RSA Conference 2019

BETTER.

Peer2Peer

Making MITRE ATT&CK™ Work for You: Sharing Best Practices for Success

P2P2-R03: Making MITRE ATT&CK™ Work for You: Sharing Best Practices for Success

Katie Nickels, ATT&CK Threat Intelligence Lead, MITRE

Making MITRE ATT&CK™ Work for You: Sharing Best Practices for Success

MITRE ATT&CK™ is quickly becoming the industry standard for describing adversary behaviors and improving defenses, but many organizations who want to use it don't know where to start. This was the focus of attendees of this Peer2Peer session as they discussed best practices to allow participants to leave with actionable insights to apply to their own ATT&CK use cases. A full house of attendees representing organizations ranging from the energy sector to cybersecurity product vendors shared insights between those who were more advanced in using ATT&CK to those who were just getting started.

The discussion started out by focusing on what use cases the attendees believed ATT&CK could help with. A key theme that many participants identified was that ATT&CK was a useful tool to help organizations understand their coverage and visibility, a common challenge for network defenders. Specifically, discussion centered around how ATT&CK provided a framework to allow organizations to identify what gaps they had and prioritize which of those gaps to fill first.

To help achieve those use cases, attendees shared actionable recommendations for implementing them. One suggestion for how to do this gap analysis was by creating heat maps, such as with the ATT&CK Navigator. Other recommended actions included writing detections in security information and event management systems (SIEMs), creating threat models, tracking incidents over time, performing threat hunting, and validating controls. Attendees also noted that ATT&CK could be used across both vendors and end user organizations, as well as by both blue teams and red teams.

All frameworks and models have limitations, and the group discussed what some of these were with ATT&CK. The attendees felt an important point to remember when using ATT&CK is that it doesn't cover everything, so users should make sure not to get a false sense of security by using it – it's not a silver bullet. One limitation that an attendee pointed out was that it focused more on adversary behaviors, but in some cases, traditional indicator-based approaches like anti-virus were still effective, so users should remember those approaches have value as well. Along the same lines, another attendee noted that defenders should still focus on simple tasks like patching and asset management that are key to a successful security program but are not the focus of ATT&CK.

Along with limitations, the group discussed challenges with using ATT&CK. One challenge that multiple attendees noted was that to successfully use ATT&CK-based detections, they had to know what "normal" looked like for their own environment, since some techniques would be anomalous in some organizations but not others. One challenge with this approach is what "green" detections really mean (in the common practice of designating technique coverage as red, yellow, or green) – how does an organization decide when their detection coverage of a technique is "good enough"?

The group finished up the session by discussing best practices to help address some of these challenges. On the question of marking techniques as “green,” one suggestion was to use traditional intelligence language surrounding confidence: high, medium, and low. Another participant suggested getting rid of the red/yellow/green coloring and using a “gray scale” of different shades instead.

Many organizations in the room attended the discussion with the goal of figuring out how to get started using ATT&CK, and more mature organizations shared ideas with them on how to do this. A common suggestion was to start simply with information you already have, such as a log source your organization already has. If an organization has an endpoint tool in place, several attendees recommended this as a good place to look for data sources. Attendees recommended getting started with simple, “low-hanging fruit,” which for many organizations would include Windows techniques due to it being a common operating system. Another suggested way to start with ATT&CK was by looking at a specific threat actor and focusing on trying to detect their techniques. Continuing with the theme of “narrowing the scope” of what you focus on to start with ATT&CK, another attendee suggested focusing just on critical assets, then broadening the focus from there.

Whether they were from end user security operations centers or vendors who were looking for a common language to incorporate into their product, attendees of the Peer2Peer session agreed ATT&CK had potential to help their organizations improve how they track and defend against adversary behaviors. By sharing common use cases, limitations, and best practices, attendees empowered each other with actionable insights to take back to their respective organizations to allow them to use ATT&CK to move toward a threat-informed defense.

©2019 The MITRE Corporation. ALL RIGHTS RESERVED. Approved for public release. Distribution unlimited 18-1528-46.