ОБГРУНТУВАННЯ
(на виконання пункту 4[1] постанови Кабінету Міністрів України
від 11 жовтня 2016 р. № 710 «Про ефективне використання бюджетних коштів»)

Предмет закупівлі: Програмна продукція для підключення до системи моніторингу, аналізу та реагування на інциденти кібербезпеки, (ДК 021:2015 код 48730000-4 «Пакети програмного забезпечення для забезпечення безпеки»).

1. **Вид процедури:** відкриті торги з публікацією англійською мовою.
2. **Номер оголошення закупівлі:** UA-2024-06-14-010724-a.

4. Обґрунтування технічних та якісних характеристик предмета закупівлі:

Відповідно до Положення про Секретаріат Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 12 серпня 2009 р. № 850, основними завданнями Секретаріату є організаційне, експертно-аналітичне, правове, інформаційне, матеріально-технічне забезпечення діяльності Кабінету Міністрів України, урядових комітетів, Прем'єр-міністра України, Першого віце-прем'єр-міністра України, віце-прем'єр-міністрів України.

Війна в кіберпросторі є невід'ємною складовою сучасної війни. Хакерські атаки на інформаційні ресурси та інформаційний простір Секретаріату постійно збільшуються за інтенсивністю та складністю. Кіберзахист інформаційних ресурсів та інформаційного простору Секретаріату є на даний час надважливим завданням.

Програмна продукція для підключення до системи моніторингу, аналізу та реагування на інциденти кібербезпеки включає в себе активацію доступу до інтернет-платформи технічної підтримки програмного забезпечення системи управління подіями та інцидентами інформаційної безпеки Wazuh. Система управління подіями та інцидентами інформаційної безпеки Wazuh (далі – Система), надає функції XDR і SIEM для захисту хмари, контейнера та сервера, включаючи аналіз даних журналу, виявлення вторгнень і зловмисного програмного забезпечення, моніторинг цілісності файлів, оцінку конфігурації, виявлення вразливостей.

Система встановлюється на кінцевих точках, таких як ноутбуки, настільні комп'ютери, сервери, хмарні робочі місця та віртуальні машини. Вона забезпечує запобігання загрозам, їх виявлення та реагування. Вона працює на таких операційних системах, як Linux, Windows, macOS, Solaris, AIX і HP-UX.

Функціональні можливості Системи:

- Система забезпечує моніторинг подій безпеки для хмарних середовищ.
- Система відстежує параметри конфігурації систем та програм, щоб переконатися, що вони відповідають політикам безпеки організації, стандартам та/або посібникам із захисту, виконується періодичне сканування, щоб виявити неправильні конфігурації або прогалини в безпеці в кінцевих точках, якими можуть скористатися зловмисники. Сповіщення безпеки включають рекомендації щодо кращої конфігурації, посилання та зіставлення з стандартами конфігурації.
- Система має можливість виявлення загроз, які дозволяють виявляти зловмисне програмне забезпечення на основі поведінки. Система зосереджується на моніторингу та аналізі ненормальної поведінки шкідливих програм. Система має готові набори правил, які спеціально розроблені для ініціювання сповіщень про розпізнані шаблони зловмисного програмного забезпечення, забезпечуючи швидку реакцію на потенційні інциденти безпеки.
- Моніторинг цілісності файлів, відстежує дії, що виконуються в контрольованих каталогах або файлах, щоб отримувати розширену інформацію про створення, зміну та видалення файлів.
- Система має функціонал автоматизації дій реагування на загрози.

5. Обґрунтування розміру бюджетного призначення:

Розмір бюджетного призначення на закупівлю програмного комплексу для підключення до системи моніторингу, аналізу та реагування на інциденти кібербезпеки був встановлений на підставі проведених попередніх консультації з організаціями та установами відповідно до частини 4 статті 4 Закону України «Про публічні закупівлі», аналізу ринку щодо наявних технологічних рішень та аналізу курсу іноземних валют. Отримана інформація була використана для підготовки технічної специфікації програмного комплексу.

Всі консультації та надані рекомендації не призводять до порушення статті 5 Закону України «Про публічні закупівлі».

6. Обґрунтування очікуваної вартості закупівлі:

Очікувана вартість закупівлі підтверджена проведенням моніторингу цінових пропозицій.