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 «14» листопада 2022 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 2019-2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 13.03.2022 №4547/4588)

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 №93 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 – 2022 роки у 2021 – 2022 роках від 9 листопада 2022р.

Очікувана мінімальна вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 20 020 100,00 (двадцять мільйонів двадцять тисяч сто гривень нуль копійок) без ПДВ.

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

Вид предмету закупівлі – програмне забезпечення.

Кількість – 3 комплекта.

Місце поставки програмного забезпечення – місто Київ.

Строк поставки програмного забезпечення – до 31.12.2022.

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 30 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 2 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 4 арк.

4. Додаток 4. Протокол №93 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 - 2022 роки у 2021 – 2022 роках на 4 арк
5. Додаток 5. Пояснення моделі ліцензування запропонованого програмного забезпечення Dynatrace на 2 арк.

Ініціатор закупівлі **М.А. Журбенко**

«ПОГОДЖЕНО»:

Головний бухгалтер **Г. А. Букша**

Провідний юрисконсульт **В. В. Тихонов**

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 2019-2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (у редакції рішення Київської міської ради від 13.03.2022 №4547/4588)

Загальні вимоги

Відповідно до поточних потреб Центру моніторингу та кібербезпеки міських сервісів включає але не обмежуватиметься наступними підсистемами, в рамках яких очікується досягнення наступних завдань:

1) Підсистема моніторингу IT-сервісів, яка призначена для моніторингу веб-додатків, додатків та контролю якості взаємодії користувачів із IT сервісами, забезпечення контролю продуктивності IT-сервісів (щонайменше критичних, з можливістю подальшого масштабування), забезпечення аналізу активності користувачів для ключових IT-систем.
   - Продовження строку дії пакетів програмної продукції для забезпечення сталого функціонування існуючого технічного рішення;
   - Розширення домену функціонування підсистеми щодо поточних та наявних активів Замовника;

2) Підсистема моніторингу та контролю дій привілейованих користувачів, що забезпечує організацію єдиної платформи для управління доступом адміністраторів і зовнішніх підрядників (з єдиною «точкою входу») в мережах існуючої IT-інфраструктури Замовника:
   - Продовження строку дії пакетів програмної продукції для забезпечення сталого функціонування існуючого технічного рішення;
   - Розширення домену функціонування підсистеми щодо поточних та наявних активів Замовника.

3) 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;
   - Розширення номенклатури послуг підсистеми (комплексна оцінка веб додатків Замовника на наявність потенційно шкідливих вразливостей).

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

Зазначене програмне забезпечення Системи повинно розгортатися на обладнані Замовника, з вже встановленими на ньому операційними системами та базами даних.

№ з/п	Найменування технічні характеристики та вимоги	Одиниця виміру	Кіль-кість
1.	Програмна продукція **Підсистеми моніторингу IT-сервісів** у складі: **- примірник програмної продукції** для забезпечення моніторингу IT-сервісів, що розміщені в інфраструктурі із загальним обсягом оперативної пам'яті не менш ніж 800 GB (за умови розподілення агентів блоками по 16Gb) строком дії не менше ніж 12 місяців – **1 од.**; **- примірник програмної продукції** для забезпечення контролю якості взаємодії користувачів із IT сервісами та моніторингу не менш ніж 1 000 000 сесій реальних користувачів 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 пристроїв/ систем 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
Архітектура та форм-фактор	– Запропоноване рішення має мати можливість бути реалізовано у вигляді віртуалізованого або програмно-апаратного рішення; ▪ Якщо запропоноване рішення являє собою віртуальну машину, то вона буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником (заздалегідь має погоджуватися обсяг необхідних ресурсів); – Запропоноване рішення має забезпечувати відмовостійкість (high availability): ▪ Підтримка об'єднання декількох систем в один логічний кластер для відмовостійкості; ▪ Можливість створення Active/Active та Active/Passive кластеру.
Ліцензування	– Запропоноване рішення повинно бути ліцензоване для підтримки роботи не менше ніж 3 аналітиків та підтримувати збільшення кількості аналітиків, що будуть працювати у системі при додатковому ліцензуванні;
Функціональні вимоги	– Має забезпечувати моніторинг взаємодії користувачів із IT сервісом через наступні канали: веб, мобільна версія сайту, мобільний застосунок; – Запропоноване рішення повинно мати вбудований механізм автоматичного виявлення всіх компонентів сервісу, та будувати

		зв'язки між ними через весь IT-стек: хости, процеси, сервіси і застосунки; – Запропоноване рішення повинно автоматично виявляти всі процеси, які виконуються на хості, незалежно від технології, яка використовується; – має автоматично інтегрувати метрики моніторингу застосунків, хостів, CPU, мережі, дискової підсистеми, віртуалізації, ЦОД в єдину модель даних; – Запропоноване рішення повинно збирати інформацію із лог-файлів та мати вбудований механізм для централізованого їх зберігання; – Запропоноване рішення повинно забезпечувати проактивний моніторинг роботи IT сервісу, із можливістю швидкого виявлення проблем, аналізу їх впливу на взаємодію користувачів із IT сервісом та інформування про причину такої проблеми; – Запропоноване рішення повинно мати вбудовані механізми пріоритезації проблем, в залежності від рівня їх впливу на роботу IT сервісу та взаємодії користувачів із ним – За рахунок вбудованих алгоритмів кореляції запропоноване рішення повинно виявляти причину(и) проблем в роботі IT сервісу; – має показувати всі операції між компонентами IT сервісу, а також взаємодію цих компонентів їх зовнішніми сервісами; – Запропоноване рішення повинно будувати графіки та звіти на базі даних, що зібрано під час моніторингу IT сервісу; – Запропоноване рішення повинно мати вбудований механізм автоматичного розрахунку «базової лінії» (baseline) для метрик моніторингу; – Запропоноване рішення повинно давати можливість створювати панелі моніторингу (dashboards) із різним рівнем доступу і деталізації даних; – Запропоноване рішення повинно автоматично визначати та візуалізувати топологію на рівні ЦОД, хостів, процесів, сервісів, застосунків; – Запропоноване рішення повинно мати функціональність автоматичної ідентифікації наявності Docker Farm на хості та автоматичної інсталяції в Docker-контейнери, що запускаються без модифікації скриптів завантаження контейнерів; – Запропоноване рішення повинно мати вбудовану функціональність моніторингу дій реальних користувачів у застосунках; – Запропоноване рішення повинно мати вбудовану функціональність виявлення та аналізу вразливостей програмних елементів застосунку; – Запропоноване рішення повинно аналізувати та виконувати пріоритизацію вразливостей в залежності від критичності впливу за допомогою штучного інтелекту;

		– Запропоноване рішення повинно мати вбудований механізм налаштування та моніторингу показників SLO; – Запропоноване рішення повинно автоматично будувати шлях проходження транзакції (синхронної і асинхронної) з розбивкою за часом, витраченому на кожному з компонентів, які брали участь в транзакції; – Запропоноване рішення повинно надавати дані про методи, класи або API в рамках всієї транзакції, за принципом end-to-end; – Запропоноване рішення повинно мати можливість об'єднувати розрізнені повідомлення про помилки в єдину сутність, з консолідованою інформацією про кореневі причини виникнення помилок, кількості користувачів, що постраждали від інциденту і проблемних компонентів IT сервісу додатків; – Запропоноване рішення повинно мати можливість візуального відтворювати процес розповсюдження проблеми по компонентам IT сервісу; – Запропоноване рішення повинно мати можливість ретроспективного аналізу проблеми з роботою сервісу з прив'язкою помилок і подій до часових проміжків і топології сервісів; – Запропоноване рішення повинно мати механізм автоматичного тегування об'єктів моніторингу; – Запропоноване рішення повинно мати вбудовану функціональність для централізованого збору та зберігання лог-файлів додатків з об'єктів моніторингу, з можливістю пошуку за подіями; – Запропоноване рішення повинно мати можливість надавати параметри методів і параметри SQL-запитів; – Запропоноване рішення повинно підтримувати автоматичний збір трейсів в Java у разі виявлення проблеми з продуктивністю компонентів додатку; – Запропоноване рішення повинно мати вбудовані механізми очищення, деперсоналізації і маскування чутливих даних, які можуть бути зібрані в процесі моніторингу; – Запропоноване рішення повинно мати можливість побудови звітів про доступність сервісів; – Запропоноване рішення повинно підтримувати можливість відправки звітів про стан сервісу за розкладом; – Запропоноване рішення повинно мати можливість графічного зображення даних компонентів моніторингу в режимі реального часу; – Запропоноване рішення повинно підтримувати функціональність створення довільно налаштованих графічних зображень даних моніторингу;

		– Запропоноване рішення повинно мати можливість організації рольового доступу до замаскованих даних, що зібрані в процесі моніторингу; – Запропоноване рішення повинно надавати деталізований доступ до інтерфейсу, з можливістю налаштування прав користування для кожної з ролей та для кожного із компонентів;
	Вимоги до архітектури	– Запропоноване рішення повинно мати єдиний веб-інтерфейс для взаємодії з усіма її компонентами і функціями; – Запропоноване рішення не повинно встановлювати більше одного агента на хост, моніторинг якого вона здійснює; – Агент моніторингу повинен бути універсальним для всіх технологій Замовника і однією інсталяцією має встановлювати всі необхідні компоненти IT сервісу: мережева взаємодія, ОС, лог-файли, процеси, служби, транзакції, застосунки, дії користувачів; – Агенти відразу після встановлення мають автоматично визначати які служби і процеси запущені на хості, визначити взаємозв'язки між ними і почати виконувати їх моніторинг; – Запропоноване рішення повинно містити механізми штучного інтелекту, що автоматично знаходять компоненти, що викликають проблеми та ідентифікують першопричини їх виникнення; – Запропоноване рішення повинно мати власний мобільний застосунок з функцією push для повідомлень у разі виникнення проблем; – Агент повинен мати можливість автоматично визначати такі типи змін в додатку: перезапуск процесу, новий реліз, зміна файлів релізу; – Агент повинен виконувати читання записів з журналів подій додатків, служб або процесів на тому хості, на якому він встановлений; – Управління, оновлення, чи зміна конфігурацій агентів має відбуватися централізовано з основного інтерфейсу управління, без необхідності будь-яких дій на хостах моніторингу; – Запропоноване рішення повинно підтримувати інтеграцію з системами рівня ServiceDesk для автоматичного відкриття / модифікації / закриття інцидентів; – Оновлення системи мають встановлюватися автоматично; – Запропоноване рішення повинно підтримувати роботу в кластері для високої доступності та балансування навантаження даних від агента; – Робота в режимі високої доступності має будуватися виключна за принципом active-active та будуватися виключно на вбудованих механізмах в середині системи, без необхідності використання чи конфігурування будь-якого стороннього ПЗ;

		– Запропоноване рішення повинно використовувати власну сховище для зберігання всіх даних моніторингу, без використання будь-якого стороннього ПЗ; – Платформа повинна мати відкритий та задокументований API для інтеграції із іншими системами.
	Вимоги до технічних характеристик для забезпечення роботи з інфрастр-ю Замовника	– Агент має підтримувати моніторинг веб-серверів MS IIS, NGNIX та Apache HTTP; – Агент має підтримувати можливість автоматичної інструментації застосунків без необхідності змін на рівні коду застосунків; – Агент має підтримувати моніторинг застосунків на Java; – Запропоноване рішення повинно підтримувати збір даних щодо стану хостів віртуалізації безпосередньо з Vmware vCenter; – Запропоноване рішення повинно ідентифікувати помилки javascript з деталізацією до рівня опису помилки та можливістю аналізу minifield файлів в веб-інтерфейсі; – Запропоноване рішення повинно підтримувати моніторинг баз даних Oracle та MySQL; – Агент моніторингу має автоматично збирати дані про стан хоста Docker; – Агент моніторингу має автоматично виявляти контейнери, що запускаються на хості Docker та автоматично виконувати інструментацію об'єктів всередині контейнера, без будь-яких додаткових конфігурації на хості Docker; – Агенти моніторингу мають автоматично встановлюватись в нові Docker контейнери, що запускаються на хості Docker, без будь-яких додаткових конфігурацій чи скриптів в середовищі Docker; – Моніторинг сервісів застосунка, що виконуються в контейнерах Docker повинен реалізовуватись без необхідності запуску додаткових контейнерів в цьому середовищі; – Моніторинг Kubernetes/OpenShift кластеру повинен бути реалізований за допомоги універсального агенту без додаткової конфігурації кластеру та без змін на рівні застосунку; – Можливість збору та візуалізації додаткових даних з Kubernetes/OpenShift та Docker за допомоги API; – Запропоноване рішення повинно підтримувати моніторинг Docker for Windows та Docker for Linux; – Запропоноване рішення повинно підтримувати автоматичний збір трейсів з Java, Golang, Node.js, PHP в разі виникнення проблеми в роботі компонента IT сервісу; – Агент моніторингу має працювати на ОС Windows та Linux; – Агент моніторингу має підтримувати моніторинг компонентів на Golang, .Net та ASP.NET, Java, PHP;

		– Агент моніторингу має підтримувати автоматичну інсталяцію агентів в контейнерних середовищах на Docker, CRIO, Garden; – Запропоноване рішення повинно повинна ідентифікувати користувачів у сесіях, якщо вони пройшли ідентифікацію в застосунку; – Функціональність моніторингу дій реальних користувачів повинна реалізовуватись через технологію javascript, без необхідності використання даних мережевого трафіку; – Запропоноване рішення повинно мати можливість діставати бізнес-метрики із технологічних транзакцій. – Запропоноване рішення повинно підтримувати автоматичне додавання агенту javascript у веб-сторінку застосунку для моніторингу дій реальних користувачів; – Автоматичне додавання агенту javascript у веб-сторінку повинно підтримуватись для Java, Node.js, Apache HTTP Server, MS IIS, NGINX; – Автоматичне додавання агенту javascipit для технології Apache не повинно потребувати ручної зміни чи конфігурації налаштувань httpd.conf та/або ручного створення додаткових файлів конфігурацій Apache; – - Автоматичне додавання агенту javascript для технології NGNIX не повинно потребувати додаткових змін чи конфігурації модулів NGNIX.
	Вимоги до моніторингу і контролю якості взаємодії користувачів із IT сервісами	– Запропоноване рішення повинно мати вбудований механізм запису та емуляції дій користувачів у застосунку; – Запропоноване рішення повинно мати механізм моніторингу дій реальних користувачів у застосунку; – В запропонованому рішенні має бути передбачений механізм повного візуального відтворення сесій реальних користувачів на веб-сайті, із можливістю покрокового аналізу кожної дії; – Запропоноване рішення повинно мати можливість візуального відтворення сесій кожного окремого користувача в додатку; – Моніторинг дій реальних користувачів у застосунку має включати логування всіх дій користувача під час його сесії, із прив'язкою до часу цієї дії та технологічними транзакціями, що виникли після цієї дії між компонентами IT сервісу; – Запропоноване рішення повинно мати можливість ідентифікації сесій окремих користувачів використовуючи їх унікальні ідентифікатори під час моніторингу користувачів; – Запропоноване рішення повинно мати можливість аналізувати дії користувачів в мобільних додатках iOS і Android; – Запропоноване рішення повинно мати вбудовану функцію штучних перевірок доступності веб-додатків, з можливістю запису

		послідовності дій і подальшого періодичного відтворення операцій користувачів в інтерфейсі; – Запропоноване рішення повинно виявляти гнівні кліки незадоволених користувачів у веб-застосунку; – Запропоноване рішення повинно мати вбудований алгоритм скорінгу дій користувача: в залежності від його досвіду взаємодії із застосунком. – Всі дані дій користувачів мають зберігатися в інфраструктурі Замовника;		
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **12 місяців** що включає: ▪ можливість оновлення та модернізації програмного забезпечення за допомогою автоматичних завантажень із серверів Виробника, не рідше ніж 1 раз на місяць; ▪ Інтернет-доступ до документації та технічних ресурсів, бази знань на офіційному веб-сайті компанії Виробника (розробника), при чому всі його загальнодоступні сторінки мають бути відкритими для користувачів із України; ▪ дистанційну підтримку від Виробника (розробника) за допомогою телефону чи Інтернет з необмеженою кількістю заявок; ▪ Постійний (24x7) доступ для відкриття заявок на надання технічної підтримки в персональному кабінеті, закріпленого за Замовником на офіційному веб-сайті компанії Виробника (розробника) програмного забезпечення віртуалізації; ▪ сервіс, що пропонується, не повинен залежати від Виробника інфраструктури (від наявності підтримки), на якій буде встановлено та працюватиме запропоноване рішення (у випадку програмної продукції); ▪ гарантований час первинної реакції на звернення рівня Critical в рамках критичної проблеми має бути не більше 4 (чотирьох) годин;		
2.	Програмна продукція **Підсистеми моніторингу та контролю дій привілейованих користувачів** для забезпечення одночасної роботи з відповідними контрольованими (цільовими) системами не менш ніж 70 (сімдесят) привілейованих користувачів в межах існуючої у Замовника інсталяції строком дії не менше ніж 12 місяців.		**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; – Запропоноване рішення має включати всі необхідні компоненти для побудови комплексу технічних засобів та програмного забезпечення (далі КТЗ) з високою доступністю: забезпечувати функціонування комплексу в цілому при виході з ладу будь-якого компонента, за рахунок механізмів автоматичного балансування навантаження та побудови кластеру(ів) високої доступності; – Запропоноване рішення має забезпечувати можливість розгортання КТЗ як на базі апаратних серверів так і у віртуальному середовищі VMware або Hyper-V поточних (підтримуваних виробником) версій; – Під час роботи, рішення повинно бути захищено від впливу інших систем, включаючи зміни та оновлення. – Запропоноване рішення повинно мати вбудований механізм захисту від несанкціонованого доступу до інформації що зберігається у КТЗ. Даний захист повинен забезпечувати використання спеціального ключа захисту (пароля або апаратного ключа) під час кожного запуску КТЗ (після вимкнення або перезавантаження). – Запропоноване рішення має забезпечувати вбудоване захищене сховище для збереження записаних сесій привілейованих користувачів, реквізитів доступу (логін, пароль, ключі, доменні імена тощо) до КТЗ і цільових систем, журналів подій. – Запропоноване рішення має забезпечувати можливість розгортання КТЗ без необхідності інтеграції з корпоративною службою каталогів (AD), тобто забезпечувати функціонування компонент КТЗ незалежно від функціонування корпоративного каталогу. – Запропоноване рішення має забезпечувати наявність окремого веб-порталу або додатку для налаштування та адміністрування. – Запропоноване рішення має забезпечувати можливість створення відмовостійких конфігурацій КТЗ на базі вбудованих технологій, використання сторонніх (зовнішніх) засобів для побудови таких (відмово стійких) конфігурацій – не допускається. – Запропоноване рішення має забезпечувати можливість створення резервних копій що мають включати в себе всі параметри та налаштування КТЗ, а також записані сесії привілейованих

		користувачів. Резервні копії мають створюватися з використанням шифрованих (захищених) протоколів обміну даними (наприклад, на базі пари відкритого та приватного SSH ключа). Створені резервні копії повинні бути захищені від несанкціонованого перегляду даних що в них зберігаються та несанкціонованого відновлення. – Запропоноване рішення має забезпечувати підтримку розширених мережевих налаштувань для серверів КТЗ, що виконують такі функції: ▪ підтримка віртуальних мереж (VLAN); ▪ агрегація мережевих каналів; ▪ налаштування статичної маршрутизації для окремих мереж. – Запропоноване рішення має обов'язково забезпечувати можливість створення безпечних (шифрованих) каналів зв'язку на основі сертифікатів SSL між привілейованими користувачами і Системою та між Системою і цільовими системами. – Запропоноване рішення має забезпечувати можливість налаштування таких безпечних (шифрованих) каналів зв'язку по наступним параметрам: ▪ на основі само підписних сертифікатів (за допомогою пари «відкритий»-«приватний» ключі) ▪ на основі сертифікатів центру сертифікації (CA). – Схема кластеризації повинна надавати можливість взаємодії користувачів та інтеграцію в режимі Active-Active для всіх вузлів кластеру. – Записи привілейованих сесій не мають зберігатись у форматі відео або знімків екрану. – Рішення повинно записувати файли, що передаються через SFTP або буфер обміну в RDP підключеннях з можливістю відновлення їх у початковому вигляді. – Запропоноване рішення повинно мати експертний висновок Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів з технічного захисту інформації.
	Ліцензування	– Запропоноване рішення повинно включати усі необхідні ліцензії та підписки для забезпечення можливості одночасної роботи з відповідними контрольованими (цільовими) системами не менш ніж 50 (п'ятдесяти) привілейованих користувачів.
	Функціональні вимоги	– Запропоноване рішення має забезпечувати підтримку не менше двох одночасних систем зовнішньої автентифікації привілейованих користувачів та адміністраторів Системи – серверів служби каталогів користувачів AD та LDAP;

		– Запропоноване рішення має забезпечувати можливість задавати пріоритет використання кожного серверу каталогу користувачів (AD або LDAP), по відношенню до інших таких серверів; – Запропоноване рішення має забезпечувати можливість налаштування наступних параметрів пошуку користувачів у службах каталогів користувачів: ▪ ім'я та пароль користувача що має доступ на читання груп користувачів на сервері каталогу користувачів AD та LDAP; ▪ організаційна група (OU) в каталозі користувачів в якій потрібно шукати привілейованих користувачів; ▪ адресу (FQDN або IP) та порт серверу каталогу користувачів; ▪ можливість використання шифрованого (безпечного) з'єднання за допомогою сертифікатів. – Запропоноване рішення має забезпечити можливість включення/виключення доступу до буфера обміну на основі параметрів: ▪ час підключення; ▪ членство користувача в групі AD; ▪ IP-адреса робочої станції користувачів чи кінцевого сервера підключення. – Запропоноване рішення має забезпечувати можливість використання облікових записів з паролями для підключення до цільових систем що зберігаються в сторонніх (зовнішніх) сховищах паролів. – Запропоноване рішення має забезпечувати автоматичне надання окремим групам привілейованих користувачів доступу до пулу цільових систем на базі заданої групи на сервері каталогу користувачів (AD або LDAP). – Запропоноване рішення має забезпечувати веб-портал(-и) для доступу до контрольованих (цільових) систем. Використання даного порталу повинно бути опціональним (не обов'язковим), тобто КТЗ повинна забезпечувати доступ до контрольованих (цільових) систем в тому числі й без такого порталу (за допомогою використання спеціалізованих додатків: Putty, Kitty, SecureCRT, Windows RDP client, Royal TSX на Mac OS X, тощо). – Кожен веб-портал для привілейованих користувачів повинен надавати привілейованим користувачам наступні можливості: ▪ перелік доступних для підключення цільових систем з можливістю відкриття сесій за допомогою стандартних клієнтів (для RDP, VNC та SSH протоколів); ▪ перелік адрес (FQDN або IP) цільових систем; ▪ тип протоколу що використовується для підключення до цільової системи;

		▪ перегляд паролю до цільової системи (в разі якщо такі права надані привілейованому користувачу відповідною парольною політикою). – Запропоноване рішення має забезпечувати можливість додавання привілейованих користувачів такими способами: ▪ в ручному режимі; ▪ синхронізація з існуючого каталогу користувачів (AD/LDAP); – Для кожного облікового запису привілейованого користувача повинна бути підтримка одночасно кількох способів автентифікації, щонайменше: ▪ за допомогою статичного паролю що зберігається в захищеному сховищі Системи; ▪ одноразового паролю що генерується зовнішніми сервісами (наприклад, RADIUS-сервером); ▪ за допомогою зовнішнього каталогу користувачів (AD/LDAP); ▪ за допомогою SSH ключа; – Запропоноване рішення має забезпечувати функціональність додавання цільових систем, в процесі чого мають підтримуватися наступні можливості: ▪ додавання цільових серверів по одному (за IP-адресою або FQDN, мережевою маскою та портом); ▪ групового додавання цільових систем (за допомогою мережевої маски накладеної на діапазон IP-адрес). – Запропоноване рішення має забезпечувати роботу з цільовими системами, автентифікація привілейованих користувачів на яких виконується наступним чином: ▪ за допомогою введення локального облікового запису; ▪ за допомогою введення доменного облікового запису; ▪ за допомогою SSH-ключа. – Запропоноване рішення має забезпечувати наступні можливості роботи з реквізитами доступу (логіни, паролі, ім'я домену, ключі SSH тощо) що використовуються привілейованими користувачами для підключення до цільових систем: ▪ ручне створення та збереження реквізитів доступу в захищеному сховищі Системи; ▪ використання зовнішніх систем автентифікації (в тому числі – зовнішніх спеціалізованих сховищ паролів); – Запропоноване рішення має забезпечувати функціонал додаткової (повторної) примусової автентифікації на цільових системах навіть в разі якщо реквізити доступу привілейованих користувачів на Систему та на цільових системах повністю співпадають. – Запропоноване рішення має забезпечувати можливість примусової зміни паролів на окремих цільових системах за заданою парольною політикою для окремо заданих облікових записів привілейованих

		користувачів. Така парольна політика повинна забезпечувати можливості управління вимогами до: ▪ довжини паролю; ▪ складності паролю (в тому числі, вимоги до великих літер, цифрових символів, спеціальних символів); ▪ частоти зміни паролю. – Примусова зміна паролів відповідно до заданої парольної політики повинна підтримуватися щонайменше на таких цільових системах: ▪ Unix/Linux-based операційні системи (через SSH); ▪ Windows операційні системи (через WMI); – Запропоноване рішення має забезпечувати функціональність керування різноманітними об'єктами такими як користувачі, цільові системи, способи підключення як локально (за допомогою веб-порталу) так й віддалено (за допомогою відкритих API-інтерфейсів). – Запропоноване рішення має забезпечувати можливість вибору нумерації портів по яким підключаються привілейовані користувачі та портів по яким виконується підключення до цільових систем, тобто, адміністратор Системи повинен мати можливість примусової зміни портів підключення для привілейованих користувачів для кожної окремої або групи цільових систем.
	Функціонал контролю привілейованих користувачів	– Запропоноване рішення має забезпечувати запис дій привілейованих користувачів вбудованими засобами без необхідності встановлення буд-якого компоненту (агенту, сервісу, драйверу тощо) як на кінцеві робочі точки привілейованих користувачів, так й на системи до яких підключаються привілейовані користувачі (цільові системи). – Запропоноване рішення має забезпечувати можливість підтвердження незмінності записаних сесій привілейованих користувачів за допомогою спеціалізованих ключів/сертифікатів від довірених постачальників таких ключів/сертифікатів. – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу RDP, в тому числі – в режимах Enhanced RDP Security (TLS), SSH, Telnet, VNC. – Запропоноване рішення має забезпечувати можливість роботи зі стандартом X11 через протокол SSH, в тому числі – можливість відтворення графіки через X11. – Запропоноване рішення має забезпечувати можливість примусового обмеження чи запису файлових операцій (заборону протоколів файлового обміну SFTP та SCP). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколу Telnet у вигляді відеозапису або текстового журналу дій (команд користувача та відповідей цільової системи на такі команди).

		– Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколу RDP, SSH (або X11), VNC у вигляді відеозапису, та забезпечувати можливість: ▪ перегляду відеозаписів вбудованими засобами; ▪ експорту збережених відеоматеріалів (відеозаписів) в зовнішні відео формати в AVI або WEBM форматі, з заданою роздільною здатністю. – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу HTTP та HTTPS (з підтримкою стандартів SSLv2 та SSLv3). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколам HTTP та HTTPS у вигляді записаного текстового журналу дій (методи передачі даних POST/GET, посилання URL, контент (крім конфіденційних даних), відповіді серверів, дані cookies тощо). – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу ICA (з підтримкою стандартів SSLv2 та SSLv3). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколу ICA у вигляді відеозапису або текстового журналу дій (команд користувача та відповідей цільової системи на такі команди). ПЗ має забезпечувати можливість експорту збережених текстових журналів в зовнішні формати з текстовою структурою. – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем для роботи з додатками, які використовують службові протоколи підключення до MS SQL (з підтримкою стандартів TDS - Tabular Data Stream). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколам MS SQL у вигляді текстового журналу дій (команд користувача та відповідей цільової системи на такі команди). – Запропоноване рішення має забезпечувати можливість створення політик щодо команд які вводять привілейовані користувачі під час роботи з цільовими системами. ПЗ має забезпечувати підтримку синтаксису регулярних виразів на базі PCRE. – Запропоноване рішення має забезпечувати можливість налаштування щонайменше наступних правил реагування на спрацювання таких політик: повідомлення відповідальної особи, роз'єднання сесії.

		– Запропоноване рішення має забезпечувати можливість створення політик щодо часових інтервалів в які привілейовані користувачі мають можливість доступу до цільових систем. – Запропоноване рішення має забезпечувати можливість налаштування щонайменше наступних правил для таких політик: дні тижня в які привілейовані користувачі можуть підключатися до цільових систем, час коли привілейовані користувачі можуть підключатися до цільових систем, інтервал дії такої політики (з вказівкою початкових та кінцевих дат та часу). – Запропоноване рішення має забезпечувати можливість примусового запиту причини підключення до цільової системи привілейованим користувачем з відображенням відповідного поля для відповіді користувача. – Запропоноване рішення має забезпечувати можливість повідомлення зацікавлених сторін, якщо під час сеансу виявлено нетипову поведінку користувача – Запропоноване рішення має забезпечувати можливість налаштування додаткового підтвердження (схвалення) підключення до цільової системи привілейованих користувачів збоку адміністратора цільової системи. – Запропоноване рішення має забезпечувати можливість налаштування відправки повідомлень за допомогою каналів електронного зв'язку (email) адміністратора цільової системи щодо дії привілейованих користувачів (підключення до цільової системи, відключення від цільової системи, приєднання до сесії іншої особи, спрацювання заданої політики). – Запропоноване рішення має забезпечувати можливість повного примусового припинення роботи сесій привілейованих користувачів відповідальними особами в режимі реального часу. Також ПЗ має забезпечувати можливість налаштування блокувати обліковий запис привілейованого користувача сесія якого припиняється, одночасно з припиненням сесії привілейованого користувача.
	Візуалізація даних та звітність	– Запропоноване рішення має забезпечувати функціональність перегляду активних сеансів в режимі реального часу з можливістю його переривання. – Запропоноване рішення має забезпечувати вбудований фунціонал збереження та обробки подій в вигляді журналів що зберігаються в захищеному сховищі. – Всі журнали подій повинні бути захищені від видалення, в тому числі адміністраторами Системи з найвищими рівнями доступу (правами). Журнали подій повинні включати щонайменше наступну інформацію: ▪ події пов'язані з працездатністю КТЗ (в тому числі – журнали налагоджувань);

		▪ події пов'язані з роботою привілейованих користувачів на цільових системах; ▪ події пов'язані з адмініструванням КТЗ. – Запропоноване рішення має забезпечувати функціональність автоматичної передачі таких подій в зовнішні системи обробки подій в реальному часі за допомогою стандартних протоколів, таких як syslog, тощо. – Запропоноване рішення має забезпечувати можливість експорту повного або часткового журналу подій в зовнішній файл текстового формату. Частковий експорт повинен здійснюватися за різноманітними критеріями, за такими як обліковий запис привілейованого користувача(-ів), тип події, ім'я цільової системи, дата тощо. – Запропоноване рішення має забезпечувати вбудовані механізми перегляду результатів дій привілейованих користувачів, а саме – перегляд записаних сесій, команд що вводилися та відповідей цільової системи на такі команди. Перегляд результатів повинен забезпечуватися в веб-порталі адміністрування без необхідності встановлення буд-яких засобів (програмних додатків, плагінів тощо). – Запропоноване рішення має забезпечувати наявність вбудованих фільтрів пошуку результатів дій привілейованих користувачів за різноманітними критеріями, щонайменше за ім'ям привілейованого користувача або користувачів, введеними командами, типом протоколу, ім'ям цільової системи, а також в заданому діапазоні дат. – Запропоноване рішення має забезпечувати можливість створення звітів на базі отриманих результатів за заданими фільтрами. Такі звіти повинні мати можливість бути експортовано в вигляді файлів формату не меньше ніж: CSV форматі. – Запропоноване рішення має забезпечувати можливість перегляду відповідальними особами сесій привілейованих користувачів в режимі реального часу без будь-якого явного інформування привілейованих користувачів під час такого перегляду. Додатково має забезпечуватися можливість надавати відповідальній особі інформацію щодо сесії: ім'я та IP-адресу цільової системи, ім'я привілейованого користувача, тип протоколу що використовується, час початку сесії.
	Можливості інтеграції	– Запропоноване рішення має мати можливість інтеграції з іншими системами, в тому числі: CyberArk, Lieberman, Duo, Inwebo, Okta, Splunk, YubiKey, TPAM, ServiceNow, Remedy, Azure MFA, Azure AD, Azure KeyVault, AWS SecretsManagerVault, HashiCorpVault, Jenkins, Kubernetes. – Запропоноване рішення повинно мати інтерфейс для автоматизованого запиту паролей та доступу через REST API.

	Атентифікація та рольовий доступ	– Запропоноване рішення має забезпечувати рольову модель керування та нагляду за привілейованими користувачами. ПЗ має підтримувати наступні розмежування прав на базі різних облікових записів: ▪ повні права адміністрування – в тому числі – можливість конфігурування Системи; ▪ частково обмежені права адміністрування – буд-які дії крім конфігурування Системи; ▪ обмежені права адміністрування – можливість налаштувань та подальшого нагляду за конкретно заданими цільовими системами та привілейованими користувачами; ▪ права користувача - можливість тільки підключення до заданих цільових систем без можливості адміністрування (read only). – Запропоноване рішення має забезпечувати функціональність додавання адміністраторів з можливістю вибору ролі, строку дії облікового запису та способу автентифікації адміністратора. Для кожного облікового запису адміністратора повинна бути підтримка одночасно кількох способів автентифікації, щонайменше: ▪ за допомогою статичного паролю що зберігається в захищеному сховищі Продукту; ▪ за допомогою зовнішнього каталогу користувачів (AD/LDAP); ▪ за допомогою SSH ключа. – Повинна забезпечуватися підтримка аутентифікації користувачів через GSSAPI, Kerberos і Agent Forwarding в SSH сесіях. – Запропоноване рішення має забезпечувати можливість створення політик доступу на перегляд окремими привілейованими користувачами паролю(-ей) до цільових систем до яких вони підключаються, в разі якщо такий пароль їм невідомий. – Запропоноване рішення має забезпечувати вбудовані механізми перегляду таких паролів за будь-який потрібний час (в минулому) в разі якщо вони (паролі) змінювались за допомогою відповідного функціоналу ПЗ (парольної політики).
	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.

3.	Програмна продукція **Підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-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 третьо 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.

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 обладнання та матеріально-технічної бази**	Довідка в довільній формі за підписом уповноваженої особи учасника та завірена печаткою (у разі її використання) про наявність обладнання та матеріально-технічної бази, що будуть використовуватись для поставки товару, що є предметом закупівлі, із зазначенням найменування обладнання та матеріально-технічної бази, кількості та інформації про власність (власне/орендоване). Для підтвердження наявності матеріально-технічної бази необхідно надати скановані документи на право власності/користування офісу, технічного приміщення, складу чи іншого приміщення (документація має передаватися в PDF-форматі, сканована з оригіналу документу).
2.	**Наявність працівників відповідної кваліфікації, які мають необхідні знання та досвід**	Довідка в довільній формі за підписом уповноваженої особи учасника та завірена печаткою (у разі її використання), що підтверджує наявність в учасника працівників відповідної кваліфікації, які мають необхідні знання (вищу освіту) із зазначенням: посади, прізвища, ім'я, по батькові, освіти та загального стажу роботи.
3.	**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.*
4.	**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

№	Кваліфікаційний критерій	Перелік документів на підтвердження відповідності учасника встановленим кваліфікаційним критеріям
		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**

Додаток 3

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

Вих. №111122-1

Комерційна пропозиція

для СКП «Київтелесервіс»

№ п/п	Найменування товару	Кількість	Ціна за од., грн. без ПДВ	Ціна разом, грн. без ПДВ**
1	**Комплект програмної продукції Підсистеми моніторингу IT-сервісів** для забезпечення моніторингу IT-сервісів, що розміщені в інфраструктурі із загальним обсягом оперативної пам'яті 800 GB, забезпечення контролю якості взаємодії користувачів із IT сервісами та моніторингу 1 000 000 сесій реальних користувачів, включаючи технічну підтримку від Виробника строком на 12 місяців та супутні Послуги з інтеграції рішення в інфраструктуру Замовника	**1**	963 473,50	8 670 607,55
11	Примірник ПП Dynatrace - *Dynatrace - 1Year Term-per Host Unit - 1-25 Host Units* - з технічною підтримкою від Виробника строком на 12 місяців (DTR-MTU-PB-50-1Y)	50	157 288,45	7 864 422,50
12	Примірник ПП Dynatrace - *Dynatrace Term DEM-1Year Term-per M Annual Units - 0,3-2,4M* - з технічною підтримкою від Виробника строком на 12 місяців (DTR-SMT-PB-2,4-1Y)	1	806 185,05	806 185,05
2	**Комплект програмної продукції Підсистеми моніторингу та контролю дій привілейованих користувачів** для забезпечення одночасної роботи з відповідними контрольованими (цільовими) системами 70 (семидесяти) привілейованих користувачів в межах існуючої у Замовника інсталяції з технічною підтримкою від Виробника строком на 12 місяців	**1**	853 425,27	6 490 556,02
21	Примірник ПП ONE IDENTITY SAFEGUARD - ONE IDENTITY SAFEGUARD PRIVILEGED SECURITY BUNDLE PER IDM USER 24X7 MAINTENANCE RENEWAL PACK - з технічною підтримкою від Виробника строком на 12 місяців (BZI-BAL-KS-247)	50	77 280,88	3 864 044,00

WM.GROUP

22	Примірник ПП ONE IDENTITY SAFEGUARD - ONE IDENTITY SAFEGUARD PRIVILEGED SECURITY BUNDLE PER IDM USER LICENSE/24X7 MAINT PACK - з технічною підтримкою від Виробника строком на 12 місяців (BZI-BAL-PK-247)	20	97 387,77	1 947 755,40
23	Примірник ПП ONE IDENTITY SAFEGUARD - ONE IDENTITY SAFEGUARD SESSION VIRTUAL APPLIANCE 24X7 MAINTENANCE RENEWAL - з технічною підтримкою від Виробника строком на 12 місяців (BAO-BAL-PS-247)	1	508 995,57	508 995,57
24	Примірник ПП ONE IDENTITY SAFEGUARD - ONE IDENTITY SAFEGUARD PASSWORD VIRTUAL APPLIANCE 24X7 MAINTENANCE RENEWAL - з технічною підтримкою від Виробника строком на 12 місяців (BAS-BAL-PS-247)	1	169 761,05	169 761,05
3	**Комплект програмної продукції Підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури** для забезпечення роботи підсистеми у відповідності до технічних включаючи роботу функціоналу Web Application Scanning для 10 (десяти) FQDN з технічною підтримкою від Виробника строком на 12 місяців	**1**	4 858 936,43	4 858 936,43
31	Примірник ПП Tenable - Tenable.sc - Subscription - з технічною підтримкою від Виробника строком на 12 місяців (TSC)	1	4 565 051,63	4 565 051,63
32	Примірник ПП Tenable - (10xFQDN) Tenable.io Web Application Scanning - з технічною підтримкою від Виробника строком на 12 місяців (TIO-WAS)	1	293 884,80	293 884,80
		Загальна вартість Товару, грн. без ПДВ (**не оподатковується**)		**20 020 100,00**

Загальна вартість пропозиції, грн. 20 020 100 грн. 00 коп. (двадцять мільонів двадцять тисяч сто гривень 00 копійок)

Комерційний Директор Комар Олександр

IT-Solutions
Інновації, що змінюють

04050, м. Київ, вул. Студентська, 3
тел.: (044) 586-26-76
info@it-solutions.ua, www.it-solutions.ua

№ вихідного листа – №92/11-22 від 14.11.2022
ЗАМОВНИК – СКП «КИЇВТЕЛЕСЕРВІС»

КОМЕРЦІЙНА ПРОПОЗИЦІЯ

Пакети програмного забезпечення операційного центру кібербезпеки

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

н/п	Найменування	Кількість	Од. вим.	Ціна без ПДВ	Сума без ПДВ
Програмна продукція Підсистеми моніторингу та контролю дій привілейованих користувачів OneIdentity/ВКТ					
1	BAO-BAL-PS-247 // ONE IDENTITY SAFEGUARD SESSION VIRTUAL APPLIANCE 24X7 MAINTENANCE RENEWAL	1	шт	516 582.36	516 582.36
2	BAS-BAL-PS-247 // ONE IDENTITY SAFEGUARD PASSWORD VIRTUAL APPLIANCE 24X7 MAINTENANCE RENEWAL	1	шт	171 709.39	171 709.39
3	BZI-BAL-KS-247 // ONE IDENTITY SAFEGUARD PRIVILEGED SECURITY BUNDLE PER IDM USER 24X7 MAINTENANCE RENEWAL PACK	50	шт	78 736.45	3 936 822.50
4	BZI-BAL-PK-247 // ONE IDENTITY SAFEGUARD PRIVILEGED SECURITY BUNDLE PER IDM USER LICENSE/24X7 MAINT PACK	20	шт	99 222.04	1 984 440.80
Програмна продукція Підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури Tenable/ВКТ					
5	TSC // Tenable.sc - Subscription (TSC)	1	шт	4 651 033.11	4 651 033.11
6	TIO-WAS // (10xFQDN) Tenable.io Web Application Scanning / Програмна продукція Tenable.io Web Application Scanning	1	шт	299 420.02	299 420.02
Програмна продукція Підсистеми моніторингу IT-сервісів Dynatrace/ВКТ					
7	DTR-MTU-PB-50-1Y // Dynatrace - 1Year Term-per Host Unit - 1-25 Host Units - renewal	50	шт	159 732.45	7 986 622.50
8	DTR-SMT-PB-2.4-1Y // Dynatrace Term DEM-1Year Term-per M Annual Units - 0.3-2.4 M - renewal	1	шт	821 369.32	821 369.32
Всього					20 368 000.00
Податок на додану вартість (%)					0.00
Загальна сума з ПДВ					20 368 000.00

З повагою,
Технічний директор
ТОВ «АЙТІ-СОЛЮШНС»

Іван Зімін

Інновації, що змінюють

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 13411-2022
від 14 11 2022 р.

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ІНФОРМАЦІЙНА БЕЗПЕКА
ЄДРПОУ 40217886
ІПН 402178826580

Юр. адреса 04073, Київ, вул. Кирилівська 121-А
Від «Концепт»
+38 044 334 42 35
www.itis.net.ua

Вих.№ 202 від 14.11.2022р.

СКП «КИЇВТЕЛЕСЕРВІС»

Комерційна пропозиція

У відповідь на Ваш запит від 10.11.2022 щодо закупівлі - Пакети програмного забезпечення операційного центру кібербезпеки (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника), просимо розглянути нашу комерційну пропозицію:

Розділ	Асортимент, комплектність, якість	К-сть	Од. вим.	Ціна без ПДВ	Сума без ПДВ
Dynatrace/BKT					
1	DTR-MTU-PB-50-1Y // Dynatrace - 1Year Term-per Host Unit - 1-25 Host Units - renewal	50	шт	158 002,53	7 900 126,50
2	DTR-SMT-PB-2.4-1Y // Dynatrace Term DEM-1Year Term-per M Annual Units - 0.3-2.4 M - renewal	1	шт	812 923,80	812 923,80
Tenable/BKT					
3	TSC // Tenable.sc - Subscription (TSC)	1	шт	4 600 661,91	4 600 661,91
4	TIO-WAS // (10xFQDN) Tenable.io Web Application Scanning / Програмна продукція Tenable.io Web Application Scanning	1	шт	296 176,48	296 176,48
OneIdentity/BKT					
5	BAO-BAL-PS-247 // ONE IDENTITY SAFEGUARD SESSION VIRTUAL APPLIANCE 24X7 MAINTENANCE RENEWAL	1	шт	512 969,06	512 969,06
6	BAS-BAL-PS-247 // ONE IDENTITY SAFEGUARD PASSWORD VIRTUAL APPLIANCE 24X7 MAINTENANCE RENEWAL	1	шт	170 627,25	170 627,25
7	BZI-BAL-KS-247 // ONE IDENTITY SAFEGUARD PRIVILEGED SECURITY BUNDLE PER IDM USER 24X7 MAINTENANCE RENEWAL PACK	50	шт	77 883,72	3 894 186,00
8	BZI-BAL-PK-247 // ONE IDENTITY SAFEGUARD PRIVILEGED SECURITY BUNDLE PER IDM USER LICENSE/24X7 MAINT PACK	20	шт	98 147,45	1 962 949,00
Всього					**20 150 620,00**
Податок на додану вартість					**0,00**
Загальна сума з ПДВ					**20 150 620,00**

Загальна вартість пропозиції становить: 20150620,00 грн (двадцять мільйонів сто п'ятдесят тисяч шістсот двадцять гривень нуль копійок).

Умови поставки:

- Термін оплати: 100%-постоплата протягом 10 робочих днів з моменту поставки.
- Строк поставки: протягом 10 робочих днів з моменту підписання Договору.
- Гарантійна підтримка: 12 місяців.

З повагою
Генеральний директор
ТОВ «АЙТІС»

Федченко І.В.

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вихідний № 133/11-2022
від 14 11 2022 р.

ПРОТОКОЛ № 93

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 - 2022 роки у 2021 – 2022 роках

м. Київ «09» листопада 2022 року

ПРИСУТНІ:

Члени робочої групи:
В. Жучков
В. Іцкович
І. Лагутіна
Д. Рябіченко
О. Поліщук
Т. Самойленко
Д. Цвігун

ПОРЯДОК ДЕННИЙ:

1. Розробка та погодження проєктів технічних вимог до закупівель у межах виконання заходів Комплексної міської цільової програми «Електронна столиця» на 2019–2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512 (із змінами) (далі – Програма), у 2022 році, а саме:

доопрацьований 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:

О. Поліщука, який поінформував, що з метою підтримки роботи центру моніторингу та кібербезпеки міських сервісів необхідно провести закупівлю «Пакети програмного забезпечення операційного центру кібербезпеки» та

представив доопрацьований проєкт технічних вимог до цієї закупівлі (пункт 16.22 переліку завдань і заходів Програми).

В обговоренні брали участь: Д. Цвігун, В. Іцкович.

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 доопрацьований проєкт технічних вимог, розглянутий на засіданні робочої групи.

ГОЛОСУВАЛИ: «ЗА» - 7, «ПРОТИ» - 0, «УТРИМАЛОСЬ» - 0.

Протокол вела Тамара САМОЙЛЕНКО

Інформація про електронні підписи (ЕП)

№ документа 075-1912
Дата реєстрації 09.11.2022
Документ зареєстровано у картотеці: Вихідна
Вид документа: Лист
Стислий зміст:
Матеріали засідання робочої групи 09.11.2022 (Протокол № 93 від 09.11.2022)

Кількість файлів: 2
Кількість ЕП: 14

ДОКУМЕНТ СЕД АСКОД ІТС ЄІПК

Департамент інформаційно-комунікаційних технологій
09.11.2022 № 075-1912

Перелік електронних підписів

ПІБ	Дати і час нанесення ЕП	Погодження	Час останнього нанесення ЕП
РЯБІЧЕНКО ДМИТРО ВОЛОДИМИРОВИЧ **Кількість ЕП:** 2	09.11.2022 17:28:54 ; 09.11.2022 17:28:56 ;	09.11.2022 17:28:56 Погодив;	09.11.2022 17:28:56 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 2	09.11.2022 16:59:22 ; 09.11.2022 16:59:22 ;	09.11.2022 16:59:22 Погодив;	09.11.2022 16:59:22 Погодив
Іцкович Вікторія Євгенівна **Кількість ЕП:** 2	09.11.2022 16:59:22 ; 09.11.2022 16:59:22 ;	09.11.2022 16:59:22 Погодив;	09.11.2022 16:59:22 Погодив
ЖУЧКОВ ВАСИЛЬ АНАТОЛІЙОВИЧ **Кількість ЕП:** 2	09.11.2022 16:11:07 ; 09.11.2022 16:11:08 ;	09.11.2022 16:11:08 Погодив;	09.11.2022 16:11:08 Погодив

ЦВІГУН ДМИТРО ВІКТОРОВИЧ **Кількість ЕП:** 2	09.11.2022 15:16:32 ; 09.11.2022 15:16:33 ;	09.11.2022 15:16:33 Погодив;	09.11.2022 15:16:33 Погодив
Самойленко Тамара Анатоліївна **Кількість ЕП:** 2	09.11.2022 14:12:59 ; 09.11.2022 14:13:10 ;		09.11.2022 14:13:10
Поліщук Олег Федорович (2684213893) **Кількість ЕП:** 2	09.11.2022 14:00:02 ; 09.11.2022 14:00:03 ;	09.11.2022 14:00:03 Погодив;	09.11.2022 14:00:03 Погодив
ЛАГУТІНА ІННА ІГОРІВНА **Кількість ЕП:** 2	09.11.2022 13:55:10 ; 09.11.2022 13:55:11 ;	09.11.2022 13:55:11 Погодив;	09.11.2022 13:55:11 Погодив

Додаток 5

Моніторинг додатків та інфраструктури (хост-блоки)

Моніторинг додатків та інфраструктури Dynatrace забезпечується шляхом встановлення одногоDynatrace OneAgentна кожному контрольованому хості у вашому середовищі. OneAgent ліцензується на основі кожного хоста (віртуальний або фізичний сервер).

Однак не всі хости мають однаковий розмір. Більші хости споживають більше**одиниць хоста**, ніж хости меншого розміру. Ми використовуємо обсяг оперативної пам'яті на контрольованому сервері як вимірювальну паличку для визначення розміру хоста (тобто скільки хост-блоків він містить). Перевагою цього підходу є його простота — ми не беремо до уваги специфічні для технології фактори (наприклад, кількість JVM або кількість мікросервісів, розміщених на сервері). Не має значення, чи є господар . На основі NET, на основі Java або чогось іншого. Ви можете мати 10 JVM або 1,000 JVM; Такі фактори не впливають на обсяг моніторингу, який споживає навколишнє середовище.

OneAgent може працювати в двох різних режимах. За замовчуванням OneAgent працює в**режимі Full-Stack Monitoring.** Крім того, ви можете використовуватирежим моніторингу інфраструктури для моніторингухостів, які не потребують повної видимості. Інфраструктурний режим споживає менше хост-одиниць, ніж режим Full-Stack.

Приймаючі підрозділи

Зверніться до таблиці зважування головного блоку нижче, щоб побачити, скільки одиниць хоста споживається на основі обсягу оперативної пам'яті, яку має контрольований сервер. Загальне споживання хост-одиниці розраховується на основі суми всіх хост-одиниць всіх режимів і контрольованих систем. Детальніше про розподіл квоти на одиницюхоста дивіться у розділі Розподіл квот на одиницю хоста.

Оперативна пам'ять	Хост-блоки (Full-Stack[1])	Хост-блоки (інфраструктура)[2])
1.6 ГБ	0.10	0.03
4 ГБ	0.25	0.075
8 ГБ	0.50	0.15
16 ГБ	1.0	0.3

16 ГБ	1.0	0.3
32 ГБ	2.0	0.6
48 ГБ	3.0	0.9
64 ГБ	4.0	1.0
80 ГБ	5.0	1.0
96 ГБ	6.0	1.0
112 ГБ	7.0	1.0
nx16 ГБ	n	1.0

[1] Коли обсяг оперативної пам'яті на хості падає між значеннями, наведеними в таблиці вище, число округлюється в більшу сторону. Наприклад, хост з 12 ГБ оперативної пам'яті споживає 1 хост-блок, оскільки 12 ГБ падає від 8 ГБ до 16 ГБ.

[2] Для режиму моніторингу інфраструктури застосовується той самий принцип округлення. Якщо для вашої ліцензії хмарної інфраструктури ввімкнено обмеження хост-одиниці, кількість одиниць хоста, споживаних хостом, обмежена 1.0. Якщо у вас є існуюча угода, яка не відображає обмеження на кількість одиниць хоста на хост, будь ласка,зв'яжіться зі своїм торговим представником Dynarace. 1.0

Моніторинг лише для додатків, включаючи PaaS та деякі безсерверні

Перевитрати головного блоку (необов'язково)

Якщо ви організували виділення хост-одиниць для моніторингу ваших хостів і маєте право перевищити це число (тобто перевитрати дозволені для вашого облікового запису), перевитрати будуть розраховані в одиницю часу розміщення. Наприклад, якщо ви організували моніторинг до 10 хост-одиниць (максимум 160 ГБ загальної оперативної пам'яті) і ваш обліковий запис допускає перевитрати, якщо ви підключите інший хост, який дорівнює 2 хост-одиницям, у вас буде 12 хост-одиниць загалом і, отже, ви перевищите свою квоту на 2 хост-одиниці. Якщо ви продовжите стежити за своїми хостами за допомогою 12 хост-блоків протягом цілого тижня, ви нарахуєте перевитрату в розмірі 336 годин хоста.

Щоб додати або видалити перевитрати зі свого облікового запису, зверніться до компанії Dynatrace Sales. 2 (host units) x 24 (hours a day) x 7 (days) = 336 (host unit hours overage)