MITRE ENGENUITY | Center for Threat Informed Defense

PICUS

Adoption Spotlight

# Picus Security Adopts Top ATT&CK Techniques

GOLD
Center for Threat-Informed Defense
AFFILIATE
MITRE ENGENUITY

## R&D Project Introduction

Defending against all MITRE ATT&CK® techniques is not practical, and without guidance, determining which techniques to focus on is overwhelming. Top ATT&CK Techniques project helps defenders systematically prioritize techniques for defense. The project provides a methodology and tool that enables defenders to focus on the adversary behaviors that are most relevant to their organization and have the most significant effect on their security posture.

## About Picus Security

At Picus, we help organizations to continuously validate, measure and enhance the effectiveness of their security controls in order to assess cyber risk and strengthen resilience. As the pioneer of Breach and Attack Simulation, our Complete Security Validation Platform is trusted to proactively identify gaps and deliver actionable insights to address them.

## Why Picus Security Adopted Top ATT&CK Techniques

The Picus Platform simulates cyber threats and maps results to ATT&CK enabling customers to visualize prevention and detection coverage and prioritize mitigation of gaps. Picus chose this project to help security teams identify the highest priority gaps in their ATT&CK coverage and optimize their controls to address them.

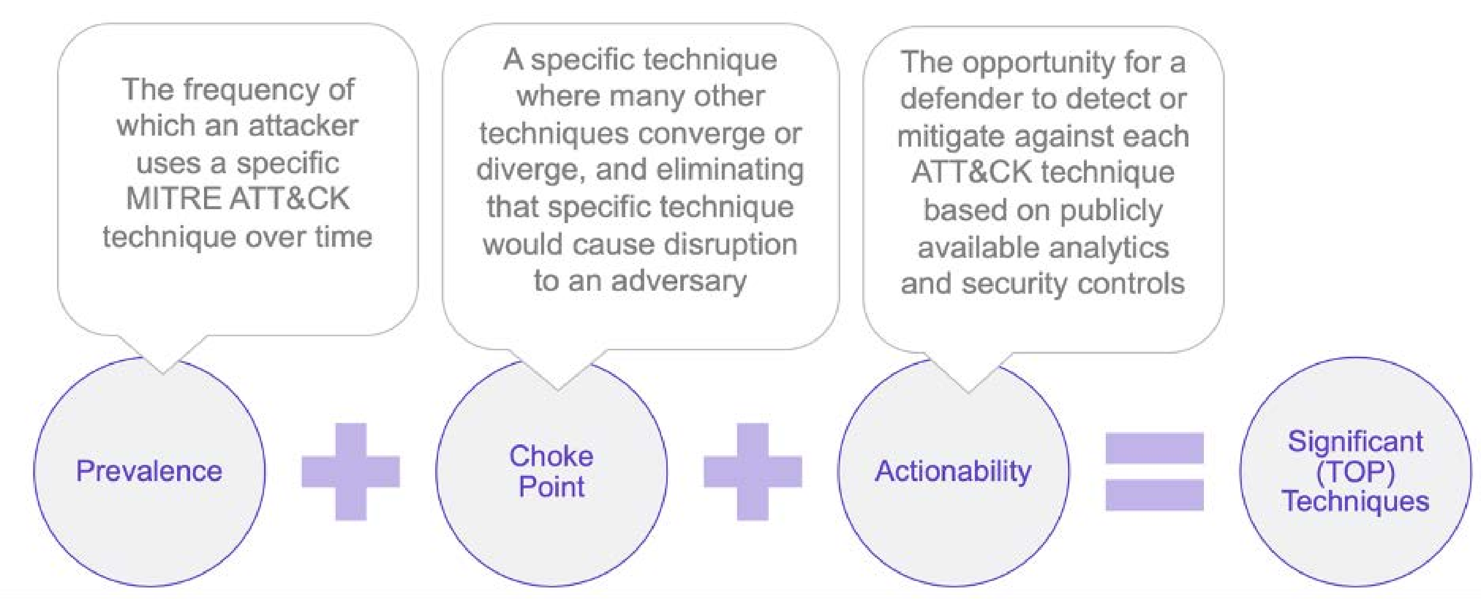
## How Picus Security Uses Top ATT&CK Techniques

Picus has directly integrated the project into The Picus Complete Security Validation Platform to enable users to test their security controls against MITRE Engenuity's Top ATT&CK Techniques. The Picus Platform includes threat templates that contain multiple threats related to a specific theme. Picus customers can now find two dedicated templates derived from the Top ATT&CK Techniques project. The first template, "Top 10 ATT&CK Techniques," is calculated with the Top ATT&CK Techniques Calculator, and the second is "Ransomware Top Ten ATT&CK Techniques". These templates consist of dozens of implementations of ATT&CK techniques. Picus provides prioritized attack simulations to effectively identify gaps in security controls via these templates, which are updated continuously with new attacks. Moreover, Picus offers easy-to-apply prevention signatures and detection rules to mitigate these gaps and improve the effectiveness of security controls.

> “ *When setting out on a journey to operationalize ATT&CK, it can be challenging to know where to focus attention. By making it quick and easy to simulate the Center's most observed ATT&CK techniques, The Picus Platform enables security teams to continuously measure and strengthen organizations' readiness to prevent and detect commonly observed adversary behaviors.*
>
> - Volkan Ertürk
> CTO and Co-Founder, Picus Security ”

# About the Research: Top ATT&CK Techniques

Top ATT&CK Techniques provides defenders with a systematic approach to prioritizing ATT&CK techniques. Our open methodology considers technique prevalence, common attack choke points, and actionability to enable defenders to focus on the ATT&CK techniques that are most relevant to their organization.


The frequency of which an attacker uses a specific MITRE ATT&CK technique over time
A specific technique where many other techniques converge or diverge, and eliminating that specific technique would cause disruption to an adversary
The opportunity for a defender to detect or mitigate against each ATT&CK technique based on publicly available analytics and security controls
Prevalence
Choke Point
Actionability
Significant (TOP) Techniques

The Top ATT&CK Technique Calculator makes the methodology actionable, allowing users to easily build their own tailored "top 10" technique lists as well as apply the methodology to different use cases. Along with the Top ATT&CK Technique Calculator, the project applied the methodology to create a Top Ransomware Technique list. This list creates a starting point for defending against ransomware attacks and a demonstration of applying the Top ATT&CK Technique methodology to a specific use case – ransomware.

# The Methodology

A top technique list should be actionable and driven by threat intelligence. This belief guided the creation of the methodology. Each component of the methodology includes its own algorithm to determine a technique's weight within the component. Then an overall score is computed by combining each component weight. There are three components in the methodology:

### The methodology is composed of three different components:

**Actionability:** The opportunity for a defender to detect or mitigate an ATT&CK technique based on publicly available analytics and security controls. Techniques that have a greater number of detections and mitigations are weighted more heavily.

**Choke Point:** A specific technique where many other techniques converge or diverge and where eliminating that specific technique would disrupt an adversary. Open-source threat reports were analyzed to identify techniques that had many other techniques occur directly before and directly after. Techniques with a greater amount of before and after techniques were weighted more heavily.

**Prevalence:** The frequency of use for a specific ATT&CK technique over a period of time. Through data populated from the Sightings Ecosystem project, frequency analysis was used and adjusted based on the recency of the technique's usage. A technique seen more frequently over time has a higher weight than a technique seen last month.

## Resources & How to Get Involved

Visit the Top ATT&CK Techniques project page for access to all the resources, including:

- Top ATT&CK Techniques Web Calculator
- Top ATT&CK Techniques Excel Calculator
- GitHub project documentation and source
- Project announcement blog

There are several ways that you can get involved with this project and help advance threat-informed defense:

- Review the methodology, use the calculator, and tell us what you think. We welcome your review and feedback on the calculator and our methodology.
- Help us prioritize improvements. Let us know where we can improve. Your input will help us prioritize improvements.
- Share your use cases. We are interested in hearing from you about your use cases and ideas. Tell us how you leverage the Top ATT&CK Techniques resources and share your ideas for improving upon this foundation.

MITRE ENGENUITY. Center for Threat Informed Defense

For more information:
Center for Threat-Informed Defense
ctid@mitre-engenuity.org
https://ctid.mitre-engenuity.org/

**About the Center for Threat-Informed Defense**

The Center is a non-profit, privately funded research and development organization operated by MITRE Engenuity. The Center's mission is to advance the state of the art and the state of the practice in threat-informed defense globally. Comprised of participant organizations from around the globe with highly sophisticated security teams, the Center builds on MITRE ATT&CK®, an important foundation for threat-informed defense used by security teams and vendors in their enterprise security operations. Because the Center operates for the public good, outputs of its research and development are available publicly and for the benefit of all.

PICUS

For more information:
Picus Security
info@picussecurity.com
https://www.picussecurity.com/