USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

CTO PEER MENTORING PROGRAM

TOPIC 4

This publication was produced at the request of the the United States Agency for International Development. It was prepared independently by implementing partner, Catalisto LLC for the USAID Cybersecurity for Critical Infrastructure in Ukraine Activity. The authors' views expressed in this publication do not necessarily reflect the views of the United States Agency for International Development or the United States government.

DEVELOPMENT OF A DEFENSIVE CYBERSECURITY PROGRAM FOR PROACTIVE DEFENSES THROUGH STRUCTURED CYBERSECURITY FRAMEWORKS

In Topic 3 we discussed "Offensive Cybersecurity" Practices. The point of that concept is to "think like an attacker" to assess your environment while finding ways to best defend it.

In this topic, Topic 4, we are visiting one of the most fundamental concepts of Cybersecurity – Defense.

Defense as a Framework?

- We all rely on defensive frameworks to guide us in what to secure/how to secure it.
  - Specifically, for this topic, the Centre for Internet Security (CIS) Critical Control Framework
- Other frameworks:
  - NIST Cybersecurity Framework
  - ISO 27000
  - MITRE D3FEND (More aimed at Network Defense)
  - …Amongst Others

WHY CIS CRITICAL CONTROLS?

Why would we use CIS Critical Controls?

Has anyone ever used them? (Please put your “Zoom” hand up!)

Critical Controls allow us to:

1. Quickly measure your own security maturity without requiring an in-depth understanding of cybersecurity
2. Utilize a well-researched, experience and real-life scenario-based cybersecurity defense model
3. Choose which controls are most relevant, and most critical for yourself
4. Break down implementation from “Mountains” to “Bite-Sized Chunks & Quick-Wins”
5. Participate in a community of experts and reciprocally receive expert-level advice
6. It is budget friendly & mostly open sourced!

WHY DEFENSE AS A TOPIC?

Why not!

Offense is the best defense. But you need a good defense to withstand an adversary's offense!

For example:

- In the controls, penetration testing is only listed at control 18!
- There are several steps to perform to secure yourself, before you begin thinking offensive tactics to test your own security.
- Why do a penetration test, if you don't have an asset inventory or structured account management? You know you will fail on those controls, if you don't have them in place, so why test them before implementing them!

CIS CRITICAL CONTROLS DEFINITION

The CIS Critical Security Controls® (CIS Controls®) started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience.

The original goals were modest—to help people and enterprises focus their attention and get started on the most important steps to defend themselves from the attacks that really mattered.

https://www.cisecurity.org

HOW ARE THE CRITICAL CONTROLS CONSTRUCTED?
CIS COMMUNITY DEFENSE MODEL!

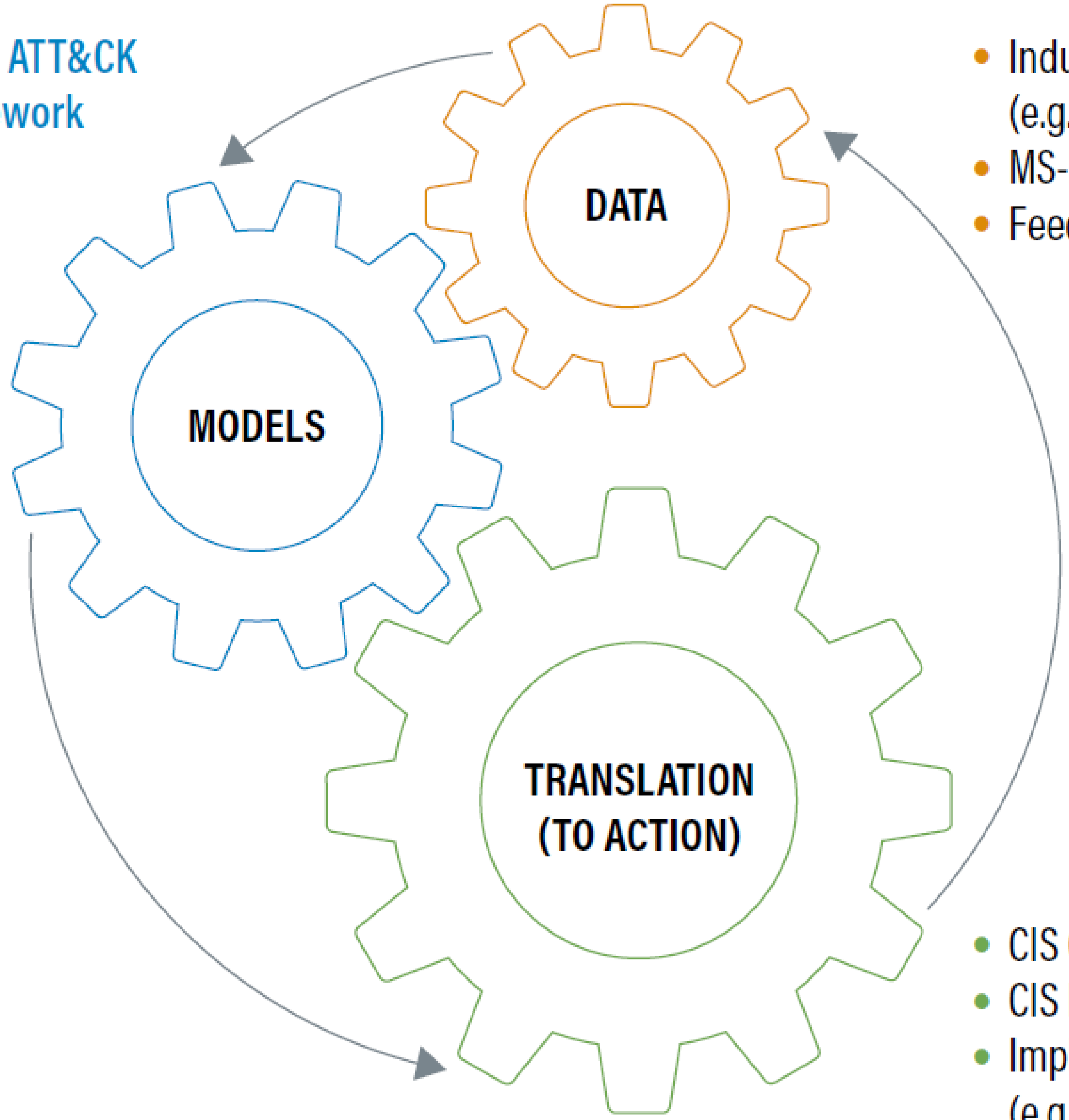
The CIS Community Defense Model's (CDM) goal is to bring another level of rigor and detail to support the development and prioritization of the CIS Controls.

The CDM process takes data sources (such as the Verizon Data Breach Investigations Report (DBIR)), drives them into models (such as the MITRE ATT&CK framework), and then translates them into action—creating our best practices (e.g., CIS Controls and CIS Benchmarks).

The CDM is continuous, with each cycle starting the process again.

https://www.cisecurity.org

MITRE ATT&CK Framework



DATA

MODELS

TRANSLATION (TO ACTION)

- Industry Attack Summaries (e.g., Verizon DBIR)
- MS-ISAC Operations
- Feedback from User Implementation

- CIS Controls
- CIS Benchmarks
- Implementation Groups (e.g., IG1 “Essential Cyber Hygiene”)

BUT HOW DO YOU PRIORITIZE RISK?!
CIS RISK ASSESSMENT MODEL (RAM)

CIS RAM uses the Duty of Care Risk Analysis Standard8 (DoCRA) as its foundation.

DoCRA presents risk evaluation methods that are familiar to legal authorities, regulators, and information security professionals to create a "universal translator" for these disciplines.

The standard includes three principles and 10 practices that guide risk assessors in developing this universal translator for their enterprise. The three principles state the characteristics of risk assessments that align to regulatory and legal expectations.

The 10 practices describe features of risk assessments that make the three principles achievable.

https://www.cisecurity.org

THAT’S GREAT!
BUT WHERE DO I BEGIN ON THIS JOURNEY…?

- Understand the CIS Community Defense Model (read through it and get to know it!)
- Understand the CIS Risk Assessment Model (RAM can be used to prioritize your risks!)
- Understand and use the CIS Critical Control Framework:
  - Use it to classify the size of your organization (Implementation Groups)
  - Use the Implementation Groups to understand how to prioritize the controls that you require!
  - Plan the implementation of tasks and ask your Mentors & Colleagues questions!

https://www.cisecurity.org

DEMO …

- CIS CDM
- CIS RAM
- CIS Controls
- CSAT

https://www.cisecurity.org

RESOURCES

- CIS: https://www.cisecurity.org
  - CIS CDM
  - CIS RAM
  - CIS Controls:
    - https://cisecurity.wistia.com/medias/9qnuy1s5vb
    - https://cisecurity.wistia.com/medias/tcelnntxig
- CSAT: https://csat.cisecurity.org/

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

THANK YOU