**ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ**

(відповідно до пункту 41 постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

**1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, його категорія:** ДЕРЖАВНА УСТАНОВА "ЦЕНТР ІНФРАСТРУКТУРИ ТА ТЕХНОЛОГІЙ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ"; 03151, Україна, м. Київ, вул. Володимира Сікевича, 28; категорія замовника – бюджетна неприбуткова установа.

## 2. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності): Закупівля програмного забезпечення для захисту шкідливого програмного забезпечення за кодом CPV за ЄЗС ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів

**3. Ідентифікатор закупівлі: —** UA-2024-11-28-015334-а

**4. Обґрунтування технічних та якісних характеристик предмета закупівлі**: Закупівля програмного забезпечення для захисту шкідливого програмного забезпечення за кодом CPV за ЄЗС ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів

**ТЕХНІЧНІ ВИМОГИ**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Назва системи** | **Одиниця виміру** | **Кількість** |
| **1** | **Програмне забезпечення для захисту від шкідливого програмного забезпечення** | **шт.** | **500** |

***У ціну мають бути включені прямі, загальновиробничі та адміністративні витрати з урахуванням витрат, у тому числі, але не виключно: транспортні витрати, доплати працівникам у зв’язку з втратою часу в дорозі, зв’язок, страхування, спецзасоби, а також економічно обґрунтований прибуток, який Постачальник планує отримати в результаті продажу, кошти на покриття ризиків та/або додаткових витрат, пов’язаних з інфляційними процесами, усі податки і збори, обов’язкові платежі, що сплачуються або мають бути сплачені Постачальником для поставки Товару, зокрема податок на додану вартість, інші витрати, необхідні для виконання проєкту Договору до моменту його повного завершення.***

1. Товар (складові товару) повинен постачатись новим в упаковці та з маркуванням виробника, а також повинна бути в наявності технічна документація, яка входить до комплекту постачання фірми-виробника.

2. У разі постачання неякісного Товару, Постачальник забезпечує заміну неякісного Товару якісним за власний рахунок при пред’явлені Покупцем не пізніше 7 робочих днів після отримання Товару.

3. Наявність заявлених Покупцем недоліків та причини їх виникнення повинно встановлюватись актом обстеження технічного стану Товару, який обов’язково укладається між Сторонами і є підставою для усунення Постачальником недоліків Товару у термін, що узгоджується за домовленістю Сторін. Акт обстеження технічного стану складається сервісним (технічним) центром Постачальника за участю представника Покупця.

4. Всі елементи повинні бути сертифіковані в Україні (надати сканкопії оригіналів сертифікатів (паспортів) на обладнання) у разі необхідності сертифікації даного обладнання.

5. Виконання постачання повинно здійснюватися відповідно до діючих нормативно-правових документів та умов цього проєкту Договору.

6. Вартість доставки товару повинна бути включена до загальної вартості товару та додатково Замовником не оплачується (до доставки мають бути включені наступні супутні послуги: доставка, розвантаження).

7. Надати у складі пропозиції гарантійний лист, що Учасник гарантує постачання Товару та виконання супутніх послуг у строки встановлені в проєкті Договору.

**ТЕХНІЧНЕ ЗАВДАННЯ**

|  |  |
| --- | --- |
| Загальні вимоги | * Забезпечення захисту не менше ніж для 500 робочих станцій та серверів;
* Строк дії підписки не менше ніж 12 місяців;
* Забезпечення отримання основних та проміжних релізів програмного забезпечення через сайт Виробника, підтримка програмних кодів у актуальному стані відповідно до рекомендацій Виробника протягом 12 місяців;
* Забезпечення застосування Cisco Secure Endpoint з підтримкою актуальності (оновлення) захисту протягом 12 місяців для 3 500 робочих станцій та серверів;
* Забезпечення обстежень, не менше ніж, 200 виконуваних файлів (семплів) у хмарній пісочниці за день;
* Забезпечення, не менше ніж, 3-х облікових записів у хмарній пісочниці для завантаження виконуваних файлів (семплів) вручну;
* Підтримка моніторингу шкідливого коду на рівні робочої станції;
* Виявлення та запобігання складному шкідливому коду (malware), атакам нульового дня та цільовим атакам або без використання, або з мінімальним використанням бази даних сигнатур;
* Вендор послуги захисту безпеки повинен мати окремий підрозділ безпеки, що фокусується на дослідженнях шкідливого коду (malware).
* Розширення ліцензії до типу Premier.
 |
| Функціональні вимоги | * Підтримка робочих станцій та серверів;
* Можливість інтерактивної та прозорої інсталяції;
* Наявність єдиної графічної консолі керування, моніторингу та налаштування;
* Підтримка наступних операційних систем:
	+ Windows;
	+ Windows Server;
	+ Mac;
	+ Linux (Amazon Linux, RHEL/CentOS, SUSE Enterprise, Leap, Ubuntu);
	+ Android;
	+ iOS;
* Рішення не повинно вимагати жодних системних змін на рівні ОС, таких як: увімкнення служби тіньового копіювання томів, віддаленого реєстру, спільного доступу до принтерів/файлів та увімкненого за замовчуванням локального адміністратора, або будь-яких інших змін на рівні користувача;
* Рішення повинно мати єдину інформаційну панель управління EDR для всіх операційних систем, а саме:
	+ Windows;
	+ Windows Server;
	+ Linux;
	+ MacOS;
	+ Android;
* Можливості аналізу на підозрілих станціях та серверах:
	+ Послідовний та хронологічних запис подій, з деталями, що включає хост, ім’я користувача, IP-адреси, клієнтські додатки;
	+ Деталі, що включають інформацію про те, який файл чи процес постраждав;
* Відслідковування на мережевому рівні і візуалізація системи і користувачів, що постраждали: користувач, метод та точка входу;
* Можливість видачі інформації про шкідливий код (malware), який був невідомий на момент його проходження через систему з можливістю отримання звіту про джерело, приймача і автоматичне блокування спроб передачі його в майбутньому (cloud recall);
* Рішення повинно підтримувати моніторинг шкідливого коду як на рівні мережі, так і на рівні робочої станції, повинно виявляти та запобігати складному malware, атакам нульового дня та цільовим атакам або без використання, або з мінімальним використанням бази даних сигнатур;
* Рішення повинно виявляти та блокувати підозрілі файли:
	+ Виявлення та блокування всіх видів шкідливого коду (malware), як відомого, так і невідомого;
	+ Аналіз всіх файлів, включаючи формати PDF, Flash, RTF, MS Office, Multimedia, архіви;
* Рішення повинно підтримувати можливість проведення безперервного аналізу файлів, виявлення причини зараження для подальшої класифікації інцидентів безпеки:
	+ Можливість видачі інформації про шкідливий код (malware), яка була невідома на момент його проходження через систему з можливістю отримання звіту про джерело, отримувача і автоматичне блокування спроб передачі його в майбутньому;
	+ Можливість відправити шкідливе ПЗ (malware) на додатковий аналіз в «пісочницю» як автоматично, так і вручну;
* Рішення повинно підтримувати можливість проведення розслідувань, що включають (але не обмежують) наступне:
	+ Джерело інфекції на аналіз причин виникнення загроз типу malware;
	+ Масштаби загрози, що включають звіти по кількості і типах машин, що були атаковані, первинне виявлення і детальна історія про зараження шкідливим кодом (malware), включаючи профіль вузлів, а також інша підозріла діяльність на вузлах (підключення до C&C тощо);
	+ Візуальна репрезентація руху шкідливого коду по мережі та по робочих станціях;
* Рішення повинно фіксувати і записувати всю активність файлів і процесів, а не тільки виявлення шкідливих програм, і відображати їх на часовій осі у єдиному центрі керування;
* Аналіз файлів в захищеній хмарній пісочниці для швидкого виявлення зловмисного ПЗ та підозрілої поведінки файлів;
* Підтримка типів файлів пісочницею:
	+ .BAT – Batch files;
	+ .CHM – Compiled HTML Help – Microsoft Compiled HTML Help;
	+ .DLL – See: PE32 and P32+;
	+ .ISO – ISO image files;
	+ .HTA – HTML Application;
	+ .HWP, .HWT, .HWPX – Available on the win7-x64-kr VM only (specific to Hancom Office);
	+ .JAR – Java Archives;
	+ .JS – JavaScript;
	+ .JSE – Encoded JavaScript;
	+ .JTD, .JTT, .JTDC, .JTTC: Available on the win7-x64-jp VM only (specific to Ichitaro);
	+ .LNK – Windows shortcut files;
	+ .MSI – Microsoft Installer files;
	+ MHTML – Mime HTML Files;
	+ Microsoft Office Documents, including .DOC, .DOCX, .RTF, .XLS, .XLSX, .PPT, .PPTX;
	+ PDF – Portable Document Format (detailed static forensics, including JavaScript resources);
	+ PE32 Files and Executables (.EXE);
	+ Libraries (.DLL);
	+ .PE32+ files – Available on the win7-x64 VM only;
	+ Executable (.EXE);
	+ Libraries (.DLL);
	+ .PS1 – PowerShell;
	+ .SWF – Flash Files;
	+ URLs (As Internet Shortcut file, or submit the URL directly. Detailed static forensics or JavaScript resources);
	+ .VBE – Encoded Visual Basic;
	+ .VBN – Virus Bin;
	+ .VBS – Visual Basic Script;
	+ .WSF – Windows Script File;
	+ .XML and XML Based Office Document Types (.DOCX, .XLSX, .PPTX);
	+ XML – Extensible Markup Language;
	+ ZIP – Archive and Quarantine Formats, as well as .BZ2, .GZip, .XZ;
	+ Quarantine file types including .SEP, .VBN;
* Блокування можливих підключень до серверів керування ботнетами і активності дроперів, а також стримування розповсюдження шкідливого ПЗ (malware);
* Можливість використання служби osQuery для надання інформації про хости у мережі (Orbital Advanced Search);
* Вбудований функціонал розширеної хмарної пісочниці (Secure Malware Analytics);
* Функціонал на робочих станціях та серверах для реагування на інциденти повинен включати (але не обмежувати) наступне:
	+ Відслідковування та захоплення файлів на підозрілій машині;
	+ Блокування підозрілих файлів/процесів/сервісів, що показують шкідливу поведінку;
	+ Виявлення дроперів та блокування завантажень з URL/вузлів;
	+ Відправлення підозрілих файлів для аналізу;
* Динамічний аналіз в реальному часі для виявлення загроз нульового дня чи цільових атак;
* Для роботи функції пошуку в реальному часі не має бути потрібен репозиторій або окреме сховище даних;
* Виведення результатів аналізу в формі графічної панелі або звіту, що показує деталі поведінки загрози і повинно, як мінімум, включати наступне:
	+ Операції ОС системного рівня;
	+ API виклики - Роботи процесів/потоків;
	+ Криптографічні операції;
	+ Можливості по захисту від налагодження (debuggers);
	+ Можливості протидії “засинанню” шкідливих програм чи затримці часу;
	+ Модифікації файлової системи;
	+ Модифікації реєстру;
	+ Мережеві порти та протоколи;
	+ Визначення Command and Control підключень;
	+ Характеристики протоколів;
	+ Аналіз наступних файлів: Microsoft Office, Executable Files (exe, com, dll), PDF, Flash, Shockwave, Java7 JDK і JRE, Windows Media Player, Multimedia, Microsoft .NET framework, Microsoft Visual C++ redistributable, Microsoft Silverlight, Microsoft VMScript;
	+ Захист популярних додатків від атак, що завантажують шкідливе ПЗ безпосередньо в пам’ять цих процесів, не залежачи від бази даних Common Vulnerabilities and Exposures (CVE): Microsoft Office, Internet Explorer, Chrome, Adobe Reader та інші.
* Рішення повинно мати можливість відстежувати та реєструвати активність користувача, наприклад, завантажені файли, запущені програми, на таких платформах, як Windows, Mac та Linux, безперервно протягом щонайменше 30 днів;
* Рішення також має відслідковувати дисковий простір, пам'ять та інші події;
* Рішення повинно мати можливість створювати запити подій на кінцевих пристроях за допомогою вбудованих або користувацьких скриптів.
 |

*У разі, якщо у цій тендерній документації (у тому числі у технічній специфікації) міститься посилання:*

*- на стандартні характеристики, технічні регламенти та умови, вимоги, умовні позначення та термінологію, пов’язані з товарами, роботами чи послугами, що закуповуються, передбачені існуючими міжнародними, європейськими стандартами, іншими спільними технічними європейськими нормами, іншими технічними еталонними системами, визнаними європейськими органами зі стандартизації або національними стандартами, нормами та правилами – вважати, що міститься вираз «або еквівалент»;*

*- на конкретні марку чи виробника або на конкретний процес, що характеризує продукт чи послугу певного суб’єкта господарювання, чи на торгові марки, патенти, типи або конкретне місце походження чи спосіб виробництва – вважати, що міститься вираз «або еквівалент».*

*У випадку надання учасником еквіваленту він має надати порівняльну таблицю запропонованих товарів з товарами, які вимагаються Замовником. Якщо Учасник пропонує товар, технічні характеристики якого відрізняються від наведених вище, він повинен обов’язково надати порівняльну таблицю щодо відповідності технічних характеристик запропонованого товару наведеним Замовником характеристикам. Товар має бути з технічними та якісними характеристиками рівноцінними, або покращеними, ніж визначені Замовником.*

У разі надання Товару, характеристики якого відрізняються від характеристик що вказав Замовник, Учаснику необхідно надати Таблицю відповідності за встановленою формою.

**Таблиця відповідності**

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Характеристика | Опис технічних вимог, які визначені Замовником | Опис технічних вимог, які пропонуються Учасником |

У разі надання гарантійного листа (або інших документів) від виробника (-ів) іноземною мовою, цей лист повинен супроводжуватись перекладом на українську мову.

Замовник має право звернутися за підтвердженням інформації, наданої учасником, до органів державної влади, підприємств, установ, організацій відповідно до їх компетенції. У разі отримання достовірної інформації про його невідповідність вимогам кваліфікаційних критеріїв, наявність підстав, зазначених у частині першій статті 17 цього Закону, або факту зазначення у тендерній пропозиції будь-якої недостовірної інформації, що є суттєвою при визначенні результатів процедури закупівлі, замовник відхиляє тендерну пропозицію такого учасника.

Товар повинен відповідати вимогам:

- Закону України від 14.08.2014р. № 1644-VІІ «Про санкції»,

- Указу Президента України від 15.05.2017р. № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»

- п/п. 4 п.2 частини першої Розпорядження Кабінету Міністрів України від 11.09.2014 р. №829-р «Про пропозиції щодо застосування персональних спеціальних економічних та інших обмежувальних заходів», згідно з якими заборонено здійснення державних закупівель товарів, робіт і послуг у юридичних осіб - резидентів Російської Федерації державної форми власності та юридичних осіб, частка статутного капіталу яких перебуває у власності Російської Федерації, а також у інших суб’єктів господарювання, що здійснюють продаж товарів, робіт і послуг походженням з Російської Федерації, крім випадків, коли заміщення таких предметів закупівлі іншими неможливе, що підтверджено Міністерством економічного розвитку і торгівлі.

У разі якщо товар не відповідає технічним вимогам Замовника або Учасник не в змозі виконати умови поставки, які визначені Замовником, Пропозиція відхиляється.

**5. Обґрунтування розміру бюджетного призначення:** розмір бюджетного призначення визначено Законом України «Про Державний бюджет України на 2024 рік» за КПКВК 1001050 «Забезпечення діяльності органів, установ та закладів Міністерства внутрішніх справ України, підготовка кадрів закладами вищої освіти із спеціальними умовами навчання» відповідно до бюджетного запиту на 2024 рік.

**6. Очікувана вартість предмета закупівлі:** 1 718 733,33 грн. (один мільйон сімсот вісімнадцять тисяч сімсот тридцять три гривні 33 коп.) з ПДВ.

**7. Обґрунтування очікуваної вартості предмета закупівлі:** Очікувана вартість визначена відповідно до частини 1 та 2 пункту 1 Розділу ІІІ «Методи визначення очікуваної вартості» Примірної методики визначення очікуваної вартості предмета закупівлі затвердженої Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 18.02.2020 № 275 та розрахована, як середньоарифметичне значення масиву отриманих даних, що розраховується за такою формулою: Цод = (Ц1 +… + Цк) / К.

**8. Процедура закупівлі:** Застосовується процедура відкритих торгів з особливостями.