https://prozorro.gov.ua/tender/UA-2024-12-05-021049-a

*«Послуги з постачання антивірусного програмного забезпечення» (ДК 021:2015: 48760000-3: Пакети програмного забезпечення для захисту від вірусів)*

На виконання постанови КМУ від 11 жовтня 2016 р. № 710 «Про ефективне використання державних коштів» у зв'язку із необхідністю проведення закупівлі *«Послуги з постачання антивірусного програмного забезпечення» (ДК 021:2015: 48760000-3: Пакети програмного забезпечення для захисту від вірусів)* для потреб Департаменту економічного розвитку Львівської міської ради - забезпечити оприлюднення обґрунтування технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення на власному веб-сайті.

***1. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником:***

- «Послуги з постачання антивірусного програмного забезпечення» (ДК 021:2015: 48760000-3: Пакети програмного забезпечення для захисту від вірусів)

***2. Обґрунтування технічних та якісних характеристик предмета закупівлі:***

Розвиток електронного урядування, впровадження різних інструментів електронної демократії, а також технологій "розумного міста" у різних сферах життя є важливою складовою у розвитку сучасного європейського міста.

Електронне урядування забезпечує нові форми комунікації між громадянами, бізнесом та владою, безперешкодний доступ до публічної інформації сприяє участі громадян у процесах управління містом чи громадою, покращенню якості надання послуг населенню та наближенню їх до вимог мешканців.

З кожним роком формуються та, постійно оновлюючись і розширюючись, розвиваються технологічні сервіси муніципалітету, які на сьогодні охоплюють:

- офіційний сайт Львівської міської ради, електронні сервіси Гарячої лінії міста (веб-сайт та мобільний додаток) та інші веб-ресурси, впроваджені для інформування громадян про роботу виконавчих органів влади, доступу до адміністративних послуг та інших важливих муніципальних функцій, взаємодії мешканців з владою;
- сучасну систему електронного документообігу у муніципалітеті;
- електронні сервіси, які спрощують та пришвидшують систему комунікації між органами місцевої влади та мешканцями, роблять процеси відкритими та прозорими. Серед них, портал "Особистий кабінет мешканця", функціонал якого дозволяє замовляти адміністративні послуги у режимі онлайн;
- екосистема порталів та сервісів "Відкриті дані Львова", яка охоплює в себе Портал відкритих даних Львова, сайт "Панель міста", Геопортал Львова та чатбот City Helper Bot, які забезпечують доступ громадян до публічної інформації у різних зручних форматах;
- реєстр територіальної громади міста як основний ресурс, за допомогою якого реалізуються всі послуги, пов'язані з реєстрацією місця проживання населення;
- електронні сервіси для відстеження руху транспорту, які стали невід'ємними інструментами для пасажирів громадського транспорту, а також щораз популярнішим серед мешканців є електронний спосіб оплати проїзду у громадському транспорті, котрий реалізований за допомогою різних аплікацій та на завершальній стадії впровадження повноцінної автоматизованої системи оплати проїзду у громадському транспорті (електронний квиток);
- система муніципального відеоспостереження, яка щороку охоплює все більшу територію міста, використовуючи системи розпізнавання обличчя та номерних знаків автомобілів, та є невід'ємною складовою забезпечення громадського порядку у місті.

Відтак, проаналізувавши елементи електронного урядування, які впроваджені та функціонують у м. Львові, інших населених пунктах, які ввійшли до складу Львівської міської територіальної громади, а також нові виклики у сфері цифрової трансформації суспільства, пропонується нова Програма цифрового перетворення Львівської міської територіальної громади на 2021 – 2025 роки (надалі – Програма) та визначено її нові завдання.

Метою впровадження Програми є досягнення світових стандартів надання адміністративних та комунальних послуг, відкритості та доступності влади, ефективності управління господарством громади, з використанням інформаційних технологій у всіх сферах життєдіяльності.

Основними завданнями розвитку Програми є:

1. Забезпечення доступу до всіх електронних послуг та сервісів для мешканців усіх населених пунктів Львівської міської територіальної громади, зокрема через забезпечення безперешкодного доступу до високошвидкісного Інтернету у всіх населених пунктах та закладах соціальної інфраструктури на території Львівської міської територіальної громади.
2. Оновлення, консолідація та уніфікація програмних та технічних ресурсів для забезпечення гнучкості їх використання та надійної роботи інформаційно-комунікаційної інфраструктури.
3. Підтримка та вдосконалення системи інформаційної безпеки функціонування міських електронних сервісів.

4. Підвищення рівня автоматизації управлінських процесів Львівської міської ради, а також підпорядкованих комунальних підприємств та установ.
5. Впровадження електронних сервісів для оптимізації комунікації між мешканцями та виконавчою владою.
6. Впровадження проектів інформатизації для модернізації усіх сфер життєдіяльності Львівської міської територіальної громади.
7. Розвиток співпраці з ІТ-компаніями та асоціаціями ІТ-компаній.
8. Реалізація програм навчання та підвищення комп'ютерної грамотності мешканців.

**Враховуючи вищенаведене викикла необхідність у проведенні закупівлі ««Послуги з постачання антивірусного програмного забезпечення» (ДК 021:2015: 48760000-3: Пакети програмного забезпечення для захисту від вірусів) із наступними технічними та якісними характеристиками:**

**Програмна продукція Trend Micro (антивірусне програмне забезпечення)**

**Кількість: операція з постачання антивірусного програмного забезпечення – 1 шт. на 1600 (одна тисяча шістсот) користувачів**

## ВИМОГИ ДО ФУНКЦІЙ (ЗАДАЧ) АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

1. Підтримка операційних систем клієнтської частини: Windows 10 і новіші
2. Windows Server версії: починаючи від Microsoft Windows Server 2012 і новіші.
3. Централізована система управління (адміністрування) захистом робочих станцій, підключених до локальної мережі.
4. Безпека і шифрування команд при віддаленому адмініструванні на основі підпису агент-серверної комунікації цифровими сертифікатами.
5. Віддалене розгортання, конфігурування і адміністрування клієнтів на робочих станціях.
6. Відсутність ліцензійних обмежень на розгортання додаткових серверів віддаленого адміністрування.
7. Можливість створення в системі управління груп керованих комп'ютерів як вручну (на основі імен комп'ютерів), так і автоматично (на основі структури Active Directory або діапазонів IP-адрес).
8. Наявність функцій централізованого збору статистичної інформації про роботу антивірусного програмного забезпечення на робочих станціях.
9. Можливість експортувати певні журнали та / або події про роботу антивірусного програмного забезпечення на робочих станціях.
10. Можливість інтеграції з середовищем динамічного аналізу («пісочницями») того ж виробника.
11. Наявність сканеру файлів.
12. Можливість формування списків довірених додатків.
13. Можливість відключення сканування для довірених додатків.
14. Можливість виключити з перевірки файли і папки з конкретним шляхом.
15. Наявність поведінкового аналізатора, що дозволяє на підставі поведінки додатка зробити висновок, зловмисне воно чи ні.
16. Можливість додавати виключення зі сканування для модулю поведінкового аналізу.
17. Наявність технологій, що дозволяють по репутації файлу, його давності та розповсюдженості виносити вердикт про його зловмисності.
18. Можливість автоматичної зміни параметрів роботи при старті поза периметром корпоративної мережі.
19. Наявність резидентного монітору.
20. Використання евристичних технологій під час сканування та забезпечення захисту в режимі реального часу.
21. Захист від шпигунського та рекламного ПЗ.
22. Виявлення руткітів (прихованих файлів / системних аномалій).
23. Має містити модуль, який при виявленні змін, що були ініційовані зловмисним скриптом – здійснює дії усунення наслідків шкідливого впливу:
    - Видалення активних файлів-вірусів та троянів;
    - Видалення завантажених файлів зловмисним ПЗ;
    - Відновлення файлів, модифікованих троянами;
    - Зупинку процесів, запущених вірусами;
    - Видалення створених гілок системного реєстру або їх значень модифікованих зловмисними скриптами;
24. Система захисту повинна забезпечувати захист від наступних типів загроз:
    - Віруси
    - Трояни
    - Мережеві черв'яки

- Рекламні програми
- Шпигунські програми
- Програми - "дзвонилки"
- Програми-жарти
- Генератори піратських ключів
- Віруси-вимагачі та шифрувальники

25. Наявність моніторингу подій типу
    - Появи нової служби;
    - Поява нового об’єкту у списку автозапуску при старті ОС;
    - Ін’єкції сторонніх бібліотек у типові системні процеси;
    - Модифікацій системних файлів/процесів;
    - Появи файлів з іменами, що дублюють системні;
    - Зміну політик безпеки ОС, і т.п.

    та можливість задання автоматичної дії при виявленні подібної поведінки з переліку: дозвіл/блокування/запит дії у користувача за потреби. При цьому має бути можливість вказування часу застосування дії автоматично, якщо користувач не відповів на запит щодо дозволу чи блокування підозрілої поведінки.
26. Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.
27. Докладне журналювання, формування зведених звітів та звітів щодо кожної робочої станції.
28. Наявність антивірусної перевірки файлів в архівах форматів ARJ, UPX, MSCOMP, PKLite, ASPAC, DIET, LZEXE, ACE, BZIP, BZIP2, CAB, CHM, GZIP, LHA, RAR, TAR, ZIP, BIN, TD0.
29. Можливість сканування файлів під час запуску системи.
30. Можливість сканування за розкладом.
31. Можливість запуску антивірусного сканування по команді користувача з підзахисної машини або адміністратора з консолі централізованого управління.
32. Можливість відключення антивірусного захисту або окремих модулів захисту при необхідності.
33. Автоматична антивірусна перевірка змінних носіїв.
34. Можливість запуску завдань за розкладом.
35. Можливість регулювання розподілу ресурсів робочої станції між антивірусом і іншими додатками в залежності від рівня навантаження Центрального Процесора ЕОМ (паузи між скануванням файлів при досягненні порогових значень 20% або 50%).
36. Наявність захисту від ще невідомих шкідливих програм на основі аналізу їхнього поводження та контролю змін системного реєстру (поведінковий аналіз та модулю прогнозного машинного навчання).
37. Наявність захисту від ботнетів: виявляти шкідливі програми, аналізуючи їх схеми обміну даними і протоколи.
38. Розширений сканер пам'яті, який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами, або ж малорозповсюдженими програмами-архіваторами.
39. захист від RansomWare – автоматичне створення резервних копій модифікованих (шифрованих) файлів і відновлення їх у разі, якщо їх модифікує шкідлива програма-шифрувальник;
40. Наявність персонального міжмережевого екрану.
41. Міжмережевий екран повинен мати можливість блокувати мережевий трафік кінцевої точки не лише за IP, адресою, напрямком, портом призначення та іншими мережевими атрибутами, але і для визначених додатків за шляхом їх розміщення у файловій системі, а також за шляхом асоційованих гілок системного реєстру конкретного ПЗ.
42. Регламентне оновлення виробником системи баз даних загроз та програмних модулів в автоматичному режимі та/або за розкладом не менш ніж 24 рази на добу.
43. Можливість централізованого оновлення системи антивірусного захисту робочих станцій, підключених до локальної мережі з одного комп’ютера, який розташований в локальній мережі (проміжний сервер оновлень).
44. Можливість оновлення програмних засобів і антивірусних баз з різних джерел, як по каналах зв'язку, так і зі змінних носів інформації.
45. Можливість створення дзеркала оновлень та локального репозиторію файлової і веб-репутації для зменшення навантаження на зовнішні канали зв’язку.
46. Можливість налаштування часу оновлень і сканування в межах заданого терміну.
47. Наявність ієрархічної системи управління політиками з можливістю успадкування частини політик від батьківських груп.
48. Сервер адміністрування повинен підтримувати функціонал резервного копіювання та відновлення згідно наданої виробником інструкції.

49. Наявність антивірусного сканування трафіку за такими протоколами: FTP, HTTP, HTTPs і POP3 трафіку.
50. Можливість захисту веб-трафіку - перевірка об'єктів, що надходять на комп'ютер користувача при взаємодії з ресурсами мережі Інтернет.
51. Можливість блокування Інтернет-ресурсів за веб-адресою або IP-адресою.
52. Можливість захисту від зміни параметрів ПЗ паролем.
53. Наявність захисту від фішингу: захист від спроб отримати паролів та іншу конфіденційну інформацію, забороняючи доступ до шкідливим веб-сайтів, які приймають вид нормальних веб-сайтів.
54. Можливість імпорту для виявлення зловмисного ПЗ сигнатур у форматі- OpenIOC.
55. Наявність функції автоматичного сповіщення адміністраторів системи антивірусного захисту про виявлення шкідливого програмного забезпечення.
56. Можливість інтеграції з центром безпеки Windows.
57. Наявність технічного сервісу по надсиланню зразків нового шкідливого програмного забезпечення для проведення аналізу та надання рекомендацій.
58. Якщо модуль не здатний заблокувати шкідливий файл в автоматичному режимі, повинні бути запропоновані наступні механізми ручного стримування епідемії:
    - блокування файла по імені;
    - блокування запису в певні папки;
    - блокування мережевої взаємодії з певних портів;
    - блокування запису в мережеві папки.
59. Має бути реалізовано механізм відправки довільних повідомлень на підзахисних комп’ютер для інформування користувача адміністратором.

## ВИМОГИ ДО ПІДТРИМУВАНИХ ПОТЕНЦІЙНИХ КАНАЛІВ ВИТОКУ ДАНИХ

1. Функціонал має бути реалізований засобами єдиного з антивірусним агентом, без необхідності встановлення будь-якого додаткового ПЗ / агенту.
2. Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються “всередину” і “назовні” корпоративної мережі по протоколам як мінімум: SMTP, HTTP, HTTPS, FTP.
3. Підсистема захисту від витоків даних повинна бути здатна виявляти передавання конфіденційних даних в клієнтах електронної пошти (як мінімум Microsoft Outlook) та через веб-сторінки онлайн поштових сервісів.
4. Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються на друк.
5. Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що записуються на зовнішні накопичувачі: CD/DVD, USB Flash.
6. Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються по локальній мережі
7. Система повинна підтримувати як мінімум наступні види параметрів, за якими проводиться пошук конфіденційних даних:
    - Словник (в т.ч. споріднені слова за коренем, кількість входжень, співпадіння від вказаного за порядком символу)
    - Регулярні вирази
    - Метадані файлів
    - Номери банківських карт
    - Номери паспортів та інших регулярних алфавітно-цифрових комбінацій
8. Система повинна підтримувати експорт та імпорт налаштувань фільтрації у форматі XML
9. Система повинна забезпечувати наступні види реакції на виявлення в переданому файлі конфіденційних даних:
    - Блокування передачі
    - Фіксація факту передачі в журналі
    - Повідомлення Користувачу
    - Повідомлення Користувачу з полем введення, яке дозволяє зафіксувати в централізованому журналі виробничу необхідність для передачі конфіденційної інформації
    - Повідомлення Користувачу з готовими варіантами відповіді, яке дозволяє зафіксувати в централізованому журналі одну із заздалегідь вказаних адміністраторами причин, по якій Користувачу треба було передати конфіденційну інформацію.
10. Система повинна мати функціонал періодичного сканування визначених адміністратором каталогів на предмет знаходження в них файлів, що містять інформацію, яка порушує політики захисту від витоків

даних та фіксувати в журналі подій факти порушення або ж автоматично шифрувати виявлені файли заздалегідь вказаним паролем.

## ВИМОГИ ДО ЗАХИСТУ ВІД ВРАЗЛИВОСТЕЙ

1. Система захисту від вразливостей повинна забезпечувати можливості запобігання вторгненням на рівні мережі, націлених на вразливості як ОС так і стороннього програмного забезпечення встановленого на робочій станції.
2. Виробник антивірусного продукту має мати власну команду дослідників поширеного ПЗ та ОС на предмет наявності вразливостей, а не лише спиратись на результати досліджень сторонніх організацій.
3. Система повинна мати модуль захисту від вразливостей без установки окремого від антивіруса агента, щоб уникнути перенавантаження на кінцеві точки.
4. Система захисту повинна бути здатна конфігуруватися з метою активації тільки тих фільтруючих правил, які актуальні для даного комп'ютера або групи комп'ютерів.
5. Система захисту повинна забезпечувати роботи в режимах:
6. Inline (в розрив)
7. TAP (в режимі прослуховування трафіку та фіксації подій)
8. Система захисту повинна мати можливість вибору попередньо сконфігурованого профілю для захисту, наприклад, оптимізованого з точки зору безпеки або з точки зору продуктивності задля спрощення та прискорення впровадження.
9. Система має містити розділ з детальною конфігурацією дій щодо джерела з якого походять небезпечні команди, зокрема:
    - ESTABLISHED Timeout
    - LAST_ACK Timeout
    - Cold Start Timeout
    - UDP Timeout
    - Maximum TCP Connections
    - Maximum UDP Connections
    - Ignore Status Code
    - Block Same Src-Dest IP Address
    - Minimum Fragment Offset
    - Minimum Fragment Size
10. Перелік правил має містити назву правила, його статус (активовано / деактивовано), тип або сімейство ПЗ до якого правило може бути застосованим, індекс за глобальною класифікацією CVE, Microsoft CVE (якщо вразливість стосується ПЗ Microsoft), ступінь критичності CVSS, дату останнього оновлення правила, та інші.

## ВИМОГИ ДО КОНТРОЛЮ ДОДАТКІВ

1. Робота модулю повинна налаштовуватися як для окремих користувачів імпортованих з Active Directory (чи груп), так і для комп'ютерів в цілому.
2. Повинна бути можливість дозволити / заборонити повідомлення користувача про блокування
3. Підсистема повинна забезпечити наступні критерії визначення додатка:
    - Контрольна сума SHA1
    - Сертифікат цифрового підпису
    - Розташування файлу
    - Розробник
    - Належність певної категорії, типу додатка
    - Загальний рейтинг довіри (за даними виробника)
    - Глобальна розповсюдженість
4. Повинні бути реалізовані наступні можливості контролю сертифікатів додатків:
    - Довірений сертифікат
    - Довірений, але застарілий сертифікат
    - Недовірений сертифікат
    - Країна емітента
    - Назва емітента
    - Організація емітент
    - Інші атрибути емітента
5. Повинні бути реалізовані наступні критерії визначення місця розташування файлу:
    - Файл з шляхом, відповідним масці
    - Файл з шляхом, відповідним регулярному виразу
    - Файл на будь-якому локальному сховищі з шляхом, відповідним масці
    - Файл на будь-якому локальному сховищі з шляхом, відповідним регулярному виразу

- Файл на знімному носії з шляхом, відповідним масці
- Файл на знімному носії з шляхом, відповідним регулярному виразу
- Файл на мережевому ресурсі з шляхом, відповідним масці
- Файл на мережевому ресурсі з шляхом, відповідним регулярному виразу

6. Система повинна дозволяти визначати як мінімум наступних виробників програмного забезпечення: Microsoft, Adobe, Oracle, Apple та інш.
7. Система повинна дозволяти визначати програмне забезпечення наступних категорій:
    - Браузери
    - Інструменти розробки
    - Засоби розподілених обчислень
    - Ігри
    - Прошивки пристроїв і драйвери
    - Потенційно небезпечні програми
    - Системи миттєвого обміну повідомленнями
    - Інструменти роботи з мультимедіа
    - Засоби синхронізації з мобільними пристроями
    - Клієнти хмарних сховищ
    - Утиліти запису та емулятори оптичних дисків
    - Клієнти пірінгових мереж
    - Засоби підвищення продуктивності
    - Системні утиліти
8. Система повинна забезпечувати довільну комбінацію перерахованих вище критеріїв визначення файлів з використанням булевої логіки дозволяючу або блокуючу дію запуску програм.
9. Сукупність блокуючих і дозволяючих правил повинна динамічно застосовуватися до робочих станцій, згідно довільної комбінації наступних критеріїв з використанням булевої логіки:
    - Версія агента
    - Домен
    - Ім'я робочої станції
    - Діапазон IP-адрес
    - Належність домену підсистеми антивірусного захисту
    - Ім'я користувача
    - Група користувача
    - Версія Windows

## ВИМОГИ ДО ЗАХИСТУ ІНФРАСТРУКТУР VDI

1. Підсистема захисту інфраструктур VDI повинна безшовно інтегруватися з системою захисту робочих станцій
2. Підсистема повинна підтримувати наступні платформи віртуалізації:
    - Citrix XEN
    - VMware vSphere
    - Microsoft Hyper-V
3. Підсистема повинна підтримувати інтеграцію з більш, ніж з одним гіпервізором одночасно
4. Підсистема повинна дозволяти зробити еталонний образ ОС Windows з вбудованим агентом захисту
5. Підсистема повинна дозволяти налаштовувати максимальну кількість агентів що одночасно можуть виконувати оновлення компонент
6. Підсистема повинна дозволяти налаштовувати максимальну кількість агентів що паралельно здійснюють перевірку за розкладом
7. Система повинна пропонувати такі обов’язкові механізми антивірусної перевірки:
    - З повною базою (для автономних інфраструктур)
    - З мінімальною базою і використанням сервісу файлової репутації антивірусного серверу, чи ресурсів виробника

## ВИМОГИ ДО ЗАХИСТУ РОБОЧИХ СТАНЦІЙ НА БАЗІ MACOS

1. Система захисту повинна забезпечувати підтримку наступних ОС:
    - macOS™ 10.15 та вище
2. Агент повинен пропонувати наступні механізми захисту:
    - Сигнатурний аналіз по "повній базі" для комп'ютерів, розміщених в автономних мережах
    - Сигнатурний аналіз по скороченій базі для комп'ютерів, що мають доступ до онлайн-ресурсів виробника

- Сигнатурний аналіз по скороченій базі для комп'ютерів, що мають доступ до внутрішнього сервера з копією даних з онлайн-ресурсів виробника
- Технології «машинного навчання» для захисту від загроз «нульового дня»

3. Система захисту повинна підтримувати наступні типи сканування:
    - У реальному часі (при створенні / зміні файлу)
    - За запитом користувача
    - За розкладом
4. Система захисту повинна мати функціонал контролю пристроїв:
    - Блокування підключення зовнішніх пристроїв за їх типом
    - Дозволяти тільки відображення вмісту зовнішніх пристроїв
    - Повний доступ
5. Система контролю зовнішніх пристроїв повинна налаштовуватися як для окремих користувачів імпортованих з Active Directory (чи груп), так і для комп'ютерів в цілому.
6. Система контролю зовнішніх пристроїв повинна мати можливість автоматично змінювати параметр роботи в разі роботи комп'ютера поза корпоративної мережею.
7. Система контролю зовнішніх пристроїв повинна надавати можливість створення виключень як за параметрами самого пристрою (модель, виробник, серійний номер), так і за програмним забезпеченням, яке матиме дозвіл на взаємодію попри глобальну заборону для решти ПЗ.
8. Система захисту повинна мати функціонал самозахисту
9. Підсистема повинна забезпечувати належний рівень самозахисту:
    - Контроль цілісності агента
    - Запобігання блокування роботи агента
    - Запобігання доступу непривілейованих користувачів до файлів агента, журналів
10. Система захисту повинна дозволяти використовувати не тільки локальну антивірусну базу, але і перевіряти репутацію файлів по хмарній базі виробника
11. Повинна бути можливість розміщення всередині корпоративної мережі копії хмарної репутаційної бази виробника для перевірки файлів та веб-посилань.
12. Підсистема повинна забезпечувати очищення заражених систем від наслідків зараження
13. Підсистема повинна забезпечити блокування підключень до шкідливих веб-ресурсів

**ВИМОГИ ДО МОДУЛЯ ДЕТЕКТУВАННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ ВУЗЛІВ МЕРЕЖІ (EDR):**

1. Агент повинен мати можливість записувати події пов'язані з файлами, процеси, зміни в реєстрі, події пов'язані з певними користувачами / обліковими записами / комп’ютерами.
2. Збереження та опрацювання зібраної телеметрії має здійснюватись виключно засобами локального антивірусного серверу та локальної консолі управління без обов’язкового залучення хмарних сервісів виробника.
3. Здійснення розслідувань повинно бути реалізовано як по метаданим, збереженим на локальному сервері управління, так і через запит на кінцеві точки у режимі реального часу.
4. Агент повинен мати можливість передачі інформації з кінцевої точки на сервер як в автоматичному режимі з різними інтервалами часу, так і за запитом з консолі управління.
5. Агент на кінцевій точці повинен мати можливість підтримки власної бази для зберігання подій. Якщо база даних на кінцевій точці буде переповнюватися, то повинні автоматично перезаписуватися дані старше останніх 30 днів.
6. Агент повинен мати можливість запису та вивантаження метаданих у форматах алгоритмів хешування SHA-1, MD5 і SHA-256.
7. Центральна консоль повинна дозволяти побудову ланцюжка подій, пошук індикаторів компрометації щоб зрозуміти потенційний негативний вплив та дозволяти пошук за індикаторами компрометації
8. Агент повинен мати можливість проведення розслідувань інцидентів інфраструктури робочих станцій в режимі реального часу або за розкладом;
9. Розслідування має здійснюватися за такими критеріями (як мінімум, але не обмежуючись) для кінцевих точок Windows:
    - Host (name / IP address)
    - User account
    - File name
    - File path
    - Hash values (SHA-1, SHA-256 and MD5)
    - Registry key
    - Registry data
    - Registry name

- Command line

для робочих станцій з ОС macOS:

- Host (name / IP address)
- User account
- File name
- File path
- Hash values (SHA-1, SHA-256 and MD5)
- Command line

10. Можливість здійснення розслідувань на основі одного або декількох критеріїв.
11. Можливість візуалізації дерева подій, отриманих з кінцевих точок;
12. Можливість створення різних фільтрів пошуку та їх подальше збереження за даними моніторингу з робочих станцій;
13. Можливість реагування на події, виявлені на робочих станціях за допомогою виконання наступних дій:
    - завершити процес / заблокувати об'єкт,
    - ізолювати робочу станцію
    - додавання об'єктів до списку потенційно небезпечних
    - додавання об'єкта в нове розслідування
14. Можливість при ізоляції кінцевої точки відправляти команди на агент з консолі управління.
15. Можливість проведення розслідувань на основі Open IoC або YARA правил
16. Можливість вивантаження деталей розслідування в табличному вигляді, а також ланцюжків розслідувань.
17. Наявність механізму виявлення атак, який на основі вбудованих в механізм правил відстежує поведінку об'єктів що запускаються і генерує події, які можуть стати відправною точкою для проведення розслідувань.
18. Можливість проведення аналізу впливу на користувачів на основі ретроспективних даних з метою виявлення “нульового” пацієнта – хоста чи облікового запису користувача, з якого почався каскад небезпечних подій.
19. Можливість інтеграції з глобальним порталом Threat Intelligence від виробника.

*Якщо в технічній специфікації міститься посилання на конкретні марку чи виробника або на конкретний процес, що характеризує продукт чи послугу певного суб’єкта господарювання, чи на торгові марки, патенти, типи або конкретне місце походження чи спосіб виробництва, то слід розуміти у значені «або еквівалент».*

***3. Очікувана вартість та/або розмір бюджетного призначення:***

- Очікувана вартість закупівлі становить – 1 150 000,00 грн. з ПДВ

Відповідно до Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки, затвердженої ухвалою № 85 від 25.02.2021 «Про затвердження Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки», департамент економічного розвитку являється одним із виконавців програми (4.2.1.). На департамент покладені функції одного із реалізаторів програми, у частині забезпечення матеріально-технічної бази для впровадження електронних сервісів та засобів інформаційної безпеки для забезпечення потреб цільових груп Програми (п.4.4.1.). А також є головним розпорядником коштів Програми (6.2.). (Ухвала №85 від 25.02.2021) (https://www8.city-adm.lviv.ua/inteam/uhvaly.nsf/(SearchForWeb)/681B316687D1AE80C225868B003604D3?OpenDocument)

Рішенням виконавчого комітету № 64 від 12.01.2024 «Про затвердження на 2024 рік кошторису Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки» затверджено на 2024 рік кошторис Програми цифрового перетворення Львівської міської територіальної громади на 2021-2025 роки (Рішення №64) (https://www8.city-adm.lviv.ua/Pool/Info/doclmr_1.NSF/(SearchForWeb)/A7BEE902A1E0E115C2258AA2003D96AB?OpenDocument)

При визначенні очікуваної вартості замовник неухильно дотримувався принципів проведення публічних закупівель, визначених статтею 5 Закону України "Про публічні закупівлі" та враховував методи визначення очікуваної вартості предмету закупівлі, що визначені в Наказі Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 № 275 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі» із застосуванням методу порівняння ринкових цін. Для повноцінного аналізу ринку та належного розрахунку очікуваної вартості предмета закупівлі застосовано різнобічні джерела та ресурси отримання інформації щодо ціни, зокрема комерційні пропозиції (№4-0406-61470 від 06.11.2024, №4-0406-63796 від 18.11.2024), загальнодоступна відкрита інформація даних системи електронних закупівель Prozorro, професійного модуля аналітики bi.prozorro, електронного каталогу Prozorro.Market, а також Google пошук (огляд веб-сайтів, прайси тощо).