HACKER COMBAT COMMUNITY

Hackercombat.com

MITRE ATT&CK Framework

Everything You Need To Know

SWIPE ←

HACKER COMBAT COMMUNITY

The Nuts And Bolts Of MITRE ATT&CK: Tactics

Initial Access

The cyber attacker is trying to enter your network.

Execution

The attacker is trying to execute malicious code.

Persistence

The attacker is attempting to keep up their foothold.

Privilege Escalation

The cyber attacker is attempting to increase more significant level authorizations.

Defense Evasion

The attacker is attempting to abstain from being identified.

Credential Access

The attacker is attempting to steal names and passwords of accounts.

Discovery

The cyber attacker is attempting to make sense of your environment

Lateral Movement

The attacker is attempting to travel through your environment.

Collection

The attacker is attempting to assemble information important to their objective.

Command And Control

The cyber attacker is attempting to communicate with compromised frameworks to control them.

Exfiltration

The attacker is attempting to steal information.

Impact

The cyber attacker is attempting to control, intrude, or obliterate your frameworks and information.

How Organizations Can Use MITRE ATT&CK?

HACKER COMBAT COMMUNITY

01

Red Teaming

ATT&CK can be utilized for planning, reporting, and execution of the red group to maintain a strategic distance from certain cautious measures that might be set up inside a network.

02

SOC Maturity Assessment

The Security Operations Center (SOC) and occurrence reaction group can reference ATT&CK strategies that have been distinguished or revealed. It helps as one measurement to establish how effective a SOC is at analyzing, detecting, and responding to intrusions.

03

Assessing Defensive Controls

Organizations can use ATT&CK to assess tools, supervising, and mitigations of current defenses in the enterprise.

04

Cyber Security Strategy

Organizations can use ATT&CK to plan their strategy for cybersecurity. It can help you build your defense to counter the known strategies and prepare your monitoring to recognize proof of ATT&CK procedures in your network. By assessing the overall strategy of cybersecurity, ATT&CK help you fill any gaps that you might find.

05

Nature Of threats

Using ATT&CK, your team can determine the nature of threats you are facing. It also helps in mitigating the threats. It can also be used as a reference for the latest cybersecurity threats.

Hackercombat.com

Next ▶

HACKER COMBAT COMMUNITY

01

How prepared are you for security incidents?

02

Does your cyber defense system work effectively?

03

Do you have a well-crafted comprehensive incident response plan?

If you are shaking your head "no," you need a proactive analysis of attacks and threats. And when our talk turns to the rigorous analysis of cyber theft and defense, we cannot fail to mention the MITRE ATT&CK model that is trusted by security professionals for organizing various sorts of threats or adversarial behaviors and testing the efficiency of your security defense system.

Apparently, MITRE ATT&CK is not just a red hot and trending ampersand-infused acronym because it holds the attention of cybersecurity pros. So what is it all about?

What Is MITRE ATT&CK?

MITRE, a government-funded organization, spun out of MIT, has worked to strengthen cyber defenses for the past forty years. It is associated with a lot of commercial and top-secret projects for many agencies.

It advocates for a threat-based defense solution with a balanced security posture and leveraging cyber threat intelligence for quick adoption of a cyber-attack responsive plan.

Cyber-attacks can pose a threat to your organization, and hence comprehensive threat detection is important, which has three key elements:

- Understanding common adversary techniques
- Detecting actual threats to your organization
- Mitigating the attacks.

The Nuts and Bolts of ATT&CK: Techniques

Adversarial techniques answer “how” an adversary attains a tactical objective, and the course of action they take to get what they seek.

Many techniques contain contextual information. It includes the required permissions, the platform, the method commonly seen, and how to detect the commands and the processes used in it.

When aligning a defensive program on ATT&CK, this can be somewhat overwhelming as more than 291 techniques are identified until today. And enlisting all of these is beyond the scope of the article. Though, organizations can then leverage this information from other hubs to ensure that their security programs cover the most common techniques used to target the peer organizations.

And while a security program that deals only with these techniques will be feeble, a robust security program, like MITRE security will make sure that these techniques are addressed as a broader and more comprehensive approach to securing organizational assets.

To detail out a few of the techniques and its associated tactics in all industries for a brief exposure.

Techniques

01

Command-Line Interface:

TACTIC-Execution: Command-line interfaces provide a means of interacting with computer systems and are a common feature of many types of operating system platforms. For this execution, command-line interfaces can interact locally or remotely via a remote desktop application, reverse shell session, etc.

02

Process Discovery

TACTIC- Discovery: Cyber hackers can attempt to obtain information about the execution of processes on a system. The information obtained could be used to gain an understanding of common software running on network systems. Opponents can use information from process discovery during automated discovery to shape follow-up behaviors, including if the adversary completely hacks the target and/or attempts specific actions.

SWIPE ←

How Does ATT&CK Help In Sharing Threat Intelligence?

The ATT&CK framework helps all technical and corporate organizations, end-users, and governing institutions by sharing threat intelligence. Apart from books that share threat intelligence, ATT&CK provides a common language that is standardized and globally accessible.

It is possible for analysts and defenders to work together with data to compare and contrast cyber threat groups. It gives a structured description of adversary tactics, techniques, and procedures and the real-time behavior of hackers. And hence we can draw significant comparisons amongst the adversary groups.

Security analysts and defender both can structure their information through ATT&CK matrices. The former can create and share intelligence about the behavior of cyber attackers, while the latter can structure gen for behavior used in detection and mitigation by prioritizing risk.

Together, they create and share a threat-based awareness by filling in the information voids or gaps that attackers were exploiting. So the MITRE ATT&CK framework is beneficial in rapid decision making and incident responsive plans for all organizations.

Who Does The ATT&CK Framework Benefit?

ATT&CK can help both red teams and blue teams in the same way. Red teams can pursue emulation plans of MITRE’s adversaries to test their systems and defenses by demonstrating off adversary conduct characterized by ATT&CK.

Campaigns that are based around ATT&CK can make it simpler and easier to interpret patterns, track attacks, and rate the adequacy of tools for a defense that is already in place.

Blue teams can use the ATT&CK system to show signs of improvement, keeping an eye on what enemies are doing, and organizing threats by prioritizing them.

Conclusion:

HACKER COMBAT
COMMUNITY

Understand, Deploy, and Hunt cyber-attacks with MITRE ATT&CK Framework

There is no silver bullet that can stop or dodge rapidly evolving cyber-attacks. However, being prepared to respond to such security incidents will limit damage and reduce recovery time and costs.

MITRE ATT&CK evaluation is one of the most comprehensive and conclusive resources of hacker tactics and techniques available until date. Cyber professionals and security analysts are increasingly concerned about cyberattack techniques in the ATT&CK matrix, and they are building defense solutions and software based on the MITRE ATT&CK navigator.

There is a demand for this fast-changing world to get more gen about the use of the elements in penetrating targets' defense. The MITRE security model satisfies the needs as it can apply technical and corporate organizations to leverage cyber threat intelligence, which responds and adapts quickly to a cyber-attack. To accomplish this, we need to encourage the promotion of sharing cyber threat information and its effective tools. This strategy thrives on a foundation of unrelenting innovation and operational databases.

Hackercombat.com

Follow. Learn. Share

Save For Later

Follow us!

Find us Online

Like and Comment