**Обґрунтування**

**технічних та якісних характеристик, очікуваної вартості**

**Предмет закупівлі:** ДК 021:2015 48730000-4 Пакети програмного забезпечення для забезпечення безпеки продовження ліцензій на програмне забезпечення антивірусного захисту, виявлення та блокування атак на кінцеві пристрої ESET  PROTECT Entry та ESET Inspect).

**Технічні та якісні характеристики предмета закупівлі:**

На робочих станціях користувачів та серверах УДЦР використовується антивірусний програмний засіб та програмний засіб забезпечення виявлення та блокування атак на кінцевих точках розробки компанії ESET. Наразі є потреба у придбанні права на користування зазначеними програмними засобами на наступний рік.

Відсутність захисту, що забезпечують ці засоби призводить до порушення функціонування інформаційно-комунікаційної інфраструктури УДЦР в наслідок кібератак та ураження шкідливим програмним забезпеченням або запуску несанкціонованих процесів на обчислювальної техниці.

Таким чином, вчасне придбання ліцензій на новий термін необхідно для забезпечення функціонування інформаційно-комунікаційної інфраструктури УДЦР.

Програмне забезпечення антивірусного захисту та блокування атак на кінцевих точках ESET PROTECT Entry та ESET Inspect з локальним управлінням ESET Protect web-консоль, має відповідати наступним вимогам**:**

1. ESET PROTECT Entry (або еквівалент) має відповідати таким вимогам:

|  |  |  |
| --- | --- | --- |
| № | Вимога | Параметри |
| 1.1 | Експертні висновки | Копія експертного висновку або копії експертних висновків (на запропоноване програмне забезпечення або його складові), зареєстрованих в Адміністрації Державної служби спеціального зв’язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні. |
| 1.2 | Технічна підтримка | Наявність української служби технічної підтримки, яка працює в режимі 24х7х365. |
| 1.3 | Інтерфейс | Інтерфейс та документація до продукту українською та англійською мовами. |
| 1.4 | Підтримка ОС | Microsoft Windows 10/8.1/8/ 32 та 64 розрядні;Microsoft Windows Server 2008R2 (x86 та x64);Microsoft Windows Server 2012;Microsoft Windows Server 2016;Microsoft Windows Server 2019;Linux версії 2.5.x та вище. |
| 1.5 | Елементи захисту | Надання захисту від: шкідливих програм, троянського програмного забезпечення, клавіатурних шпіонів, рекламного програмного забезпечення, фішингу, шпигунського програмного забезпечення, руткітів, скриптів, потенційного небажаного та небезпечного програмного забезпечення, мережевих атак та спаму.Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків.Захист від ботнетів, технологія яка забезпечує захист від загроз типу "ботнет".Захист уразливостей мережевого протоколу що покращує виявлення загроз, які використовують недоліки мережевих протоколів SMB, RPC, RDP.Використання евристичних технологій під час сканування та забезпечення захисту в режимі реального часу.Модуль захисту документів.Можливість сканування файлів під час запуску системи.Сканування комп'ютера у неактивному стані. |
| 1.6 | Додаткові рівні захисту | Наявність персонального брандмауера, який містить в собі майстер для створення правил брандмауера та редактор зон та правил.Наявність модуль захисту від спаму з можливістю інтеграції до поштового клієнту. Можливість використовувати білі та чорні списки як користувальницькі, так і глобальні, інформація до яких надходить з серверів оновлення. |
| 1.7 | Додаткові налаштування параметрів роботи | Можливість визначення детальних параметрів роботи антивірусного сканера, таких як: визначення об’єктів та методів сканування, можливість встановлення максимального розміру та часу сканування файлу, максимальну глибину вкладення архіву та створення виключень. |
| 1.8 | Захист змінних носіїв | Автоматична антивірусна перевірка змінних носіїв. Контроль змінних носіїв з можливістю створення правил за типом пристрою, діями, виробником, моделлю та серійним номером пристрою. |
| 1.9 | Контроль периферійних пристроїв | Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції периферійних пристроїв шляхом створення правил доступу за типом пристрою, за рівнем доступу, за виробником, моделлю або серійним номером пристрою. Правила можуть створюватись як для всіх, так і для окремих користувачів або груп Windows. |
| 1.10 | Оновленнябаз | Регламентне оновлення вірусних баз не менше 4 разів за добу (в тому числі відповідно до вимог наказу Адміністрації Держспецзв’язку від 26.03.2007 № 45, зареєстрованого в Міністерстві юстиції України 10.04.2007 за № 320/13587).Можливість отримання оновлення клієнтів з локального дзеркала на сервері.Можливість створення дзеркала оновлень засобами програмного забезпечення. Можливість отримання оновлення вірусних баз з загальної мережевої папки або з носія інформації.Відкат оновлень з можливість повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.Можливість мобільним співробітникам отримати оновлення з серверів виробника он-лайн у разі перебування поза корпоративною мережею. |
| 1.11 | Взаємодія з ОС | Наявність механізму контролю за актуальністю оновлень операційної системи. Наявність інструменту для діагностики системи, який має можливість створювати знімки стану операційної системи для подальшого глибоко аналізу різноманітних аспектів роботи операційної системи, включаючи запущені процеси, контент реєстру, інстальоване програмне забезпечення, мережеві з'єднання. |
| 1.12 | Планувальник задач | Наявність планувальника завдань, який дасть можливість створювати заплановані завдання, серед яких: запуск зовнішньої програми, перевірка файлів під час запуску системи, створення знімка стану системи, перевірка комп’ютера, оновлення вірусних баз та модулів програми. Можливість планування завдань, які запускатимуться одноразово, періодично та за умови виникнення конкретних подій.Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску. |
| 1.13 | Система виявлення вторгнень | Наявність системи виявлення вторгнень (HIPS), яка захищає комп’ютер від шкідливих програм і небажаної активності. Також цей модуль має містити в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру. |
| 1.14 | Перевірка шифрованого трафіку | Можливість перевірки протоколу SSL та перевірки дійсності та цілісності сертифікатів. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим |
| 1.15 | Перевірка ВЕБ-сторінок | Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес. |
| 1.16 | Перевірка поштових протоколів | Забезпечення захисту поштового клієнту на робочій станції з можливістю інтеграції до поштового клієнту, перевіркою POP3, POP3S, SMTP, IMAP та IMAPS та забезпечення перевірки поштових вкладень. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті |
| 1.17 | Створення завантажувальних носіїв | Можливість створення завантажувального диску як на CD-, так і на USB-носіях засобами антивірусного продукту |
| 1.18 | Захист паролем | Можливість захисту від зміни параметрів ПЗ паролем |
| 1.19 | Віддалене управління | Наявність інструменту віддаленого управління.Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: перевірка зв'язку, пробудження віддаленого комп’ютера, перегляд спільних ресурсів, завершення роботи та перезавантаження, відправка повідомлень, увімкнення RDP сеансу та редактор мережевих команд.Наявність диспетчера груп, який дозволяє створювати та редагувати статистичні і динамічні групи клієнтів, а також здійснювати їх експорт/імпорт. Можливість імпорту з Active Directory, після якого створюється аналогічне дерево груп з користувачами, а також можливість виконувати періодичну синхронізацію з Active Directory.Можливість крім основного вказати резервний сервер адміністрування.Можливість виконання віддаленої інсталяції антивірусного програмного забезпечення на кілька кінцевих точок одночасно.Майстер конвертації баз даних.Майстер правил політик, який дає можливість налаштувати автоматичне розподілення клієнтів по групах, та призначення їм відповідних політик, в залежності від виконаних умов розподілу.Захист з'єднань за допомогою самостійно випущених сертифікатів.Можливість видалення сторонніх антивірусних продуктів за допомогою сервера адміністрування.Наявність спеціального компоненту для управління антивірусним захистом на віддалених робочих станція без необхідності використання додаткових серверів адміністрування.Спеціальний компонент, що спрощує виявлення незахищених робочих станцій.Можливість автентифікувати адміністраторів за допомогою груп безпеки Active Directory.Можливість використовувати двофакторну автентифікацію для облікових записів адміністраторів. |
| 1.20 | Додаткові можливості | Доступність усього вищевказаного функціоналу у рамках ліцензії, без додаткових придбань.Можливість замовити безкоштовні навчальні курси для системних адміністраторів.Можливість запросити технічних спеціалістів виробника для участі у внутрішніх конференціях з інформаційної безпеки, з метою інформування про сучасні загрози та методи протистояння шляхом впровадження необхідних налаштувань існуючої інфраструктури |
| 1.21 | Термін дії та кількість | Термін дії трьох ліцензій антивірусного програмного забезпечення повинен бути не менше ніж 1 рік, загальна кількість об’єктів, що покривають ліцензії: 1 436 шт. |

2. Програмне забезпечення виявлення та блокування атак на кінцевих пристроях ESET Inspect (або еквівалент) повинно:

2.1. Мати наявність панелі моніторингу для відслідковування актуальної інформації про аномальні події що виникли в корпоративній мережі.

2.2. Забезпечувати отримання попереджень про аномальні події, що виникли в роботі ПЗ на основі правил.

2.3. Мати можливість створювати список правил за замовчуванням та можливість створення власних правил що характеризують поведінку, як аномальну.

2.4. Автоматично класифікувати попередження за критичністю, що дозволяє швидко визначати та реагувати на критичні події.

2.5. Встановлювати пріоритет для попереджень для більш гнучкого сортування та фільтрації подій.

2.6. Групувати попередження за різними критеріями, такими як: тип, комп’ютер, правило, процес, файл.

2.7. Фіксувати інциденти інформаційної безпеки шляхом створення тривожних виявлень, які будуть містити як зведену інформацію про подію (коли і де це сталося (комп'ютер), від якого користувача, який виконуваний файл запускався, навіть який конкретний процес викликав запуск), так і детальну інформацію по кожному із перерахованих параметрів.

2.8. Мати в кожному тривожному виявленні спеціального інформаційного розділу, в якому буде надано детальний опис події, що викликала спрацювання правила, перелік можливих причин, можливі ризики та наслідки та рекомендації стосовно необхідних дій для подальшого аналізу інциденту.

2.9. Надавати, у разі виявлення критичних інцидентів, інформацію про перелік відомих технік та засобів, які раніше використовували зловмисники в подібних ситуаціях з посиланнями на відповідні розділи ресурсу MITRE ATT&CK, де можна ознайомитись з більш детальною інформацією про дії зловмисників.

2.10. Мати інтерактивний інтерфейс тривожних виявлень, що дозволяє поглиблюватись у більш детальний розгляд інциденту інформаційної безпеки для основних параметрів із наявних у зведеному тривожному виявленні.

2.11. Надавати детальну інформацію про процес, що викликав спрацювання, такої як дерево процесів, зміни в файловій системі та в реєстрі ОС, мережева активність, з'єднання з URL-адресами, додатково завантажені виконувані файли, а також найдетальніший журнал подій в ОС.

2.12. Автоматично класифікувати EXE/DLL файли за критичністю, що дозволяє швидко визначати та реагувати на аномальну поведінку файлів.

2.13. Автоматично класифікувати скрипти за критичністю, що дозволяє швидко визначати та реагувати на аномальну поведінку.

2.14. Створювати деталізовані виключення для окремих подій що повинні включати інформацію про контрольні суми виконуваних файлів, їх місцезнаходження, цифровий підпис та іншу інформацію.

2.15. Створювати білі/чорні списків EXE/DLL файлів.

2.16. Надавати можливість позначати EXE/DLL файли як довіренні або безпечні.

2.17. Надавати можливість позначати EXE/DLL файли як перевірені або проаналізовані.

2.18. Надавати можливість позначати перевірені скрипти як довіренні або безпечні.

2.19. Надавати можливість перегляду детальної інформації про EXE/DLL файли, попередження з ним пов’язані, статистику використання, зміни файлів, реєстру, створені мережеві підключення.

2.20. Створювати перелік всіх EXE/DLL файлів на робочих станціях і серверах з метою подальшого аналізу.

2.21. Вести список заблокованих EXE/DLL файлів з можливістю їх відновлення, видалення та завантаження для більш детального аналізу.

2.22. Надавати можливість завантаження підозрілих файлів з кінцевих точок для подальшого аналізу.

2.23. Надавати можливість здійснення прямо з консолі миттєвого пошуку додаткової інформації про файли на сторонніх ресурсах, таких як Virus Total тощо.

2.24. Надавати можливість отримання детальної інформації про тіло скрипта, задіяні EXE/DLL файли і процеси, список створених дочірніх процесів, зміни файлів, реєстру, створені мережеві підключення.

2.25. Надавати можливість завантаження підозрілих файлів-сценаріїв (скриптів) з кінцевих точок для подальшого аналізу.

2.26. Створювати список всіх сценаріїв, скриптів, що виконувалися на робочих станціях і серверах.

2.27. Надавати можливість групування скриптів за різними критеріями, такими як: батьківський процес, перший дочірній процес, командний рядок.

2.28. Формувати список комп’ютерів з детальною інформацією про події, EXE/DLL файли, скрипти.

2.29. Надавати можливість створення та збереження завдань пошуку по всій базі даних, що збираються з усіх підконтрольних комп'ютерів, за будь якими параметрами (навіть кількома символами з виконаного командного рядку) та з використанням різноманітних фільтрів.

2.30. Надавати можливість додавання підозрілих файлів EXE/DLL по контрольній сумі до переліку заблокованих, що призведе до блокування їх на робочих станціях і серверах.

2.31. Надавати можливість додавання любих контрольних сум файлів EXE/DLL до переліку заблокованих, що призведе до блокування їх на робочих станціях і серверах.

2.32. Надавати можливість віддалено здійснювати видалення та переміщення до карантину любих підозрілих файлів EXE/DLL.

2.33. Надавати можливість віддаленого перезавантаження робочої станції або її повного відключення.

2.34. Надавати можливість миттєвого запуску глибокого антивірусного сканування на віддаленій робочій станції.

2.35. Надавати можливість миттєвого створення на віддаленій робочій станції знімку стану операційної системи, що зафіксує інформацію про всі поточні запущені процеси, мережеві з'єднання, а також надасть інформацію про критичний контент реєстру ОС, завдання в планувальнику ОС, користувачів ОС та їх привілеї, вміст критичних файлів ОС, таких як "hosts", "win.ini" тощо, та всю детальну інформацію про ОС та встановлене ПЗ.

2.36. Надавати можливість використання рішення за умови, що управління ними буде здійснюватися існуючими наявними серверами адміністрування, які налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту інфраструктури регіональних та центрального підрозділів.

2.37. Надавати можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління.

2.38. Запропоноване ПЗ повинно мати центр технічної підтримки на території України, який має забезпечувати надання технічної підтримки користувачам відповідно до наступних вимог: обслуговування 24х7х365, включаючи святкові, вихідні та неробочі дні; розширені технічні консультації з питань конфігурації та функціонування ПЗ по телефону (з можливостю зв’язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв’язку) та електронній пошті; виїзд інженера на місце розташування Замовника у випадках збоїв роботи ПЗ.

2.39. Запропоноване програмне забезпечення повинно мати діючий експертний висновок Адміністрації Державної служби спеціального зв’язку та захисту інформації України на відповідність запропонованого програмного забезпечення вимогам технічного захисту інформації за результатом його державної експертизи у сфері технічного захисту інформації.

2.40. Має бути поставлена одна ліцензія на 500 об’єктів захисту. Термін дії ліцензій має бути не менш ніж 1 рік.

3. Програмне забезпечення, вимоги до якого зазначені в розділах 1 та 2 мають управлятися з єдиної консолі управління з web-інтерфейсом

Очікувана вартість предмета закупівлі:

Очікувана вартість предмета закупівлі: очікувана вартість визначена відповідно до процедур, які зазначені у примірній методиці визначення очікуваної вартості предмета закупівлі, введеної наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18.02.2020 №275 «Про затвердження примірної методики визначення очікуваної вартості предмета закупівлі». На підставі зазначеної вартості представництва компанії ESET та аналізу комерційних пропозицій очікувана вартість становить орієнтовно 1 250 000 грн.

**Директор департаменту ІТ Сергій СИРОВЕЦЬ**

Виконав: Бондаренко В.І. т.422-85-81