Додаток 1

ОБҐРУНТУВАННЯ
технічних та якісних характеристик, очікуваної вартості предмету закупівлі

Найменування замовника: Український центр з фізичної культури і спорту осіб з інвалідністю "Інваспорт";

Місцезнаходження замовника: 01601, Україна , Київська обл., м. Київ, вул. Еспланадна, буд. 42;

Ідентифікаційний код замовника: 21453585;

Категорія замовника: Юридична особа, яка забезпечує потреби держави або територіальної громади;

Предмет закупівлі: **«Програмна продукція з правом користування строком на 1 рік Cisco FPR1140 Threat Defense Threat, Malware and URL з розширеним захистом за допомогою Cisco Advanced Malware Protection (AMP) включаючи AMP for Networks та AMP Threat Grid (L-AC-PLS-1Y-S1 – 25шт)»;**

Ідентифікатор закупівлі: **UA-2025-10-24-013047-a.**

Технічні та якісні характеристики предмета закупівлі.

Ліцензія Cisco та підписка на використання функціоналу контролю додатків та NGIPS у режимі NGFW – строком на 1 рік.

Захист від мережевих атак з наступним функціоналом:

- IPS;
- statefull DPI на рівнях 3–7 моделі OSI;
- виявлення спроб НСД в режимі реального часу;
- попередження спроб НСД в режимі реального часу шляхом блокування або завершення небажаних мережевих сесій;
- вбудовані сигнатури IPS довічної дії;
- протидія технікам обходу захисту;
- підписка на оновлення сигнатур (IPS) та отримання динамічного автоматичного сповіщення про джерела глобальних атак (SIO).
- Забезпечення URL-фільтрації:
- не менш ніж 80 категорій;
- можливість перенаправити http(s) трафік до зовнішнього сервісу багаторівневої фільтрації з автоматичним балансуванням навантаження;
- Забезпечення захисту від злоякісного ПЗ:
- з можливістю ретроспективного аналізу, пошуку та відображення шляхів розповсюдження.

Технічні вимоги до Програмної продукції для існуючих пристроїв мережевої безпеки Cisco Firepower 1140 (L-AC-PLS-1Y-S1 – 25)

Програмна продукція на сервіси для існуючого у замовника пристрою Firepower серії 1140 на 12 місяців та включає в себе застосування на обладнанні наступних функцій:

•Виявлення та запобігання вторгненням, що дозволяє аналізувати мережевий трафік на предмет здійснення несанкціонованого доступу (вторгнення), використання вразливостей (експлойтів) та, за необхідністю, видалення кінцевих пакетів.

•Керування файлами, що дозволяє виявляти та, за бажанням, блокувати користувачів від надсилання або отримання файлів конкретних типів за конкретними протоколами додатків.

•Розширення можливостей захисту за допомогою Cisco Advanced Malware Protection (AMP) включаючи AMP for Networks та AMP Threat Grid. За допомогою цієї функції пристрої Firepower використовують Threat Defense для виявлення та блокування шкідливих програм у файлах, що передаються через мережу.

•Обміну індикаторами компрометації, а саме здійснення періодичного підключення до хмари AMP з метою актуалізації наявних даних.

•Ліцензування VPN з'єднання для 25 користувачів з підтримкою функціоналу базових VPN-сервісів, таких як VPN для пристрою та для окремих додатків (включаючи підтримку стороннього підключення до віддаленого доступу VPN через IKEv2), виявлення довірених мереж, базовий збір контексту пристроїв.

•Виявлення користувачів, які здійснюють надсилання/отримання файлів конкретних типів за конкретними протоколами додатків.

•Здійснення локального аналізу шкідливих програм для попередньої класифікації проаналізованих файлів з метою перевірки обмеженого набору цих типів файлів на наявність шкідливого програмного забезпечення.

•Автоматичного блокування або розблокування виявлених файлів, на основі списків дозволених/заборонених файлів. Можливість включення файлу до списку наявна в політиці файлу.

•Застосування можливості писати правила контролю доступу, які визначають трафік, що може перетинати мережу на основі URL-адрес, запитуваних відстежуваними хостами, з кореляцією інформації про такі URL-адреси з метою отримання детального контролю над веб-трафіком.

•Фільтрування Security Intelligence дозволяє заносити в чорний список/забороняти вхідний та вихідний трафік для певних IP-адрес, URL-адрес та доменних імен DNS, перш ніж трафік буде піддано аналізу за допомогою правил контролю доступу. Динамічні канали дозволяють відразу ж заносити з'єднання до чорного списку на основі останніх даних.

Очікувана вартість предмета закупівлі.

Найменування	Одиниця виміру	Кількість	Ціна за одиницю, грн. без ПДВ	Ціна за одиницю, грн. з ПДВ	Загальна вартість, грн. без ПДВ	Загальна вартість, грн. з ПДВ
Програмна продукція з правом користування строком на 1 рік Cisco FPR1140 Threat Defense Threat, Malware and URL з розширеним захистом за допомогою Cisco Advanced Malware Protection (AMP) включаючи AMP for Networks та AMP Threat Grid (L-AC-PLS-1Y-S1 – 25шт)	комплект	1	226 666,67	272000	226 666,67	272000
Очікувана вартість закупівлі						272000

Очікувана вартість одиниці товару, кількість та очікувана вартість закупівлі були визначені відповідно до службової записки Бєляєва О.О. від 22.10.25 б/н, а також даних відкритих джерел, комерційних пропозицій тощо.