**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 забезпечення безпеки за кодом ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки (Лотова закупівля)

**3. Ідентифікатор закупівлі: —** UA-2024-12-04-011295-а

**4. Обґрунтування технічних та якісних характеристик предмета закупівлі**: Закупівля програмного забезпечення для забезпечення безпеки за кодом ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки (Лотова закупівля)

**ТЕХНІЧНІ ВИМОГИ**

**ЛОТ1: Закупівля програмного забезпечення «Системи аудиту дій користувачів» за кодом ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки**

|  |  |  |  |
| --- | --- | --- | --- |
|  **№ п/п** | **Назва системи** | **Одиниця виміру** | **Кількість (ліцензій)** |
| **1** | Програмна Продукція WORКSTАТІОN AGENT - EКRAN SYSTEM, 51-200 AGENTS - ANNUAL SUBSCRIPТION WITH ADDED ENTERPRISE ADVANCED SUPPORT | шт. | 65 |
| **2** | Програмна Продукція WORКSTАТІОN AGENT - EКRAN SYSTEM, 201-1000 AGENTS - ANNUAL SUBSCRIPТION WІТН ADDED ENTERPRISE ADVANCED SUPPORT | шт. | 35 |
| **3** | Програмна Продукція ENTERPRISE EDIТION - EКRAN SYSTEM APPLICAТION SERVER- ANNUAL SUBSCRIPТION WІТН ADDED ENTERPRISE ADVANCED SUPPORT | шт. | 1 |
| **4** | Програмна Продукція WORКSTАТІОN AGENT - EКRAN SYSTEM , 1-50 AGENTS - ANNUAL SUBSCRIPТION WITH ADDED ENTERPRISE ADVANCED SUPPORT | шт. | 50 |
| **5** | Програмна Продукція WORКSTАТІОN AGENT - EКRAN SYSTEM, 51-200 AGENТS - ANNUAL SUBSCRIPТION WITH ADDED ENТERPRISE ADVANCED SUPPORT | шт. | 150 |

***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.***

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.

**ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ВИМОГИ**

**Технічні, характеристики програмного забезпечення «Системи аудиту дій користувачів»**

|  |  |
| --- | --- |
|  | **ЗАГАЛЬНІ Характеристики** |
|  | Адміністрування системи має відбуватися через веб-консоль |
|  | Управління налаштуваннями та щоденна робота з рішенням має здійснюватися виключно через веб-інтерфейс |
|  | Управління базою користувачів має здійснюватися тільки через веб-інтерфейс |
|  | Система повинна мати механізм протидії атакам з підбору пароля на веб-інтерфейс |
|  | Система повинна мати централізовану панель для перегляду сесій з різних інсталяцій незалежних між собою. |
|  | Система має мати веб-інтерфейс користувача та адміністратора українською мовою  |
|  | Система має підтримувати можливість входу на веб-консоль через облікові записи Active Directory, локально, через SSO (Single-Sign-On) та багатофакторну автентифікацію. |
|  | Система повинна підтримувати можливість розподілення веб-консолі на декілька адміністративних гілок управління незалежних між собою. Для кожної з них встановлюється відповідальний адміністратор який буде керувати власними налаштуваннями. Дані що обробляються в кожній з гілок повинні зберігатися централізовано на 1 інсталяції. |
|  | Система повинна мати рольове управління з наступними можливостями:* Розмежування прав доступу для налаштування безпосередньо системи для аудиту дій користувачів
* Призначення відповідальних офіцерів безпеки на окремі сегменти робочих станцій та серверів
* Призначення відповідальних офіцерів безпеки на аудит певних агентів.
 |
|  | Система має надавати можливість перегляду аналітиком будь-якої активної сесії для контролю дій користувачів |
|  | Система має базуватися на агентному методі |
|  | Система повинна базуватися на архітектурі клієнт-сервер |
|  | Система має забезпечити можливість встановлення агентів віддалено через веб-консоль як в доменну інфраструктуру, так і на локальні кінцеві точки. |
|  | Система повинна підтримувати автоматичне оновлення агентів на кінцевих робочих станціях відразу при оновленні серверної частини |
|  | Агенти рішення не повинні залежати від IP адрес кінцевих точок та від облікових записів користувачів – «плаваючі ліцензії». |
|  | Рішення повинно покрити наступний об’єм кінцевих точок:* Сервер управління - 1 шт
* Робочі станції (Windows) – 100 шт
 |
|  | Система повинна легко масштабуватися до кількох тисяч агентів |
|  | Зв'язок між агентом та сервером управління має бути захищений за допомогою симетричного або асиметричного шифрування з ключем AES-256 або подібним  |
|  | Зв'язок між сервером та базою даних має бути захищений за допомогою SSL сертифікату |
|  | Система повинна використовувати криптостійкий сертифікат (наприклад,  SHA-2 та подібні) для захисту збережених даних, за замовчуванням, або з можливістю використання власного сертифіката клієнта. |
|  | Система повинна мати можливість сповіщати користувача про те, що всі його дії записуються при вході на робочу станцію |
|  | Система повинна мати можливість сповіщавати користувачів про запис сесії в процесі роботи користувача |
|  | Система повинна мати механізм ознайомлення користувача з політиками використання службових ресурсів після входу в систему |
|  | Система повинна мати можливість показувати повідомлення користувачам на робочій станції під час входу в ОС |
|  | Система повинна мати можливість переглядати сесії користувачів як наживо, так і в записі |
|  | Система повинна записувати дії користувачів (знімки екранів + метадані) та у вигляді відеозапису. |
|  | Система має забезпечувати перевірку результатів моніторингу для гарантування цілісності даних які контролюються |
|  | Записані сесії повинні мати механізм захисту їх цілісності |
|  | Система повинна записувати локальні сесії |
|  | Система повинна записувати віддалені сесії (RDP, SSH та інші) |
|  | Система повинна мати можливість приховання реальних ідентифікаторів (анонімізація) співробітників для відповідності міжнародним стандартам по GDPR |
|  | Система повинна мати можливість ідентифікувати користувача, який використовує спільний обліковий запис |
|  | Запис сесій повинен відбуватися як у кольоровому, так і у чорно-білому режимах |
|  | Система повинна підтримувати запис дій тільки активних вікон для економії сховища даних. |
|  | Система повинна мати можливість записувати тільки визначені додатки. |
|  | Система повинна підтримувати моніторинг відвідування сайтів |
|  | Система повинна мати моніторинг буфера обміну |
|  | Система має визначати весь текст буфера обміну, при цьому дані мають бути збережені в хешованому вигляді |
|  | Система повинна мати можливість відображення сесїї співробітника який працював одночасно на двох або більше моніторах |
|  | Система повинна мати можливість записувати тільки окремі URL або записувати всі URL, крім виокремлених |
|  | Система повинна мати можливість збирати тільки метадані, без відеозапису сесії користувача |
|  | Система має виявляти підключення пристроїв по USB, відслідковувати USB носії та мати можливість блокувати носії, що не внесені у списки дозволенних (білі списки) для використання на кінцевих точках |
|  | Система повинна мати можливість контролювати та блокувати окремі USB пристрої (миші, клавіатури, аудіопристрої і т.д.) |
|  | Система повинна надавати\забороняти доступ до сесії (локальної чи віддаленої) на основі груп AD |
|  | Система повинна мати можливість віддаленого блокування користувача з консолі адміністратора системи. |
|  | Система має надавати можливість дозволити або закрити доступ користувачу до систем |
|  | Впродовж активної сесії рішення повинно забезпечити можливість заблокувати користувача для подальшого розслідування інциденту |
|  | Система має надавати доступ кінцевим користувачам тільки за обов’язковим коментарем (представлення необхідної інформації адміністратору системи) та дозволом адміністратора системи |
|  | Система повинна підтримувати можливість припинення запису сесії при відсутності активності на комп’ютері |
|  | Система повинна продовжувати запис дій навіть після втрати з’єднання з сервером управління (оффлайн режим)  |
|  | Дані, що зберігаються в оффлайн режимі, мають бути збережені локально та з обмеженням доступу  |
|  | Система має забезпечувати можливість архівування результатів моніторингу та перегляд даних з архіву |
|  | Система має підтримувати експортування окремих сесій та їх епізодів в зашифрованому вигляді |
|  | Система має забезпечувати перевірку результатів експорту даних для гарантування цілісності даних |
|  | Система повинна мати можливість завантажити з веб-консолі журнал подій агентів в разі розслідування неналежної роботи агента. |
|  | Система має підтримувати аудит використання системи, аудит змін в середині системи, аудит має бути захищений від будь-яких модифікацій. |
|  | Логування всіх дій користувачів та моніторинг результатів з можливістю фільтрації даних |
|  | Система повинна забезпечувати можливість пошуку по зібраним даним:* Мульти-параметри при пошуку в результатах моніторингу

(Моніторинг віддалених ІР, з яких здійснювався доступ до моніторингової системи. Фільтрування сесій моніторингу по віддалених IP адресах і т.д.)* Можливість фільтрації користувачів під час моніторингу
* Можливість фільтрації додатків або веб сайтів під час моніторингу
* Можливість моніторингу активності користувачів під час конкретного інтервалу часу
 |
|  | Система повинна мати початкові шаблони політик для виявлення інцидентів безпеки |
| 1. \
 | Система повинна мати можливість створювати політики сповіщень на основі даних, зібраних з агентів. |
|  | Система має підтримувати **Regex** якості параметрів для політик сповіщення |
|  | Сповіщення повинні надходити в режимі реального часу |
|  | Система повинна мати механізм взаємодії з користувачем у реальному часі у випадку порушення політик безпеки, із можливістю інформування користувача про порушені політики або блокування дій, або примусового переривання його сесії |
|  | Система повинна мати можливість блокування роботи користувача у випадку спрацювання правила |
|  | Система повинна виявляти та зупиняти завантаження файлів на веб ресурси |
|  | Система має виявляти та зупиняти активність з файлами при переміщені на хмарні сховища. |
|  | Можливість блокування користувача як автоматично так і в ручному режимі при виявленні протиправних дій |
|  | Система повинна мати змогу виконувати наступні автоматичні дії:* Надіслати повідомлення користувачу про порушення ним політик безпеки без блокування його дій
* Надіслати повідомлення користувачу про порушення ним політик безпеки з блокуванням його дій
* Закриття веб сайту
* Закриття додатку
* Блокування користувача на всіх робочих точках, де встановлений агент
 |
|  | Можливість відключення протиправних (не дозволених) процесів на робочій станції за допомогою системи алертів |
|  | Система повинна мати можливість пакетного імпорту-експорту правил сповіщень. |
|  | Система повинна мати можливість повідомлення адміністратора у випадку порушення політик безпеки та потенційного витоку даних |
|  | Система повинна мати вбудований модуль аналізу поведінки користувачів в режимі реального часу. |
|  | Система повинна мати вбудовану систему звітності |
|  | Звіти повинні відправлятися обраним користувачам за розкладом |
|  | Система повинна мати можливість підтримки режиму Multi-tenant для всіх видів підтримуваних операційних систем з можливістю створення окремих користувачів тенанта які не матимуть доступ до інших тенантів, клієнтів, конфігурацій, правил сповіщення, репортів та іншого |
|  | Система повинна підтримувати можливість роботи на кластерах бази даних в режимі високої доступності (High Availability) |
|  | Архітектура системи має підтримувати паралельний збір даних з агентів за рахунок розгортання декількох серверів додатків та підтримувати роботу з системою балансування навантаження. |
|  | В разі зміни адреси сервера додатків, агенти повинні мати можливість переключитися на іншу адресу сервера без втручання адміністратора.  |
|  | Система повинна підтримувати централізовано роботу з розгалуженими (distributed) серверами в різних географічних місцях |
|  | Система не повинна змінювати топологію мережі чи змінювати звичний спосіб автентифікації користувачів |
|  | Система має забезпечити шифрування конфіденційної інформації в базі даних |
|  | Система повинна підтримувати можливість зберігання записів сесій на файлових серверах |
|  | **Характеристики Windows систем** |
|  | Система повинна збирати наступні дані на ОС Windows:* Назву запущеного додатку
* Назви заголовків вікон
* URL
* Назви веб сайтів
* Назви запущених процесів
* Відстеження скопійованого тексту наступними методами:
* Натискання правої кнопки миші в контекстному меню «Копіювати», «Вирізати», «Вставити»
* Виклик через меню додатку Змінити > Копіювати, Змінити > Вирізати>Вставити
 |
|  | Система повинна мати наступні можливості налаштування політик запису на ОС Windows:* Записувати лише обраних користувачів
* Виключити з запису обраних користувачів
* Система повинна записувати обраних користувачів на основі груп AD
* Відслідковувати певні ІР адреси віддалених підключень
* Записувати лише обрані додатки
* Виключити з запису обрані додатки
* Записувати лише мета дані, без запису екрану
* Записувати лише обрані/виключені URL
* Починати запис екрану після введення “ключового” слова.
 |
|  | Система повинна мати модуль контролю та логування натискання клавіш з клавіатури на сайтах та додатках |
|  | Система повинна мати захист від призупинення / зупинки процесу Агента та зміни / видалення Агента навіть для користувачів із правами адміністратора |
|  | **Характеристики підтримуваних систем** |
|  | Система повинна підтримувати збір, аналіз та аудит дій на сервери та робочі станції з підтримкою наступних ОС:Для серверів:* Windows Server 2012 (32-bit та 64-bit)
* Windows Server 2016 (32-bit та 64-bit)
* Windows Server 2019 (32-bit та 64-bit)
* Windows Server 2022 (32-bit та 64-bit)
* Terminal Server – Windows

Для робочих станцій: * Windows 7 (32-bit і 64-bit)
* Windows 8 (32-bit і 64-bit)
* Windows 8.1 (32-bit і 64-bit)
* Windows 10 (32-bit і 64-bit)
* Windows 11
 |
|  | **Загальні функціональні характеристики** |
|  | Сервісна підтримка повинна надаватися від виробника |
|  | Доступ до технічної документації |
|  | Перша лінія підтримки має бути наявна в Україні від розробника або його офіційного представника |
|  | Система має підтримувати режим відновлення після технічних проблем |
|  | Система повинна мати вбудовану систему моніторингу стану своїх компонентів та агентів |
|  | Система повинна мати моніторинг ресурсів та розміру бази даних з можливістю повідомлення через електронну пошту про проблеми. |
|  | Система повинна підтримувати наступні версії баз даних як сховища інформації:* SQL Server 2012/2014/2017/2019 і вище
* PostgreDB 10.1 і вище
 |
|  | Система повинна підтримувати можливість роботи на кластерах бази даних в режимі високої доступності (High Availability) |
| 1. \
 | Система має підтримувати можливість незалежного адміністрування та підтримку бази даних (дефрагментація, реіндексація, shadow backup, shadow copy, shrink) офіційними інструментами обслуговування бази даних поза рішенням і не впливати на його функціонал.  |
|  | Система має підтримувати інтеграцію з Active Directory |
|  | Система повинна інтегруватися із LDAP системами |
|  | Система має підтримувати інтеграцію з SIEM Splunk та IBM QRadar, Trellix 7.0 або іншими. |
|  | Система має підтримувати надсилання логів у форматах CEF та LEEF. |
|  | Система повинна мати можливість передачі даних через протокол syslog |
|  | Система повинна мати можливість інтеграції з системами підтримки користувачів (ServiceNow або аналогами).  |
|  | Система повинна мати відкритий API |
|  | Система повинна мати можливість вивантаження інформації через API або іншими способами для майбутнього написання конекторів в сторонні системи під потреби адміністратора.  |

*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.*

**ЛОТ2: Закупівля програмного забезпечення для «Системи керування вразливостями» за кодом ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки**

|  |  |  |  |
| --- | --- | --- | --- |
|  **№ п/п** | **Назва системи** | **Одиниця виміру** | **Кількість (ліцензій)** |
| **1** | Програмна продукція Tenable Vulnerability Management (Assets: 1ОО) | шт. | 1 |
| **2** | Програмна продукція Tenable Vulnerability Management (Assets: 500) | шт. | 1 |
| **3** | Програмна продукція Tenable Web Арр Scanning(8 Web Apps) | шт. | 1 |

***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.***

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.

**ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ВИМОГИ**

**Технічні, характеристики програмного забезпечення «Системи керування вразливостями»**

|  |
| --- |
| **Загальні вимоги до системи** |
|  |  Рішення повинне мати можливість сканувати до 600 активів з можливістю придбання додаткових ліцензій для їх сканування. |
|  | Рішення повинне включати можливість активного та пасивного сканування для повної видимості активів, вразливостей та конфігурацій. |
|  | Рішення повинне визначати пріоритет для вразливості на основі ризиків.  |
|  | Пропозиція з рішення повинна включати технічну підтримку 24/7/365. |
|  | Рішення повинне включати автоматичне оновлення нових перевірок на вразливості кожні 24 години. |
|  | Рішення повинне мати ліцензію на основі активів, враховуючи інші параметри мережі, крім IP, у випадку, якщо пристрій має 2 IP. |
|  | Рішення не повинне покладатися на IP-адреси, як єдиний засіб відстеження ліцензування активу. |
|  | Рішення повинне враховувати IP-адресу, тип обладнання, операційні системи, UUID BIOS, MAC-адресу, ім’я NetBIOS, повне доменне ім’я для визначення активу. |
|  | Рішення повинне мати можливість привласнювати декілька IP-адрес одному активу, для пристроїв, які мають кілька IP-адрес одночасно. |
|  | Рішення повинне забезпечувати еластичну модель ліцензування, щоб забезпечити безперервне функціонування продукту, коли тимчасово перевищено ліцензійне обмеження. |
|  | Рішення повинне дозволити тимчасово перевищити ліцензію у разі необхідності сканувати додаткові ресурси. |
|  | Всі компоненти, модулі сканування повинні постачатися тим же виробником, що і основна система. |
| **Архітектура** |
|  | Рішення повинне забезпечувати інтегровану модель зберігання, яка не покладається на сторонні продукти баз даних. |
|  | Рішення повинне мати можливість постійного моніторингу мережевого трафіку для виявлення та оцінки систем які знаходяться короткий час в мережі та важко скануючих пристроїв, таких як чутливі системи OT та IoT. |
|  | Рішення повинне забезпечувати повний і повністю задокументований API для автоматизації процесів та інтеграції зі сторонніми додатками. |
|  | API повинен надаватися без додаткових витрат і бути частиною єдиної підписки. |
|  | Рішення має масштабуватися до мільйонів активів. |
|  | Рішення повинне включати опцію для агентів, які забезпечують виявлення вразливостей та оцінку конфігурації безпеки кінцевого пристрою. |
|  | Рішення повинне мати можливість використовувати групу сканерів в одному скануванні. |
|  | Рішення повинне мати можливість сканувати об’єкти у внутрішніх мережах, а також об’єкти, які є зовнішніми та загальнодоступними. |
|  | Сканерами повинна керувати платформа, наприклад, оновлення для виявлення вразливостей, код та інші оновлення. |
|  | Рішення повинне забезпечувати можливість розгортання необмежених повнофункціональних пасивних сканерів без додаткових витрат.  |
|  | Рішення повинне забезпечувати можливість розгортання необмежених повнофункціональних активних сканерів без додаткових витрат.  |
|  | Рішення повинне забезпечувати можливість розгортання необмежених повнофункціональних агентів без додаткових витрат.  |
|  | Загальна кількість повнофункціональних сканерів, агентів та пасивних сканерів має бути необмеженою. |
|  | Всі модулі сканування повинні постачатися одним виробником. |
|  | Усі повнофункціональні агенти, активні сканери, пасивні сканери повинні бути частиною єдиної підписки. |
|  | Рішення повинне надавати можливість розгортання віртуального пристрою для єдиної точки комунікації з SaaS платформою всіх підключених сенсорів розгорнутих локально. Сенсори повинні надсилати інформацію до віртуального пристрою, який централізовано передає до SaaS платформи інформацію про вразливості, а не кожний сенсор напряму  |
|  | Повністю функціональний віртуальний пристрій для централізованої комунікації з SaaS платформою повинен надаватися без додаткових витрат. |
|  | Агент повинен мати можливість підключатися до консолі через проксі-сервер. |
|  | Сканери повинні мати можливість підключатися до консолі через проксі-сервер. |
|  | Агент повинен мати можливість встановлюватися за допомогою сторонніх рішень, таких як Active Directory або SCCM. |
| **Управління доступом** |
|  | Рішення повинне забезпечувати рольову модель доступу (RBAC) для контролю прав користувачів над певними наборами даних та функціональних можливостей. |
|  | Рішення повинне надавати можливість приймати або змінювати ризик вразливостей, при цьому така функціональність обмежується роллю користувача і будь-яке прийняття ризику вразливості повинне бути задокументоване. |
|  | Рішення повинне мати можливість визначати та керувати групами користувачів, включаючи обмеження функцій сканування та доступу до звітів. |
|  | Рішення повинне мати можливість гарантувати, що певні IP-адреси або порти можуть бути заблоковані від сканування. |
|  | Рішення повинне мати двофакторну автентифікацію. |
| **Сканування** |
|  | Рішення повинне підтримувати різні платформи для механізму сканування, які включають Windows, Linux, macOS, а також віртуальні пристрої. |
|  | Рішення повинне підтримувати кілька географічно розподілених механізмів сканування, керованих центральною консоллю. |
|  | Рішення повинне включати можливість заборони сканування в визначені години. |
|  | Рішення повинне передбачати можливість конфігурування портів, протоколів та служб для підключення до сканерів, розгорнутих у мережі. |
|  | Рішення повинне мати можливість налаштовувати навантаження на кінцеві станції для планового сканування, щоб дозволяти регулювати сканування для запобігання генерації трафіку, який може порушити нормальну роботу мережевої інфраструктури. |
|  | Рішення повинне передбачати можливість введення та безпечного зберігання облікових даних користувачів, включаючи локальні облікові записи Windows та домени, а також Unix su та sudo через SSH. |
|  | Рішення повинне забезпечувати можливість підвищення привілеїв сканера на цільових системах із звичайного доступу користувача до адміністраторського доступу. |
|  | Рішення повинне підтримувати індивідуальне планування сканування, включаючи можливість запускати сканування у визначений час із заздалегідь визначеною частотою. |
|  | Рішення повинне мати можливість виконувати пошук конфіденційних даних в системах Windows, Unix та Linux. |
|  | Рішення повинне включати в модель ліцензування «автоматичне старіння», щоб активи які не скануються протягом 90 днів, більше не враховувались у ліцензії. |
|  | Система повинна дозволяти користувачам запускати сканування на перевірку усунення вразливостей, щоб переконатися, що вони виправлені, без необхідності налаштовувати параметри сканування. |
| **Виявлення активів** |
|  | Продукт повинен підтримувати можливість виявлення активів, які не враховуються в ліцензуванні. |
|  | Продукт повинен забезпечувати можливість пасивного моніторингу мережі для виявлення активів. |
|  | Продукт повинен підтримувати можливість отримувати видимість активів в режимі реального часу та проводити інвентаризацію загальнодоступних хмарних активів, коли хмарні екземпляри вмикаються або виводяться з експлуатації. |
|  | Рішення повинне мати можливість виявляти мобільні пристрої та інтегруватися з декількома різними системами управління мобільними пристроями (MDM). |
|  | Рішення повинне забезпечувати виявлення служб Інтернету та баз даних. |
|  | Рішення повинне мати можливість виявлення служб, що працюють на нестандартних портах. |
|  | Рішення повинне мати можливість виявлення служб, налаштованих не відображати банери з’єднання. |
|  | Рішення повинне мати можливість тестувати кілька екземплярів однієї і тієї ж служби, що працює на різних портах. |
|  | Рішення повинне мати можливість сканувати мертві хости (пристрої, які не реагують на ICMP запити). |
|  | Рішення повинне підтримувати використання netstat для швидкого та точного перерахування відкритих портів у системі при наданні облікових даних. |
|  | Рішення повинне підтримувати використання SMB та WMI для сканування систем Windows. |
|  | Рішення повинне мати можливість автоматичного запуску віддалених служб реєстру в системах Windows під час виконання сканування, а потім автоматично зупиняти служби після завершення сканування. |
|  | Сканер повинен підтримувати безпечне з’єднання(ssh) з можливістю підвищення привілеїв для сканування на наявність вразливостей і аудиту конфігурацій в системах Unix. |
|  | Рішення повинне забезпечувати можливість налаштування політики сканування для мінімального впливу на мережі та цілі сканування. |
|  | Продукт повинен забезпечувати активне та пасивне виявлення бездротових точок доступу (WAP). |
| **Групування активів на основі тегів** |
|  | Рішення повинне надавати можливість створювати статичні групи активів на основі тегів. |
|  | Рішення повинне надавати можливість створювати динамічні групи активів на основі тегів за допомогою написання правил. |
|  | Рішення повинне надавати можливість створювати теги за шаблоном Категорія: Значення |
|  | Рішення повинне надавати можливості створення правил тегів за допомогою фільтрів або мови запитів |
|  | Панель створення правил тегів повинна містити як мінімум такі фільтри: Risk Metrics, Account ID, Agent Name, ARN,ASN, Assessed vs. Discovered, Asset ID, AWS Availability Zone, AWS EC2 AMI ID, AWS EC2 Instance ID, AWS EC2 Name, AWS EC2 Product Code, AWS Instance State, AWS Instance Type, AWS Owner ID, AWS Region, AWS Security Group, AWS Subnet ID, AWS VPC ID, Azure Resource ID, Azure Resource Type, Azure Subscription ID, Azure VM ID, BIOS ID, Cloud Provider, Created Date, Custom Attribute, Deleted, Deleted Date, DNS(FQDN), Domain, First Seen, Google Cloud Zone, Has Plugin Results, Host Name(Domain Inventory), Hosting Providers, IaC Resource Type, Installed Software, IPv4 Address, IPv6 Address, Is Attribute, Is Auto Scale, Is Unsupported, Last Audited, Last Authenticated Scan, Last Licensed Scan, Last Seen, Licensed, MAC Address, Mitigation Last Detected, Name, NetBIOS Name, Network, Open Ports, Operating System, Port, Public, Record Type, Region, Repositories, Resource Category, Resource Tags(By Key), Resource Tags(By Value), Resource Type, ServiceNow Sys ID, Source, SSL/TLS, System Type, Tags, Target Groups, Tenable ID, Terminated, Type, Updated Date, VPC |
|  | Рішення повинне надавати можливість додавати/видаляти активи в тегах |
|  | Рішення повинне надавати можливість обирати теги під час створення скану |
| **Пасивне сканування** |
|  | Пасивний сканер повинен включати можливість сканування вразливостей шляхом моніторингу мережевого трафіку без активного сканування. |
|  | Пасивний сканер повинен відображати вразливості в режимі реального часу, виявлені в трафіку. Ці дані слід застосовувати до додатків, портів, протоколів, загроз та інших мережевих пристроїв з можливістю аналізу трафіку під час розслідування. |
|  | Пасивний сканер повинен надавати інформацію про окрему мережу, всю мережу або будь-яку групу хостів. |
|  | Пасивний сканер повинен мати можливість аналізувати трафік та повідомляти про зміни відповідно до певних граничних змін значень. |
|  | Пасивний сканер повинен виявляти потенційно небезпечні програми в мережевому трафіку (шкідливе програмне забезпечення, ботнет, тимчасова мережа). |
|  | Пасивний сканер повинен постачатися тим же виробником, що і основна система. |
|  | Пасивний сканер повинен мати можливість аналізувати трафік та надавати інформацію про вразливі місця без підключення до Інтернету. |
| **Оцінка вразливості** |
|  | Рішення не повинне покладатися на будь-які сторонні сканери для сканування на вразливість. |
|  | Рішення повинне мати можливість як автентифікованого, так і неавтентифікованого сканування для виявлення вразливостей, без необхідності встановлення клієнтського агента на цільовому пристрої. |
|  | Рішення повинне мати можливість сканування агентом для локального виявлення вразливостей без додаткової плати. |
|  | Рішення повинне надавати сканери, що розміщуються у хмарі, для сканування периметра мережі. |
|  | Рішення повинне мати можливість відстежувати зміни DHCP, пов’язуючи результати сканування однієї і тієї ж системи в випадку зміни IP. |
|  | Рішення повинне виявляти проблеми, ризики та вразливості. Він також повинен надавати детальну інформацію щодо характеру вразливості та рекомендації щодо її усунення. |
|  | Рішення повинне включати детальний висновок щодо результатів сканування, включаючи таку інформацію, як знайдені версії DLL. |
|  | Рішення повинне бути сумісним з CVE та забезпечувати оцінкою CVE щонайменше 10 років. |
|  | Рішення повинне передбачати аудит виправлення для операційних систем та програм Microsoft, що включає Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange та багато іншого. |
|  | Рішення повинне передбачати аудит виправлень для всіх основних операційних систем Unix, включаючи macOS, Linux, Solaris, IBM AIX, HP-UX та багато іншого. |
|  | Рішення повинне виявляти вразливості в сторонніх програм, таких як Java та Adobe. |
|  | Рішення повинне забезпечувати інтеграцію із системами управління виправленнями для аудиту виправлень та створення звітів щодо результатів сканування, таких як Microsoft WSUS / SCCM, Red Hat Satellite, IBM Tivoli Endpoint Manager (раніше BigFix), Symantec Altiris, Ques / Dell KACE. |
|  | Рішення повинне забезпечувати інтеграцію з продуктами управління мобільними пристроями (MDM), такими як VMware AirWatch, Apple Profile Manager, BlackBerry UEM, Good MDM, Microsoft Intune, IBM MaaS360 та MobileIron, для виявлення вразливостей та аудиту мобільних пристроїв. |
|  | Система повинна забезпечувати пріоритизацію вразливостей з використанням аналітики загроз в реальному часі і алгоритмів машинного навчання для оцінки вразливостей і прогнозування того, які з них з найбільшою ймовірністю будуть використані в найближчому майбутньому. |
|  | Система повинна забезпечувати пріоритизацію вразливостей, яка допомагає користувачам зрозуміти ключові фактори, що впливають на кожну оцінку вразливості (наприклад, новизну загрози, зрілість коду використання, категорії джерел Intel).Рішення також повинне включати оцінку вразливості відповідно до Загальної системи оцінки вразливості версії 3 (CVSS v3). |
|  | Рішення повинне надавати інформацію про вразливість із сторонніх джерел, таких як Core Impact, Metasploit та Canvas. |
|  | Рішення повинне містити інформацію про наявність експлойтів для вразливості, включаючи короткий опис вразливих місць, які можуть використовуватися шкідливим програмним забезпеченням для зараження активів. |
|  | Рішення повинне розумно вибирати тести для виявлення вразливостей та конфігурацій в активі на основі інформації, отриманої в результаті первинного сканування цього активу. |
|  | Рішення повинне відстежувати історичні дати виявлення вразливості, які можуть бути використані для фільтрації та складання звітів з часовими фільтрами. |
|  | Рішення повинне дозволяти вмикати або вимикати тести на виявлення вразливості та змінювати конфігурації для планового сканування. |
|  | Рішення повинне підтримувати сканування IPv6 з пасивним виявленням цілей IPv6. |
|  | Рішення має аналізувати загальнодоступні хмарні ресурси на предмет неправильної конфігурації та наявність вразливостей за допомогою активного сканування та агентів. |
|  | Рішення повинне мати Vulnerability Intelligence для можливості аналізу актуальних вразливостей у кіберпросторі та відстежувати їх виявлення у власній інфраструктурі. |
|  | Рішення повинне відстежувати активи та їх вразливості, включаючи високодинамічні ІТ-ресурси, такі як мобільні пристрої, віртуальні машини та хмарні ресурси. |
| **Вимоги до системи комплексного сканування вразливостей для сучасних веб-додатків** |
|  | Рішення повинне мати можливість сканувати до 8 веб-додатків з можливістю придбання додаткових ліцензій для їх сканування. |
|  | Рішення повинне мати можливість сканувати як внутрішні, так і зовнішні веб-додатки. |
|  | Рішення повинне вміти визначати частини критично важливих веб-додатків, які безпечно сканувати, та визначати інші частини, які ніколи не слід сканувати, щоб запобігти затримці роботи або порушенням. |
|  | Рішення повинне мати можливість сканувати веб-програми HTML5, AJAX, HTML. |
|  | Рішення повинне мати можливість звітувати про всі вразливості в веб-додатках - як внутрішніх, так і зовнішніх - в одній єдиній інформаційній панелі. |
|  | Рішення повинне мати можливість сканувати веб-програми за допомогою: облікових даних для автентифікації на основі сервера HTTP, автентифікації за допомогою форми входу, автентифікації за допомогою файлів cookie, автентифікації за допомогою Selenium. |
|  | Рішення повинне мати можливість регулювати навантаження для сканування. |
|  | Рішення повинне мати можливість обирати тести, які будуть використовуватися для сканування. |
|  | Рішення має ідентифікувати та класифікувати проблеми, ризики та вразливості. Він також повинен надавати детальну інформацію про ризики, вразливості та рекомендації щодо їх мінімізації. |
|  | Рішення повинне відстежувати дату виявлення вразливості. |
|  | Рішення повинне мати можливість розгортання локального сканера веб-додатків для виявлення вразливостей у веб-програмах, недоступних з мережі Інтернет. |
|  | Рішення повинне забезпечувати можливість розгортання локального сканера веб-додатків без додаткових витрат. |
|  | Сканер веб-додатків повинен надавати той самий виробник. |
|  | Рішення повинне мати власний сканер у хмарі для виявлення вразливостей у веб-додатках, до яких можна отримати доступ через мережу інтернет. |
|  | Рішення повинне мати можливість імпортувати сценарій Selenium, який містить один або кілька сценаріїв для відтворення дій сканера на певних сторінках для оцінки. |
|  | Рішення має оцінювати веб-програми і специфічні компоненти в веб-додатках та класифікувати вразливості по OWASP Top 10. |
|  | Рішення повинне бути простим у використанні та масштабуватися, щоб включати всі веб-додатки організації. |
|  | Рішення повинне сканувати та виявляти вразливості в API. |
|  | Рішення повинне перевіряти реалізацію SSL / TLS в веб-додатках. |

*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.*

**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:** 3 942 412,44 грн. (три мільйони дев’ятсот сорок дві тисячі чотириста дванадцять гривень 44 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.