1. Q: Детально дослідивши документацію Запиту на закупівлю та доставку обладнання, підписок та ліцензій, тренінгів для Державної митної служби України (Модернізація Єдиної автоматизованої інформаційної системи Державної митної служби України) в рамках Проєкту USAID/ Кібербезпека (REQ-KYI-24-0132), наші експерти зіштовхнулися з одним пунктом, щодо якого відсутні технічні вимоги, або детальний опис позиції, а саме:

ICS2			
ICS2	Розробка концептуальної моделі Системи управління імпортом (ICS2), Додаток ICS2	1	---

Просимо вас або надати детальне технічне завдання, або надати контакти організації, яка може надати таку послугу, задля отримання пропозиції від цього виконавця.

A: У даному проєкті розглядається виконання саме першого етапу. Документальним результатом першого етапу має стати документ “Концептуальна модель Системи управління імпортом”, який повинен містити наступні розділи (загальний обсяг до 50-60 стор.):

1. ЗАГАЛЬНІ ВІДОМОСТІ
1.1 Призначення документа
1.2 Джерело та порядок фінансування
1.3 Найменування сторін
1.4 Перелік нормативно-правових актів та стандартів, які мають враховуватися при розробці

2. РЕЗЮМЕ ПРОЄКТУ
2.1 Передумови
2.2 Призначення та мета
2.3 Рушійні фактори

3 ОГЛЯД БІЗНЕС-ПРОЦЕСІВ
3.1 Бізнес-процес взаємодії
3.2 Рольова модель Електронної системи
3.2.1 Ролі та права доступу
3.2.2 Електронний кабінет користувача
3.2.3 Реєстрація користувачів та їхніх уповноважених представників
3.2.4 Призупинення, відновлення та анулювання доступу користувачів та їхніх уповноважених представників
3.3 Адміністрування Електронної системи
3.4 Компоненти Електронної системи
3.5 Електронні документи

4. ФУНКЦІОНАЛЬНІ ВИМОГИ ДО ЕЛЕКТРОННОЇ СИСТЕМИ

2. Q: Документи, довідки, підтвердження можна подавати українською мовою? Англійською мовою бажано подавати тільки цінову пропозицію, Додаток В?

A: Будь ласка, зверніться до розділу #11 “Загальні інструкції” Запиту на надання пропозиції: Учасники тендеру, які бажають відповісти на цей Запит на надання пропозицій, повинні подавати пропозиції англійською або українською мовою (бажано англійською) відповідно до інструкцій, вказаних у цьому документі

3. Q: Просимо надати основні умови Договору, в тому числі умови та терміни оплат.

A: Загальні умови контракти будуть надані обраному переможцеві. Умови оплати наступні: оплата після надання послуг/доставки товарів впродовж 20 днів після отримання DAI повного та правильного рахунку-фактури.

4. Q: Просимо надати максимально розширений перелік робіт та надання послуг цього проекту стосовно інсталяції/імплементації по вендорам Cisco, Palo Alto, Oracle, ICS2. Щоб кожен учасник мав змогу прорахувати об’єми.

A: Перелік робіт, які повинні бути виконані в рамках поставки рішення.
[Oracle]:
· Активація ліцензій та технічної підтримки
[PAN]:
· розробка відмовостійкого архітектурного рішення по впровадженню рішення в мережевій архітектурі реципієнта
· впровадження та налаштування PAN Broker VM в серверній інфраструктурі реципієнта
· впровадження та налаштування центральної хмарної частини рішення (включаючи налаштування відповідних політик безпеки)
· розробка інструкції з адміністрування рішення
· розробка інструкції користувача рішення
[Cisco]:
· розробка відмовостійкого архітектурного рішення по впровадженню обладнання в мережевій архітектурі реципієнта (на 3-х ЦОД-ах)
· оновлення ОС/ПЗ та базова конфігурація обладнання (VPN концентраторів)
· впровадження та налаштування VPN концентраторів (оновлення ОС/ПЗ, базова конфігурація, VPN)
· розробка та налаштування правил, політик та сервісів безпеки VPN концентраторів (як NGFW)
· інтеграція з LDAP реципієнта
· інтеграція VPN концентраторів з існуючими у реципієнта центром управління NGFW (Firepower Management Center)
· впровадження та налаштування центральної частини MFA-сервісу
· розробка інструкції з адміністрування рішення
· розробка інструкції користувача рішення

Перелік уточнюючих запитань по частині ICS2:

5. Q: Просимо надати детальну інформацію стосовно ICS2, перелік вимог, можливо якісь опис, шаблон чи опитувальник. З документації не зрозуміло що входить до «Розробка концептуальної моделі Системи управління імпортом (ICS2), Додаток ICS2» і де саме цей Додаток ICS2 можна подивитися. Просимо надіслати ТЗ стосовно ICS2.

A: У даному проєкті розглядається виконання саме першого етапу. Документальним результатом першого етапу має стати документ “Концептуальна модель Системи управління імпортом”, який повинен містити наступні розділи (загальний обсяг до 50-60 стор.):

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Призначення документа
1.2 Джерело та порядок фінансування
1.3 Найменування сторін
1.4 Перелік нормативно-правових актів та стандартів, які мають враховуватися при розробці

2. РЕЗЮМЕ ПРОЄКТУ
2.1 Передумови
2.2 Призначення та мета
2.3 Рушійні фактори

3 ОГЛЯД БІЗНЕС-ПРОЦЕСІВ
3.1 Бізнес-процес взаємодії
3.2 Рольова модель Електронної системи
3.2.1 Ролі та права доступу
3.2.2 Електронний кабінет користувача
3.2.3 Реєстрація користувачів та їхніх уповноважених представників
3.2.4 Призупинення, відновлення та анулювання доступу користувачів та їхніх уповноважених представників
3.3 Адміністрування Електронної системи
3.4 Компоненти Електронної системи
3.5 Електронні документи

4. ФУНКЦІОНАЛЬНІ ВИМОГИ ДО ЕЛЕКТРОННОЇ СИСТЕМИ

Перелік уточнюючих запитань по частині Palo Alto:

6. Q: На які операційні системи планується встановити агенти Cortex XDR?
   A: Windows 7-11, Windows Server 2019, 2019, 2022, AIX7

7. Q: З якими системами планується інтеграція Cortex XDR?
   A: Інтеграція не передбачається

8. Q: Скільки правил та які типи правил планується налаштувати на Cortex XDR?

A: Типи правил

a) Детекційні правила (Detection Rules)
Ці правила використовуються для виявлення підозрілої активності або загроз на основі заздалегідь визначених умов. Вони можуть включати сигнатури, поведінкові патерни, аномалії та інші індикатори загроз.
2. Кореляційні правила (Correlation Rules)
Кореляційні правила поєднують кілька окремих подій для виявлення складних загроз, які можуть не бути помітними на основі однієї події. Вони допомагають виявити загрози, що проявляються через різні етапи атаки.

b) Аналітичні правила (Analytics Rules)
Ці правила використовують машинне навчання та інші аналітичні методи для виявлення аномальної поведінки, яка може свідчити про загрозу. Вони можуть виявити нові та невідомі загрози.

c) Автоматизаційні правила (Automation Rules)
Автоматизаційні правила використовуються для автоматизації відповідей на загрози. Вони можуть виконувати різні дії, такі як ізоляція пристроїв, блокування IP-адрес або запуск скриптів для зменшення впливу загрози.

d) Мережеві правила (Network Rules)
Ці правила контролюють мережевий трафік і можуть включати блокування або дозволи для певних типів трафіку на основі політик безпеки.

e) Індикатори компрометації (Indicators of Compromise, IoC)
Ці правила використовуються для виявлення специфічних індикаторів компрометації, таких як шкідливі файли, URL-адреси, IP-адреси тощо.

f) Правила реагування на інциденти (Incident Response Rules)
Ці правила визначають дії, які повинні бути виконані в разі виявлення інциденту безпеки, включаючи створення алертів, сповіщення відповідальних осіб та інші заходи реагування

Перелік уточнюючих запитань по частині Cisco:

9. Q: Налаштування Cisco Firepower із відповідними зонами, правилами також буде покладено на нашу компанію? Чи реципієнт самостійно підключає/налаштовує Cisco Firepower, в ми лише допомагаємо з налаштуванням Cisco Anyconnect?

A: На Виконавця буде покладено:

- розробка відмовостійкого архітектурного рішення по впровадженню обладнання в мережевій архітектурі реципієнта (на 3-х ЦОД-ах)

- оновлення ОС/ПЗ та базова конфігурація обладнання (VPN концентраторів)
- впровадження та налаштування VPN концентраторів (оновлення ОС/ПЗ, базова конфігурація, VPN)
- розробка та налаштування правил, політик та сервісів безпеки VPN концентраторів (як NGFW)
- інтеграція з LDAP реципієнта (HLC Notes)
- інтеграція VPN концентраторів з існуючими у реципієнта центром управління NGFW (Firepower Management Center)
- впровадження та налаштування центральної частини MFA-сервісух

10. Q: Чи відомо який тип авторизації планує використовувати реципієнт для Cisco Anyconnect (basic login & password, certificate authorisation чи login&password + MFA)?
    A: login&password + MFA

11. Q: В рамках даного проекту - це буде заміна поточного застарілого обладнання чи впровадження нового обладнання в поточну інфраструктуру реципієнта?
    A: впровадження нового обладнання в поточну інфраструктуру реципієнта

12. Q: Чи потрібно буде бути офлайн присутнім під час монтування CISO Firepower в стійки замовника?
    A: Ні

13. Q: Налашутання Cisco Duo буде відбуватися на робочих станціях співробітників , як другий фактор входу?
    A: Так

14. Q: Доступ до приватної мережі реципієнта з віддалених робочих станцій планується налаштувати із використанням VPN тунелю чи через портал Cisco DUO (https, rdp, ssh тощо)?
    A: із використанням VPN тунелю

15. Q: З якими додатками замовника планується інтеграція Cisco DUO та налаштування MFA?
    A: інтеграція з LDAP реципієнта (HLC Notes)

16. Q: Чи є у реципієнта вимоги до документації чи її оформлення?
    A: Виконавець повинен розробити та надати: Інструкцію з адміністрування рішення, інструкцію користувача рішення. Документи повинні бути українською мовою

17. Q: Скільки часу буде виділено зі сторони реципієнта для проведення впровадження?
    A: Поставку та впровадження ми очікуємо протягом 60 днів з моменту підписання контракту. Бажано все зробити до 31 жовтня 2024 року