ОБГРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі послуг згідно з ДК 021:2015 код 72260000-5 «Послуги, пов'язані з програмним забезпеченням» (Послуга у сфері інформатизації з постачання програмного забезпечення «ESET PROTECT Enterprise» з локальним управлінням зі строком дії на 1 рік для оновлення та захисту 500 об'єктів на виконання п. 4.4. завдань регіональної програми інформатизації "Електронна Дніпропетровщина" на 2020–2022 роки)

1. Замовник

Департамент цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської облдержадміністрації.

2. Підстави закупівлі

Закупівля здійснюється відповідно до пункту 4.4. завдань регіональної програми інформатизації «Електронна Дніпропетровщина» на 2020–2022 роки, яку затверджено рішенням сесії Дніпропетровської обласної ради від 25 жовтня 2019 року № 506-18/VII.

Метою закупівлі є забезпечення антивірусним захистом серверного обладнання електронного комунікаційного центру області, поштових шлюзів, автоматизованих робочих місць користувачів корпоративної мережі системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації відповідно до вимог комплексної системи захисту інформації.

Одним із головних компонентів комплексної системи захисту інформації є програмне забезпечення антивірусного захисту.

На даний час система інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації функціонує на базі захищеного електронного комунікаційного центру (далі – ЕКЦ) області комунального підприємства "Головний інформаційно-комунікаційний і науково-виробничий центр" Дніпропетровської обласної ради", який об'єднує 47 серверів, 6 технологічних систем, 4 сховища даних та має близько 2000 користувачів корпоративної мережі, до якої входять: працівники апарату та структурних підрозділів облдержадміністрації, обласної ради, райдержадміністрацій, відповідних органів місцевого самоврядування області, у т.ч. територіальних громад.

На базі захищеного ЕКЦ області активно функціонують та розвиваються корпоративні хмарні сервіси (система електронного документообігу, реєстр територіальних громад, віртуальний офіс електронних послуг, платформа створення веб-сайтів тощо).

Відповідно до вимог комплексної системи захисту інформації необхідно проводити заходи щодо захисту автоматизованих робочих місць від проявів шкідливих програмних засобів, забезпечення технічних умов для безперебійного функціонування комп'ютерного обладнання та захисту інформації на них.

Одним з найдієвіших заходів для вирішення вищезазначених завдань є встановлення сучасного антивірусного програмного забезпечення на автоматизовані робочі місця.

При цьому слід зауважити, що згідно з дорученням Прем'єр-міністра України від 29.04.2022 № 9178/1/1-22 до листа Головнокомандуючого Збройних Сил України від 14.04.2022 № 300/1/С/1205 щодо підвищення рівня кіберзахисту системи електронного документообігу (далі – СЕДО) доручено при роботі у програмно-апаратних комплексах СЕДО здійснити низку заходів, у тому числі забезпечити використання функції розширеного виявлення та реагування на інциденти (XDR).

На даний час на базі електронного комунікаційного центру області функціонує версія захисту ESET PROTECT Entry, у якій не підтримується функція XDR. Найближчою за ціновою категорією у лінійці продуктів захисту ESET PROTECT, у якій забезпечено роботу функції XDR, є програмний продукт ESET PROTECT Enterprise.

ESET PROTECT Enterprise дозволяє, окрім виконання функції захисту робочих станцій із потужним машинним навчанням та зручним управлінням (функції базового програмного продукту ESET PROTECT Entry), додатково здійснювати захист робочих станцій від програм-вимагачів та “0-денних” загроз, а також забезпечувати безпеку даних, розширене виявлення та реагування на інциденти (XDR) з можливостями огляду корпоративної мережі.

Кількість необхідних ліцензій визначається кількістю користувачів, які користуються СЕДО, і складає 500 примірників програмної продукції.

Ввідповідно до Закону України “Про Національну програму інформатизації” та постанови Кабінету Міністрів України від 25.07.2002 № 1048 “Про затвердження Порядку проведення експертизи національної програми інформатизації та окремих її завдань (проектів)” (зі змінами), на виконання ст. 48 Бюджетного кодексу України департаментом цифрової трансформації, інформаційних технологій та електронного урядування Дніпропетровської облдержадміністрації в установленому порядку отримано погодження проведення закупівлі послуг згідно з ДК 021:2015 код 72260000-5 «Послуги, пов’язані з програмним забезпеченням» (Послуга у сфері інформатизації з постачання програмного забезпечення «ESET PROTECT Enterprise» з локальним управлінням зі строком дії на 1 рік для оновлення та захисту 500 об’єктів на виконання п. 4.4. завдань регіональної програми інформатизації “Електронна Дніпропетровщина” на 2020–2022 роки) від Міністерства цифрової трансформації України (лист від 02.09.2022 №1/06-2-7566).

3. Очікувана вартість предмета закупівлі: 635 000 грн з ПДВ. (обласний бюджет).

Очікувана вартість сформована на підставі запиту безпосередньо до виробника програмної продукції антивірусного захисту, самостійного аналізу цін на аналогічні за технічними характеристиками типи програмної продукції через мережу Інтернет та в електронній системі закупівель Prozorro, а також з урахуванням необхідності економії бюджетних коштів в умовах воєнного стану.

4. Технічні та якісні характеристики предмета закупівлі

ТЕХНІЧНА СПЕЦИФІКАЦІЯ

Найменування програмного забезпечення	Кількість, од.
Програмне забезпечення “ESET PROTECT Enterprise” з локальним управлінням зі строком дії на 1 рік для оновлення та захисту 500 об’єктів на виконання п. 4.4. завдань регіональної програми інформатизації “Електронна Дніпропетровщина” на 2020–2022 роки	1

ESET PROTECT Enterprise з локальним управлінням повинно відповідати наступним обов’язковим функціональним вимогам:

1. Надання захисту від: вірусів, троянського програмного забезпечення (далі – ПЗ), рекламного ПЗ, фішингу, а також шпигунського ПЗ.
2. Надання захисту від шкідливого ПЗ – певного шкідливого коду, який одається на початок або кінець коду наявних файлів на комп’ютері. Виявлення шкідливого ПЗ повинно здійснюватися ядром виявлення в поєднанні з компонентом машинного навчання.
3. 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.

4. 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.

5. Надання захисту від підозрілих програм – програм, які стиснуті тими пакувальниками або протекторами, що часто використовують зловмисники за для того, щоб запобігти виявленню шкідливого ПЗ.

6. Надання захисту від небезпечних програм руткітів, які надають зловмисникам з Інтернету необмежений доступ до системи, водночас приховуючи свою присутність в операційній системі.

7. Можливість для різних категорій загроз налаштовувати окремі рівні реагування як для захисту, так і для звітування.

8. Можливість робити виключення зі сканування певних файлів, які не є шкідливими, але сканування яких може спричинити відхилення в роботі або впливати на продуктивність системи.

9. Можливість створювати виключення для загальносистемних процесів з метою покращити швидкість роботи системних служб та мінімізувати втручання в процес роботи ОС.

10. Можливість здійснювати перевірку завантажувальних секторів на наявність вірусів у головному завантажувальному записі, в тому числі у інтерфейсі UEFI.

11. Забезпечення антивірусного захисту в режимі реального часу.

12. Використання евристичних технологій власної розробки під час сканування.

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

14. Модуль захисту документів, що дає можливість перевіряти макроси MS Office на наявність зловмисного коду.

15. Можливість сканування файлів під час запуску ОС.

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

17. Сканування комп'ютера у неактивному стані.

18. 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.

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

20. Можливість використання технологій машинного навчання для більш поглибленого аналізу коду з метою виявлення зловмисної поведінки та характеристик зловмисного ПЗ.

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

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

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

24. 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.

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

26. Додаткова перевірка запущених процесів у хмарному репутаційному сервісі.

27. Автоматична антивірусна перевірка змінних носіїв.

28. 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.

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

30. Можливість створювати групи дозволених або заборонених зовнішніх пристроїв.

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

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

33. 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.

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

35. 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.

36. 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».

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

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

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

40. Перевірка дійсності та цілісності сертифікатів SSL-трафіку.

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

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

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

44. 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.

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

46. 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.

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

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

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

50. 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.

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

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

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

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

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

56. 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.

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

58. Фільтрація інтернет-трафіку.

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

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

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

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

63. 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.

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

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

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

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

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

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

70. 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.

71. Можливість визначення рівня критичності значень різноманітних параметрів ОС, з метою виявлення несанкціонованих та небезпечних змін у ОС.

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

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

74. Локальне зберігання журналів на робочих станціях.

75. 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.

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

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

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

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

80. 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.

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

82. Можливість гнучкого налаштовування сповіщень та повідомлень про події на робочому столі користувача.

83. Можливість віддаленого встановлення на клієнтську робочу станцію.

84. Можливість використання антивірусних продуктів 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.

85. Можливість крім основного вказати резервні сервери адміністрування.

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

87. Інвентаризація обладнання, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.

88. Інвентаризація ПЗ, що встановлено на робочих станціях та серверах під управлінням Windows, macOS та Linux.

89. Віддалена інсталяція антивірусного ПЗ для ОС Windows, Linux та Mac на кілька кінцевих точок одночасно.

90. Віддалена інсталяція користувальницького ПЗ.

91. Можливість віддаленого видалення встановленого користувальницького ПЗ.

92. Віддалене видалення антивірусного ПЗ для ОС Windows, Linux та Mac.

93. 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.

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

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

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

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

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

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

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

101. Можливість встановлення агенту управління на ARM64 процесорах.

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

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

104. Сумісність з існуючим сервером централізованого керування та активація антивірусного ПЗ шляхом додавання ключа до існуючого сервера керування. Для підтвердження відповідності пропозиції Учасника цій характеристиці та можливості перевірки відповідності запропонованого рішення заявленим технічним вимогам, на вимогу Замовника, Учасник надає тестовий ключ тривалістю не менше 5 днів для його додавання до існуючого сервера керування.

105. Можливість використання рішення за умови, що управління ними буде здійснюватися серверами адміністрування існуючого антивірусного рішення, що налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту.

106. Наявність панелі моніторингу для відслідковування актуальної інформації про аномальні події що виникли в корпоративній мережі. (*З пункту 106 по пункт 139 перелічені вимоги для забезпечення функцій розширеного виявлення та реагування на інциденти (XDR)).*

107. Отримання попереджень про аномальні події що виникли в роботі ПЗ на основі правил

108. Список правил за замовчуванням та можливість створення власних правил що характеризують поведінку ПЗ як аномальне

109. Автоматична класифікація попереджень за критичністю, що дозволяє швидко визначати та реагувати на критичні події.

110. Можливість встановлювати пріоритет для попереджень для більш гнучкого сортування та фільтрації подій.

111. Можливість групування попереджень за різними критеріями, такими як: тип, комп’ютер, правило, процес, файл.

112. 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 перерахованих параметрів.

113. 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.

114. 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.

115. Наявність інтерактивного інтерфейсу тривожних виявлень, що дозволяє поглиблюватись у більш детальний розгляд інциденту інформаційної безпеки для основних параметрів із наявних у зведеному тривожному виявленні.

116. 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.

117. Можливість створення деталізованих виключень для окремих подій що повинні включати інформацію про контрольні суми виконуваних файлів, їх місцезнаходження, цифровий підпис та іншу інформацію.

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

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

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

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

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

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

124. Можливість створення білих/чорних списків EXE/DLL файлів.

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

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

127. Автоматична класифікація EXE/DLL файлів за критичністю, що дозволяє швидко визначати та реагувати на аномальну поведінку файлів.

128. Можливість позначати EXE/DLL файли як довіренні або безпечні.

129. Можливість позначати EXE/DLL файли як перевірені або проаналізовані.

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

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

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

133. Можливість позначати перевірені скрипти як довіренні або безпечні.

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

135. Автоматична класифікація скриптів за критичністю, що дозволяє швидко визначати та реагувати на аномальну поведінку.

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

137. Можливість віддаленого перезавантаження робочої станції або її повного відключення

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

139. 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.

140. 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.

141. Можливість використання EDR-рішення за умови, що управління ним буде здійснюватися серверами адміністрування існуючого антивірусного рішення, що налаштовано на централізований моніторинг та управління всіма розгалуженими системами антивірусного захисту.

142. Підтримка ОС: Microsoft Win 10, 8.1, 8; Microsoft Win. Server 2012R2, 2012, 2008R2, 2008, Microsoft Win. Server Core 2012R2, 2012, 2008R2, 2008 Core; Linux Kernel версії 2.6.x та вище; FreeBSD версії 9.x (x86).

143. Учасник повинен надати Замовнику копії діючих Експертних висновків (на рішення або на його складові, які будуть використовуватися Замовником, згідно технічних вимог, викладених вище), зареєстрованих в Адміністрації Державної служби спеціального зв’язку та захисту інформації України щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.