INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

IJIEMR Transactions, online available on 1st July 2024. Link

https://ijiemr.org/downloads.php?vol=Volume-13& issue=issue7

**DOI: 10.48047/IJIEMR/V13/ISSUE 07/1**

Title Leveraging Threat Intelligence, AI and ML with MITRE ATT&CK for Prioritized Risk Assessments in Financial and actionable Security Strategies

Volume 13, ISSUE 07, Pages: 1 - 4

Paper Authors
ShivaDutt Jangampeta, Sai Teja Makani

International Journal for Innovative Engineering and Management Research

PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL

www.ijiemr.org

# Leveraging Threat Intelligence, AI and ML with MITRE ATT&CK for Prioritized Risk Assessments in Financial and actionable Security Strategies

**[1]ShivaDutt Jangampeta, [2]Sai Teja Makani**
[1]Senior Manager of Security Engineering
JPMorgan Chase, Plano, USA
shivadutt87@gmail.com
[2]Senior Manager, DevOps, Spotter Inc
Culver City, CA
saitejamakani@spotter.la

## Abstract

Abstract – Recently, cybercriminals are constantly devising advanced methods to evade information security measures, to steal sensitive, valuable data from victims. These cyber-attacks usually use various attack vectors to gain first access to data infrastructures. Oftentimes, security teams face the challenge of detecting malicious programs, attack vectors, or attack propagation as some attacks are regarded as multi-stage attacks that present grave threat to people, organizations, and governments. This review discusses how threat intelligence and MITRE ATT&CK can be deployed to comprehensively understand adversary techniques and tactics in the financial environment.

**Keywords:** MITRE ATT&CK, AI, ML, Cyber-attacks, cyber threats, Threat Intelligence.

## Introduction

A cyber risk assessment is the process/technique of detecting, analyzing, and gauging cyber security vulnerabilities and threats that could adversely impact organization's valuable data, operations, and reputations. This process helps organizations prioritize their security efforts, adhere to policies and regulations, and seamlessly communicate with all stakeholders. Businesses can employ different frameworks to conduct risk assessment, based on their security needs and objectives, including NIST Cybersecurity Framework, ISO/IEC 27001, Factor Analysis of Information Risk (FAIR) Model, and CyberInsight-model based on MITRE ATT&CK framework [1]. Owing to the constant evolution of the cybersecurity landscape, there is need for businesses to stay ahead of cybercriminals by understanding their tactics and techniques they leverage. This is referred to as threat intelligence. Among the aforementioned security frameworks, the MITRE ATT&CK model helps organizations to analyze threat actors and devise defense strategies to prevent potential attacks.

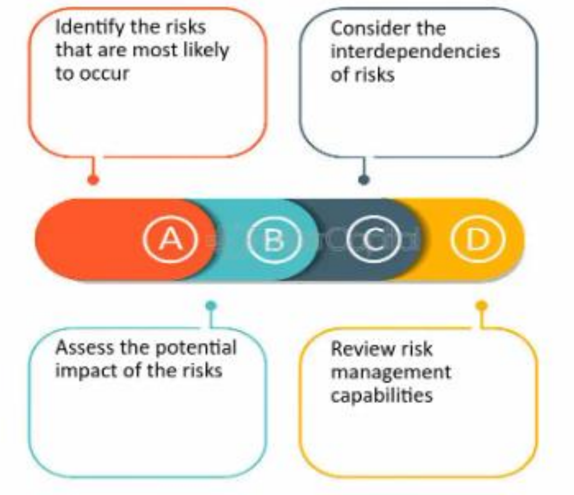
Identify the risks that are most likely to occur
Consider the interdependencies of risks
A
B
C
D
Assess the potential impact of the risks
Review risk management capabilities

Figure 1. Prioritizing risk

## A. Leveraging MITRE ATT&CK Framework to enable AI and ML, Threat Intelligence and Develop Defense Plans

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is an all-inclusive matrix of techniques and tactics used by malicious actors to launch cyber-attacks. Executing MITRE ATT&CK methods encompasses understanding and deploying the framework for multiple information security intends, like threat modelling, security testing, as well as defense strategies [2]. To successfully deploy MITRE ATT&CK techniques, security teams should strategically tailor their organization's security needs with the security posture. Apart from defensing businesses against attacks, MITRE ATT&CK techniques helps security experts to understand the evolving cyber threat landscape to effectively adapt their defenses.

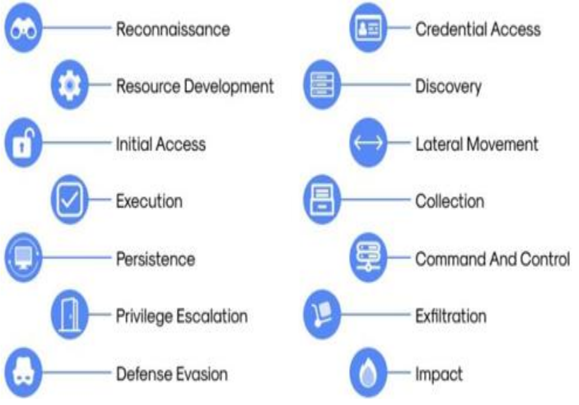

Figure 1. MITRE ATT&CK Framework

## B. Components of MITRE ATT&CK Framework

- ***Threat Intelligence:*** MITRE ATT&CK enables security experts to strategize their threat intelligence based on adversary behaviors and also identify and mitigate the impact. Security teams can overlay this information to create a threat-based awareness and determine whether their immediate defenses can identify and mitigate known adversaries.
- ***Detection and Analytics:*** the framework helps defenders map log and incident data about hackers' behaviors, enabling them to develop an all-inclusive protection model to identify attacks before they can cause damage.
- ***Adversary Emulation and Red Teaming:*** the framework enables security teams to develop adversary emulation cases to test the strength of their defenses against popular adversary techniques.
- ***Assessment and Detection Engineering:*** the framework provides an extensive lists of techniques leveraged by attackers to

achieve their goals. Security professionals can use them to better comprehend the attack techniques and put in place robust defenses systems to identify and mitigate them.

### Using MITRE ATT&CK For Prioritized Risk Assessment In Financial Sector

For banks and financial institutions, the aftermath of a successful cyber-attack could imply loss of money, theft of customer data, reputational damage, legal implications, or even insolvency. Besides, industry leaders warn that major attacks on the broader financial sector could ruin confidence in the system, derange critical infrastructures and operations, and disrupt other sectors. Lately, financial institutions have consistently been a leading target for cybercriminals [3]. Organized hackers' groups and state-sponsored cybercriminals are continuously investing in sophisticated malware and ransomware tools to compromise financial systems. These threat actors can do whatever it takes to intercept transactions, steal valuable customer identities, steal monetary assets, and acquire financial information of virtually any kind.

Financial systems can immensely benefit from deploying MITRE ATT&CK framework as part of intelligent, threat-informed defense plan. MITRE ATT&CK model is, in both depth and breath, an exhaustive attack knowledge foundation, which provides recommended threat mitigation techniques, identification procedures, and different relevant technical data. Moreover, MITRE expands the Kill Chain to encompass a broad variety of techniques supported by specific methods. The organized security approach can help financial systems to pick and analyze security events methodically, and compare the threats to their defenses' capabilities to identify potential gaps.

Guide to MITRE ATT&CK for the Financial Institutions

### a. Analyzing Threat adversaries

MITRE provides an exhaustive knowledge of familiar threat adversary Tactics, Techniques and Procedures (TTPs), enabling security analysts to acquire broader knowledge of their tactics and motivations. Security professionals can meticulously study and analyze the information about threat adversaries, in order to structure invaluable threat data to leverage in proactive security measures.

MITRE ATT&CK framework classifies threat adversary behaviors into different techniques and tactics, enabling security teams to describe and communicate the threats using systemized language. The framework enables financial institutions to align their defenses with real-life security events.

### b. Developing Defense Strategies

Financial institutions seek to develop defensive plans against specific advanced persistent threat (APT) groups. Thus, leveraging insights acquired from MITRE ATT&CK framework enables them to create an exhaustive defense plan customized to the specific techniques and tactics used by the APT gang.

Additionally, the framework enables their security teams detect vulnerabilities and potentially lethal attack vectors that hackers may exploit. Equipped with this knowledge, security experts can design multi-layered defense strategy that encompass proactive threat identification, best-in-class network monitoring, and tailored security controls. This enables financial systems to align their defenses with APT gang's TTPs, in order to prioritize their security controls and install effective counter measures.

## Conclusion

MITRE ATT&CK has merged as an immensely useful framework in threat intelligence and defense planning fields. In the financial sector, the framework provides banks and financial institutions with an exhaustive understanding of technologies and tactics employed by threat adversaries, enabling them to put in place sturdy defense strategies. MITRE enables financial organizations to close the security gap between threat intelligence and practical defense strategies. The knowledge of specific techniques adopted by threat actors enables the implementation of proactive threat mitigation measures to thwart potential cyber-attacks.

Therefore, to continually adapt to the ever-changing and evolving cyber-threat landscape, financial institutions should embrace state-of-the-art security frameworks to empower their defenses to proactively safeguard their valuable data and monetary assets against sophisticated threats, bolster their security posture, and protect their overall organizational infrastructures.

## References

[1] Yuri Diogenes, Dr. Erdal Ozkaya , Cybersecurity – Attack and Defense Strategies Improve Your Security Posture to Mitigate Risks and Prevent Attackers from Infiltrating Your System., Packt Publishing., 2022.

[2] J. Mulder, Multi-Cloud Strategy for Cloud Architects: Learn how to Adopt and Manage Public Clouds by Leveraging BaseOps, FinOps, and DevSecOps, Packt Publishing, 2023.

[3] Rebecca Blair, Aligning Security Operations with the MITRE ATT&CK Framework: Level Up Your Security Operations Center for Better Security, Packt Publishing, 2023.