USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПРОГРАМА НАСТАВНИЦТВА З КІБЕРБЕЗПЕКИ ДЛЯ IT-ДИРЕКТОРІВ

ТЕМА І: МЕНТОРСЬКА СЕСІЯ

ВСТУП ДО ПРОГРАМИ

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.

РОЗРОБКА ОРГАНІЗАЦІЙНОГО ПЛАНУ РЕАГУВАННЯ НА ІНЦИДЕНТ ДЛЯ РЕАГУВАННЯ НА ЗАГРОЗИ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Дисклеймер щодо презентації

ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ

ЧИ Є РЕАГУВАННЯ НА ІНЦИДЕНТ НЕЗМІННИМ АБО Ж ОДНОРАЗОВИМ?

Тема I

ПРИКЛАДИ КОМПРОМІСІВ, ЩО ПРИЗВОДЯТЬ ДО НЕВДАЧ ПІД ЧАС РЕАГУВАННЯ НА ІНЦИДЕНТИ

Вірус NotPetya – 2017

Глобальна інженерія та промислове виробництво

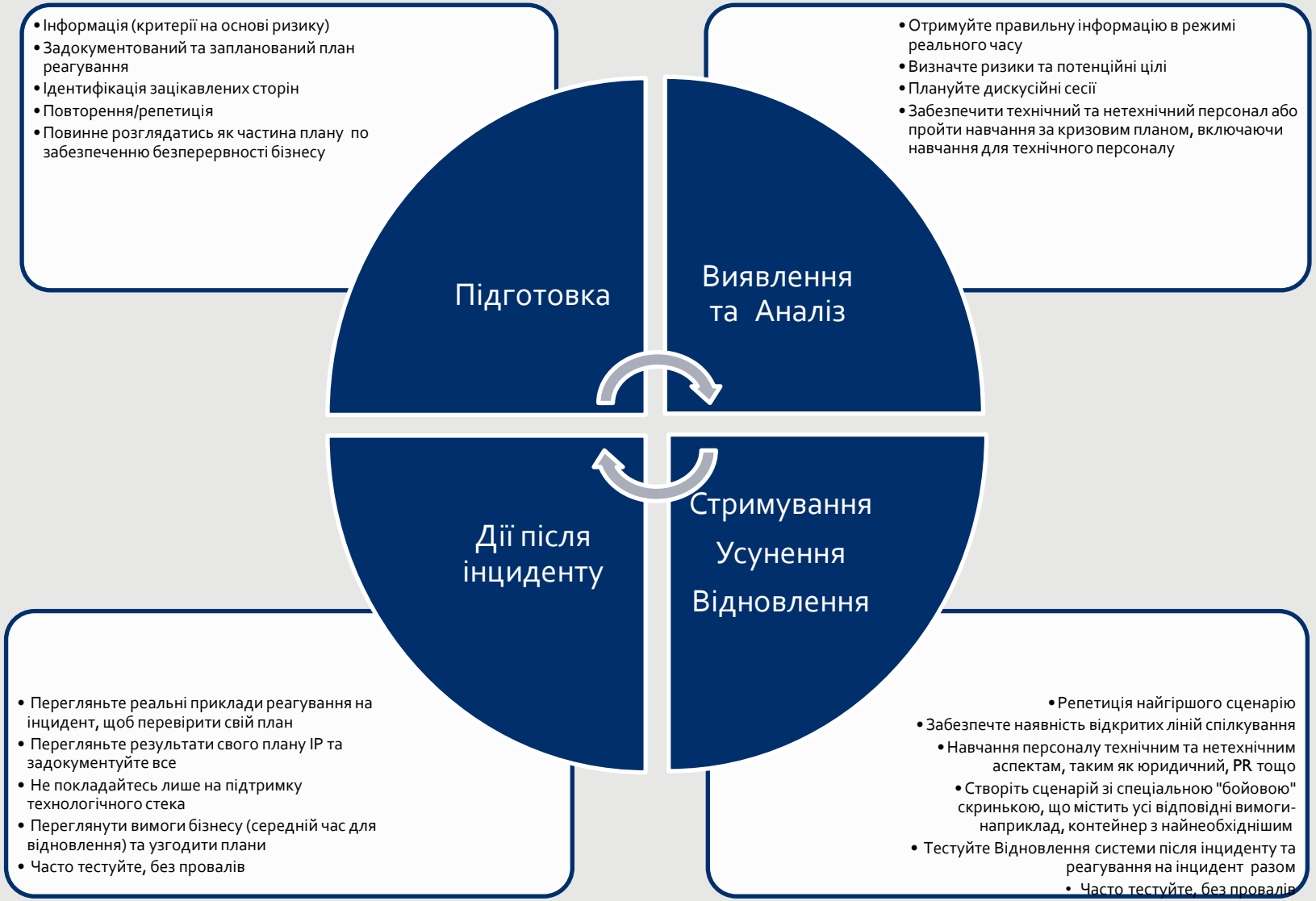
- $30.0+ мільйонний бізнес на 6 континентах
- Відсутність плану реагування на інцидент та спроможності запобігання атаці
- Глобально зупинилось на 1,5 місяця (MTTR - середній час до відновлення роботоздатності)
- Поточні збитки в розмірі 1 000 000,00 доларів США на континент (продуктивність та робочі години)

Цільові Атаки – 2018 to 2019

Африканська крупна компанія з будівництва та виробництва

- $665.0+ мільйонний бізнес, що охоплює 10+ країн
- Цільова атака,
  яка підкреслює невдачі під час Виявлення та Аналізу,
  триває більше 2 років
- Задокументований план реагування на інциденти та план забезпечення безперервності бізнесу без практичного застосування та тестування
- Орієнтовний збиток у розмірі 22 500 000,00 доларів США через викуп, крадіжку інтелектуальної власності
  інші витоки даних,
  шкоду репутації, професійну відповідальність, особисту відповідальність працівників

Досвід змусив нас повірити…



USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПИТАННЯ ТА ВІДПОВІДІ

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Сценарій 1:
Як би ви здійснювали реагування на інциденти для організації, яка щойно виявила, що вона скомпрометована? Які ключові питання ви б вирішили та визначили пріоритетними?

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

Сценарій 2:
З чого ви б почали розробляти план реагування на інциденти для організації, у якої такого плану немає? Які першочергові завдання ви б вирішили і яку методологію використали б?

USAID
ВІД АМЕРИКАНСЬКОГО НАРОДУ

ПИТАННЯ ТА ВІДПОВІДІ