Demonstration of the Cybersecurity Framework through Real-World Cyber Attack

Cameron Noakes

February 2022

1 Sentence Overview

A proposal is developed of Cybersecurity Framework (CSF) webtools which provide actionable functions that can be easily by adopted by a facility operator to enhance their overall critical infrastructure security. Including a set of “how-to” instructions for the facility operators to adopt, adapt, and apply to their critical infrastructure facilities. These functions provide a high-level, strategic overview of the lifecycle of an organization’s cybersecurity risk management which is extremely ideal for the security of specific or overall infrastructure.

The CSF webtools developed provide an ”easy to follow” set of cybersecurity best practices, policies, and procedures. The CSF webtools are also designed to facilitate communication of cybersecurity activities and outcomes across the organization from the executive (C-Level) to operations levels. The developed CSF webtools allow the assessment of the overall cybersecurity maturity and posture.

The outline goal was to demonstrate the capabilities of the CSF webtools through an illustrative cyber attack based on a real-world scenario.

The mapping for the webtools to the CSF framework for best practises is demonstrated through an illustrative use-case developed upon a real-world attack scenario.

2 Introduction

The researchers outlined how for cyber security integration, other researchers have been developing frameworks and methodologies built upon cybersecurity best practices. Specifically for a best practise known as the Cybersecurity Framework (CSF), which was designed by the National Institute of Standards and Technology (NIST), The CSF framework is a key part of the development of the proposed solution and research in this paper since the proposed model is CSF webtools.

The webtools contain a set of voluntary, risk-based standards and best practices intended to help critical infrastructure (IoT and alike) owners and operators better manage cybersecurity risks. The webtool was developed from the core functionalities of the NIST CSF framework and adapted to better target critical infrastructure facilities. The CSF webtools facilities focus on all types of buildings and critical infrastructures identified by the DHS.

The webtool helps to facilitate critical infrastructure (such as IoT and embedded devices) and to manage the cyber risk and understand their cybersecurity posture.

The researchers give reason to the rise of the conducted research and developed proposed solution by outlining securing IT/OT networks in a facility is a challenging dilemma as it requires balancing the implementation of security controls between networks that are often independently managed and largely unique.

Reference to Shodan, a popular website application to see all vulnerable IoT and computer devices was acknowledged, with the conclusion of how today many Industrial Control Systems (ICS) networks within facilities are exposed to the internet and could be exploited by attackers.

Additionally, not all facilities already incorporate NIST CSF in their current cybersecurity program, and through the development and research conducted within this literature, this should help to better protect IoT devices and critical infrastructure with the use of implementation of the CSF webtools.

The full list of functionality and what the CSF webtools can provide was referenced which can define their overall cybersecurity goals to identify their CCAs, protect their IT/OT networks from cyber threats, detect cyber events and anomalies, respond to malicious activities, and recover from critical cyber events. Such mapping to the CSF framework for the webtools will not only determine the vulnerabilities but also identify the relevant threats.

3 CSF Use Case

The researchers identify it being of use to demonstrate the efficiency of CSF by evaluating its use by a facility in response to a real-world cyber-attack. The attack propagation consists of a chronological sequence of steps.

Two cyber security assessments are performed:

- pre-assessment of the identified security controls that were potentially exploited in the real-world scenario.
- a post-mitigation assessment where the vulnerabilities are mitigated.

Another CSF assessment after the initial assessment is performed and a detailed comparative analysis of both assessments is performed to demonstrate that the facility could have been equipped to prevent the demonstrated attack if CSF was implemented in the first place.

The use of the ATT&CK framework matrix of TTPs was discussed in a given example within the literature in this section. Discussion of how the actions that were taken by the attackers in the provided example attack were identified and mapped to the ATT&CK attack vectors associated with the activities that occurred in an event. Based on the ATT&CK attack vectors mapped to the scenario timeline, the associated CSF security controls for each event are identified, each of the attack vectors has been evaluated in relation to CSF security controls and has been mapped to show the process by which the security controls should be fully implemented.

The researchers clearly outline the deliverable and the usage of their research in this section through the explanation of the contribution pertaining to the remainder of the paper and doing a cyberattack scenario-based mapping between the CSF security controls and the ATT&CK attack vectors.

This mapping exercise has identified the dependencies that need to be addressed in a sequential and subjectively logical fashion to reach a desired end state. The current state is defined as the implementation level of the security control that led to an event's success.

The attackers use an exploit on the system and gained unauthorized access to the server. In relation to the ATT&CK framework, this incident refers to the control maps, related security controls, and the paths for both incidents.

Various technical security control settings and applications are discussed within the research in this section and specific events like credential dumping and other attacker cyber attacks.

4 Conclusion

The CSF webtools offer facilities a set of voluntary, risk-based standards and best practices to help facility owners and operators better manage cybersecurity risks. The core assessment was used to determine desired maturity levels in five domains of security.

Using the proposed webtools can allow facilities to evaluate compliance with NIST CSF and keep a record of the security posture. The usage of this within this research was a fictitious facility uses CSF to defend against the real-world cyberattack scenario. ATT&CK techniques are then aligned with each of the identified events that represent the actual steps that the attackers took. CSF controls are then mapped to each of the identified ATT&CK technique.

5 What problem does this solve?

The outlined problem at hand that the literature addressed and created a solution for was for better protecting critical infrastructure and IoT devices from cyber attacks from threat actors by using NIST CSF implementations.

6 How do they solve it?

The researchers developed a CSF webtools to provide an ”easy to follow” set of cybersecurity best practices, policies, and procedures. The webtool helps to facilitate critical infrastructure (such as IoT and embedded devices) and to manage the cyber risk and understand their cybersecurity posture.

7 How do they assess it?

There is a comparative evaluation for the CSF. There is not much mention of any other evaluation approach.