**ОБҐРУНТУВАННЯ**
**технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі**

(відповідно до пункту 4[1] постанови Кабінету Міністрів України від 11.10.2016 № 710 “Про ефективне використання бюджетних коштів”)

**1. Предмет закупівлі:** Придбання (постачання) ліцензій на право користування програмним забезпеченням (пакети програмного забезпечення для захисту інформації) (код за ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів).

**2. Вид процедури:** закупівля через Централізовану закупівельну організацію – ДП «УСС».

**3. Номер оголошення закупівлі:** UA-2022-09-08-005799-a.

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

**ЗАХИСТ ІНФОРМАЦІЇ - 100 од.**

| **Параметри** | **Вимоги до Консолі управління** |
|---|---|
| Інсталяція і конфігурація: | Пакет для установи повинен бути у вигляді єдиної віртуальної установи. (віртуального образу).<br><br>Платформи для установи мають включати:<br><br>– VMware vSphere<br>– Microsoft Hyper-V<br>– Kernel-based Virtual Machine or KVM<br>– Oracle VM<br><br>Інші платформи мають бути впроваджені, якщо буде надано запит до розробника антивірусного ПЗ.<br><br>1) ПЗ має підтримувати централізоване установлення для виділеної машини сканування.<br>2) Для цілей масштабування, ПЗ має підтримувати інсталяцію будь-якого компоненту або сервісу окремо або у групі.<br>3) Для цілей масштабування ПЗ має включати окремі компоненти баз даних, сервісів комунікацій, сервісу оновлень а веб сервісів.<br>4) Для високої доступності та балансування навантажень ПЗ має включати відокремлений модуль – load balancer – балансування навантажень |
| Основні властивості. ПЗ має включати наступні | 1) Гнучке ліцензування ( окремий ключ для кожного сервісу безпеки, який дозволяє різну кількість |

| | |
|---|---|
| функції: | ліцензійних об’єктів та різні дати закінчення ліцензії, історію всіх введених ключів) або ключ на комплект, єдину ліцензію для управління сервісами безпеки.<br>2) Оновлення в один клік – один клік для оновлення всіх компонентів консолі, не залежно від порядку їх установки або інших вимог.<br>3) Оновлення по бажанню, які дозволять адміністратору вибирати – які пакети безпеки треба оновлювати, для того, щоб зберегти мережевий трафік.<br>4) Має використовуватись non-relational / non-SQL База даних, без вимоги до окремого ключа ліцензування для розгортання більше ніж поточна кількість кінцевих точок.<br>Повідомлення повинні бути відображені в головному меню, з акцентуванням на не прочитаних повідомленнях та з можливістю відправлення через почтову адресу, повідомляючи адміністратора про важливі події : проблеми ліцензій, вірусні атаки та машини без оновлень. |
| Інформаційна сторінка консолі. Для моніторингу та управління подіями, ПЗ повинен мати: | 1) Можливість додавати, видаляти, сортувати та налаштовувати багато представлень інформації про безпеку.<br>2) Підтримку багатьох сторінок з багатьма представленнями с інформаційної безпеки.<br>3) Можливість надання інформації в реальному часі з легко зчитуваними діаграмами.<br>Можливість налаштовувати ціль для звітності, підґрунтя для звіту, часові рамки для звітності та назву представлення. |
| Інвентаризація мережі у консолі. Для управління безпекою інфраструктури, ПЗ повинен мати: | 1) Інтеграцію з Microsoft Active Directory з метою імпорту інвентаря та інформації з цих платформ.<br>2) Регульований час синхронізації ( у годинах ) з Microsoft Active Directory<br>3) Інтеграцію з Microsoft Hyper-V, RedHat Linux Virtual Machine, Oracle VM, KVM та іншими віртуальними машинам, які можуть бути знайдені через Network Discovery.<br>4) Мережевий пошук не інтегрованих машин в Microsoft Active Directory, VMware vCenter, як для фізичних так і для віртуальних машин.<br>5) Пошук у реальному часі, сортування та фільтрація по назві, операційній системі, IP, FQDN чи мітці.<br>6) Можливість віддаленої установки та видалення агентів ПЗ. |

| | |
|---|---|
| | 7) Пакети для інсталяції вручну, які можна налаштувати.<br>8) Можливість налаштовувати та запускати віддалені задачі сканування.<br>9) Можливість віддалено перезавантажити кінцеву точку.<br>10) Можливість переглядати централізовані результати задач із деталями по кожної під-задачі.<br>11) Можливість назначати політики на кожному рівні управління.<br>12) Можливість налаштовувати наслідування політик та примусово змінювати політики.<br>Можливість переглядати детальні властивості кінцевих точок під управлінням системи, а саме – IP, Ім'я, операційну систему, групу, політику, останні відомості про загрози, останні логи сканування |
| Політики консолі управління.<br>Для управління безпекою інфраструктури ПЗ повинен мати: | 1) Можливість призначати політики згідно з локацією та поточним користувачем.<br>2) Можливість застосовувати декілька політик до однієї кінцевої точки, але тільки одну активну одночасно.<br>3) Можливість застосовувати політику до групи кінцевих точок.<br>4) Єдиний шаблон для кожної служби безпеки<br>5) Кожна служба безпеки має свій налаштовуваний шаблон політики з конкретними параметрами для активації / дезактивації та налаштування таких функцій, як сканування антивірусних програм, можливості роботи з пісочницею, опції машинного навчання, гіпервізор - самонагляд, брандмауер, контроль доступу до мережі, додавання до білого списку, чорний список програм, контроль веб-доступу, керування пристроєм, місцезнаходження пристрою, дотримання автентичності та дії, які слід вживати у випадку виявлення зловмисного ПЗ та несумісних пристроїв, наприклад, віддалене блокування, розблокування, стирання, шифрування за допомогою SD.<br>6) Адміністратор повинен мати можливість створювати однакову політику для Windows, Mac і Linux, робочих станцій і серверів, як віртуальних, так і фізичних.<br>7) Адміністратор повинен мати можливість створити єдину політику для всіх функцій агента кінцевої точки. |

| | |
|---|---|
| | 8) Будь-яка нова політика, створена Адміністратором, повинна містити функції Antimalware за замовчуванням.<br>9) Адміністратор повинен мати можливість створити сповіщення, яке буде надіслано електронною поштою на його адресу електронної пошти, без необхідності вручну додавати свою електронну адресу під час налаштування сповіщення.<br>10) Консоль управління повинна мати можливість не оновлювати себе автоматично.<br>Консоль керування повинна запобігати плутанини політик, не допускаючи кількох політик з однаковим ім'ям. |
| Звіти консолі управління: | 1) Велика кількість звітів.<br>2) Простота використання: резюме та деталі на тій самій сторінці, в розділі активного підсумку (інформація про фільтри, натиснувши розділ резюме).<br>3) Планування, можна надіслати поштою будь-якій кількості одержувачів (у консолі також не потрібно мати обліковий запис).<br>4) Фільтри для запланованих звітів з метою отримати поштою тільки релевантну інформацію для кожного користувача.<br>5) Архів всіх згенерованих примірників запланованого звіту.<br>6) Експорт резюме до файлу .pdf, деталі до файлу .csv.<br>Повністю настроюваний движок звітування для об'єднання подій з будь-якого модуля безпеки в єдиний звіт. |
| Карантин: | 1) Віддалене відновлення, з налаштовуваним розташуванням та видаленням.<br>2) Можливість централізувати карантин для заражених файлів<br>Встановлення часу файли будуть зберігатися в карантині до 180 днів. |
| Користувачі: | 1) Розподіл ролей адміністратора.<br>2) Кілька попередньо визначених типів: суперадміністратор, адміністратор, репортер або користувач.<br>a. Суперадміністратор : керує компонентами розчину;<br>b. Адміністратор: керує службами безпеки;<br>c. Репортер: моніторинг та створення звітів.<br>3) Список користувачів, що імпортуються з Microsoft |

| | |
|---|---|
| | Active Directory (автентифікація AD буде використовуватися для входу).<br>Детальна конфігурація для адміністративних цільових прав, щоб вибрати, якими послугами та об'єктами користувач має право керувати. Автоматичний вихід для будь-якого типу користувача для підвищення безпеки щодо інформації, яка відображається на консолі керування. |
| Журнали: | 1) Зареєструйте дії користувача для відповідності.<br>2) Детальні журнали для кожної дії користувача.<br>Комплексний пошук. |
| Сертифікати безпеки: | 1) Доступ до консолі керування повинен бути захищений (https).<br>2) Веб-сервер із центральної консолі керування повинен дозволяти імпорт цифрових сертифікатів, виданих ліцензованим органом сертифікації або власною організацією. Імпорт сертифікатів інтуїтивно зрозумілий і зроблений з центральної консолі керування.<br>3) Управління та спілкування з мобільними пристроями (iOS) повинні бути виконані за допомогою цифрових сертифікатів. Ці сертифікати підписуються сертифікаційним органом, уповноваженим або їх власною організацією.<br>4) Це дозволяє імпортувати ланцюжок сертифікатів PKI (інфраструктура відкритого ключа).<br>5) Необхідно підтримувати ключі шифрування цифрових сертифікатів з мінімальною довжиною 1024 біт.<br>6) Цифрові сертифікати, коли вони імпортуються, повинні бути змінні у разі їх закінчення або їх скасування.<br>7) Прийняті сертифікати у процесі імпорту повинні бути у форматі pfx або p12 і захищені паролем.<br>8) Рішення має бути в змозі самостійно генерувати цифрові сертифікати.<br>Рішення повинно бути в змозі показати в центральній консолі інформацію про сертифікати: ім'я, орган, що видав, дата видачі та термін придатності виданих сертифікатів. |
| Очікування оновлень: | 1) Рішення має дозволяти тестування нових комплектів або оновлень ПЗ в закритому середовищі.<br>2) Рішення повинно мати можливість вирішити, які комплекти будуть опубліковані в мережі. |

| | |
|---|---|
| | 3) Рішення повинен мати можливість визначати та застосовувати різні політики для критичних кінцевих точок з виробництва та оновлювати їх після того, як новий пакет перевірено.<br>4) Рішення має бути в змозі відключити можливість постановки.<br>5) Платформа для постановки повинна бути доставлена як віртуальний пристрій.<br>6) Сервер оновлень може працювати як шлюз для даних.<br>7) Платформа консолі та встановлення повинна мати можливість автоматично завантажувати нові комплекти.<br>8) Консоль повинен мати можливість налаштовувати максимальну кількість комплектів, які ви можете зберігати.<br>Параметр стажувань може визначати кілька кількох оновлень для застосування оновлень ПЗ. |
| Автономні оновлення: | 1) Рішення може використовувати офлайн-оновлення в ізольованій інфраструктурі.<br>2) Оновлення можна завантажувати та переносити за допомогою USB HDD / USB Stick, File Server, FTP та встановити в ізольовану інфраструктуру. |
| Ключі API: | 1) Рішення повинно дозволити адміністраторам використовувати виклик API.<br>2) Рішення повинно включати в себе методи керування акаунтами користувачів, налаштування сповіщень, керування групами, папками та кінцевими точками, керування політикою, створення звітів за допомогою ключів API. |
| **Параметри** | **Вимоги до системи в частині захисту фізичних робочих станцій та серверів** |
| Мінімальні та усунені властивості: | 1) Існування єдиного ядра антивірусного захисту.<br>2) Щоб звести до мінімуму споживання ресурсів, ПЗ антивірусного ПЗ повинні дозволяти встановлювати власні модулі (наприклад, встановлювати ПЗ Antimalware без модуля керування доступом до мережі або без модуля брандмауера). |
| Системні вимоги: | 1) Операційні системи робочої станції: Windows 10, Windows 8.1, Windows 8,<br>2) Серверні операційні системи: Windows Server 2019, Windows Server 2016, Windows Server 2012, |
| Управління та віддалене встановлення: | 1) Перед встановленням адміністратор може налаштовувати інсталяційні пакети, включаючи тільки потрібні модулі: аналіз на основі поведінки, брандмауер, контроль вмісту, керування пристроєм, управління програмами. |

| | |
|---|---|
| | 2) Установку можна виконати кількома способами:<br>a. Завантажуючи пакет антивірусної програми безпосередньо на робочу станцію, де вона буде встановлена.<br>b. Встановлюючи дистанційно, безпосередньо з веб-консолі.<br>3) Установка на машини з віддаленого місця буде виконуватися за допомогою існуючого встановленого клієнта в цих місцях, щоб мінімізувати трафік WAN.<br>4) Консоль управління повідомить про кількість робочих станцій, на яких встановлено антивірус, та про кількість незахищених робочих станцій.<br>5) Консоль керування буде включати зконфігуровані портлети / віджети на інформаційній панелі.<br>6) Консоль управління включатиме докладну інформацію про робочі станції / сервери: ім'я, IP, операційна система, встановлені модулі, застосовану політику, інформацію про оновлення тощо.<br>7) Консоль керування дозволить адміністратору надсилати політику для налаштування всього антивірусного ПЗ як для робочих станцій, так і для серверів.<br>8) Консоль керування дозволить використовувати два типи облікових записів: Адміністратор та Репортер, які можуть бути призначені для того, які групи користувачів вони можуть змінювати налаштування або створювати звіти.<br>9) Консоль управління включатиме розділ логів, в якому будуть відображені всі дії, з докладною інформацією: вхід, редагування, створення, вихід із системи, переміщення тощо.<br>10) Консоль управління дозволить створювати єдиний пакет, який використовується як для 32-розрядних операційних систем, так і для 64-розрядних, MAC та Linux.<br>11) Консоль керування дозволить адміністратору створювати групи або підгрупи для керування робочими станціями.<br>Можливість вибирати який клієнт буде мати змогу бачити інші комп’ютери в мережі. |
| Основні особливості та функціональні можливості антивірусного та анти шпигунського модуля: | 1) Автоматичне сканування в режимі реального часу може бути встановлено таким чином, що адміністратор рішення не сканує архіви чи файли, розмір яких не перевищує розмір файлу "x" MB.<br>2) Автоматичне сканування в режимі реального часу може підтримувати архіви сканування з рівнем глибини до 16.<br>3) Поведінкове евристичне сканування та моніторинг процесу.<br>4) Технологія Cloud Scanning і Machine Learning.<br>5) Anti-ransomware та anti-exploit технології. |

| | |
|---|---|
| | 6) Можливість виявлення безфайлових атак, у тому числі тих, які використовують законні інструменти операційної системи, такі як Powershell або інтерпретатори сценаріїв. Рішення не повинно блокувати скрипти для досягнення цього.<br>7) Додатковий рівень захисту нового покоління на основі агресивної евристики та технології машинного навчання дозволяє виявляти та блокувати нове покоління передових або цілеспрямованих атак та складного шкідливого ПЗ перед виконанням. Вона повинна забезпечити:<br>a. Класифікацію типів нападу.<br>b. Можливість повідомляти лише про виявлені загрози, не блокуючи їх.<br>c. Можливість настроювання агресивності виявлення для кожної категорії нападу, з можливістю вжити заходів щодо виявлення вищих виявлень, а також повідомити про всі інші дрібніші виявлення. Має бути доступно щонайменше 3 рівня виявлення.<br>d. Можливість приймати різні дії на різні виявлені файли та мережеві загрози.<br>8) Сканування носіїв інформації (компакт-дисків, зовнішніх жорстких дисків, спільного диска) на вимогу та сканування при доступі. Крім того, процес сканування може бути зупинений, якщо носії інформації для зберігання містять інформацію більше, ніж "х" МБ.<br>9) Автоматична перевірка електронних листів на рівні робочої станції, незалежно від поштового клієнта, для протоколів SMTP та POP3.<br>10) Налаштування шляхів сканування, до рівня файлу.<br>11) Рішення повинно забезпечувати вбудовані виключення для ролей сервера Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).<br>12) ПЗ Antimalware дозволить визначити список виключень сканування як для сканування на вимогу "on-access", так і "on-demand" для певних папок, дисків, файлів, розширень або процесів.<br>13) За допомогою повної бази даних шпигунських підписів та евристичного виявлення цих програм ПЗ має запропонувати антишпигунський захист.<br>14) Щоб не перевантажувати системні ресурси, ПЗ Antimalware повинен містити єдиний механізм сканування. Він зможе запускати заплановані сканування з низьким пріоритетом і може автоматично вимикатися після сканування робочої станції.<br>15) Для більшого захисту Antimalware повинна мати 4 типи виявлення: сигнатурний, евристичний, безперервний моніторинг процесів та сканування у хмарі. |

| | |
|---|---|
| | 16) Щоб забезпечити більший захист, Antimalware також повинен мати можливість сканувати HTTP та SSL.<br>17) Для кращого управління анти-вірусом, встановленим на робочих станціях, ПЗ повинен включати в себе можливість встановити пароль для захисту від видалення.<br>18) Для забезпечення безпеки користувачів клієнт має включати модуль антифішингу, який матиме можливість перевірки посилань на пошукові системи (Search Advisor).<br>19) Програма Antimalware повинна мати сканування при доступі для ОС Linux. |
| Брандмауер: | 1) Можливість встановлення режиму "стелс" на рівні локальної мережі або на рівні Інтернету.<br>2. Модуль може бути встановлений / видалений відповідно до налаштувань адміністратора. |
| Карантин: | 1) ПЗ Antimalware повинен дозволити автоматичну передачу карантинних файлів у вірусну лабораторію.<br>2) Відправка карантинних файлів буде автоматично виконана заздалегідь із визначеним інтервалом часу (кількість годин), встановленими адміністратором.<br>3) ПЗ Antimalware повинен дозволяти автоматичне видалення карантинних файлів, які перевищують певний період часу, щоб не займати місце на диску.<br>4) Можливість переміщення файлу з карантину до його оригінального розташування.<br>5) Централізований карантин.<br>6) Карантин дозволить сканувати об'єктів після кожного оновлення сигнатур. |
| Захист даних: | Дозволяє блокувати конфіденційні дані (контактна картка, банківський рахунок тощо) як для HTTP, так і для SMTP шляхом створення спеціальних правил. |
| Контроль користувачів: | 1) У ПЗ наявний інтегрований модуль керування користувача з такими функціями:<br>a. Блокування доступу до Інтернету для певних клієнтів або груп клієнтів.<br>b. Блокування доступу до певних програм.<br>c. Блокування доступу до Інтернету протягом певних періодів часу.<br>d. Блокування веб-сторінок, які містять певні ключові слова.<br>e. Дозвіл на доступ до певних веб-сторінок, вказаних адміністратором.<br>f. Обмеження доступу до певних веб-сайтів певними визначеними категоріями (наприклад, онлайн-знайомство, насильство тощо). |

| | |
|---|---|
| Контроль та інвентаризація додатків: | 1) Можливість виявити запущені програми та процеси та організувати їх у групи.<br>2) Організація та пошук програм та процесів за назвою, версією, видавцем / автором тощо.<br>3) Дозволити або відхилити процес .<br>4) Авторизувати додаток на основі хешу.<br>5) Дозволити додаток на підставі сертифікату.<br>6) Можливість застосування правил до порожніх дитячих процесів, під процесів.<br>7) Модуль може працювати в тестовому режимі та повідомляти про програму, але не блокувати її.<br>8) Модуль може працювати у режимі виробництва та може заблокувати всі невідомі додатки.<br>9) Автоматично виключати процеси операційної системи Microsoft. |
| Контроль пристроїв: | 1) Запобігання виявленню конфіденційної інформації та інфікуванням шкідливими програмами через приєднані пристрої.<br>2) Застосування правил блокування та виключень через політику до великої кількості пристроїв і типів.<br>3) Надсилатиме інформацію, таку як ім'я пристрою, ідентифікатор класу, дату та час з'єднання.<br>4) У заздалегідь визначених типах пристроїв, таких як: CDROM, пристрої для обробки зображень, диски для штрих-кодів, COM / LPT-порти, SCSI-рейди, принтери, мережеві карти, внутрішня і зовнішня пам'ять тощо.<br>5) Підтримувати різні конфігурації та привілеї, такі як Allowed, Blocked або Custom<br>6) Підтримка режиму читання лише для пристроїв зберігання даних.<br>7) Можливість заблокувати лише USB і дозволити використовувати всі інші порти.<br>8) Дозволити встановлення виключень для різних типів пристроїв<br>9) Підтримка визначення виключень пристроїв:<br>a. За ідентифікатором ПЗ<br>b. Ідентифікатор пристрою, ідентифікатор обладнання<br>10) Можливість виявити пристрої. |
| Автоматичний аналіз підозрілих файлів у Пісочниці-аналізаторі: | 1) Рішення повинно мати можливість здійснювати поглиблений аналіз підозрілих файлів.<br>2) Рішення має мати можливість автоматично або вручну надсилати файли на сервери-пісочники.<br>3) Рішення може бути налаштовано таким чином, щоб дати доступ до представлених об'єктів користувачам або заблокувати їх до повернення результатів аналізу. |

| | |
|---|---|
| | 4) Рішення повинно дозволяти різні дії, якщо поданий файл є загрозою.<br>5) Рішення повинно мати можливість використовувати проксі-сервер для трафіку пісочниці.<br>6) Рішення повинно мати можливість детонувати файли окремо або як групу.<br>Рішення пропонує докладний звіт про надані файли. |
| Оновлення: | 1) Можливість очікувати перезавантаження комп'ютера після оновлення, не повідомляючи користувача.<br>2) Каскадні системи оновлення за допомогою локального сервера оновлень.<br>3) Оновити клієнтів у віддаленому розташуванні через існуючий клієнт із вбудованою роллю сервера оновлення.<br>Роль сервера оновлення клієнта повинна бути доступною для операційних систем Windows і Linux. |
| Модуль для захисту пошти для Microsoft Exchange Server 2012 та вище: | 1) Рішення повинне забезпечувати фільтрацію загроз для вхідного, внутрішнього та вихідного трафіку електронної пошти.<br>2) Рішення має підтримувати можливості запланованого сканування для поштових скриньок і загальнодоступних папок, включаючи можливість виключення певних поштових скриньок або загальних папок, а також параметри сканування лише електронних листів із вкладенням або електронними листами, отриманими протягом останніх декількох годин / днів.<br>3) Можливість налаштовувати різні дії для зараження, підозрілих або нескануємих файлів.<br>4) Можливість вилучення потенційно небажаних програм (PUA) від фільтрації проти вірусів.<br>5) Можливість сканування шкідливих програм всередині архівів.<br>6) Рішення повинне забезпечувати антиспам-фільтр для трафіку електронної пошти з можливістю включення до списку окремих адрес електронної пошти та доменів.<br>7) Можливість запитувати сервери, що визначаються адміністраторами Realtime Blackhole Lists (RBL) і фільтрувати електронні повідомлення як спам на основі репутації сервера відправника.<br>8) Можливість автоматично позначати як спам повідомлення електронної пошти, написані на азіатській або кирилиці.<br>9) Можливість виконувати хмарні запити для покращення захисту від нового спаму.<br>10) Можливість здійснення різних дій щодо виявлених електронних поштових повідомлень із спамом, включаючи префіксацію теми електронної пошти з певним тегом, видалення, перенаправлення або |

| | |
|---|---|
| | переадресація повідомлення на певну поштову скриньку.<br>11) Рішення повинно забезпечувати можливості фільтрування вмісту для вхідного, внутрішнього та вихідного трафіку електронної пошти, виходячи з конкретних текстових або регулярних виразів, що відповідають предмету електронної пошти та / або вмісту тіла.<br>12) Можливість приймати різні дії на електронні листи, що відповідають правилам фільтрації вмісту, включаючи префіксацію тема електронної пошти з певним тегом, видалення, перенаправлення або переадресацію електронної пошти на певну поштову скриньку.<br>13) Рішення має забезпечити можливість фільтрації вкладень для вхідного, внутрішнього та вихідного трафіку електронної пошти, залежно від типу вкладення або назви файлу.<br>14) Можливість здійснювати різні дії на електронні листи, що відповідають правилам фільтрації прихильності, включаючи видалення або заміну вкладеного файлу, префіксацію теми електронної пошти певним тегом, видалення, перенаправлення або переадресацію електронної пошти на певну поштову скриньку.<br>15) Можливість блокувати SMTP-з'єднання на основі електронної адреси або домену відправника.<br>16) Можливість визначати IP-адреси, уповноважені надсилати електронну пошту для власних доменів для перевірок, пов'язаних із врученням вручну.<br>17) Можливість визначення власних правил фільтрування на основі груп користувачів.<br>18) Можливість перегляду статистики та звітів про діяльність фільтрації електронної пошти.<br>19) Можливість централізованого перегляду та керування елементами карантину, включаючи можливість завантажувати або відновлювати елементи, що підлягають карантину. |
| Наявність eXtended Endpoint Detection and Response (XDR) | 1)Вживати заходів для усунення вразливостей і усунення ризику повторних атак.<br>2)Виявляти дії, які ухиляються від класичних механізмів запобігання кінцевим точкам.<br>3)Пошук конкретних індикаторів компрометації (IoC) і підозрілих елементів, які дозволяють аналітикам безпеки виявляти атаки на ранніх стадіях. |
| **Параметри** | **Вимоги до системи в частині захисту для віртуальних робочих станцій і серверів** |
| Захист від Antimalware, | 1) ПЗ інтегрується з VMware VShield або VMware NSX і |

| | |
|---|---|
| призначений віртуальним середовищам.<br>Мінімальні вимоги: | пропонує можливість антивірусного сканування без встановлення агента сканування на віртуальну машину.<br>2) Центральний компонент керування рішення інтегрується з декількома vCenter від VMware.<br>3) Для всіх систем, що працюють під Windows та Linux, ПЗ включає:<br>a. Сканування процесу;<br>b. Сканування пам'яті;<br>c. Сканування файлів у реальному часі;<br>d. Сканування файлів за вимогою;<br>Сканування файлів у реальному часі та на вимогу для віртуальних машин Linux. |
| Загальні характеристики: | 1) Методи для виявлення вірусів, шпигунських програм, руткітів та інших шкідливих програм.<br>2) ПЗ повинен дозволити автоматичне оновлення віртуального пристрою безпеки, для підписів проти антивірусних програм та для операційної системи віртуальної установи безпеки.<br>3. ПЗ повинен повідомляти про поточний стан хоста безпеки - віртуальних пристроїв, захищених / незахищених і віртуальних пристроїв безпеки. |
| Мінімальні системні вимоги: | 1) В частині підтримки платформ віртуалізації:<br>Не нижче VMware vSphere, 6.0<br>Microsoft Hyper-V 2012<br>2) В частині підтримки Операційних систем для віртуальних машин (64 біт):<br>Не нижче Windows 10<br>Не нижче Windows Server 2012 R2<br>• Не нижче Red Hat Enterprise Linux 5.6<br>• Не нижче CentOS 5.6<br>• Не нижче SUSE Linux Enterprise Server 11<br>• Не нижче Debian 7.0 |
| Основні особливості та функціональність модуля Antimalware: | 1) Автоматичне сканування файлів, які копіюються на зовнішню пристрої та з LAN або WAN.<br>2) Автоматичне сканування файлів у режимі реального часу може бути встановлено для сканування тільки певних типів файлів з певними розширеннями, визначеними адміністратором.<br>3) Автоматичне сканування файлів у режимі реального часу може бути встановлене так, щоб не сканувати архіви більше, ніж "x" Кб, розміри файлів можуть бути визначені адміністратором рішення.<br>4) Сканування за вимогою включатиме наступні опції:<br>a. Сканування будь-яких носіїв даних, підключених до віртуальної машини;<br>b. Сканування електронних листів;<br>5) Налаштування шляхів для сканування на рівні файлу; |

| | |
|---|---|
| | 6) Необхідно дозволити адміністратору визначати певні папки, диски, файли та розширення, які потрібно виключити зі сканування у реальному часі та скануванням за запитом.<br>7) Щоб не перевантажувати системні ресурси, ПЗ Antimalware повинен містити єдиний механізм сканування.<br>8) Дозволяти оптимізацію обсягу трафіку, відправленого в мережу, за допомогою механізму кешуваня на сканері та віртуальній машині.<br>9) Підключення агента відновлення/балансування навантажень до сканеру.<br>Політики можуть бути застосовані до пулу ресурсів VMware vCenter. |
| Карантин: | 1) ПЗ Antimalware повинен дозволяти автоматичне видалення карантинних файлів, які перевищують певний період часу, не займаючи зайвого місця для зберігання.<br>2) Можливість переміщення файлу з карантину до його оригінального розташування.<br>3) Централізований карантин. Можливість безпечно збирати всі перевірені файли з захищених кінцевих точок в унікальне місце в мережі для більш глибокого вивчення.<br>4) Можливість повторно сканувати файли, що зберігаються, після кожного оновлення підписів.<br>5) Можливість автоматичного надсилання файлів з карантину до лабораторій-виробників в інтервалі часу, встановленому адміністратором. |
| Управління та віддалена установка: | 1) Віртуальний пристрій безпеки може бути налаштований перед установкою. Він автоматично масштабується за кількома характеристиками: кількість віртуальних машин на хості, мережі, IP-адреси виділених ресурсів (процесор, пам'ять) тощо.<br>2) Консоль керування повідомить про кількість віртуальних машин, які встановили чи не встановили рішення щодо захисту від вірусів та стан машини: Увімкнено або Вимкнено.<br>3) Можливість консолі керування звітувати про те, чи включений модуль захисту від вірусів на віртуальній машині. |
| Спеціальні вимоги до технічної підтримки: | 1) Технічна підтримка та доступ до оновлень ПЗ терміном не менше 12 місяців.<br>2) Звернення співробітників Покупця в технічну підтримку повинні прийматися 24 години 7 днів на тиждень по телефону та через веб-сайт.<br>3) Час реакції на звернення протягом 2 годин від звернення, протягом 7 днів на тиждень та 24 години на добу. |

| | |
|---|---|
| | Відповідність запропонованого товару зазначеним трьом вимогам підтверджуються окремим листом від Виробника (розробника), або його офіційного представника (дистриб'ютора) в Україні програмного забезпечення |

**5. Обґрунтування розміру бюджетного призначення:**

Розмір бюджетного призначення визначено відповідно до Закону України «Про Державний бюджет України на 2022 рік», кошторису КРАІЛ на 2022 рік за бюджетною програмою КПКВК 0418010 «Керівництво та управління у сфері регулювання азартних ігор та лотерей» з урахуванням середньої ринкової вартості аналогічних послуг, наданих цінових пропозицій і граничних сум витрат для бюджетних установ, визначених постановою Кабінету Міністрів України від 04.04.2001 № 332.

**6. Обґрунтування очікуваної вартості закупівель:**

Розрахунок очікуваної вартості визначено на підставі середньо ринкової вартості аналогічних послуг, цінових пропозицій та граничних сум витрат для бюджетних установ, визначених постановою Кабінету Міністрів України від 04.04.2001 № 332. Очікувана вартість закупівлі становить 135 800,00 грн. (з урахуванням ПДВ).