# 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 програмною продукцією ESET PROTECT MDR код ДК 021:2015: 48760000-3 Пакети програмного забезпечення для захисту від вірусів

**2. Вид процедури:** відкриті торги з особливостями (закупівля через Централізовану закупівельну організацію – ДП «УСС»)

**3. Номер оголошення закупівлі:** UA-2025-11-06-016630-a

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

**Вимоги до сервера керування**

1. Можливість централізованого управління антивірусним захистом всієї мережевої інфраструктури.
2. Можливість будування ієрархічної структури адміністрування, що складається з головного серверу та підпорядкованих серверів, що дає можливість здійснювати ценралізоване управління антивірусним захистом робочих станцій, серверів, та мобільних пристроїв, що належать як головному, так і регіональним підрозділам.
3. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
4. Інвентаризація програмного забезпечення, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.
5. Віддалена інсталяція антивірусного програмного забезпечення для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно.
6. Віддалена інсталяція користувальницького програмного забезпечення.
7. Можливість віддаленого видалення встановленого користувальницького програмного забезпечення.
8. Віддалене видалення антивірусного програмного забезпечення для ОС Windows, Linux та Mac
9. Можливість виконувати за допомогою інструменту віддаленого управління додаткові мережеві дії, такі як: завершення роботи та перезавантаження, відправка сигналу пробудження комп'ютера, відправка повідомлень, виконання конкретних інструкцій командного рядка на клієнтському комп'ютері, старт оновлення операційної системи клієнтського комп'ютера.
10. Наявність інструменту для створення та редагування інсталяційних пакетів для операційних систем Windows, Linux та Mac з попередньо встановленими настройками конфігурації, що дає можливість експортувати інсталяційні пакети для розгортання повноцінного антивірусного захисту на кінцевих точках в ізольованій

мережі, а також на кінцевих точках, що потребують захисту, але тимчасово не мають з'єднання з сервером адміністрування.

11. Наявність диспетчера користувачів, який дозволяє створювати різних користувачів сервера адміністрування, та призначати їм різні права доступу до окремих розділів, груп комп'ютерів на сервері адміністрування, що дає можливість надати різні права доступу для регіональних системних адміністраторів розгалуженої системи антивірусного захиту.

12. Можливість аутентифікувати адміністраторів консолі за допомогою груп безпеки Active Directory.

13. Можливість використовувати двофакторну аутентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованному підключенню до серверу централізованого управління.

14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації і всі дії, які виконують користувачі сервера адміністрування.

15. Можливість віддалено активувати та деактивувати модулі захисту, такі як персональний брандмауер, захист в режимі реального часу, захист поштового клієнта, захист доступу до Інтернету, контроль пристроїв, веб-контроль, антиспам на окремо взятому клієнті.

16. Можливість створювати та редагувати статичні групи та можливість імпорту з Active Directory дерева комп'ютерів.

17. Можливість налаштування автоматичного розподілу клієнтів по динамічних групах за багатьма критеріями, з наступним призначенням відповідних політик безпеки, а також запуском необхідних завдань.

18. Можливість імпорту користувачів та груп з Active Directory, для подальшого використання їх для персоналізації правил контролю пристроїв та веб-контролю.

19. Можливість використовувати як вбудовані так і користувальницькі політики, призначені для постійного обслуговування конфігураційних налаштувань антивірусних продуктів. Можливість здійснювати експорт/імпорт політик.

20. Наявність панелі моніторингу, яка надає всю необхідну детальну інформацію стосовно рівня захисту безпеки інфраструктури, стану захищених кінцевих точок, а також стану самого сервера адміністрування.

21. Наявність близько 100 передвстановлених шаблонів звітів, що можуть використовуватися як для панелі моніторингу, так і для формування різноманітних звітів.

22. Можливість створювати та редагувати шаблони звітів, які використовуються як для панелі моніторингу, так і для формування звітів у форматах PDF, CSV та подальшого зберігання за вказаним шляхом або відправлення на вказану електронну пошту.

23. Підтримка інструментом віддаленого адміністрування наступних баз даних: MS SQL Server, MySQL.

24. Можливість експортувати журнали в syslog для подальшої інтеграції з SIEM.

25. Можливість налаштовувати параметри журналів та звітів або вибрати з більш ніж 50 шаблонів для різних систем/клієнтів.

26. Можливість створювати дзеркало оновлень за допомогою антивірусного продукту, спеціальної утиліти або проксі серверу.

27. Можливість створення дзеркала оновлень на базі сторонніх HTTP-серверів.

28. Наявність веб-орієнтованого інтерфейсу, який дає можливість керувати сервером через будь який браузер шляхом з'єднання, захищеного сертифікатом.

29. Використання незалежного агенту, який дає можливість здійснювати віддалене управління антивірусним продуктом на кінцевих точках, а також контролювати рівень захисту антивірусного захисту на робочих станціях, та стан операційної системи.

30. Можливість відслідковувати все встановлене на робочій станції ПЗ, а також видаляти встановлене ПЗ за вибором.

31. Додатковий компонент, що дозволяє керувати антивірусним захистом на мобільних пристроях

32. Спеціальний компонент, який здійснює виявлення в мережі незахищенних робочих станцій для подальшого розгортання антивірусного захисту.

33. Захист з'єднань між компонентами сервера за допомогою як самостійно випущених сертифікатів, так і існуючих наявних сертифікатів.

34. Інструмент для керування станом ліцензій (навіть без використання сервера адміністрування.

35. Можливість деактивувати ліцензію антивірусних продуктів навіть на робочих станція до яких немає фізичного або віддаленого доступу

36. Можливість встановлення серверу адміністрування на ОС Windows та Linux

37. Постачання сервера адміністрування у розгорнутому вигляді, готовому для використання у таких віртуальних середовищах, як Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation).

38. Підтримка систем віртуалізації таких як VMware Horizon 8.x або Citrix XenCenter/XenServer 8+

39. Можливість визначати, яка віртуальна машина буде джерелом для копіювання або клонування у системах VDI.

40. Наявність майстра налаштування для визначення детальних параметрів для інтеграції з системами VDI

41. Можливість обирати варіанти обробки ідентифікаторів клонованих комп’ютерів, такі як зіставляння з наявними комп’ютерами або створення нових комп’ютерів.

42. Можливість визначати параметри шаблону іменування VDI для миттєвих клонів або каталогів машин.

43. Наявність передвстановлених шаблонів в системі сповіщень для інформування про некоректну індентифікацію клонованнних машин, що дає можливість сповіщати про некоректно налаштовану інтеграцію с системами VDI.

44. Сумісність з існуючим сервером централізованого керування та активація антивірусного ПЗ шляхом додавання ключа до існуючого сервера керування.

45. Наявність автоматичного оновлення агенту управління, що дає можливість без втручання адміністраторів використовувати актуальні версії.

46. Наявність механізму розподілу автоматичного процесу оновлення, що дозволяє знизити навантаження на мережу та комп'ютери в цілому.

47. Можливість встановлення агенту управління на ARM64 процесорах.

48. Наявність функціоналу створення площадок відповідно до філій компанії, що дозволяє назначити певну частину ліцензії окремим філіям.

49. Наявність функціоналу визначення адміністратора площадки або філії з відповідною частиною ліцензії.

**Вимоги до захисту кінцевих точок**

1. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
2. Надання захисту від: вірусів, троянського ПЗ, рекламного ПЗ, фішингу, а також шпигунського ПЗ.
3. Надання захисту від шкідливого ПЗ - певного шкідливого коду, який додається на початок або кінець коду наявних файлів на комп’ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.
4. Надання захисту від потенційно небажаних програм, яких не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни, але ці програми можуть інсталювати додаткове небажане ПЗ, змінювати налаштування системи, а також виконувати неочікувані дії або дії, не підтверджені користувачем.
5. Надання захисту від потенційно небезпечних програм - різноманітного ПЗ, що може використовуватися для зловмисних цілей, таких як несанкціонований віддалений доступ, викрадення або злам паролів, клавіатурні шпигуни тощо.
6. Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого програмного забезпечення.
7. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.
8. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.
9. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.
10. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.
11. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.

12. Забезпечення антивірусного захисту в режимі реального часу.

13. Використання евристичних технологій власної розробки під час сканування.

14. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.

15. Модуль захисту документів, що дає можливість перевіряти макроси Microsoft Office на наявність зловмисного коду.

16. Можливість сканування файлів під час запуску ОС.

17. Можливість сканування WMI та системного реєстру, усіх розділів та підрозділів, що забезпечує захист від шкідливого програмного коду та зловмисних посилань, які поширюються у вигляді даних.

18. Наявність вбудованого інструмента, що об'єднує в собі декілька утиліт для очищення залишків складних стійких загроз, таких як Conficker, Sirefef, Necurs та ін.

19. Сканування комп'ютера у неактивному стані.

20. 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.

21. Використання 64-бітового ядра для сканування, що зменшує навантаження на систему та дозволяє зробити найшвидші та найефективніші сканування

22. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного програмного забезпечення.

23. Модуль захисту від експлойтів який забезпечує захист від загроз здатних використовувати уразливості різноманітних додатків, таких як Java, Flash тощо.

24. Модуль, який глибоко аналізує запущені процеси та їх діяльність в файловій системі, що забезпечує додатковий рівень захисту від програм-вимагачів (Ransomware).

25. Модуль сканування оперативної пам'яті, який здатен відстежувати роботу підозрілих запущених процесів, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами.

26. Наявність системи виявлення вторгнень (HIPS), що слідкує за запуском програм та змінами в системному реєстрі та захищає комп’ютер від шкідливих програм і небажаної активності.

27. Можливість створювати власні правила для контролю запущених процесів, виконуваних файлів та розділів реєстру.

28. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.

29. Можливість інтеграції захисту робочих станцій та серверів з хмарною пісочницею (при наявності додаткової ліцензії), без необхідності встановлення додаткових програмних продуктів.

30. Автоматична антивірусна перевірка змінних носіїв.

31. Наявність інструменту, який зможе здійснювати контроль підключення до робочої станції змінних носіїв шляхом створення правил доступу, а саме: блокування, дозвіл, тільки читання, читання та запис, попередження.

32. Можливість здійснювати контроль підключення до робочої станції зовнішніх пристроїв за типом пристрою, за виробником, моделлю або серійним номером пристрою.

33. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.

34. Можливість забороняти або дозволяти підключення зовнішніх пристроїв як для всіх, так і для окремих користувачів або груп Windows або домену.

35. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила контролю пристроїв.

36. Забезпечення додаткового рівня захисту поштового трафіку на робочій станції шляхом інтеграції до поштового клієнту, з можливістю перевірки POP3, POP3S, SMTP, IMAP та IMAPS та перевірки поштових вкладень, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.

37. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.

38. Наявність модуля захисту від спаму власної розробки з можливістю інтеграції до поштового клієнту, що забезпечує додатковий рівень захисту від спаму, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.

39. Можливість використовувати білі та чорні списки спам-адресатів як користувальницькі (гнучка персоналізація інтелектуального спам-модулю), так і глобальні, інформація до яких надходить з серверів оновлення.

40. Забезпечення додаткового рівня захисту інтернет-трафіку шляхом перевірки HTTP, HTTPS трафіку, що дає можливість не тільки блокувати файли, що передаються цими протоколами, а й блокувати адреси таких небезпечних ресурсів, як фішингові сайти, сервери ботнетів, командні (C&C) сервери APT, а також сервери, що розповсюджують загрози класу «ransomware».

41. Можливість створення списків заблокованих, дозволених або виключених з перевірки URL-адрес.

42. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням, особливо на тих ПК, що тимчасово або постійно знаходяться за межами корпоративної мережі.

43. Можливість перевірки протоколу SSL як в автоматичному, так і в інтерактивному режимах.

44. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.

45. Можливість керувати списками довірених сертифікатів та сертифікатів виключених з перевірки, а також можливість вибору дії при визначенні сертифіката недіючим, невизначеним або пошкодженим .

46. Наявність додаткового модуля, який дає можливість запускати браузери у захищеному режимі з метою блокування спроб втручання в область пам'яті браузера та вмісту його вікон, а також додаткового захисту критичних інтернет з’єднань таких як інтернет-платежі та інтернет-банкінг тощо.

47. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).

48. Наявність персонального брандмауера для здійснення мережевої фільтрації та захисту як від зовнішніх, так і локальних мережевих атак.

49. Наявність у персональному брандмауеру інтерактивного режиму, що надає детальну інформацію про нове невідоме мережеве з'єднання та дає можливість не тільки створювати на ПК нове правило мережевої фільтрації для виявленого з'єднання, а й вказувати детальні налаштування для нього.

50. Наявність у персональному брандмауеру режиму навчання, що дає можливість адміністратору віддалено налаштовувати дозвільні правила для мережевих додатків та обладнання.

51. Наявність редактора правил, що дає можливість не тільки редагувати створені правила, а й керувати вбудованими правилами, яких достатньо для первинного ретельного захисту від несанкціонованих мережевих з'єднань та локальних мережевих атак.

52. Можливість створювати правила мережевої фільтрації для конкретних програм і сервісів.

53. Можливість створювати для персонального брандмауеру різні профілі , які можуть автоматично переключатися, в залежності від того, до якої мережі підключено комп'ютер.

54. Можливість використовувати у персональному брандмауері додаткову автентифікацію мережі з метою запобігання несанкціонованого підключення ПК до невідомих небезпечних мереж.

55. Наявність додаткового функціоналу персонального брандмауеру, що дозволяє переглядати всю детальну інформацію по всіх наявних мережевих з'єднаннях, а також попереджати користувача про підключення до незахищеної мережі Wi-Fi.

56. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп’ютер.

57. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет".

58. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP і т.д.

59. Наявність упроваджених методів виявлення різноманітних атак, що намагаються використовувати вразливості програмного забезпечення та надання докладнішої інформації про ідентифікатори CVE

60. Можливість переглядати на ПК автоматично заблоковані мережеві з'єднання та, за необхідністю, тимчасово дозволяти конкретні безпечні мережеві з'єднання.

61. Наявність додаткового функціоналу персонального брандмауеру, що дає можливість переглядати на ПК перелік заблокованих IP-адрес, надає інформацію про причини потрапляння до чорного списку, та дозволяє зробити виключення для конкретних безпечних адрес.

62. Наявність додаткового функціоналу персонального брандмауеру, який здатен виявляти ті зміни в мережевих програмах, що спричинили нові несанкціоновані мережеві з'єднання.

63. Фільтрація інтернет-трафіку.

64. Наявність модуля веб-контролю, що дає можливість обмежувати доступ до певних категорій сайтів.

65. 27 категорій фільтрації інтернет-трафіку, в яких розподілені більш ніж 100 підкатегорій, а також можливість створювати групи з категорій та підкатегорій.

66. Можливість створювати правила фільтрації інтернет-трафіку для різних користувачів та груп ОС Windows або домену.

67. Можливість задавати часові інтервали, що дозволяє більш гнучко налаштовувати правила веб-фільтрації.

68. Регламентне оновлення вірусних баз не менше 24 разів за добу.

69. Отримання оновлення клієнтів з локального сховища на сервері, що дозволяє підтримувати актуальність антивірусного захисту в закритих ізольованих мережах, що не мають доступу до мережі Інтернет.

70. Можливість створення дзеркала оновлень на базі рішень для захисту кінцевих точок.

71. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.

72. Можливість для портативних комп'ютерів отримувати оновлення з серверів виробника он-лайн, у разі перебування поза корпоративною мережею.

73. Відкат оновлень з можливістю повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.

74. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.

75. Інструменти моніторингу, оцінки стану безпеки та реагування:

76. Наявність механізму контролю за станом безпеки та актуальністю оновлень ОС.

77. 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 ПЗ, мережеві з'єднання.

78. Можливість визначення рівня критичності (небезпечний, невідомий, маловідомий, безпечний) значень різноманітних параметрів операційної системи, з метою виявлення несанкціонованих та небезпечних змін у операційній системі.

79. Можливість порівнювати різні знімки стану системи з метою виявлення змін, які відбулись в системі за визначений час.

80. Можливість створювати та віддалено виконувати скрипти, що дасть змогу на віддаленому ПК зупиняти запущені процеси та служби, видаляти гілки реєстру, блокувати мережеві з'єднання.

81. Локальне зберігання журналів на робочих станціях.

82. 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.

83. Можливість планування завдань, які запускатимуться одноразово, періодично, а також за умови виникнення конкретних подій.

84. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.

85. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.

86. Можливість захисту паролем параметрів рішення для захисту кінцевої точки.

87. Наявність режиму перевизначення політики, що дає системному адміністратору тимчасову можливість змінювати на ПК ті налаштування антивірусного ПЗ, що призначаються політикою, та недосяжні для редагування, з метою гнучкого налаштування антивірусного ПЗ у специфічному середовищі.

88. Графічний інтерфейс, сумісний із сенсорним екраном високої роздільної здатності.

89. Можливість гнучко налаштовувати сповіщення та повідомлення про події на робочому столі користувача.

90. Можливість віддаленого встановлення на клієнтську робочу станцію.

91. Можливість предвстановлення на окремих ПК або у образі VDI за допомогою комплексного інсталятору, що дасть можливість з'єднуватись з сервером управління одразу після підключення до мережі або запуску у середовищі VDI.

92. Можливість дозволити оновлення компонентів в автоматичному режимі, що дає можливість завантажити та інсталювати компоненти без втручання адміністратора або користувача.

93. Можливість оновлення компонентів в ручному режимі, що дає можливість оновлення компонентів на некерованих робочих станціях.

94. Можливість оновлення деяких компонентів без необхідності перезавантаження для початку функціонування.

95. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.

96. У антивірусному продукті мають використовуватися не запозичені, а власні технологічні розробки для ефективної роботи усіх основних модулів та сервісів.

97. Можливість крім основного вказати резервні сервери адміністрування.

98. Наявність інструменту віддаленого управління.

99. Низьке споживання ресурсів ПК актуальними антивірусними продуктами (сукупно усіма процесами: графічний інтерфейс, процес комплексного захисту, служба віддаленого адміністрування): 50-100 МБ оперативної пам'яті, 2-35 % центрального процесору.

100. Наявність багатомовного інсталятора, який містить в собі в тому числі українську мову.

101. Підтримка ОС: Microsoft Windows 7 (SP1); Microsoft Windows 8; Microsoft Windows 8.1; Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit; Ubuntu Desktop 20.04 LTS; Ubuntu Desktop 22.04 LTS; Red Hat Enterprise Linux 7,

8 .; SUSE Linux Enterprise Desktop 15; Linux Mint 20; macOS 10.12 та більш нові версії: Android 5 (Lollipop) та більш нові версії:

102. Підтримка Microsoft Windows 10 Multi-session та Azure virtualized Windows 10

**Вимоги до захисту серверів**

1. Автоматичне визначення ролей сервера для створювання автоматичних виключень для специфічних файлів, папок, програм, що дозволяє мінімізувати вплив на роботу серверної операційної системи.
2. Надання захисту від: шкідливих програм, троянського ПЗ, клавіатурних шпіонів, рекламного ПЗ, фішингу, шпигунського ПЗ, руткітів, скриптів, потенційного небажаного та небезпечного ПЗ.
3. Забезпечення захисту в режимі реального часу.
4. Використання евристичних технологій під час сканування.
5. Антивірусне сканування за вимогою користувача або адміністратора та згідно графіку.
6. Сканування Hyper-V на наявність вірусів, що дозволяє сканувати диски сервера Microsoft Hyper-V Server, тобто віртуальних машин (ВМ), без необхідності установки будь-яких агентів на відповідних віртуальних машинах.
7. Модуль захисту документів Microsoft Office, що дає можливість перевіряти макроси на наявність зловмисного коду.
8. Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків
9. Додатковий рівень захисту користувачів від програм-вимагачів контролює та оцінює всі програми на основі їхньої поведінки та репутації.
10. Можливість інтеграції захисту робочих станцій та серверів з хмарною пісочницею (при наявності додаткової ліцензії), без необхідності встановлення додаткових програмних продуктів.
11. Сканування інтерфейсу UEFI - перевірка на наявність шкідливого програмного забезпечення в головному завантажувальному записі.
12. Можливість сканування файлів під час запуску операційної системи.
13. 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.
14. Сканування комп'ютера у неактивному стані.
15. 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.
16. Автоматична антивірусна перевірка змінних носіїв.
17. 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.

18. Наявність системи виявлення вторгнень (HIPS), яка захищає комп'ютер від шкідливих програм і небажаної активності. Також цей модуль містить в собі майстер для створення правил та редактор правил для контролю запущених процесів, використовуваних файлів та розділів реєстру.

19. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.

20. 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.

21. Можливість автоматично видаляти або переміщувати заражену пошту до вказаного каталогу у поштовому клієнті.

22. Перевірка HTTP, HTTPS трафіку з можливістю створення листів виключених з перевірки, заблокованих та дозволених URL-адрес.

23. Можливість блокувати завантаження з Інтернету файлів за вказаним розширенням.

24. 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 .

25. Можливість створення виключень з перевірки трафіку для окремих програм та окремих IP-об'єктів (IP-адресів, діапазонів IP-адресів, підмереж).

26. Можливість налаштування додаткових параметрів модуля системи виявлення вторгнень (IDS) з метою виявлення різних типів можливих мережевих атак на комп'ютер.

27. Можливість використання технології, яка забезпечує захист від загроз типу "ботнет".

28. Захист уразливостей мережевого протоколу, що покращує виявлення загроз, які використовують недоліки мережевих протоколів, таких як SMB, RPC, RDP тощо.

29. Регламентне оновлення вірусних баз не менше 24 разів за добу.

30. Отримання оновлення клієнтів з локального дзеркала на сервері.

31. Можливість створення дзеркала оновлень засобами антивірусного ПЗ.

32. Можливість отримувати оновлення вірусних баз з резервних джерел, якщо основне джерело оновлення буде недосяжне.

33. Відкат оновлень з можливість повернутися до попередніх версій баз вірусних сигнатур і модулів оновлення, та можливістю тимчасово призупинити оновлення або встановлювати нові вручну.

34. Можливість оновлення у режимі отримання регулярних, тестових та відкладених оновлень.

35. Можливість крім основного вказати резервні сервери адміністрування.

36. Наявність механізму контролю за актуальністю оновлень операційної системи.

37. 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 ПЗ, мережеві з'єднання. Завдяки вмінню порівнювати різні знімки стану системи цей інструмент може виявити зміни, які відбулись в системі. Також він може створювати та виконувати скрипти, що дасть можливість зупиняти запущені процеси, видаляти гілки реєстру, блокувати мережеві з'єднання.

38. 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.

39. Можливість створення у планувальнику декількох однотипних завдань з різною періодичністю або різними умовами запуску.

40. Можливість роботи в кластерах як домена так і робочої групи

41. Можливість налаштовувати швидкодію, вказуючи кількість потоків сканування.

42. Можливість налаштовувати режим запуску шляхом відключення графічного інтерфейсу для термінальних користувачів, що дає можливість зменшити навантаження на сервер, який працює у режимі серверу терміналів.

43. Можливість створення завантажувального диску як на CD-, так і на USB-носіях з встановленим антивірусним продуктом.

44. Підтримка роботи програм, що працюють в повноекранному режимі, з можливістю приховати всі повідомлення від антивірусного ПЗ.

45. Можливість захисту паролем від зміни параметрів та видалення антивірусного ПЗ.

46. Можливість віддаленого встановлення на файловий сервер.

47. Можливість предвстановлення на окремих файлових серверах за допомогою комплексного інсталятору, що дасть можливість з'єднуватись з сервером управління одразу після підключення до мережі.

48. Можливість інтеграції з хмарним сервісом Microsoft Azure.

49. Підтримка ОС: Microsoft Windows Server 2022; Microsoft Windows Server 2019; Microsoft Windows Server 2016; Microsoft Windows Server 2012 R2; Microsoft Windows Storage Server 2016; Microsoft Windows Server 2019 Essentials; Microsoft Windows Server 2016 Essentials; Microsoft Windows Server 2012 R2 Essentials; Microsoft Windows Server 2012 Essentials; Microsoft Windows Server 2012 Foundation; Microsoft Windows MultiPoint Server 2011; Microsoft Windows MultiPoint Server 2010; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8, Amazon Linux 2.

**Вимоги до розширеного виявлення та реагування (EDR/XDR)**

1. Наявність панелі моніторингу для відслідковування актуальної інформації про аномальні події що виникли в корпоративній мережі
2. Отримання попереджень про аномальні події що виникли в роботі ПЗ на основі правил
3. Список правил за замовчуванням та можливість створення власних правил що характеризують поведінку ПЗ як аномальне
4. Автоматична класифікація попереджень за критичністю, що дозволяє швидко визначати та реагувати на критичні події.
5. Можливість встановлювати пріоритет для попереджень для більш гнучкого сортування та фільтрації подій.
6. Можливість групування попереджень за різними критеріями, такими як: тип, комп’ютер, правило, процес, файл.
7. Можливість 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 зазначених параметрів.
8. Наявність 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.
9. Можливість надати, 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.
10. Наявність інтерактивного інтерфейсу тривожних виявлень, що дозволяє поглиблюватись у більш детальний розгляд інциденту інформаційної безпеки для основних параметрів із наявних у зведеному тривожному виявленні.
11. Надання детальної інформації 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.
12. Автоматична класифікація EXE/DLL файлів за критичністю, що дозволяє швидко визначати та реагувати на аномальну поведінку файлів.
13. Автоматична класифікація скриптів за критичністю, що дозволяє швидко визначати та реагувати на аномальну поведінку.
14. Можливість створення деталізованих виключень для окремих подій що повинні включати інформацію про контрольні суми виконуваних файлів, їх місцезнаходження, цифровий підпис та іншу інформацію
15. Можливість створення білих/чорних списків EXE/DLL файлів.
16. Можливість позначати EXE/DLL файли як довіренні або безпечні.
17. Можливість позначати EXE/DLL файли як перевірені або проаналізовані

18. Можливість позначати перевірені скрипти як довіренні або безпечні.

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

20. Створення переліку всіх EXE/DLL файлів на робочих станціях і серверах з метою подальшого аналізу.

21. Список заблокованих EXE/DLL файлів з можливістю їх відновлення, видалення та завантаження для більш детального аналізу

22. Можливість завантаження підозрілих файлів з кінцевих точок для подальшого аналізу.

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

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

25. Можливість завантаження підозрілих файлів-сценаріїв (скриптів) з кінцевих точок для подальшого аналізу.

26. Створення списку всіх сценаріїв, скриптів, що виконувалися на робочих станціях і серверах

27. Можливість групування скриптів за різними критеріями, такими як: батьківський процес, перший дочірній процес, командний рядок.

28. Формування списку комп’ютерів з детальною інформацією про події, EXE/DLL файли, скрипти.

29. 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.

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

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

32. Можливість віддалено здійснювати видалення та переміщення до карантину любих підозрілих файлів EXE/DLL

33. Можливість віддаленого перезавантаження робочої станції або її повного відключення

34. Можливість миттєвого запуску глибокого антивірусного сканування на віддаленій робочій станції.

35. 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.

36. Можливість використовувати двофакторну автентифікацію для облікових записів адміністраторів, що дає можливість запобігти несанкціонованому підключенню до серверу централізованого управління.

37. Microsoft Windows 7 (SP1); Microsoft Windows 8; Microsoft Windows 8.1; Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit; Ubuntu Desktop 20.04 LTS; Ubuntu Desktop 22.04 LTS; Red Hat Enterprise Linux 7, 8 .; SUSE Linux Enterprise Desktop 15; Linux Mint 20; macOS 10.12 та більш нові версії; Microsoft Windows Server 2012R2, 2012, 2016, 2019, 2022; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12,SUSE Linux Enterprise Server (SLES) 15,Oracle Linux 8, Amazon Linux 2.

**Вимоги до двуфакторної автентифікації**

1. Можливість додання 2FA для безпечного доступу входу в як локальний обліковий запис, так і доменний обліковий запис системи під управлінням: Miscrosoft Windows, Linux або MAC OS X.
2. Можливість отримання паролів 2FA за допомогою смс-повідомлень, push-повідомлень, OTP.
3. Підтримку апаратних токенів, які працюють по стандартам OATH, HOTP, TOTP, FIDO, FIDO2.
4. Можливість додання 2FA для веб-додатків Microsoft: Microsoft Outlook Web App, Microsoft Exchange, Microsoft SharePoint, Microsoft Exchange Mailbox Server Role, Microsoft SharePoint Foundation, Microsoft Dynamics CRM, Microsoft Remote Desktop Web Access, Microsoft Remote Desktop Gateway, Microsoft Terminal Services Web Access, Microsoft Exchange Admin Center
5. Наявність API, яка дозволяє швидко додавати двофакторну аутентифікацію в наявні додатки.
6. Наявність пакету SDK, що надає доступ до функцій керування користувачами та їх аутентифікаціями.
7. Захист VPN TA VDI систем, таких як : Microsoft Forefront Threat Management Gateway, Barracuda, F5 FirePass, Cisco ASA IPSEC,Cisco ASA SSL, Fortinet FortiGate, Citrix Access Gateway, Juniper, Citrix NetScaler, Palo Alto, Check Point Software, SonicWall, Netasq, VMware Horizon View и Citrix XenApp, Cyberoam.
8. Можливість захисту RADIUS PAM для Linux, Mac.
9. Наявність Identity Provider Connector для забезпечення 2FA хмарних служб (постачальником послуг) і постачальником ідентифікаційних даних, таких як : OpenAM, Okta, Azure AD, AD FS, Shibboleth, Keycloak, Dropbox, Confluence
10. Захист через SSO та Microsoft Active Directory Federation Services для входу до Office 365 або Azure.
11. Можливість захисту мобільного додатку за допомогою біометрики на базі операційних систем IOS та Android.

12. Інформування користувача про спробу авторизації з можливістю підтвердити або відхилити подальшу автентифікацію.

13. Наявність системи звітності, що можуть використовуватися як для панелі моніторингу, так і для формування звітів.

14. Наявність журналу аудиту, у якому реєструються і відстежуються всі зміни в конфігурації, запуск та зупинки служби двофакторної автентифікації.

15. Можливість інтеграції з SIEM та іншими системами моніторингу, аналітики та реагування.

16. Можливість для адміністратора надавати альтернативний одноразовий пароль OTP у разі, якщо коли користувач немає доступу до токену або до мобільного додатку.

17. Можливість імпортувати користувачів у спеціальні області за допомогою файлу CSV або LDF.

18. Можливість використання 2FA для безпечного режиму, блокуванні облікового запису Windows, використання UAC.

19. Можливість налаштувати використання 2FA для користувачів, які не мають підключення до серверу 2FA.

20. Можливість обмежити кількість використання одноразовий паролів для комп'ютерів, які не мають підключення до серверу 2FA

21. Наявність захисту від підбору одноразового паролю шляхом блокування користувача .

22. Наявність системи сповіщень про вибрані типи дій.

23. Можливість виключення з 2FA для списку IP-адрес.

24. Можливість налаштування користувацького способу доставлення паролів OTP.

25. Можливість синхронізації користувачів за допомогою LDAP та Mac Open Directory.

Вимоги до системи керування вразливостями та виправленнями

1. Керування вразливостями і виправленнями для операційних систем і додатків.
2. Автоматичне сканування системи на наявність вразливостей.
3. Оцінка критичності вразливостей з урахуванням контексту системи.
4. Можливість налаштування автоматичного або ручного застосування виправлень.
5. Підтримка широкого спектра ОС і додатків (Windows, Linux, MacOS).
6. Можливість тестування виправлень перед застосуванням.
7. Налаштування розкладів для автоматичного застосування виправленнями.
8. Створення звітів про поточний стан безпеки системи.
9. Аналітика щодо усунення вразливостей і застосування оновлень.
10. Повідомлення про критичні вразливості та статус виправлень.
11. Можливість інтеграції з SIEM системами.
12. Підтримка автоматичного розгортання виправлень і оновлень.

13. Забезпечення безперервності роботи користувачів під час встановлення виправлень.

**Вимоги до сервісу MDR**

1. Цілодобовий моніторинг подій безпеки (24/7/365) спеціалізованою командою аналітиків безпеки.
2. Інтеграція з SIEM&SOAR системами вендора для забезпечення цілодобового моніторингу інфраструктури.
3. Можливість централізованого керування та моніторингу захищених пристроїв (Windows, Linux, MacOS) через єдину консоль.
4. Наявність попередньо налаштованих політик безпеки, що охоплюють основні вектори атак (мережа, процеси, скрипти, документи тощо).
5. Можливість автоматичного реагування на інциденти, зокрема ізоляція хоста, завершення процесів, блокування IP-адрес, об'єктів тощо.
6. Виявлення загроз у реальному часі з використанням як локальних, так і глобальних індикаторів компрометації (IoC).
7. Побудова та ведення повного ланцюга інциденту, включаючи джерело, вектор проникнення, дії зловмисника, цілі.
8. Можливість надання регулярних звітів про інциденти та стан безпеки, включно з рекомендаціями щодо покращення захисту.
9. Можливість кастомізації політик виявлення та автоматичного реагування відповідно до особливостей інфраструктури компанії.
10. Підтримка зворотного зв’язку з SOC-командою у вигляді кейс-менеджменту через портал, електронну пошту або через спеціальний портал.
11. Можливість створення білого та чорного списку програм/сценаріїв/процесів.
12. Наявність у вендора сертифікації за стандартом ISO/IEC 27001.
13. Наявність аудиту відповідності мінімум SOC 2 Type I для підтвердження контролю безпеки, доступності, конфіденційності, цілісності обробки та захисту персональних даних у вендора під час надання сервісу.
14. Звітність за запитом щодо динаміки інцидентів, зведеної статистики, змін активності загроз.

**5. Обґрунтування розміру бюджетного призначення:**

Розмір бюджетного призначення визначено відповідно до кошторису Державного агентства України ПлейСіті на 2025 рік за бюджетною програмою КПКВК 2902010 «Керівництво та управління у сфері регулювання азартних ігор та лотерей».

**6. Обґрунтування очікуваної вартості закупівель:**

Згідно з абзацами одинадцятим та дванадцятим пункту 1 розділу III Примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Міністерства розвитку економіки, торгівлі та сільського господарства України від 18

лютого 2020 року № 275, за результатами запиту цінових пропозицій до компаній, проведеної аналітики на платформі Prozorro, а також з урахуванням потреби у забезпеченні службових комп’ютерів для захисту від вірусів, була визначена очікувана вартість 380 000,00 (триста вісімдесят тисяч гривень 00 копійок) з урахування ПДВ.