Douglas Geddes
dgeddes@quantalytics.com
+2 (710) 500-1915

CUSTOMER PROPOSITION - MITRE ATT&CK®

3 CRITICAL ASPECTS OF MITRE ATT&CK

It's important to understand:

1. That the ATT&CK framework is not about vulnerabilities

2. And most of the adversary behaviours catalogued in ATT&CK do not rely on an exploitable vulnerability.

3. The fact that most of the publicly reported adversary behaviours in ATT&CK would work on systems that are 100% patched against all known CVEs can be tough for people to accept.

But it's true and it's true for a very simple reason—once they have achieved initial access adversaries become users, albeit unauthorized ones, of the very same systems you are using. At this point they begin to "live off the land", using the tools and resources and connections that exist to support the operations of your enterprise.

Purpose of this document –

To introduce the MITRE ATT&CK® framework, which is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations to Organizations who want to move towards a more **threat informed defence**.

To introduce the Cyber Threat Intelligence Assessment using MITRE ATT&CK which entails an External and Internal engagement process.

What is MITRE ATT&CK?

MITRE ATT&CK is a documented collection of information about the malicious behaviours advanced persistent threat (APT) groups have used at various stages in real-world cyberattacks. ATT&CK, which stands for Adversarial Tactics, Techniques, and Common Knowledge, includes detailed descriptions of these groups' observed **tactics** (the technical objectives they're trying to achieve), **techniques** (the methods they use), and **procedures** (specific implementations of techniques), commonly called **TTPs.**

ATT&CK is a tool that private and public sector organizations of all sizes and industries have widely adopted. Users include security defenders, penetration testers, red teams, and cyberthreat intelligence teams as well as any internal teams interested in building secure systems, applications, and services.

Douglas Geddes
dgeddes@quantalytics.com
+2 (710) 500-1915

The wealth of attack (and attacker) information it contains can help organizations determine whether they're collecting the right data to effectively detect attacks and evaluate how well their current defences are working.

ATT&CK intentionally takes an attacker's point of view to help organizations understand how adversaries' approach, prepare for, and successfully execute attacks.

We are proposing a Cyber Threat Intelligence analysis of your organization using the MITRE ATT&CK Framework.

Due to the scope and in-depth analysis of the organization using the framework the consultation process compromises an External / Internal Assessment. Organizations can either opt for an External assessment only or the full External/Internal Assessment process.

External Assessment

Advanced Persistent Threat (APT) Groups are well funded, highly skilled threat actors and pose a significant threat to an organization. The MITRE ATT&CK Framework assess their behavioural characteristics during the tactical phases of the attack process.

What this means is that understanding the behaviour of an attacker and their TTP's (Tactics, Techniques and Procedures) leads to a more **threat informed defence mindset** vs the reactive defensive approach where organizations have no initiative-taking control over the attacks that occur.

The external assessment takes the viewpoint of the attacker. How does the attacker see your organization /website and what TTP's are you most vulnerable to? By assessing the behavioural characteristics externally, the organization can prioritize on which techniques to focus on therefore mitigating their risk posture significantly.

The dissemination of malware/ransomware follows a similar behavioural approach. Understanding this approach creates priority techniques enabling the organization to focus its resources efficiently to mitigate risk.

Are you deploying cloud services? Are your security controls detecting the correct Tactics and Techniques of the attacker relevant to your organization?

Douglas Geddes
dgeddes@quantalytics.com
+2 (710) 500-1915

Internal Assessment

The more technical and deep dive process of a **Threat informed Defence Approach** takes place in the internal assessment phase. The organizations technical cyber security team participates during this phase. Here detection capabilities are assessed against the priority Tactics, Techniques and Procedures. Data sources are reviewed, and defensive recommendations are made. Tooling capabilities are also assessed with defensive recommendations.

What is a Threat Informed Defence Approach?

The definition can be described as "**The systematic application and deep understanding of adversary tradecraft and technology to assess, organize and optimize your defences.**" Put more simply, it's the use of known adversary behaviours as a lens through which you view your defences.

By looking at your enterprise from the perspective of the adversary, you gain critical insights into how to prioritize your security operations and investments. That shift in perspective helps you see more clearly how a skilled adversary would use your enterprise's resources against you.

Reason to Act Now

Threat-informed defence extends well beyond the boundaries of ATT&CK. Much of the value of threat-informed defence comes from relating adversary behaviours in ATT&CK with the rest of an enterprise's security context. That context can range from the specific threat groups that target organizations such as yours to the defences you currently have in place to your confidence in the efficacy of those defences based on testing.

The context can even include specific vulnerabilities that enable adversary behaviours of concern to you. In the end, it's all about connecting the dots between relevant adversary behaviours and the defences in place to stop (or at least detect) them.

Another benefit of employing a threat-informed approach is the availability of clear benchmarks for the evaluation of existing controls and capabilities. With an understanding of the specific adversary behaviours of concern within your enterprise, you now have a roadmap for how to begin to evaluate the ability of your fielded defences to protect against, detect or respond to those behaviours.