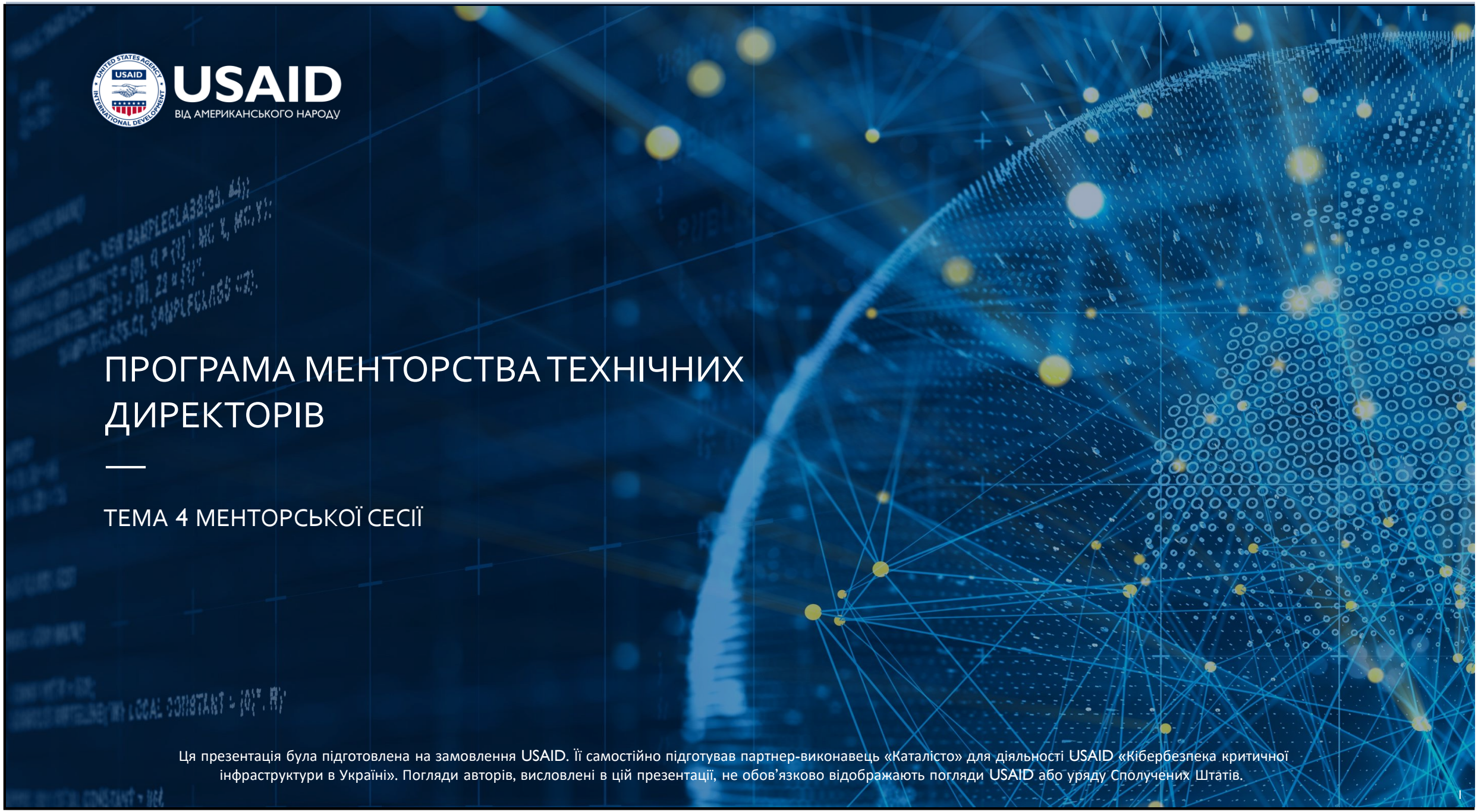


USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПРОГРАМА МЕНТОРСТВА ТЕХНІЧНИХ ДИРЕКТОРІВ

ТЕМА 4 МЕНТОРСЬКОЇ СЕСІЇ

Ця презентація була підготовлена на замовлення USAID. Її самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цій презентації, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

РОЗРОБКА ОБОРОННОЇ ПРОГРАМИ З КІБЕРБЕЗПЕКИ ДЛЯ ПРОАКТИВНОГО ЗАХИСТУ З ДОПОМОГОЮ СТРУКТУРОВАНИХ ФРЕЙМВОРКІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

РОЗРОБКА ОБОРОННОЇ ПРОГРАМИ З КІБЕРБЕЗПЕКИ ДЛЯ ПРОАКТИВНОГО ЗАХИСТУ З ДОПОМОГОЮ СТРУКТУРОВАНИХ ФРЕЙМВОРКІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

У темі 3 ми обговорювали «наступальну кібербезпеку». Суть цієї концепції полягає в тому, щоб «думати як зловмисник», для того щоб оцінити своє оточення і знайти найкращі способи для його захисту.

У сьогоднішній темі, темі 4, ми розглянемо одну з найбільш фундаментальних концепцій кібербезпеки – оборону.

Захист як основа?

Ми всі покладаємось на фреймворки для захисту, які допомагають нам у тому, що і як захистити.

- Зокрема, Центр інтернет-безпеки (CIS) Фреймворк з критичного контролю

Інші фреймворки:

- фреймворк з кібербезпеки, розроблений американським інститутом стандартів (NIST Cybersecurity Framework)
- ISO 27000
- MITRE D3FEND (Більше націлене на захист мереж)
- …Серед інших

ЧОМУ КРИТИЧНІ ЕЛЕМЕНТИ УПРАВЛІННЯ БЕЗПЕКОЮ ЦЕНТРУ ІНТЕРНЕТ-БЕЗПЕКИ (CIS CRITICAL CONTROLS)?

Чому ми повинні використовувати Критичні елементи управління безпекою Центру інтернет-безпеки?

Хтось коли-небудь користувався ним? (Будь ласка, підніміть руку вгору у Зумі!)

Критичні елементи управління безпекою дозволяють нам:

1. Швидко оцінювати свою зрілість у сфері безпеки, не вимагаючи глибокого розуміння кібербезпеки
2. Використовувати добре досліджену, перевірену на основі досвіду та реальних ситуаціях модель захисту кібербезпеки
3. Обрати, які елементи контролю є найбільш релевантними та найважливішими для вас
4. Розбити реалізацію від «Гір» до «Маленьких часток і швидко досяжних результатів»
5. Брати участь у спільноті експертів і отримувати експертні поради
6. Це бюджетно та переважно з відкритим кодом!

ЧОМУ ЗАХИСТ Є ОДНІЄЮ З ТЕМ?

Чому ні?

Напад - найкращий захист. Але вам потрібен хороший захист, щоб протистояти нападу супротивника!

Наприклад:

- У фреймворку Критичні елементи управління безпекою пентест вказаний лише на 18-му етапі!
- Щоб захистити себе, потрібно виконати кілька кроків, перш ніж почати думати про наступальну тактику для перевірки власної безпеки.
- Навіщо проводити пентест, якщо у вас немає інвентаризації активів або структурованого керування обліковим записом? Ви знаєте, що ви потерпите невдачу в керуванні цими елементами, якщо у вас їх немає, тож навіщо їх тестувати до їхньої імплементації!

ВИЗНАЧЕННЯ КРИТИЧНИХ ЕЛЕМЕНТІВ УПРАВЛІННЯ БЕЗПЕКОЮ ЦЕНТРУ ІНТЕРНЕТ-БЕЗПЕКИ

Критичні елементи управління безпекою Центру інтернет-безпеки (CIS Controls®) розпочався як простий захід для виявлення найбільш поширених і важливих кібератак у реальному світі, які щодня впливають на підприємства, перетворення цих знань і досвіду в позитивні, конструктивні дії для захисту і потім для поширення цієї інформації.

Початкові цілі були скромними — допомогти людям і підприємствам зосередити свою увагу та розпочати найважливіші кроки для захисту від атак, які дійсно мали значення.

https://www.cisecurity.org

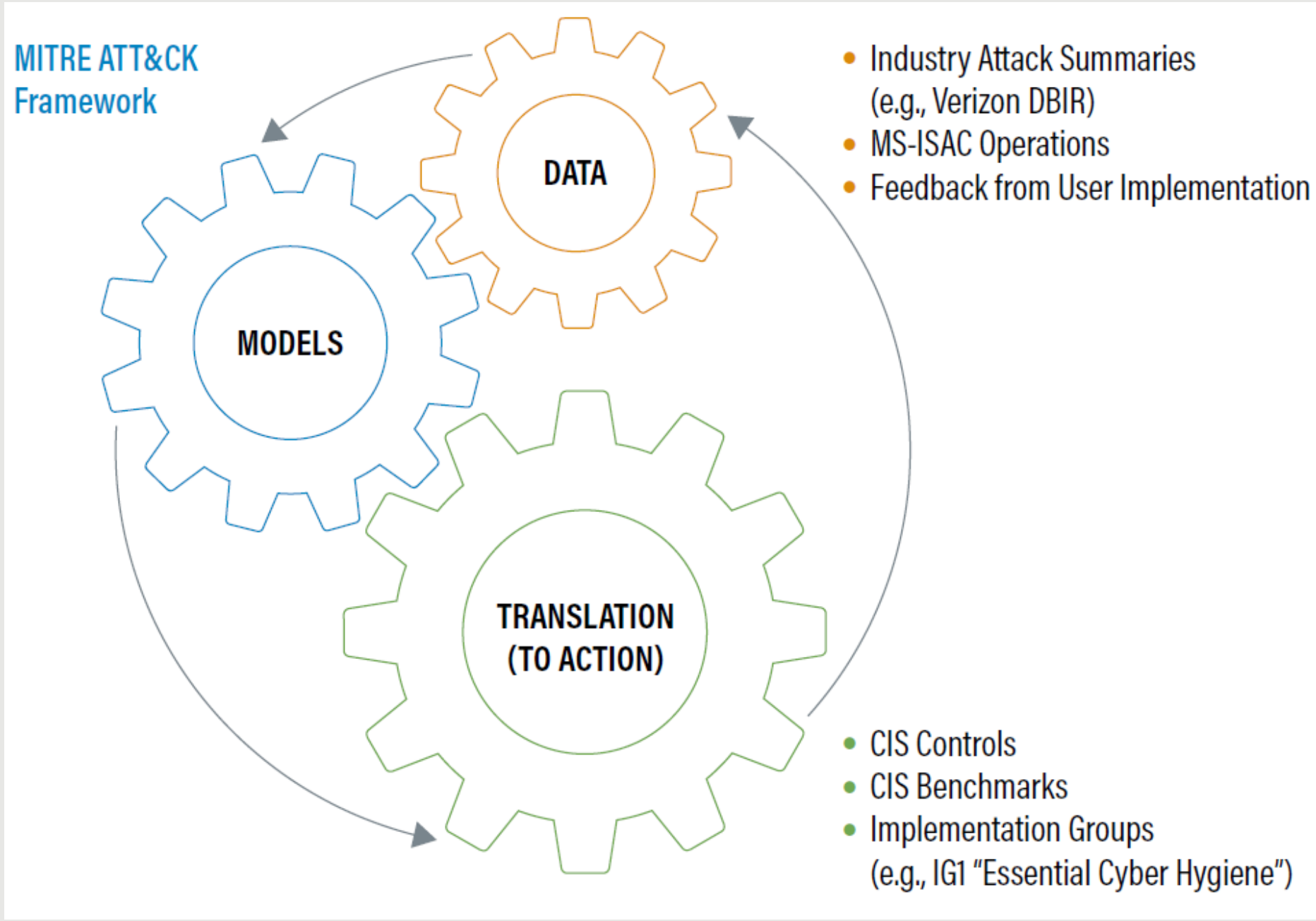
ЯК ПОБУДОВАНІ КРИТИЧНІ ЗАСОБИ КОНТРОЛЮ? МОДЕЛЬ ЗАХИСТУ СПІЛЬНОТИ ЦЕНТРУ ІНТЕРНЕТ-БЕЗПЕКИ!

Мета моделі захисту спільноти центру інтернет-безпеки (CDM CIS) полягає в тому, щоб додати ще один рівень точності та деталізації для підтримки розробки та визначення пріоритетів засобів контролю CIS.

Процес CDM джерела даних (наприклад, звіт Verizon Data Breach Investigations Report (DBIR)), перетворює у моделі (наприклад, фреймворк MITER ATT&CK), а потім перетворює їх у дію, створюючи наші найкращі практики (наприклад, CIS Controls та CIS Benchmarks).

CDM є безперервним, і кожен цикл запускає процес знову.

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")

АЛЕ ЯК РОЗСТАВИТИ ПРІОРІТЕТИ РИЗИКІВ?!
МОДЕЛЬ ОЦІНКИ РИЗИКІВ ЦЕНТРУ ІНТЕРНЕТ-БЕЗПЕКИ (CIS RAM)

Модель оцінки ризиків Центру інтернет-безпеки (CIS RAM) використовує стандарт аналізу ризиків (Duty of Care Risk Analysis Standard (DoCRA)) як свою основу.

DoCRA представляє методи оцінки ризиків, знайомі юридичним органам, регуляторам та фахівцям із інформаційної безпеки, щоб створити «універсальний перекладач» для цих дисциплін.

Стандарт включає три принципи та 10 практик, якими керуються оцінювачі ризиків при розробці цього універсального перекладача для свого підприємства. Ці три принципи визначають характеристики оцінки ризику, які відповідають нормативним та правовим очікуванням.

10 практик описують особливості оцінки ризиків, які роблять три принципи досяжними

https://www.cisecurity.org

ЧУДОВО!
АЛЕ З ЧОГО ПОЧАТИ…?

- Зрозумійте модель захисту спільноти CIS (прочитайте її та дізнайтеся!)
- Зрозумійте модель оцінки ризиків CIS (RAM можна використовувати для визначення пріоритетів ваших ризиків!)
- Зрозумійте та використовуйте фреймворки з критичних систем CIS:
  - Використовуйте його, щоб класифікувати розмір вашої організації (групи впровадження)
  - Використовуйте групи впровадження, щоб зрозуміти, як визначити пріоритети елементів контролю, які вам потрібні!
  - Плануйте виконання завдань та задавайте запитання своїм наставникам та колегам!

https://www.cisecurity.org

ДЕМО …

- CIS CDM (Модель захисту спільноти Центру інтернет-безпеки)
- CIS RAM (Модель оцінки ризиків Центру інтернет-безпеки)
- CIS Controls (Критичних елементів управління безпекою Центру інтернет-безпеки)
- CSAT (Інструмент контролю оцінювання)

https://www.cisecurity.org

РЕСУРСИ

- 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

Дякуємо!