"ATT&CK in Practice" Workshop Summary

About ATT&CK™

ATT&CK is a MITRE-developed, globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. ATT&CK is open and available to any person or organization for use at no charge.

On 24-25 May 2018, over 40 participants met at C3 (the Cybersecurity Competence Center) in Luxembourg to discuss how MITRE ATT&CK™ can help strengthen cyber defense. The participants hailed from over 30 different organizations, ranging from national CERTs to financial sector organizations to cybersecurity vendors. Despite their differences in country of origin, sector, and background, attendees came together with a common goal of sharing how ATT&CK can be used in practice.

The workshop was organized by Freddy Dezeure, an independent consultant and former head of CERT-EU and was hosted by CIRCL. The focus was on attendee organizations sharing how they use ATT&CK or plan to in the future. MITRE provided framing presentations for each topic, followed by "lightning talks" from attendees, which encouraged active discussion and exchange of ideas. The workshop focused on 5 main topics: Taxonomy and Content, Tactical and Strategic Analysis, Prevention, Detection, and Automation/Orchestration/Playbooks.

Lightning talks consisted of discussions both from those using ATT&CK for defending their organization as well as vendors incorporating ATT&CK into their products. Topics included how organizations used ATT&CK for evaluating detections, enriching alerts in products, organizing threat intelligence, determining data source coverage, prioritizing threats, comparing products, performing threat hunting, mapping to security controls, and conducting red teaming. Attendees discovered multiple commonalities in their work, giving them the opportunity to share best practices and lessons learned from ATT&CK implementations.

Key themes and discussions from the workshop included:

Taxonomy and content

MITRE presented the plan for adding more detailed sub-techniques, and the audience agreed sub-techniques were a positive addition to enable more granular use cases. The group cautioned against making ATT&CK overly complex, though, and noted that one of ATT&CK's strengths was that different users, from the C-suite to analysts to engineers, can choose the level of abstraction they need. ATT&CK also lets them communicate to their management.

The group was interested in a way to express timeline and order of technique execution, including capturing technique dependencies. Attendees also supported a way to express impacts/effects (like those caused by destructive ransomware) in ATT&CK, as well as noting that content for other technology domains (e.g. network devices) would be desirable.

There was a discussion on how to represent data sources used to detect techniques, and how their representation in ATT&CK could be normalized and improved.

Several organizations noted that they had tried to create and maintain their own internal taxonomy of adversary TTPs/behaviors, but found it to be burdensome to maintain, so switched to

using ATT&CK. Since many organizations now rely on ATT&CK, it needs to remain relatively stable over time, and the community should have sufficient warning about any changes.

Detection and analytics

Many attendees mentioned how ATT&CK was helping them move away from only detecting indicators to also detecting behaviors/tactics, techniques, and procedures (TTPs). Attendees expressed that the link between ATT&CK and analytics, such as those provided in the Cyber Analytic Repository (CAR), is an important part of making ATT&CK actionable. The group wondered if CAR should be a public repo for anyone to contribute to, or if analytics should be shared among smaller groups.

The group expressed interest in having CAR be updated, maintained, and migrated from Wiki format to another structured format that would make it easier to work with. A Github repo or MISP could potentially host analytics to be shared.

The group noted that ATT&CK shouldn't try to be another threat sharing platform – it needs to focus on its purpose of maintaining a core knowledge base. ATT&CK itself isn't the right place for sharing threat information like technique sightings.

Contributions

Several organizations noted that they have contributions for new techniques that they are willing to share, particularly Linux techniques. Currently the process is to email attack@mitre.org to contribute via a manual, unstructured process. Attendees wondered if a form or other submission method would make it easier to contribute, and they also expressed interest in knowing what others had contributed. There was also a discussion of contribution guidelines and how to help people create quality contributions. One suggestion was to create a Github repo or similar central repository to make it easier to see other contributions. The group discussed the possibility of having both "MITRE-verified" techniques as well as other techniques submitted by external contributors that had not been vetted.

Community

The group found value about hearing each other's use cases and think it would be valuable to continue the conversation. There are plans to set up a forum to allow the group to communicate as well as schedule a follow-up European User Group in October 2018.

There was also a discussion about training and how to broaden the community. The participants expressed interest in training modules that could be re-used so that they could help others learn.

The MITRE ATT&CK team is using feedback from attendees to drive discussions about future plans, such as how to streamline the contribution process, what actions should be taken on CAR, and how to better support the ATT&CK community. "This event allowed us to create new relationships with the users of the ATT&CK model and also set an objective of continually improving it," says Richard J. Struse, chief strategist for cyber threat intelligence at MITRE. "This is really important for us because no one organization has answers to all of the questions."