A BEST PRACTICE: MAPPING CYBER THREAT INTELLIGENCE TO ATT&CK

Cyber analysts use the MITRE ATT&CK framework to map real-world TTPs as part of their cyber threat intelligence strategies. The steps below are from CISA’s “Best Practices for MITRE ATT&CK Mapping,” which outlines key steps to successfully map CTI reports to ATT&CK. [https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping](https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping)

**STEP 00**
UNDERSTAND MITRE ATT&CK

Ensure you know what ATT&CK is (and isn’t) and how you can use it to understand adversary behavior. Visit [attack.mitre.org](http://attack.mitre.org) to learn more about the framework.

**STEP 01**
FIND THE BEHAVIOR

Search for signs of adversaries interacting with platforms or apps to help find a chain of suspicious behavior. Work to understand what led to the initial compromise and how the adversary performed the post-compromise activity.

**STEP 02**
RESEARCH THE BEHAVIOR

Perform additional research to understand the timeline of suspicious behaviors. This may include reviewing the original source reporting, looking at technical details to better understand overall adversary behavior, or searching the ATT&CK website for key terms that help identify behaviors.

**STEP 03**
IDENTIFY THE TACTICS

Review your report to identify tactics, the adversary’s goal. Try to figure out what the adversary was trying to accomplish and why. Review tactic definitions in ATT&CK and compare them to the adversary’s behaviors. Identify all the tactics in the report to help understand specific techniques or sub-techniques they can use to achieve that goal.

**STEP 04**
IDENTIFY THE TECHNIQUES

Review the technical details in your report to understand how the adversary tried to achieve their goals. Compare this behavior with ATT&CK techniques listed under the tactic you’ve identified. Remember that techniques and sub-techniques are not isolated activities, but elements in the adversary’s larger playbook.

**STEP 05**
IDENTIFY THE SUB-TECHNIQUES

Once you’ve identified techniques, review sub-technique descriptions in ATT&CK and compare them to behavior outlined in the report. If one aligns, it is probably the right sub-technique. How effectively you can identify a sub-technique depends on the detail in your report.

**WORST PRACTICES: AVOID THESE ATT&CK PITFALLS**

MITRE ATT&CK is one tool in a cyber analyst’s toolbox, but it can take some care to use. All too often, defenders try to use ATT&CK in ways that might even hurt their defenses. Here are three common mistakes ATT&CK users make, along with steps you can take to avoid these pitfalls.

**TRYING TO ACHIEVE 100% COVERAGE**

Every organization faces its own unique cyber threats. Not every tactic or technique will apply to everyone. Instead of trying to defend against every tactic or technique in the matrix, prioritize the ones that are most relevant to you and ensure you are prepared for them.

**SHOUTING “BINGO!” WHEN YOU HAVE ONE TECHNIQUE**

Just because you’ve identified a single way an adversary has done technique doesn’t mean it’s time to declare success and color a box green. Adversaries have multiple ways they can perform most ATT&CK techniques. It’s great that you’ve found one, but be sure you’re looking for and understand other possible ways a technique might be accomplished.

**LIMITING YOURSELF TO THE MATRIX**

Remember, the ATT&CK matrix only documents observed real-world, in-the-wild behaviors. But adversaries may (and probably do) have a series of other behaviors they use that have not yet been documented in ATT&CK. To get a full picture of the threats your organization faces:

1. Leverage your own intelligence sources
2. Create and document your own observed techniques
3. Don’t limit yourself to behaviors, a timely indicator can still catch an adversary
### MITRE ATT&CK Enterprise Framework

<table>
<thead>
<tr>
<th>RESOURCE DEVELOPMENT</th>
<th>INITIAL ACCESS</th>
<th>EXECUTION</th>
<th>PERSEVERANCE</th>
<th>PRIVILEGE ESCALATION</th>
<th>DISCOVERY</th>
<th>NETWORK</th>
<th>CREDENTIAL ACCESS</th>
<th>EXTERNAL MOVEMENT</th>
</tr>
</thead>
</table>

### MITRE ATT&CK

[attack.mitre.org](http://attack.mitre.org)

© 2023 MITRE - Framework issued as of October 2023