Assessing MITRE ATTCK Risk Using a Cyber-Security Culture Framework - Notes

Cameron Noakes

November 2021

1 Sentence Overview

The concentration of this research is cyber warfare simulations for training offence and defence from real world cyber scenarios related to the MITRE ATT&CK framework.

2 Abstract - Notes

This includes but is not limited to: knowledge, methodology, assumptions with all respect to cyber security. This is the reasoning behind choosing this article, to create a strong argument before relating the framework to a specific niche.

3 Introduction and Background - Notes

Presented research from the similarity between security culture and adversary tactics and threats was discussed. It has also exhibited how it can assess the implementation of MITRE ATTACK for Enterprises ad well as the difference of tactics for Attack for ICS framework. This section speaks highly of the history and past of the framework, allowing concise condensing of information for a historical introduction. Some key statement quotes can be seen below regarding the history.

The section managed to explain sub techniques, the child tactics within each parent sector that most papers seem to overlook, which is informational and outlines key areas of more in-depth knowledge when performing offensive attacks.

4 Proposed Solution

The proposed solution was a solution that mapped Mitre Attack Framework into an industry sector to create a cyber threat simulation for professional cyber security training of blue team defenders such as threat hunters and SOC analysts. This was discussed to provide real world training from a gathering of real world scenarios which overall could potentially provide better infrastructure security.

5 Evaluation

There was no discussion of the evaluation of the proposed solution of a cyber threat simulation. The conclusion and future work discussed the simulation but no analytics were given or any success metrics that should have been attempted to provide clarity that the simulation has value.

6 Research Gaps and Questions

Some limitations however, seem to arise with regards to the content of sub techniques, brief mention of them was adequate, however, no in-depth writing or research was conducted based on examples of such offensive sub techniques. There was acknowledgement and a brief initial overview, but failed to elaborate about specific examples within the Mitre Attack Framework.

Another constraint is that the writer deliberately focused on Penetration Testing and Red Teaming, this is accurate and did mention how other areas use it but did not elaborate or expand much beyond this. The writer could articulate more about other areas within cyber security that use the framework and give some industry examples and information on such sectors.

7 What problem does this solve?

The problem outlined is that adversarial attackers are compromising critical infrastructure systems and network environments, this can lead to huge lawsuits and violations of data protection acts, these attacks can also cause negative reputation and loss of clients due to a data breach or cyber attack.

8 How do they solve it?

The proposed solution is a simulation that uses the Mitre Attack Framework for cyber warfare training for cyber professionals to develop their knowledge further to be able to catch these targeted attacks in the future and also to help reduce the overall risk to the companies assets since it will clearly outline key fundamental security implementations to secure the network and assets further, stopping the attacks before they even are initiated.

9 How do they assess it?

There was no mention of used analytics and also no form of analytics or success metrics to be tested against the simulation to make sure it works correctly and is accurate. The conclusion summarised the work carried out but did not outline any success metrics to test against the simulation to see if it provides real world value and promotes cyber security change and develops the cyber professionals knowledge and makes them better at defense.

10 Conclusion and Future Work - Notes

Expansion behind the reasoning for needing more defenses to keep the digital world and peoples information safe and secure, reiterates with the Mitre Attack Framework is and its applications to the industry and which cyber professionals would use it the most.

The security culture tool assesses the application of Mitre Attack Framework inside the industry and how the given research in this paper fills the gaps given by other literature's in terms of mapping the Mitre framework matrix to a real world simulation for cyber professional training .