Виконуючому обов'язки директора Спеціалізованого комунального підприємства «Київтелесервіс» Чернікову Павлу Олександровичу

Начальника Центру моніторингу та кібербезпеки міських сервісів Журбенко Максима Анатолійовича

СЛУЖБОВА ЗАПИСКА

місто Київ «18» вересня 2023 року

Конкретна назва предмета закупівлі – **Пакети програмного забезпечення операційного центру кібербезпеки (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника).**

Обґрунтування доцільності закупівлі:

На виконання пункту 16.22. «Створення та впровадження центру моніторингу та кібербезпеки міських сервісів його технічне обслуговування, моніторинг та підтримка сервісів, розширення та дооснащення» переліку завдань та заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 08.12.2022 №5824/5865)

Обґрунтування обсягів закупівлі:

Кількість програмного забезпечення обумовлена наявними процесами кібербезпеки Центру моніторингу та кібербезпеки міських сервісів СКП "Київтелесервіс"

Обґрунтування якісних характеристик закупівлі:

Предмет закупівлі повинен відповідати технічним, якісним та кількісним вимогам, наданим у Додатку 1.

Технічні вимоги рекомендовані протоколом №75 засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 – 2023 роки

Очікувана вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 6 238 758,80 (шість мільйонів двісті тридцять вісім тисяч сімсот п'ятдесят вісім гривень вісімдесят копійок) з ПДВ., є середньоарифметичним значенням отриманих комерційних пропозицій

Джерело фінансування закупівлі – місцевий бюджет, КЕКВ 2610 (Субсидії та поточні трансферти підприємствам (установам, організаціям)

Вид предмету закупівлі – програмне забезпечення.

Кількість – 1 комплект.

Місце поставки програмного забезпечення – місто Київ.

Строк поставки програмного забезпечення – до 01.11.2023.

Очікувана вартість не перевищує розмір бюджетного призначення

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 14 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 1 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 3 арк.
4. Додаток 4. Протокол №75 засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 - 2023 роки на 2 арк

Ініціатор закупівлі **М.А. Журбенко**

«ПОГОДЖЕНО»:

Головний бухгалтер **Г. А. Букша**

Начальник загально-правового відділу **О.М. Тертичний**

Заступник головного бухгалтера з економічних питань **Ю.В. Волочаєва**

Заступник директора з технічних питань **О.Ф. Поліщук**

Перший заступник директора **О.О. Биструшкін**

Додаток 1

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ (ТЕХНІЧНІ ВИМОГИ).

Предмет закупівлі: Пакети програмного забезпечення операційного центру кібербезпеки (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника).

На виконання пункту 16.22. «Створення та впровадження центру моніторингу та кібербезпеки міських сервісів його технічне обслуговування, моніторинг та підтримка сервісів, розширення та дооснащення » переліку завдань та заходів Комплексної міської цільової програми «Електронна столиця» на 2019-2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 08.12.2022 №5824/5865)

Загальні вимоги

Відповідно до поточних потреб Центру моніторингу та кібербезпеки міських сервісів включає, але не обмежуватиметься наступною підсистемою, в рамках якої очікується досягнення наступних завдань:

Підсистема керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури, що забезпечує процес періодичного виявлення і усунення потенційно шкідливих вразливостей, що в свою чергу знижує ризики схильності інфраструктури Замовника до можливих критичних інцидентів ІБ та підвищує зрілість інфраструктури Замовника (в контексті CyberSecurity).

- Продовження строку дії пакетів програмної продукції для забезпечення сталого функціонування існуючого технічного рішення;

Підсистема повинна мати можливості для подальшого розширення функціоналу та кількості компонентів ІТ-систем, що контролюються в Системі, без внесення суттєвих змін до існуючої ІТ-інфраструктури.

1.	Програмна продукція **Підсистеми керування процесом пошуку та мінімізації впливу вразливостей ІТ-інфраструктури** у складі: **- примірник програмної продукції** для забезпечення роботи підсистеми у відповідності до технічних вимог строком дії не менше ніж 12 місяців – **1 од**; **- примірник програмної продукції** для забезпечення роботи функціоналу Web Application Scanning для не менш ніж 10 FQDN строком дії не менше ніж 12 місяців – **1 од**;	**комплект**	**1**
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:		
	Загальні вимоги	– Якщо відповідно до функціональності запропонованого рішення або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки;	

		– Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення; – На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника
	Вимоги до архітектури	– Запропоноване рішення повинно поставлятися від одного виробника у вигляді віртуального пристрою та повинно бути виконаним у вигляді єдиної платформи, що не потребує використання будь-якого стороннього системного або прикладного програмного забезпечення (операційних систем, програмних додатків, систем керування базами даних тощо) для його впровадження; – Всі компоненти запропонованого рішення мають встановлювались локально та не потребувати підключення до мережі інтернет. – Запропоноване рішення повинно мати центральну консоль для всіх своїх компонентів, яка розгортається локально, щоб збирати, управляти і аналізувати інформацію про вразливості, не відправляючи їх в хмару. – Запропоноване рішення повинно мати можливість локально встановлювати активні сканера в мережі та підключати їх до центральної консолі – Запропоноване рішення повинно мати можливість локально встановлювати агенти на кінцеві точки та підключати їх до центральної консолі – Запропоноване рішення повинно мати можливість локально встановлювати пасивні сканера та підключати їх до центральної консолі. – Запропоноване рішення повинно централізувати і повністю автоматизувати щоденне оновлення бази вразливостей від постачальника. – Запропоноване рішення повинно підтримувати автономний процес оновлення без доступу в інтернет. – Запропоноване рішення повинно забезпечувати інтегровану модель зберігання даних, яка не залежить від третього стороннього продукту, який надає базу даних. – Запропоноване рішення повинно мати комплексний, відкритий REST API для автоматичного створення сценаріїв сканування і експорту даних з безпеки, без додаткових витрат. – Запропоноване рішення повинно мати експертний висновок Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів з технічного захисту інформації.

	Функціонал сканування	– Запропоноване рішення повинно включати в себе інтегровану можливість активного та пасивного сканування для повної видимості вразливостей і відповідності стандартам; – Запропоноване рішення повинно забезпечувати сканування без агентів і на основі агентів; – Запропоноване рішення повинно підтримувати різні платформи для розміщення сканера, включаючи Windows, Linux, macOS, а також віртуальні і апаратні пристрої. – Запропоноване рішення повинно підтримувати різні платформи для розміщення агента, включаючи Windows, Linux, macOS – Додатковий віртуальний образ модулів сканування і консолі повинен бути доступний без додаткових витрат. – Запропоноване рішення повинно підтримувати кілька географічно або логічно розподілених механізмів сканування, керованих центральною консоллю. – Запропоноване рішення повинно підтримувати балансування навантаження і перемикання між декількома сканерами шляхом динамічного розподілу навантаження сканування між сканерами в залежності від доступності сканера протягом всього завдання сканування. – Запропоноване рішення повинно надавати клієнтам можливість розгортати додаткові сканера в своєму середовищі без додаткових витрат. – Запропоноване рішення повинно надавати клієнтам можливість розгортати додаткові агенти в своєму середовищі без додаткових витрат. – Запропоноване рішення повинно надавати клієнтам можливість розгортати додаткові пасивні сканери в своєму середовищі без додаткових витрат. – Загальна кількість повнофункціональних сканерів, повнофункціональних агентів і пасивних сканерів для виявлення активів має бути необмежена. – Запропоноване рішення повинно забезпечувати можливість підключення хмарних сканерів і запуску сканування зовнішньої мережі організації з використанням єдиного системного інтерфейсу, розташованого локально, без додаткових витрат. – Запропоноване рішення повинно забезпечувати можливість настройки портів, протоколів і служб для підключень до сканерів, розгорнутим по всій мережі. – Запропоноване рішення повинно налаштовуватись, щоб регулювати сканування, для запобігання генерації трафіку, достатнього для порушення нормальної роботи мережевої інфраструктури.

		– Запропоноване рішення повинно забезпечувати можливість підтримки автономного сканування і імпорту результатів на сервер. – Запропоноване рішення повинно дозволяти введення і безпечне зберігання облікових даних користувачів, включаючи локальні і доменні облікові записи Windows, а також su і sudo для Unix систем з доступом по ssh. – Запропоноване рішення повинно забезпечувати можливість підвищення привілеїв для цілей зі звичайних користувачів до адміністратора. – Запропоноване рішення повинно підтримувати необмежену кількість облікових даних «ssh». – Запропоноване рішення повинно інтегруватися з рішеннями управління привілейованим доступом, такими як CyberArk, BeyondTrust, Thycotic і Lieberman для управління обліковими даними. – Запропоноване рішення повинно підтримувати сканування з аутентифікацією і без аутентифікації для локального і віддаленого виявлення вразливостей без необхідності установки агента на стороні клієнта на цільовому пристрої. – Запропоноване рішення повинно забезпечувати сканування цільових систем як з аутентифікацією, так і без аутентифікації. – Запропоноване рішення повинно покладатися на сторонні сканери для сканування вразливостей. – Запропоноване рішення повинно вміти відслідковувати зміни DHCP, пов'язуючи результати сканування з іменами пристроїв в системі. – Запропоноване рішення повинно підтримувати можливість збереження результатів сканування неактивних кінцевих станцій протягом налаштованого періоду часу. – Запропоноване рішення повинно включати детальні дані відносно результатів сканування, включаючи таку інформацію, як знайдені версії DLL. – Запропоноване рішення повинно повідомляти про відомі недоліки в заданій цілі, виявленої консультативними організаціями з безпеки (наприклад, база даних Common Vulnerabilities and Exposures (CVE), База даних вразливостей з відкритим вихідним кодом (OSVDB), SecurityFocus Bugtraq (BID) або будь-яке їх поєднання). – Запропоноване рішення повинно підтримувати сканування вразливостей на відповідність PCI. Система повинна включати попередньо визначені профілі сканування PCI, які відповідають поточним критеріям PCI DSS для сканування мережі. Повинна існувати функція для фільтрації всіх інших вразливостей, що не відносяться до PCI. – Запропоноване рішення повинно забезпечувати аудит виправлень для операційних систем і додатків Microsoft, таких як 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 і інші. – Запропоноване рішення повинно забезпечувати аудит виправлень для всіх основних операційних систем Unix, включаючи macOS, Linux, Solaris, IBM AIX, HP-UX та інші. – Запропоноване рішення повинно забезпечувати аудит виправлень для мережевої інфраструктури, включаючи Cisco, Juniper і інші. – Запропоноване рішення повинно підтримувати сканування SCADA пристроїв. – Запропоноване рішення повинно вміти збирати/імпортувати і відображати дані про вразливості IT і OT мереж для єдиної візуалізації вразливостей в об'єднаних мережах IT/OT. – Запропоноване рішення повинно забезпечувати сканування сторонніх додатків, таких як Java і Adobe. – Запропоноване рішення повинно забезпечувати інтеграцію з системами управління виправленнями для аудиту виправлень і створення звітів про зміни результатів сканування, таких як Microsoft WSUS / SCCM, Red Hat Satellite, IBM BigFix (раніше IBM Tivoli Endpoint Manager), Symantec Altiris, VMWare Go. – Запропоноване рішення повинно забезпечувати інтеграцію з менеджерами мобільних пристроїв (MDM) для виявлення та аудиту мобільних пристроїв. – Запропоноване рішення повинно забезпечувати можливості аудиту пристроїв і мереж SCADA. – Запропоноване рішення повинно надавати звіти про репутацію загроз, виявлених шкідливих програм і бот-мереж. – Запропоноване рішення повинно 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. – Запропоноване рішення повинно забезпечувати пріоритизацію вразливостей, яка допомагає користувачам зрозуміти ключові фактори, що впливають на кожну оцінку вразливості (наприклад, новизну загрози, зрілість коду використання, категорії джерел Intel). – Запропоноване рішення повинно включати оцінку вразливості відповідно до загальної системи оцінки вразливостей (CVSS). – Запропоноване рішення повинно забезпечувати налаштовуваний механізм оцінки вразливостей, що базується на прийнятих в галузі стандартах, таких як CVSS. – Запропоноване рішення повинно надавати інформацію про використання вразливостей з Core Impact, Metasploit і Canvas.

			– Запропоноване рішення повинно надавати інформацію про використання шкідливих програм на кінцевому пристрої. – Запропоноване рішення повинно дозволяти вибирати тести на основі інформації, отриманої при первинному скануванні, щоб проводити подальше тестування на основі отриманої інформації про даний пристрій або кінцеву точку. – Запропоноване рішення повинно відслідковувати життєвий цикл вразливостей стосовно окремих кінцевих пристроїв, а також середовищ, включаючи дату першого виявлення, останнього спостереження і усунення вразливості. – Запропоноване рішення повинно підтримувати сканування серверів VMware на вразливості і відповідність вимогам за допомогою власного API VMware. – Запропоноване рішення повинно дозволяти сканувати пристрої за розкладом. – Запропоноване рішення повинно дозволяти включати або відключати перевірки на певні вразливості під час сканування. – У запропонованому рішенні має бути передбачена можливість відключення потенційно шкідливих перевірок. – Запропоноване рішення повинно автоматично запускати і зупиняти сканування за розкладом без втручання користувача. – Запропоноване рішення повинно дозволяти припиняти і відновлювати сканування вручну. – Запропоноване рішення повинно дозволяти запускати сканування, незавершене у встановлений термін, або переносити на наступний запланований період. – Запропоноване рішення повинно мати можливість приймати цілі сканування в різних форматах, включаючи імена DNS, діапазони IP-адрес і класи IP, а також попередньо визначені списки активів. Наприклад, 10.0.1.1 - 10.0.1.100. Також повинен підтримуватися імпорт списку IP-адрес, що містяться в файлі. – Запропоноване рішення повинно підтримувати сканування IPv6 з пасивним виявленням активів IPv6. – Запропоноване рішення повинно забезпечувати можливість відключення сканування периферійних пристроїв, наприклад принтерів. – Запропоноване рішення повинно забезпечувати можливість пасивного сканування: ▪ Пасивний сканер повинен включати можливість виявлення нових активів шляхом моніторингу мережевого трафіку без активного сканування. ▪ Пасивний сканер повинен відображати виявлені в трафіку активи в реальному часі.

	▪ Пасивний сканер повинен надавати інформацію про окрему мережу, мережі в цілому або будь-якої конкретної групи хостів. ▪ Пасивний сканер повинен мати можливість відправляти події, пов'язані з трафіком, через системний журнал в системи кореляції подій. ▪ - Пасивний сканер повинен поставлятися тим же виробником, що і основна система.
Функціонал роботи з активами	– Запропоноване рішення повинно підтримувати можливість виявлення активів, що не використовують ліцензію. – Запропоноване рішення повинно забезпечувати можливість активного сканування і пасивного моніторингу мережі для виявлення активів. – Запропоноване рішення повинно вміти виявляти мобільні пристрої. – Запропоноване рішення не повинно покладатися на сторонні сканери для виявлення активів, сканування портів або ідентифікації ОС. – Запропоноване рішення повинно забезпечувати виявлення веб-служб і служб баз даних. – Запропоноване рішення повинно вміти виявляти служби, що працюють на нестандартних портах. – Запропоноване рішення повинно вміти виявляти служби, в яких не відображаються банери підключення. – Запропоноване рішення повинно бути здатна тестувати кілька примірників однієї й тієї ж служби, що працює на різних портах. – Запропоноване рішення повинно вміти сканувати «мертві» кінцеві точки (пристрої, що не відповідають на ICMP запити). – Запропоноване рішення повинно підтримувати необов'язкове використання netstat для швидкого і точного перерахування відкритих портів в системі при наданні облікових даних. – Запропоноване рішення повинно підтримувати використання SMB і WMI для сканування систем Windows. – Запропоноване рішення повинно мати можливість автоматично запускати служби віддаленого реєстру в системах Windows при виконанні сканування з обліковими даними, а потім автоматично зупиняти службу після завершення сканування. – Запропоноване рішення повинно підтримувати безпечне з'єднання(ssh) з можливістю підвищення привілеїв для сканування вразливостей і аудиту конфігурації в системах Unix. – Запропоноване рішення повинно мати можливість збирати/імпортувати і відображати дані про активи IT і OT мереж в єдиній консолі. – Запропоноване рішення повинно забезпечувати можливість налаштування політик сканування для мінімального впливу на мережі і цілі сканування.

		– Запропоноване рішення повинно забезпечувати виявлення точок бездротового доступу (WAP) за допомогою активного і пасивного сканування. – Запропоноване рішення повинно забезпечувати можливість виявлення нових пристроїв і відправки попереджень за допомогою електронної пошти, системного журналу або консольним повідомленнями. – Запропоноване рішення повинно забезпечувати можливість автоматичного запуску сканування нових пристроїв. – Запропоноване рішення повинно підтримувати використання агента для аудиту SCAP. – Запропоноване рішення повинно мати можливість виявляти всі активи, не використовуючи ліцензії, а потім мати можливість вибирати, які активи сканувати на вразливості.
	Вимоги до Агентів	– Агент повинен збирати та відправляти дані на центральну консоль для зменшення навантаження на мережу та кінцевий пристрій – Агенти можуть бути підключені та управлятися як через локальну консоль, так і хмарну – Агент повинен мати можливість встановлюватися у хмарних середовищах, таких як AWS та Azure. – Агент повинен надавати можливість регулювати власне навантаження на кінцеву точку, для запобігання порушення робочих процесів. – Агент повинен мати можливість з'єднуватись з консоллю через проксі сервер. – Агент повинен мати можливість встановлюватись через сторонні рішення такі як Active Directory або SCCM. – Запропоноване рішення повинно мати можливість створювати групи агентів для автоматизації процесу виявлення вразливостей. – Запропоноване рішення повинно надавати інформацію відносно статусу агентів. – Агент повинен мати унікальний ідентифікатор для виявлення одного і того пристрою в різних підмережах.
	Вимоги до функціоналу аудиту на відповідність	– Запропоноване рішення повинно підтримувати аудит на відповідність як з автентифікацією, так і без автентифікації, з або без необхідності встановлення агента на стороні клієнта на кінцевій точці. – Запропоноване рішення не повинно покладатися на сторонні сканери для аудиту/оцінки конфігурації безпеки. – Запропоноване рішення повинно надавати єдине представлення про всі результати аудиту вразливостей і відповідності вимогам. – Запропоноване рішення повинно забезпечувати аудит конфігурацій для відповідності нормативним вимогам та іншим галузевим стандартам і стандартам кращої практики постачальників.

		– Запропоноване рішення повинно забезпечувати аудит конфігурації, що базується на кращих практиках для таких постачальників, як Microsoft, Cisco і VMware. – Запропоноване рішення повинно забезпечувати аудит VMWare ESXi і vCenter за допомогою VMWare SOAP API. – Запропоноване рішення повинно забезпечувати аудит операційних систем Microsoft для перевірки параметрів безпеки і конфігурацій. – Запропоноване рішення повинно забезпечувати аудит всіх основних операційних систем Unix для перевірки параметрів безпеки і конфігурацій. – Запропоноване рішення повинно забезпечувати аудит баз даних для перевірки параметрів безпеки і конфігурацій таких як: PostgreSQL, MongoDB, Microsoft SQL, DB2, Sybase, Oracle, MySQL – Запропоноване рішення повинно забезпечувати аудит додатків для перевірки параметрів безпеки і конфігурацій таких як: Internet Explorer, Microsoft Edge, Google Chrome, Microsoft Office и т.д. – Запропоноване рішення повинно забезпечувати аудит мережевої інфраструктури для перевірки параметрів безпеки і конфігурацій таких як: Cisco, Arista, HP, F5 і т.д. – Запропоноване рішення повинно забезпечувати аудит певних продуктів безпеки кінцевих точок на предмет статусу установки і оновлення. – Запропоноване рішення повинно забезпечувати аудит особистої інформації (PII) і іншого конфіденційного контенту. – Запропоноване рішення повинно дозволяти налаштовувати політики аудиту відповідно до потреб організації. – Запропоноване рішення повинно надавати можливість проведення аудитів на відповідність стандартам CIS. – - Запропоноване рішення повинно надавати можливість проведення аудитів на відповідність стандартам DISA STIG.
	Візуалізація даних та звітність	– Запропоноване рішення повинно включати налаштовуванні графічні панелі і створені шаблони панелей для відображення вразливостей і стану безпеки. – Запропоноване рішення повинно забезпечувати налаштовуваний тренд результатів сканування на інформаційних панелях з використанням відфільтрованих результатів для визначення декількох ліній тренда на одному графіку. – Запропоноване рішення повинно дозволяти кожному користувачеві створювати кілька користувальницьких інформаційних панелей. – Елементи інформаційної панелі повинні легко змінюватись шляхом фільтрації, для відображення даних на основі списку активів, перевірок

		вразливостей або відповідностей, часу, пошуку за ключовими словами, IP-адреси і т.д. – Частота оновлення інформаційних панелей повинна налаштовуватись, для оновлення за розкладом. – Запропоноване рішення повинно забезпечувати можливість імпорту / експорту шаблонів інформаційних панелей. – Запропоноване рішення повинно надавати можливість додавати різні персоналізовані візуальні елементи для налаштування інформаційних панелей, включаючи кругові діаграми, гістограми, матриці і тенденції. – Запропоноване рішення повинно надавати користувачам можливість спільно використовувати інформаційні панелі. – Запропоноване рішення повинно надавати інтернет ресурс для завантаження інформаційних панелей, який включає шаблони: присвячені різним рівням користувачів, стандартам відповідності та засобів управління безпекою. – Запропоноване рішення повинно підтримувати налаштування параметрів шаблону і форматування інформаційних панелей. – Запропоноване рішення повинно підтримувати створення звітів, що налаштовуються з використанням шаблонів, наданих постачальником, або без шаблонів. – Запропоноване рішення повинно забезпечувати можливість фільтрації результатів в звітах по різним критеріям, включаючи, але не обмежуючись списками активів, репозиторіями, адресами, типами вразливостей, необробленим текстом і полями дат. – Запропоноване рішення повинно надавати вбудовані звіти про сканування та журнали системи. – Запропоноване рішення повинно забезпечувати можливість повної автоматизації звітів, включаючи виконання і відправлення за розкладом, а також відправлення звітів після сканування. – Запропоноване рішення повинно забезпечувати можливість перегляду результатів в консолі, незалежно від процесу створення звітів. – Запропоноване рішення повинно підтримувати можливість створення звітів в наступних форматах: PDF, CSV, RTF. – Запропоноване рішення повинно забезпечувати можливість налаштовувати та відображати тенденції результатів сканування в звітах на одному графіку. – Запропоноване рішення повинно надавати матричні таблиці, підсумовуючи числа по різним фільтрованим наборам результатів. – Запропоноване рішення повинно забезпечувати автоматичне відправлення звітів для аналітика безпеки на відповідність стандартам.

	– Запропоноване рішення повинно надавати звіти про відповідність нормативним вимогам без додаткових витрат. – Звіти повинні мати можливість включати імена пристроїв (NetBIOS, DNS) разом з IP-адресами. – Запропоноване рішення повинно забезпечувати можливість шифрування і захисту звітів паролем. – Запропоноване рішення повинно забезпечувати можливість автоматичної відправки звітів по електронній пошті. – Запропоноване рішення повинно забезпечувати можливість відправки звітів за допомогою служб веб-публікації. – Запропоноване рішення повинно дозволяти завантажувати та додавати зображення для створення звіту. – Запропоноване рішення повинно надавати звіти високого рівня щодо показників безпеки і відповідностей стандартам.
Автоматизація	– Запропоноване рішення повинно забезпечувати повну автоматизацію сканування, створення звітів і попереджень. – Запропоноване рішення повинно мати окремі панелі для відображення вразливостей виявлених: активно, скануванням на відповідність і в мобільних пристроях. – Запропоноване рішення повинно об'єднувати результати окремих сканувань вразливостей з можливістю фільтрації, щоб забезпечити можливість деталізації та проведення аналізу. – Запропоноване рішення повинно мати окремі представлення активних і усунених вразливостей з автоматичним перенесенням вразливостей з активних на усунуті після того, як сканування визначає, що вразливості більше немає. – Запропоноване рішення повинно мати можливість відзначати вразливість як раніше усунуту, але яка з'явилася знову, це може статися, коли система відновлюється з резервної копії або стара копія віртуальної машини повертається в оперативний режим. – Запропоноване рішення повинно забезпечувати комплексну фільтрацію виявлених вразливостей з можливістю деталізації по наступним параметрам, але не обмежуватись ними: IP адреса, ідентифікатор агента, актив, аудит файл, ідентифікатор CCE, ідентифікатор CVE, оцінка CVSS v2, оцінка CVSS v3, Ім'я DNS, доступність експлойта, порт, протокол, рівень критичності, дата першого виявлення, дата останнього виявлення, текст вразливості. – В запропонованому рішенні має бути можливість додавати теги до активів, політик, облікових даних або запитів з налаштованим описом для поліпшення фільтрації та управління об'єктами.

		– Запропоноване рішення повинно мати панель для аналітика безпеки, яка автоматично встановлює пріоритети та оптимізує рішення для виправлення вразливостей, а саме надає відсоткове значення зменшення ризиків, при закритті вразливостей на групі пристроїв. – Запропоноване рішення повинно надавати користувачам можливість запускати сканування на предмет виправлення вразливості, щоб переконатися, що вона усунута без необхідності налаштування параметрів сканування. – Запропоноване рішення повинно забезпечувати можливість автоматичного групування кінцевих точок, тобто створення динамічних списків активів, що базується на результатах сканування, по наступним критеріям, але не обмежуватись ними: IP адреса, ім'я DNS, тип ОС, рівень критичності вразливості, порт, доступність експлойту, дата першого виявлення, дата останнього виявлення, текст вразливості. – Запропоноване рішення повинно дозволяти користувачеві приймати ризик (робити виняток) з налаштованими датами закінчення терміну дії виявленої вразливості або змінювати рівень ризику (критичності) до рівня, що відрізняється від того, який постачальник визначив для цієї вразливості. – Запропоноване рішення повинно забезпечувати функцію створення задач та можливість інтеграції зі сторонніми системами для відслідковування задач. – Запропоноване рішення повинно підтримувати призначення задач окремим користувачам. – Запропоноване рішення повинно забезпечувати можливість сповіщення про вразливість і подію. – - Запропоноване рішення повинно підтримувати створення сповіщень на основі результатів сканування вразливостей або аудиту конфігурації. Сповіщення має включати: налаштовуваний електронний лист з декількома змінними контексту, створення задач, запуск сканування, створення події в системному журналі, створення звіту та повідомлення користувачів.

Автентифікація та рольовий доступ	– Запропоноване рішення повинно забезпечувати управління доступом на основі ролей, щоб контролювати доступ користувачів до певних наборів даних і функцій, доступним цим користувачам. – Запропоноване рішення повинно дозволяти адміністраторам визначати ролі в залежності від посадових обов'язків і відповідних рівнів доступу до функцій. – Запропоноване рішення повинно мати можливість інтеграції з LDAP для аутентифікації користувача. – Запропоноване рішення повинно підтримувати кілька серверів LDAP для аутентифікації. – Запропоноване рішення повинно підтримувати Security Assertion Markup Language (SAML), щоб забезпечити кілька варіантів єдиного входу / аутентифікації, таких як Shibboleth і Okta. – Запропоноване рішення повинно мати докладний звіт щодо активності користувачів. – Запропоноване рішення повинно дозволяти адміністраторам обмежувати доступ для окремих користувачів або груп до певних списків активів, політикам сканування і репозиторіїв вразливостей. – Запропоноване рішення повинно дозволяти адміністраторам призначати ресурси для кожного користувача або групи, наприклад політики сканування, списки активів, запити та облікові дані. – Запропоноване рішення повинно дозволяти адміністраторам обмежувати дозвіл на проведення: повного сканування, сканування з використанням певних політик. – У запропонованому рішенні має бути передбачена можливість планування часу, щоб запобігти сканування в заборонені години. – Запропоноване рішення повинно підтримувати створення організацій з повним поділом даних між цими організаціями в межах однієї консолі. – Запропоноване рішення повинно надавати можливість визначати обмеження для діапазону IP-адрес для кожної організації. – Запропоноване рішення повинно забезпечувати можливість прийняття та зміни ризику вразливостей.
Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **12 місяців**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт або електронною поштою для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ Можливість реєстрації сервісних випадків в режимі 24x7 в системі підтримки Виробника.

	Вимоги до супутніх робіт	**Виконавець повинен:** ▪ Спільно з Замовником здійснити оцінку впливу ідентифікованих вразливостей на IT-інфраструктуру ▪ Надати технічну підтримку для усунення ідентифікованих вразливостей ▪ Розробити та передати замовнику Паспорт поточної системи ▪ Розробити та передати План BCP (business continuity plan) **Розробити та передати План DRP (data recovery plan)**

Додаток 2

Кваліфікаційні критерії процедури закупівлі та перелік документів, що підтверджують інформацію учасників про відповідність їх таким критеріям

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
1.	**Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) договору (договорів)**	Довідка в довільній формі за підписом уповноваженої особи учасника, завірена печаткою (у разі її використання), на фірмовому бланку (у разі наявності) про наявність досвіду виконання аналогічного (аналогічних) договору (договорів)* із зазначенням: найменування контрагента, предмету договору, дати укладання. На підтвердження виконання аналогічного (аналогічних) договору (договорів), який (які) зазначений (зазначені) в довідці, надаються копії: виконаного договору, видаткової (видаткових) накладної (накладних), листа-відгука, що підтверджують його виконання. ** Під аналогічним договором розуміється договір подібний за предметом закупівлі за період з 2014 року по теперішній час. Якщо в довідці учасник вказує декілька аналогічних договорів, то всі документи щодо підтвердження виконання таких договорів надаються щодо кожного із вказаних в довідці договорів.*
2.	**Інформація про технічні, якісні та кількісні характеристики предмета закупівлі**	Для підтвердження відповідності тендерної пропозиції технічним, якісним та кількісним характеристикам (вимогам) замовника Учасник у складі тендерної пропозиції повинен надати: 1) інформацію про можливість поставки товару з урахуванням технічних вимог; 2) авторизаційний лист (авторизаційна форма тощо) від виробника товару або його офіційного представника, дистриб'ютора в Україні, який підтверджує наявність у Учасника статусу партнера та права на здійснення продажу запропонованого Учасником товару, виданого на адресу Замовника із посиланням на процедуру закупівлі.

У разі участі об'єднання учасників підтвердження відповідності кваліфікаційним критеріям здійснюється з урахуванням узагальнених об'єднаних показників кожного учасника такого об'єднання на підставі наданої об'єднанням інформації.

Ініціатор закупівлі **М.А. Журбенко**

ТОВ «ВІ ЄМ ДЖІ»
ЄДРПОУ 40844268
+380 96 001 01 61
info@wmgroup.com.ua
wmgroup.com.ua

Вих. 11092023-04

Комерційна пропозиція
для СКП «Київтелесервіс»

Предмет закупівлі:

Пакети програмного забезпечення операційного центру кібербезпеки (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника)

№	Найменування товару/послуги	Од. виміру	Кіл-ть	Ціна без ПДВ	Сума без ПДВ
1	***Комплект програмної продукції Підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури у складі:***	комплект	1	4 505 000,00	4 505 000,00
	Tenable.sc - Subscription / Програмна продукція Tenable.sc – Subscription (TSC)	шт	1	4 275 642,00	4 275 642,00
	(10xFQDN) Tenable.io Web Application Scanning/Програмна продукція Tenable.io Web Application Scanning (TIO-WAS)	шт	1	229 358,00	229 358,00
2	***Роботи з впровадження та налаштування підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури***	шт	1	641 000, 00	641 000, 00
			Всього		5 146 000,00 UAH
			Податок на додану вартість (20%)		1 029 200,00 UAH
			Загальна сума з ПДВ		**6 175 200,00 UAH**

Загальна сума з ПДВ: Шість мільйонів сто сімдесят п´ять тисяч двісті гривень 00 копійок

Комерційний Директор Комар Олександр

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 171/09-2023
Від 11 09 2023 р.

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "СПЕЦІАЛЬНІ ТЕЛЕКОМУНІКАЦІЙНІ РІШЕННЯ"
02140 Київ, вул. Єлізавети Чавдар, буд. 1 оф.9,
тел.: 0503901809, www.st-solution.com.ua

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Пакети програмного забезпечення операційного центру кібербезпеки
(48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника)

Розділ	Асортимент, комплектність, якість	Кількість	Од. вим.	Ціна без ПДВ	Сума без ПДВ
Tenable/ВКТ					
1	TIO-WAS // (10xFQDN) Tenable.io Web Application Scanning/Програмна продукція Tenable.io Web Application Scanning	1	шт	231 881,00	232 340,00
2	TSC // Tenable.sc - Subscription (TSC)	1	шт	4 365 430,00	4 365 431,00
3	Роботи з впровадження ПП	1	шт	645 487,00	645 487,00
Всього					**5 242 798,00**
Податок на додану вартість					**1 048 559,60**
Загальна сума з ПДВ					**6 291 357,60**

З повагою,

Директор **С.С. Лівенцев**

Дата: 11.09.2023

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 142/09-2023
Від 11 09 2023 р.

ТОВ «ОПТІДАТА»
04071, м. Київ, вул. Межигірська, 22,
UA103226690000026004300941299
у філії ГУ по м. Києву та Київської області, АТ «Ощадбанк» ТВБВ 10026/020, МФО: 322669, ЄДРПОУ: 39693067

Вих№ 091423/1 від 14.09.2023

Спеціалізоване комунальне підприємство
«Київтелесервіс»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

У відповідь на Ваш запит від 06.09.2023 р, ТОВ «ОПТІДАТА» надає інформацію щодо орієнтовної вартості Пакетів програмного забезпечення підсистеми керування процесом пошуку та мінімізації впливу вразливості IT - інфракструктури Tenable.sc:

н/п	Найменування	Кіль кість	Од. вим	Ціна без ПДВ	Сума без ПДВ
1	TSC // Tenable.sc - Subscription (TSC)	1	шт	4 322 674,00	4 322 674,00
2	TIO-WAS // (10xFQDN) Tenable.io Web Application Scanning /Програмна продукція	1	шт	230 964,00	230 964,00
3	Послуги з налаштування	1	шт	654 461,00	654 461,00
				Всього	**5 208 099,00**
				Податок на додану вартість (%)	**1 041 619,80**
				Загальна сума з ПДВ	**6 249 718,80**

З повагою,
Генеральний директор
ТОВ «ОПТІДАТА»

Білик М.А.

info@optidata.com
www.optidata.com.ua

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 210/09-2023
Від 14 09 2023 р.

ПРОТОКОЛ № 75

засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 - 2023 роки

м. Київ «01» вересня 2023 року

ПРИСУТНІ:

Члени робочої групи:

А. Вовнюк
М. Журбенко
В. Жучков
В. Іцкович
С. Осіпов
О. Поліщук
Д. Рябіченко
Т. Самойленко
М. Спічка
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Електронна столиця» на 2019–2023 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (зі змінами) (далі – Програма), у 2023 році, а саме:

проєкт технічних вимог до закупівлі «Пакети програмного забезпечення операційного центру кібербезпеки» (пункт 16.22 «Створення та впровадження центру моніторингу та кібербезпеки міських сервісів його технічне обслуговування, моніторинг та підтримка сервісів, розширення та дооснащення» переліку завдань і заходів Програми).

2. Різне.

По питанню 1

СЛУХАЛИ:

М. Журбенко, який поінформував про необхідність закупівлі пакетів програмного забезпечення операційного центру кібербезпеки для потреб центру моніторингу та кібербезпеки міських сервісів та представив проєкт технічних вимог до закупівлі «Пакети програмного забезпечення операційного центру кібербезпеки» (пункт 16.22 переліку завдань і заходів Програми).

В обговоренні брали участь: Д. Рябіченко, Т. Самойленко.

УХВАЛИЛИ:

Рекомендувати спеціалізованому комунальному підприємству «Київтелесервіс» під час процедури закупівлі «Пакети програмного забезпечення операційного центру кібербезпеки» (пункт 16.22 переліку завдань і заходів Програми) використовувати проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 10, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1950 **Дата реєстрації** 01.09.2023
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 01.09.2023 (Протокол № 75 від 01.09.2023)

Кількість файлів: 2 **Кількість ЕП:** 20

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
01.09.2023 № 075-1950

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
Самойленко Тамара Анатоліївна **Кількість ЕП:** 2	04.09.2023 11:27:32 ; 04.09.2023 11:27:39 ;		04.09.2023 11:27:39
ВОВНЮК АНАТОЛІЙ ВІТАЛІЙОВИЧ **Кількість ЕП:** 2	04.09.2023 11:19:55 ; 04.09.2023 11:19:57 ;	04.09.2023 11:19:57 Погодив;	04.09.2023 11:19:57 Погодив
Жучков Василь Анатолійович **Кількість ЕП:** 2	01.09.2023 14:05:37 ; 01.09.2023 14:05:38 ;	01.09.2023 14:05:39 Погодив;	01.09.2023 14:05:38
Іцкович Вікторія Євгенівна **Кількість ЕП:** 2	01.09.2023 11:06:35 ; 01.09.2023 11:06:35 ;	01.09.2023 11:06:36 Погодив;	01.09.2023 11:06:35

Іцкович Вікторія Євгенівна **Кількість ЕП:** 2	01.09.2023 11:06:35 ; 01.09.2023 11:06:35 ;	01.09.2023 11:06:36 Погодив;	01.09.2023 11:06:35
Спічка Максим Олегович **Кількість ЕП:** 2	01.09.2023 10:49:28 ; 01.09.2023 10:50:11 ;	01.09.2023 10:50:13 Погодив;	01.09.2023 10:50:11
Поліщук Олег Федорович **Кількість ЕП:** 2	01.09.2023 09:56:28 ; 01.09.2023 09:56:30 ;	01.09.2023 09:56:30 Погодив;	01.09.2023 9:56:30 Погодив
РЯБІЧЕНКО ДМИТРО ВОЛОДИМИРОВИЧ **Кількість ЕП:** 2	01.09.2023 09:49:41 ; 01.09.2023 09:49:51 ;	01.09.2023 09:50:08 Погодив;	01.09.2023 9:49:51
Журбенко Максим Анатолійович **Кількість ЕП:** 2	01.09.2023 09:42:37 ; 01.09.2023 09:42:38 ;	01.09.2023 09:42:38 Погодив;	01.09.2023 9:42:38 Погодив

ОСІПОВ СЕРГІЙ КОСТЯНТИНОВИЧ **Кількість ЕП:** 2	01.09.2023 08:51:04 ; 01.09.2023 08:51:05 ;	01.09.2023 08:51:05 Погодив;	01.09.2023 8:51:05 Погодив
ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 2	01.09.2023 07:55:16 ; 01.09.2023 07:55:18 ;	01.09.2023 07:55:18 Погодив;	01.09.2023 7:55:18 Погодив