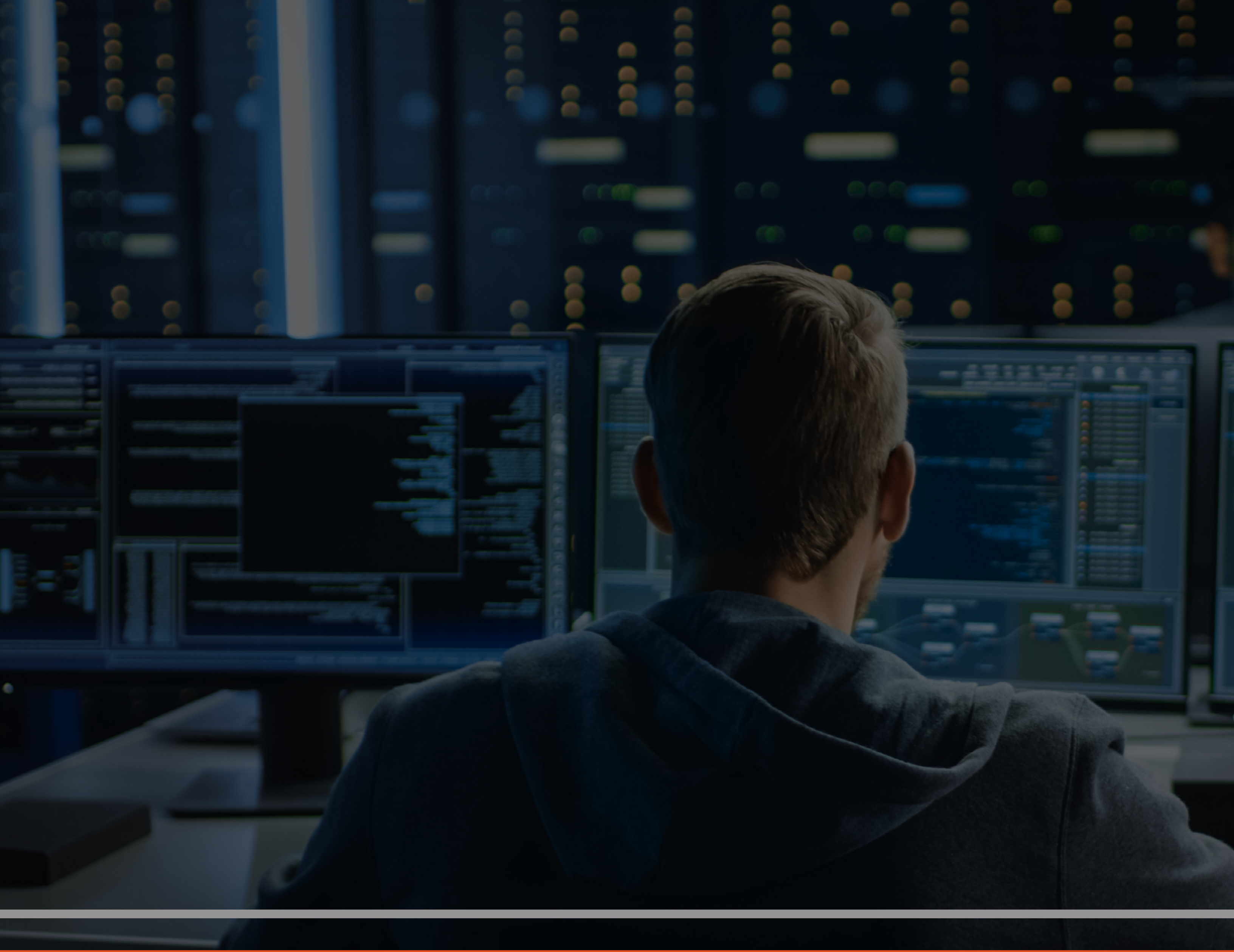


Red team tools



Analytics platform

CASB 12% | Other 10%



The Value of ATT&CK Training & Certifications

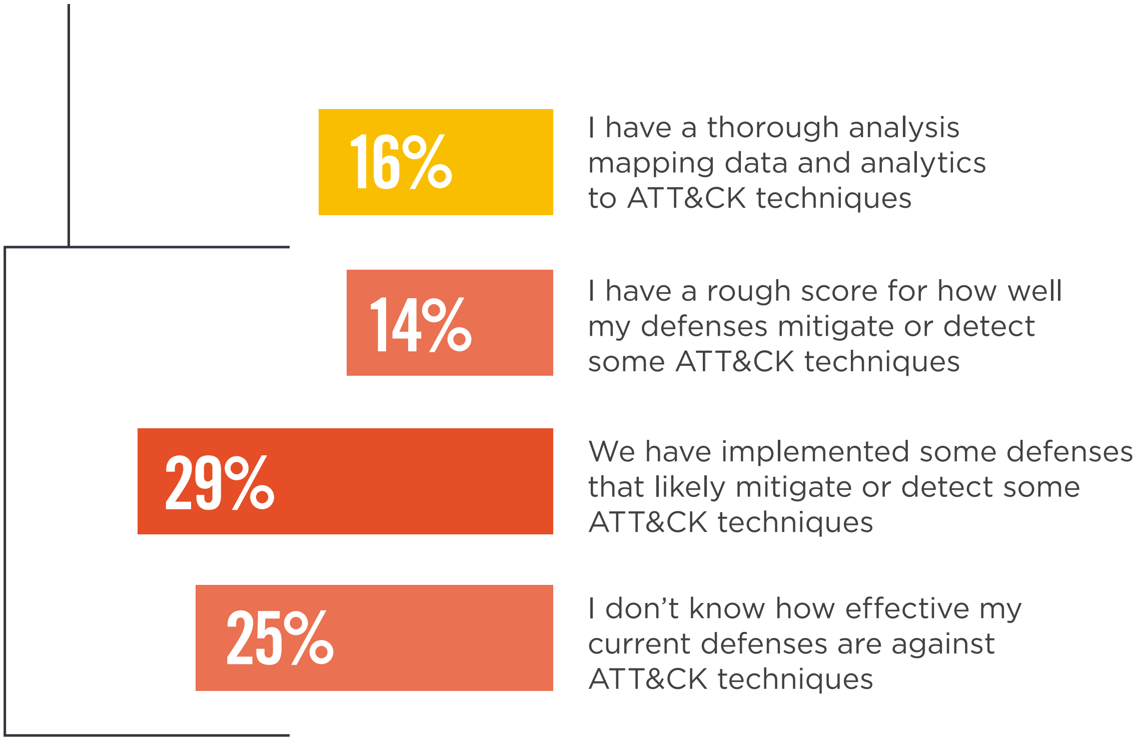
ATT&CK DEFENSE PROFICIENCY

While 16% of respondents confirm they have a thorough understanding of mapping data and analytics to ATT&CK techniques, a majority (68%) of respondents do not have a thorough mapping to ATT&CK techniques.

How clearly do you understand how well your current defenses mitigate or detect ATT&CK techniques?

68%

A majority of respondents do not have a thorough mapping to ATT&CK techniques.

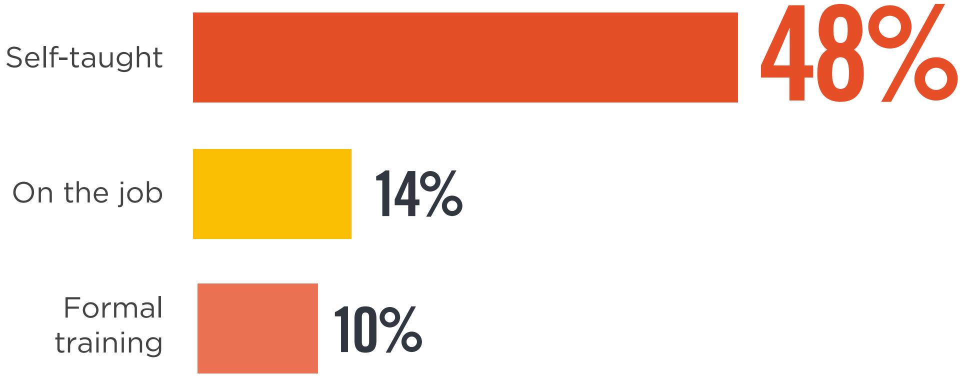


Not sure 16%

ATT&CK EDUCATION

Most ATT&CK users are self taught (48%). Twenty-four percent learned ATT&CK on the job or through formal training.

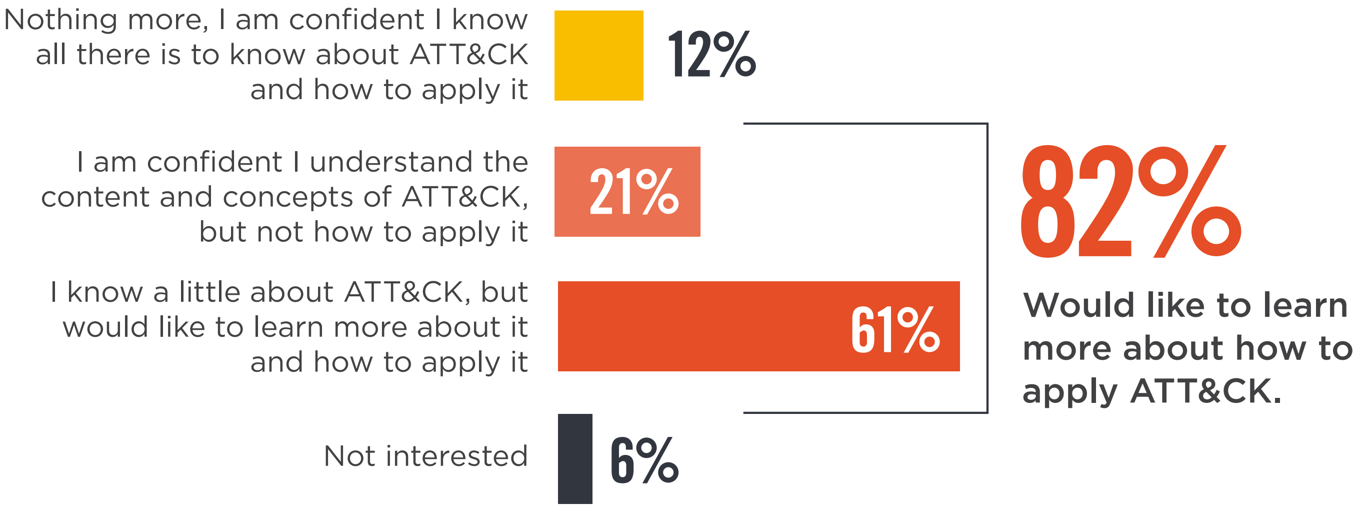
How did you get your MITRE ATT&CK knowledge?



Not applicable 20% | Other 8%

What would you like to learn about the ATT&CK framework?

Eighty-two percent of respondents would like to learn more about how to apply ATT&CK.



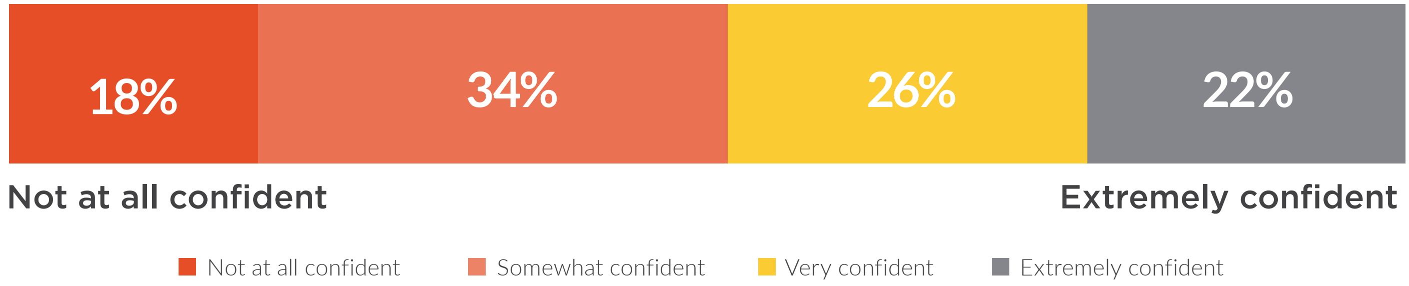
ATT&CK TRAINING

Fifty-two percent of respondents are not confident about their ability to effectively use the ATT&CK framework in their day-to-day work. Forty-eight percent confirm that they are very confident to extremely confident.

How confident are you that you can utilize ATT&CK?

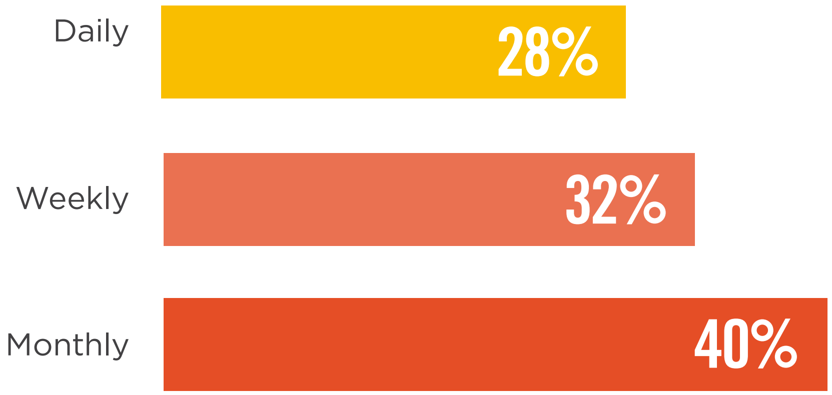
52%

Of respondents are not very confident about their ability to effectively use the ATT&CK framework in their day-to-day work.



How often do you use ATT&CK for your work?

Sixty percent of ACTIVE ATT&CK users utilize the framework at least weekly. This indicates the high value of ATT&CK. Once users understand it, they integrate it into their regular workflows.



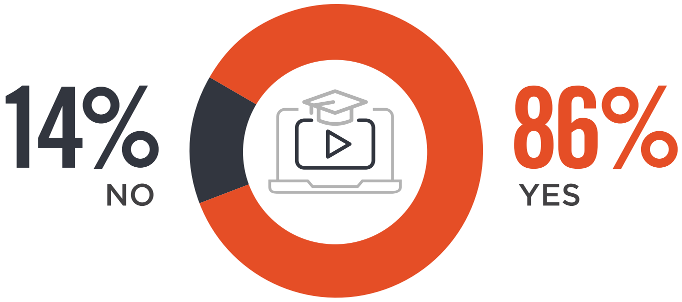
ATT&CK KNOWLEDGE

Eighty-six percent of participants seek educational videos or training to increase their ability to apply ATT&CK .

As a hiring manager, do you seek out employees who have the skill to apply ATT&CK?

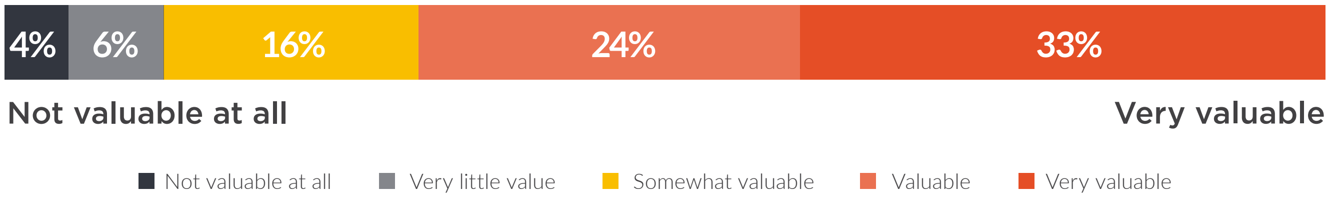
70% Of hiring managers seek out employees who have the skill to apply ATT&CK.

Given your level of experience and current professional position, would you seek educational videos or training that increased your ability to apply ATT&CK to your defensive operations?



What value would you find in a professional ATT&CK credential program for yourself if it were offered?

73% Of respondents found it valuable for a practitioner to have credentials validating mastery in applying ATT&CK.

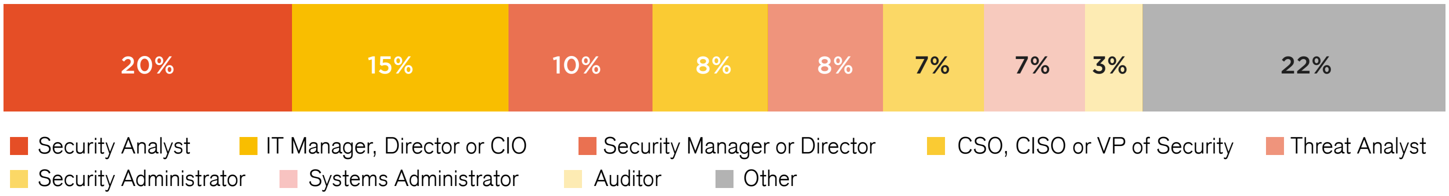


I need more information to decide 17%

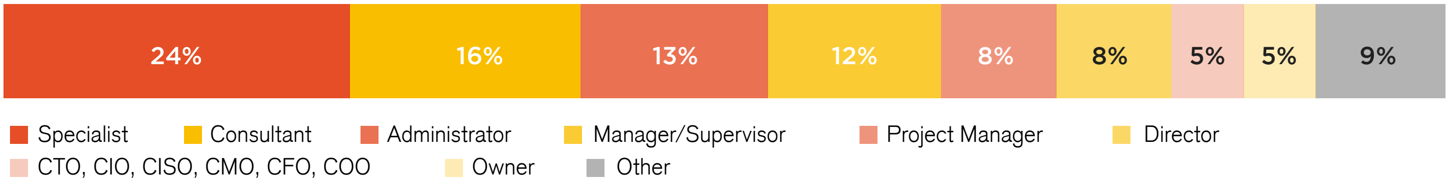
METHODOLOGY & DEMOGRAPHICS

The State of MITRE ATT&CK Threat-Informed Defense report is based on the results of a comprehensive online survey of 297 cybersecurity professionals, conducted in March 2021, to gain deep insight into the latest trends, key challenges, and solutions for MITRE ATT&CK framework. 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.

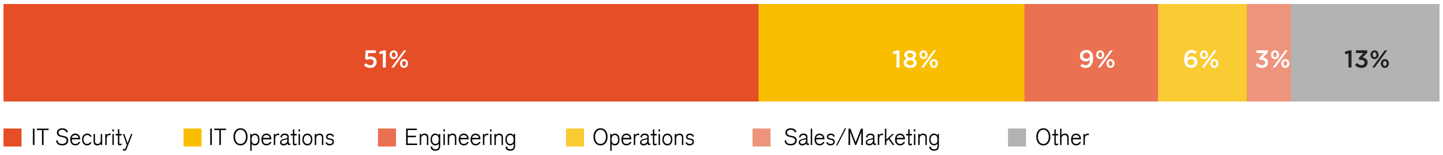
PRIMARY ROLE



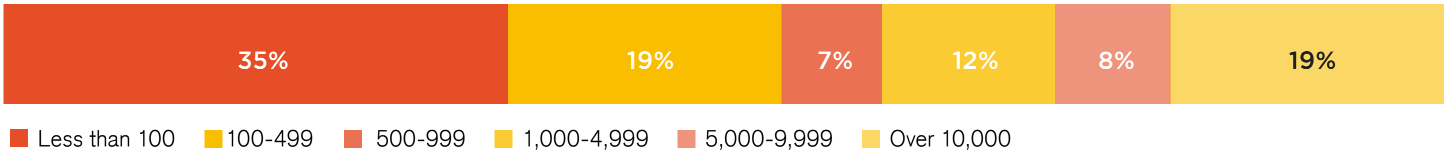
CAREER LEVEL



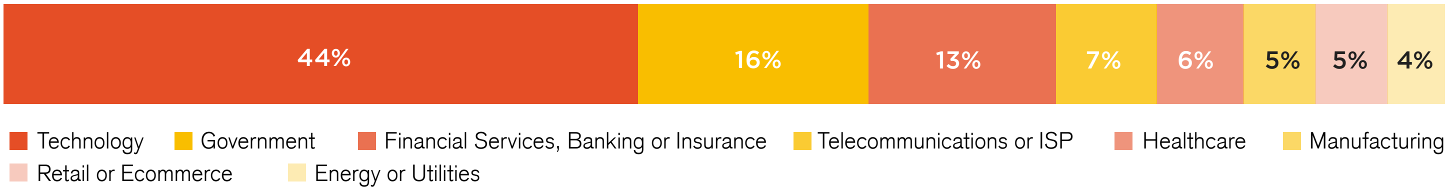
DEPARTMENT



COMPANY SIZE



INDUSTRY



MITRE ENGENUITY™

MITRE ATT&CK Defender™

MITRE Engenuity, MITRE’s tech foundation for public good, and Cybrary, the world’s largest online cybersecurity career development platform, established a partnership to offer MITRE ATT&CK Defender™ (MAD), a new globally accessible online training and certification product designed to enable defenders to gain the advantage over adversaries and close the skills gap.

Individuals and teams can now subscribe to the MITRE ATT&CK Defender training and certification product to learn ATT&CK, earn badges and certifications, and keep up-to-date as the threat landscape changes. For more information, visit mitre-engenuity.org/mad/.

CYBRARY

About Cybrary

Cybrary is the premier cybersecurity professional development platform, providing the collective knowledge of the industry’s top experts and leading organizations to equip security professionals with both the knowledge and skills to achieve their career goals. Recognized as an industry pioneer and innovator since 2015, Cybrary has grown its cyber-focused community to nearly 3 million users, including multiple Fortune 100 companies. To get more information and learn more about Cybrary, visit cybrary.it.