Cyber Threat Dictionary Using MITRE ATT&CK MATRIX and NIST Cybersecurity Framework Mapping

Cameron Noakes

January 2022

1 Sentence Overview

The researchers identify that there is a flaw in how cyber professionals respond to cyber attacks and can become a bit flustered. The researchers propose a tool that offers additional approaches to cyber threat solutions using mapping of the ATT&CK and NIST framework in order to add to attack and defense mapped frameworks.

The tool is titled the 'Cyber Threat Dictionary' and its aim is the above but also to allow cyber professionals to cope with responding to attacks better as they are executed and provide practical implementation solutions.

2 Introduction

The authors identified that IoT devices often have unattended security vulnerabilities, leaving them vulnerable to malicious adversarial attackers and open to cyber attacks, a report of how 1.2 million IoT devices were surveyed 57 percent of which were vulnerable to either medium or high severity attacks. This study concludes that most IoT devices are unsecured and open to attacker cyber attacks and cyber warfare.

Therefore it is said to be crucial to know how threats, vulnerabilities and attacker mindsets work in order to secure facilities, devices and online information systems. Facility related control systems (FRCS) are also said in this list to be crucial to secure.

Acknowledgement of how cyber mechanisms exist to help defend against attacks and improve defences but few provide defence tactics in response to specific attack tactics, allowing a cyber threat dictionary tool to be developed and created by the researchers to map systematic defensive mechanisms suitable for every step of an attack.

3 Background

The ATT&CK for ICS matrix was chosen for the research and tool development due to the criteria design similar to the cyber kill chain (CKC) as it addressed common contemporary global cyber threats. Since the research is focused on ICS and operational technology (OT), ATT&CK for ICS matrix is perfect usage for the researchers since it covers both ICS and OT.

A popular cybersecurity web application assessment tool known as facility cybersecurity framework (FCF) was provided within the literature and can be used for critical infrastructure and OT operations to discover the current cyber security posture but also to describe their target cybersecurity state. The authors then identified why a this tool or similar is required, for evaluating risk the cyber professional needs to conduct threat intelligence in order to evaluate the overall impact of a security breach event.

4 Methodology

ATT&CK for ICS catalogs 300 cyber attack tactics and 1200 strategies for detecting and remediating the listed vulnerabilities that are exploited in the attacks. Within the Methodology section of the literature, it accurately takes the methodology process and classifies the mitigation and detection categories into mapping them to the FCF controls.

Detection and mitigation mechanisms were first extracted from the ATTCK for ICS, the literature expands and the second step is to re-categorise all detection and mitigation mechanisms to grouping them based on similar attributes.

5 Conclusion

The literature recognised a gap in how cyber professionals often respond to cyber threats such as APTs and due to this enabled the researchers to proposed a solution for a tool that offers additional approaches to cyber threat solutions using mapping of the ATT&CK and NIST framework in order to add to attack and defense mapped frameworks.

Acknowledgement by the authors of how once a system is compromised it is difficult to then recover from, which provides more value to the developed tool since one of its purposes is to prevent and detect the attack early on.

6 What problem does this solve?

Due to the lack of attack and defense mapped frameworks, cyber professionals often do not know how to cope with cyber attacks when they get executed. There is a need to map one framework to another and to do this proposed solutions can be made by researchers in their literature to solve this problem.

7 How do they solve it?

the proposed solution in this literature is to present a tool the researchers developed called 'Cyber Threat Dictionary' to solve this problem. This proposed solution to the problem outlined is to offer approaches and practical implementable solutions to the cyber threats using the mapping of ATT&CK framework to the NIST framework.

8 How do they assess it?

The literature does not assess or evaluate the tool based on any metrics respectively, there was no acknowledgement of future work either but did express the applications the tool can be used for and all the features and functionality of the tooling developed.