IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Implementation of the MITRE ATT&CK Framework

Steve Rivers

Steve Rivers
Technical Director
International
ThreatQuotient

Biography

Steve Rivers is the Technical Director, International at ThreatQuotient (https://www.threatq.com/). Steve's current skill set has been built on significant experience at all levels of the industry including management, technical consulting and sales engineering.

Steve has been involved in client facing roles for many years and has travelled widely across Europe, North America and Asia. This experience has brought an understanding of the varied global marketplace and the different approaches to doing business that it brings.

Keywords Malware, Threat hunting, Cyber security, Cyber attacks, Threat intelligence, Incident analysis
Paper type Opinion

Abstract

Since the emergence of the first real malware about 25 years ago, it became clear that criminals lurk in the expanses of the World Wide Web. Nevertheless, it is no use giving up and surrendering to your fate. Instead, it is important to face up to the threats and become proactive when it comes to your own security. The new buzzword is anticipation, and the MITRE ATT&CK framework can help make this approach a reality. In this article, the author discusses the implementation of the framework, incident analysis, and the importance of threat hunting.

Introduction

Sun Tzu, the fifth-century B.C. Chinese general and philosopher, knew that knowledge is power and stated this in his oft-cited work, *Art of War*, as follows: “If you know the enemy and know yourself, you need not fear the result of a hundred battles.”

This wisdom of the military strategist is not only applied on real battlefields, but also on the digital frontlines of cyberspace. At least since the emergence of the first real malware about 25 years ago (for example, ‘Melissa’ and ‘ILOVEYOU’), it became clear that criminals lurk in the expanses of the World Wide Web. Nevertheless, it is no use giving up and surrendering to your fate. Instead, it is important to face up to

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

the threats and become proactive when it comes to your own security. The new buzzword is anticipation, and the MITRE ATT&CK framework[1] can help make this approach a reality.

The MITRE ATT&CK framework has now become an established tool for security teams to assess their organization's security posture with respect to specific attackers and attack methods. With MITRE ATT&CK, teams can access threat intelligence from the constantly updated knowledge base to better assess their own situation and thus ensure that no critical elements of an attack are overlooked.

Implementation with the help of a Threat Intelligence Platform

One of the initial difficulties many IT teams face when implementing the MITRE ATT&CK framework is the sheer overwhelming number of different techniques and use cases that are made available to you. In order not to get bogged down in wracking one's brains over implementation given the multitude of options, one should first focus on a few use cases.

To identify the relevant use cases, it is important to analyze one's own situation and to set priorities with regard to concrete data that is relevant for one's own company. What can be of enormous help here is a dedicated threat intelligence platform (TIP). Such a platform automatically aggregates threat intelligence and helps to identify and prioritize the data and information streams that are most important for the respective user.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In the following, we will present two use cases in which a TIP helps security teams get the most out of the MITRE ATT&CK framework. We are talking here about two pillars of modern IT security: the analysis of incidents and the hunting down and resolving of threats, so-called threat hunting.

Incident analysis

When analyzing incidents, it is critical to think outside the box in addition to examining the information gathered on the ground. In order to understand the bigger picture of an attack and assess how and why it occurred, the incident in question must be placed in relation to an organization's individual risk profile as well as the global situation in the cybersphere.

This is where MITRE ATT&CK comes in: the data collected during internal analysis can be compared and connected to current attack campaigns and threat actors using the framework, giving context to the incident and thus helping to better understand why one's organization in particular was attacked and whether further incidents might occur. Security analysts can use the framework's data as a detailed reference source to enrich their analysis of events and alerts, support their investigations, and determine the best actions to take based on relevance and incidents in their environment.

However, since manual data enrichment is error-prone, time-consuming, and tedious, a TIP can remedy this and free up the security team. By automating the

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

collection and aggregation of data from the MITRE ATT&CK framework, security professionals save time, which is then freed up for higher-level tasks and analysis. In addition, such a solution ensures that no important information is overlooked when aggregating threat intelligence.

Threat hunting

A relatively new, but extremely important approach in the fight against cyber threats is threat hunting. In this area, specialized security experts work with threat intelligence to proactively hunt for cyber threats. They hypothesize based on the information they gather, which they use to search for and resolve threats, contributing to the security of the organization's IT and networks. Here, too, a TIP can do important work to speed up and simplify processes.

After the initial analysis of an incident, threat hunting teams can move from looking for so-called Indicators of Compromise (IoCs) to using the full range of ATT&CK data. Instead of focusing on individual suspicious data points, threat hunters can use the platform to work from a higher-level viewpoint with detailed information about potential and actual attackers and their methods. In this way, the security team can take a more proactive approach, first identifying the organization's risk profile. The individual risks can then be mapped to specific attackers and their tactics, which then allows threat hunters to more closely examine whether appropriate data has been identified in the environment being investigated.

In summary

The usefulness of the MITRE ATT&CK framework depends not least on whether it is implemented effectively and whether security managers have the ability to aggregate and analyze the data in a simple way. Organizations can only make good use of the framework if they can properly assess and understand the relevant use cases and their organization's individual security posture. To facilitate this, technologies such as threat intelligence platforms exist that are capable of supporting security operations teams at all levels of their work. These solutions enable deeper penetration into the MITRE ATT&CK framework, thereby optimizing its effectiveness and deriving much greater benefit from the knowledge base.

Reference

[1] https://attack.mitre.org/