SOLUTION BRIEF

McAfee Advanced Threat Defense Leverages MITRE ATT&CK Framework

Simplify reporting, streamline workflows, defend faster

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) framework is increasingly gaining ground on a global level as a way of describing security issues from the adversary's perspective. This publicly shared knowledgebase is built from a compilation of relevant, real-world attack intelligence from government, industry sectors, and security vendors. It helps you understand how adversaries prepare, launch, and execute attacks. ATT&CK provides information on adversarial behavior, attack lifecycles, targeted platforms, and the techniques and tactics used to achieve the attacker's objectives. Unlike other frameworks, ATT&CK is available at no charge to everyone and does not require special access privileges. Our ongoing commitment to simplified reporting, streamlined workflows, and faster defenses has resulted in incorporating the ATT&CK framework into McAfee® Advanced Threat Defense.

Connect With Us

Why You Need the MITRE ATT&CK Framework

ATT&CK benefits your security operations center and your organization as a whole in a number of ways. It helps you:

- Expand the knowledge of the network defenders and assists in prioritizing network defense by detailing the tactics, techniques, and procedures (TTPs) cyberthreats used to gain access
- Correlate specific adversaries and the techniques they have used by providing a library that details adversary groups and the campaigns they have conducted
- Gain an understanding of the specific techniques used by adversaries for named campaigns so you can evaluate and strengthen your security architecture and strategy
- Upgrade skills of junior analysts through training, which is one important step enterprises have taken to address the global cybersecurity skills shortage. The ATT&CK framework has been incorporated into many security certification courses offered by the SANS Institute and other organizations to help junior analysts better understand adversary tactics, techniques, and processes (TTPs) and apply that knowledge to improve the efficacy of their threat-hunting processes.
- Use a common language rather than vendor-specific jargon. ATT&CK establishes a standard way to talk about cybersecurity in a way that everyone can understand—both analysts and non-analysts alike.

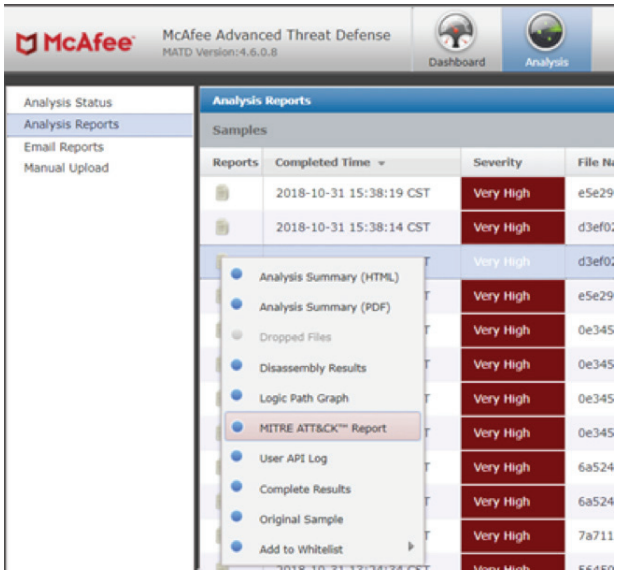

Figure 1. McAfee Advanced Threat Defense produces a range of detailed reports from summary reports for action prioritization to mapping results to the MITRE ATT&CK framework and analyst-grade malware data.

McAfee Advanced Threat Defense and ATT&CK

McAfee Advanced Threat Defense, which combines multiple analysis methods—in-depth static code analysis, dynamic analysis, and machine learning—for more accurate detection, now provides enhanced reporting that maps directly to the ATT&CK framework. This simplifies interpretation and reporting for analysts and thereby accelerates their workflow. Reports generated by McAfee Advanced Threat Defense provide a clear understanding of what tactics and techniques are being used.

McAfee Advanced Threat Defense has always been known for its easy-to-read reports. With the integration of ATT&CK, enterprises can move toward a security-first culture more quickly. Security analysts can use these reports to inform their supervisors, who can, in turn, clearly and confidently communicate these findings to executives and other stakeholders. It's much like using a textbook for an open-book exam—all the answers are readily available.

By including the ATT&CK framework in McAfee Advanced Threat Defense, you can more quickly understand the techniques, tactics, and procedures of a given threat. Once you have this information, you can act faster to implement corresponding defenses or discovery methods. This is just one of many ways that McAfee is continually evolving and improving its platform to help you achieve successful security outcomes.

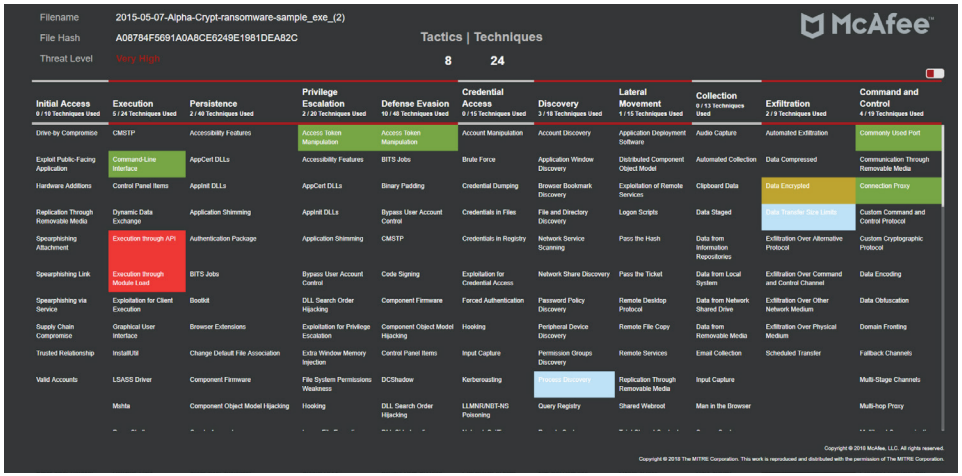

Figure 2. Results in McAfee Advanced Threat Defense map to the MITRE ATT&CK framework.

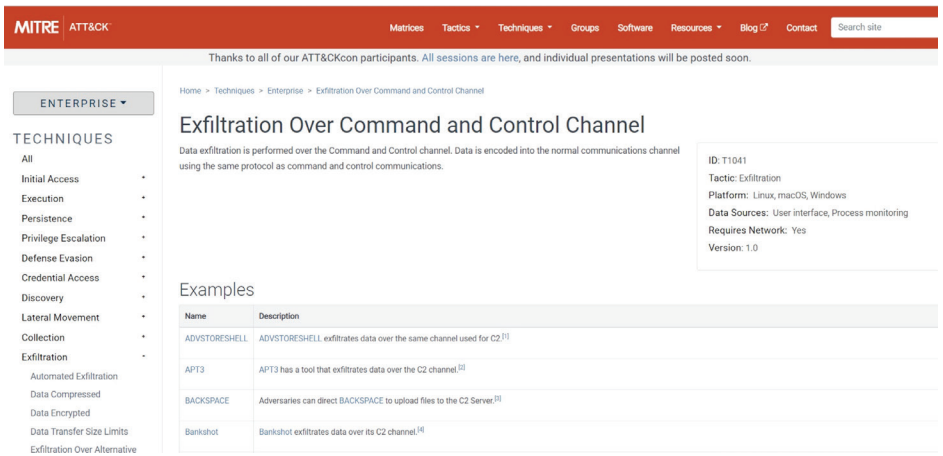

Figure 3. Analysts can easily pivot from identified tactics and techniques in the McAfee Advanced Threat Defense MITRE ATT&CK report to the ATT&CK framework for detailed information from MITRE.

About MITRE

The MITRE Corporation (MITRE) is a not-for-profit organization based in Bedford, Massachusetts and McLean, Virginia. Through federally funded R&D centers and public-private partnerships, MITRE tackles challenges to the safety, stability, and well being of our nation. With a charter to work on behalf of the public interest, MITRE has no owners or shareholders and does not in any way compete with industry. The organization gathers sensitive and proprietary information from the government, industry, and other partners to inform the work it does and never uses this data for a competitive advantage.

About McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all. **www.mcafee.com**

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com