ATTACKIQ

Case Study

Using MITRE ATT&CK in the Financial Sector

Using MITRE ATT&CK in the Financial Sector

MITRE ATT&CK is a sector-agnostic cybersecurity framework that can help any organization to improve its cybersecurity effectiveness. To explore how one major company uses MITRE ATT&CK, we spoke to a leading chief information security officer in the financial sector about how ATT&CK and the AttackIQ Security Optimization Platform help him to protect his customers and the firm's most important data. He outlined how he puts MITRE ATT&CK into practice through AttackIQ's Security Optimization Platform and the benefits he gains from generating real data about his security program's performance, lessons from which other organizations, too, might benefit.

The Company

Dimensional Fund Advisors (DFA) is an investment management service that operates with over $550 billion in assets under management. Headquartered in Austin, Texas, the 38-year-old company has over 1,700 employees and, in the words of its head of cybersecurity, Peter Luban, is "run by a group of computational geniuses." As a global distributed firm with significant financial assets, it faces similarly significant cyberthreats to its assets and personnel.

As the head of cybersecurity at Dimensional Fund Advisors, Luban watches out for a range of cybersecurity risks to his organization, using the knowledge and skills obtained over 20-plus years working in cybersecurity and risk management. MITRE ATT&CK, operationalized with AttackIQ, has helped him set a strategic baseline for his team. Luban refers to ATT&CK as the "mother brain" of cybersecurity planning and threat intelligence for his firm, a tool that helps him align his entire security team around probable threats so that he can achieve real security outcomes for his firm.

A Transformational Approach to Cybersecurity

MITRE ATT&CK's focus on threat-informed defense helps Luban stay ahead of emerging threats. Over the last decade, adversaries have changed their behavior tactics, techniques, and procedures to exploit fissures in security systems. In the past, adversaries focused more on developing unique malware payloads to achieve specific effects. Today, adversaries have shifted their emphasis to social engineering and to finding the weakest link in second- or third-party applications that could help them gain access to the institution's crown jewels.

A good example of this is North Korea's attack on the Bangladesh Central Bank in 2015. North Korea discovered a vulnerability within the Bangladesh Central Bank network, used the vulnerability to access the Bangladesh Central Bank's access point for its Society for Worldwide Interbank Financial Telecommunication (SWIFT) code, and then sent a request to withdraw over $81 million dollars from Bangladesh Central Bank's holdings in the U.S. Federal Reserve Bank in New York. The adversary hopped from one network to another.

CUSTOMER

Dimensional Fund Advisors

LOCATION

Americas

INDUSTRY

Finacial Services

HIGHLIGHTED SOLUTION AREAS

- Threat-Informed Defense
- Audit and Testing
- Security Control Validation
- Security Operations Accountability
- Real Performance Data

BUSINESS IMPACT

- Validation of security control effectiveness and compliance
- Optimization of security practice methodology
- Simpler, faster, and lower cost discovery of security gaps
- Ability to verify vendor claims when selecting new security technology

A Transformational Approach to Cybersecurity (cont.)

So how does ATT&CK help cybersecurity professionals like Luban understand the adversary and defend his firm? In Luban's mind, the principal value is that the ATT&CK framework codifies adversary capabilities into one simple and easy-to-use tool for security teams to access. It makes threat intelligence useful through its expanded view of the adversary and their capabilities. This is an historical advancement in the field of threat intelligence. By analogy, Luban notes, if in the 1980s video games presented characters through a series of single dots on a screen aligned in two dimensional space, today video games have evolved into an immersive, three-dimensional experience in which the user sees a complex environment where threats and other players move through a space.

The evolutionary analogy stands with ATT&CK. In the past, to conduct forensics and understand their cybersecurity postures, defenders focused their sensors on "indicators of compromise" (often referred to as "signatures"), remnants in the computer code of an adversary's presence; this data providing only one small insight into the attacker. Moving far beyond signatures, the ATT&CK framework gives defenders a comprehensive view of the threat landscape; it allows defenders to see the attacker move along every step in the attack ladder. With years of threat research behind it, the framework provides what Luban refers to as "a giant well of unbiased, third party analysis."

MITRE ATT&CK Applied in Practice

Practically, this makes ATT&CK useful in two principal ways for Luban and Dimensional Fund Advisors.

First, it serves as a purple team platform for a small security team. Luban has eight security professionals on his team that are responsible for defending the entire Dimensional Fund Advisors' enterprise and all of the firm's assets. On such a small team, Luban doesn't have a dedicated red or blue team to conduct malware forensics and reverse engineering; ATT&CK provides a recipe for purple teaming, and his security team can follow the framework left to right, using it as an intelligence resource for their defense operations. It gives his firm a ready-made, industry-vetted, research-informed methodology by which he can validate his security effectiveness.

The second broad utility is that ATT&CK provides him with leverage with his infrastructure and technology teams across the company. It gives a common language of risk and, when used with a breach and attack simulation platform such as AttackIQ, allows him to measure his team's performance against threats, giving him and his team real performance data that he can use to measure his organization's security effectiveness. If and when a new application is brought into the organization, he and others in the company can use ATT&CK-based scenarios to validate that application's security.

This is particularly useful when facing the demands imposed by governmental regulators, which are especially strict when it comes to financial governance. Regulations include the National Institute of Standards and Technology 853 family of reports, as well as strict laws from the European Union, New York, and Singapore. The regulations all have subtle differences between them, yet for each of the regulators and for his board, Luban can use ATT&CK to validate and display how security controls are working (or not). Luban notes that "ATT&CK gives us an edge to be able to better prepare" if and when a regulator were to ask for more data; the framework helps him validate his security control effectiveness and provide regulators and his board with granular performance data.

MITRE ATT&CK Applied in Practice (cont.)

There is another application. If Luban has data indicating ineffectiveness, he can turn to his teams or the board and outline the steps required to solve the problem. ATT&CK gives him accountability. "There's tons of configuration drift," Luban notes, on top of the "tons of people with lots of different hands in the various pieces which inevitably turn into a security nightmare." ATT&CK allows him to focus on what matters from a threat standpoint. "It helps me focus on what the relevant threat is. Then, when it comes time to identify what the threat is, we can remediate. If the report comes back green instead of red, or if it comes back red again, I can tell someone if there are problems in the environment." In this way, ATT&CK, especially used in combination with a breach and attack simulation platform, serves as a tool for driving effectiveness.

Conclusion: The Benefits of Real Performance Data

"It's nice to get real data," Luban concludes. "There is long-term value to be gained through ATT&CK. It's a unifying effort and a way that we can all refer back to it. It's the mother brain." That unifying component is to is, to Luban's mind, the biggest benefit of the framework. ATT&CK provides the security world with a clear process through which to understand threats and build intelligence about adversary behavior. It gives people at the chief information security officer level a way to think about risk effectively at the strategic and management level. As a modern, adversary-focused approach, ATT&CK is an immensely valuable tool for security leaders.

ATTACKIQ

U.S. Headquarters
9276 Scranton Road, Suite 100
San Diego, CA 92121
+1 (888) 588-9116
info@attackiq.com