|  |
| --- |
| Назва закупівлі: **Програмне забезпечення**  Класифікатор та його відповідний код: **48760000-3: Пакети програмного забезпечення для захисту від вірусів**  Тип закупівлі: **Відкриті торги з особливостями**  Очікувана вартість: **4 043 673,60 грн з ПДВ**  Дата оприлюднення: **06 червня 2025 року**  Детальна інформація за посиланням: <https://prozorro.gov.ua/tender/UA-2025-06-06-004358-a> |

**ІНФОРМАЦІЯ ПРО ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ**

**ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

**Програмне забезпечення**

**(ДК 021:2015 - 48760000-3 Пакети програмного забезпечення для захисту від вірусів)**

|  |  |  |
| --- | --- | --- |
| № з/п | Найменування ПЗ \* | Кількість  шт. |
| 1 | Програмне забезпечення антивірусна система захисту робочих станцій (подовження) | 540 |
| 2 | Програмне забезпечення антивірусна система захисту серверів (подовження) | 60 |
| 3 | Програмне забезпечення система захисту від цільових атак у електронній пошті (подовження) | 540 |
| 4 | Програмне забезпечення система динамічного аналізу в ізольованому середовищі | 540 |
| 5 | Програмне забезпечення система розширеного виявлення та реагування в мережевому трафіку (XDR for Networks) | 2 |

\*У разі якщо присутнє посилання на конкретну торговельну марку чи фірму, патент, конструкцію, вважати це «або еквівалент».

* **Вимоги до технічної підтримки**

1. Запропоновані рішення повинні мати центр технічної підтримки на території України, який має забезпечувати надання технічної підтримки користувачам відповідно до наступних вимог:

- обслуговування 24х7х365 - 24 години на добу, 7 днів на тиждень, 365 днів на рік, включаючи святкові, вихідні та неробочі дні;

- розширені технічні консультації з питань конфігурації та функціонування антивірусної ПП по телефону (з можливостю зв’язку з технічними спеціалістами по місцевому телефону без використання послуг міжнародного телефонного зв’язку) та електронній пошті;

**Інформація про кількісні та якісні характеристики предмета закупівлі:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Найменування товару** | **Технічний опис та/або характеристики товару** | **Одиниця**  **виміру** | **Кількість** |
| **1** | **2** | **3** | **4** | **5** |
| 1 | Програмне забезпечення антивірусна система захисту робочих станцій (подовження) | **Вимоги до антивірусної системи захисту робочих станцій**   1. Підтримка операційних систем:   Агент:   * + Microsoft Windows 10 і вище;   + Microsoft Windows Server 2012 та новіші.   Серверна частина повинна бути реалізована у вигляді хмарного сервісу та не вимагати розгортання додаткових компонентів локально (шлюзи комунікацій, бази даних, тощо) окрім антивірусних агентів. Також не допускається вимога придбання додаткових ліцензій на стороннє ПЗ для нормальної роботи антивірусної системи (операційні системи, бази даних, тощо).   1. Шифрування команд при віддаленому адмініструванні. 2. Інтеграція з Active Directory. 3. ПЗ має підтримувати роботу з адресами типу IPv4 та IPv6. 4. Віддалене розгортання, конфігурування і адміністрування клієнтів на робочих станціях. 5. Віддалене видалення агентів з кінцевих точок шляхом відправки команди з консолі керування. 6. Система повинна мати можливість вказання певного часового інтервалу для автоматичного видалення неактивних агентів з консолі керування. 7. Веб-консоль керування повинна надавати можливість вказання часу, після якого неактивна сесія буде завершена і для продовження роботи необхідно буде знову авторизуватись у системі адміністрування. 8. Можливість створення в системі управління груп керованих комп'ютерів як вручну, так і автоматично на основі робочих груп та структури Active Directory. 9. Повідомляти в консолі керування про необхідність перезавантаження кінцевих точок після оновлення компонент антивірусного агенту. 10. Захист комунікацій між агентом та антивірусним сервером мають бути захищені з використанням цифрових сертифікатів. 11. Для агентів має бути можливість вказування логіну/паролю для доступу до антивірусного серверу через корпоративний проксі-сервер. 12. Наявність функцій централізованого збору статистичної інформації про роботу антивірусного програмного забезпечення на кінцевих точках. 13. Можливість експортувати певні журнали та / або події про роботу антивірусного програмного забезпечення на кінцевих точках. 14. Наявність сканеру файлів, дисків та носіїв ПК. 15. Можливість формування списків довірених додатків. 16. Можливість відключення сканування для довірених додатків. 17. Можливість виключити з перевірки файли і папки з конкретним шляхом, або за "маскою". 18. Наявність поведінкового аналізатора, що дозволяє на підставі поведінки додатка зробити висновок, зловмисний він чи ні. 19. Наявність технологій, що дозволяють по репутації файлу, його віку та розповсюдженості виносити вердикт про його зловмисність. 20. Повинна бути можливість розміщення всередині корпоративної мережі копії хмарної репутаційної бази виробника. 21. Можливість автоматичної зміни параметрів роботи при старті агенту поза периметром корпоративної мережі для таких модулів як "Контроль пристроїв", "служби веб репутації", "модулю контролю за витоком даних (DLP)". 22. Факт роботи поза периметром локальної мережі антивірусним агентом має визначатись автоматично на основі доступності заздалегідь визначених локальних ресурсів за ІР, ім’ям комп’ютеру, FQDN та портом чи МАС-адресою (наприклад довільні сервіси чи корпоративні шлюзи). 23. Також має бути можливість виключати застосування окремих налаштувань для агентів, які під’єднані через VPN та PPP підключення, вважаючи їх "внутрішніми". 24. Наявність резидентного монітору. 25. Система повинна дозволяти відстежувати, або блокувати наступні потенційно небезпечні дії:     * Створення файлів з іменами, що співпадають із системними;     * Модифікації файлу hosts;     * Створення задач автозапуску сторонніх додатків у системному реєстрі;     * Запуск нових служб;     * Модифікацію політик безпеки ОС;     * Тощо. 26. Використання евристичних технологій під час сканування  та забезпечення захисту в режимі реального часу. 27. Захист від шпигунського та рекламного ПЗ. 28. Виявлення руткітів (прихованих файлів / системних аномалій); 29. Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків. 30. Докладне журналювання, формування зведених звітів та звітів щодо кожної робочої станції. 31. Можливість вказування глибини рівнів вкладеності файлів у архівах та вбудованих OLE-об’єктах. 32. Можливість сканування файлів під час запуску ОС. 33. Можливість сканування за розкладом. 34. Можливість запуску антивірусного сканування по команді користувача або адміністратора. 35. Можливість відключення антивірусного захисту або окремих модулів захисту при необхідності. 36. Автоматична антивірусна перевірка змінних носіїв / мережевих папок. 37. Можливість запуску завдань за розкладом. 38. Можливість регулювання розподілу ресурсів робочої станції між антивірусом і іншими додатками в залежності від рівня навантаження Центрального Процесора ЕОМ з передвстановленими рівнями, наприклад, 20%, 50% тощо. 39. Наявність захисту від ще невідомих шкідливих програм (загрози «нульового дня») на основі аналізу їхньої поведінки та контролю змін системного реєстру/процесів, системних файлів. 40. Наявність захисту від ботнетів: виявлення шкідливих програм, аналізуючи їх схеми обміну даними і протоколи. 41. Наявність персонального міжмережевого екрану. 42. Можливість міжмережевого екрану обмежувати доступ конкретним додаткам за:     * шляхом розміщення виконуваного файлу;     * гілкою системного реєстру;     * конкретним значенням параметру визначеного розділу системного реєстру. 43. Можливість застосування як дозвільних та і блокуючих правил міжмережевого екрану в залежності від:     * напрямку (вхідний/вихідний трафік);     * протоколу;     * окремих, або діапазонів портів;     * окремих, діапазону та за маскою мережі ІР-адрес. 44. Регламентне оновлення виробником системи баз даних загроз та програмних модулів в автоматичному режимі та/або за розкладом не менш ніж 24 рази на добу. 45. Можливість призначення ролі "локального сервера оновлень" (ЛСО) певним комп’ютерам з встановленим антивірусним агентом в локальній мережі для зменшення навантаження на зовнішні канали зв’язку при централізованому оновленні системи антивірусного захисту робочих станцій, розміщених у локальній мережі. 46. Можливість налаштування параметрів при оновленні з ЛСО, як мінімум:     * Дозвіл на оновлення компонентів (наприклад, лише оновлення сигнатурних баз);     * Дозвіл на оновлення інформації щодо змін в налаштуваннях корпоративного домену;     * Дозвіл на оновлення самих агентів (автоматичний перехід на новіші версії агентів, встановлення патчів та хотфіксів від виробника). 47. Можливість налаштування часу та періодичності оновлень. 48. Можливість налаштування часу і тривалості періодичних сканувань. 49. Можливість налаштування пропуску сканування за розкладом, якщо рівень заряду батареї комп’ютера/ноутбука нижче за певне значення (10%, 20% і т.д.) та кабель живлення від’єднано від мережі. 50. Попередження користувача спливаючим вікном, або його відключення про чергове періодичне сканування. 51. Можливість надання дозволу певним групам користувачів відключати чи переносити чергове сканування за розкладом. 52. Наявність ієрархічної системи управління політиками з можливістю успадкування частини політик від батьківських груп. 53. Наявність антивірусного сканування трафіку обов’язково за такими протоколами: SMB, FTP, HTTP, HTTPs, POP3, але не обмежуючись. 54. Можливість захисту веб-трафіку - перевірка об'єктів, що надходять на комп'ютер користувача при взаємодії з ресурсами мережі Інтернет. 55. Можливість блокування Інтернет-ресурсів за веб-адресою або ІР-адресою. 56. Можливість захисту від зміни параметрів ПЗ паролем. 57. Наявність захисту від фішингу: захист від спроб отримати паролі та іншу конфіденційну інформацію, забороняючи доступ до шкідливих веб-сайтів, які приймають вид нормальних веб-сайтів. 58. Можливість імпорту списків потенційно небезпечних об’єктів у форматах OpenIOC та STIX, а також через API. 59. Можливість віддаленої ізоляції кінцевої точки з консолі керування щодо мережевих комунікацій для стримування розповсюдження комп’ютерною мережею підозрілої активності. 60. Ізоляція повинна блокувати будь-які мережеві з’єднання кінцевої точки окрім каналу комунікації між консоллю управління та антивірусним агентом. 61. Можливість віддаленого відновлення мережевих з’єднань ізольованих кінцевих точок після проведення поглиблених сканувань з очисткою від шкідливого ПЗ чи розслідувань кіберінцидентів. 62. Наявність режиму "протидії епідеміям", що централізовано змінює роботу антивірусних агентів на робочих станціях та серверах. 63. Запровадження режиму протидії епідеміям згідно з яким обмежуються:     * Мережевий доступ до певних файлів/директорій (повна заборона, або дозвіл лише на читання);     * Доступ до певних та діапазонів портів;     * Запис у визначені локальні директорії, конкретні файли чи групи файлів за типом/розширенням назви;     * Запуск певних архівованих виконуваних типів файлів;     * Створення списків взаємних виключень для файлів, що пов’язані з діяльністю конкретного шкідливого ПЗ, аби це шкідливе ПЗ не змогло генерувати чи завантажувати необхідні для його роботи файли. 64. Режим "протидії епідеміям" повинен:     * містити опцію автоматичного відключення через певний час для відновлення штатної працездатності на необхідному рівні антивірусного комплексу;     * сповіщати користувачів спливаючим вікном про ввімкнення режиму "протидії епідемії" довільним повідомленням, текст якого складений заздалегідь адміністратором; 65. Наявність окремих паролів захисту антивірусних агентів що дозволяють:     * Завершення роботи антивірусного агенту;     * Видалення антивірусного агенту з кінцевої точки. 66. Можливість налаштовування кількості та інтервалу перезапусків щодо будь-яких служб, пов’язаних з коректною роботою антивірусного агенту, у разі їх зупинки/збою. 67. Наявність функції автоматичного сповіщення адміністраторів системи антивірусного захисту про виявлення шкідливого програмного забезпечення. 68. Можливість інтеграції з центром безпеки Windows. 69. Можливість відправки журналів подій у форматі Syslog, CEF. 70. Наявність технічного сервісу по надсиланню зразків нового шкідливого програмного забезпечення для проведення аналізу та надання рекомендацій. 71. Функціонал створення тіньових копій файлів, якщо певне ПЗ починає їх масову зміну що характерно для вірусів-шифрувальників. Та відновлення початкових версій у разі підтвердження їх зміни дійсно вірусом-шифрувальником, а не легітимним процесом. 72. Можливість автоматичної відправки підозрілих об’єктів на поглиблений аналіз у середовище динамічного аналізу типу "пісочниця" за умови додаткового ліцензування. 73. Залежно від результатів сканування у "пісочниці" об’єкт може бути дозволеним при низькому рівні ризику, або ж заблокованим агентами по всій інфраструктурі при високому ризику. 74. Карантин має бути централізованим. 75. Перед переміщенням шкідливого файлу до карантину він має бути зашифрованим та збереженим локально на комп’ютері де був виявленим. 76. Можливість перед відновленням з карантину звірити SHA-1 хеш-суму файлу, що відновлюється для уникнення підміни об’єктів з однаковими назвами. 77. Система має підтримувати можливість міграції агентів між різними антивірусними серверами без необхідності видалення та повторного встановлення агентів. 78. Система має містити та автоматично застосовувати механізми очистки від дій шкідливого ПЗ:     * Відновлення змінених конфігураційних файлів     * Видалення створених гілок в системному реєстрі     * Видалення файлів, завантажених шкідливим ПЗ     * Припинення дочірніх процесів, створених шкідливим ПЗ     * Виявляти та припиняти процеси, асоційовані з псевдо-антивірусним ПЗ (FakeAV). 79. Система має містити модуль контролю роботи із зовнішніми пристроями обов'язково, але не обмежуючись:     * Читання та запис на носії CD/DVD     * Мережеві диски     * USB Flash накопичувачі     * Пристрої Bluetooth     * Пристрої, підключені через порти COM та LPT та інтерфейси IEEE1394, PCMCIA     * Пристрої роботи із зображеннями (сканери)     * Пристрої, що працюють через інфрачервоні порти     * Модеми     * Бездротові мережеві карти 80. Для зазначених типів мають бути передбачені такі режими взаємодії:     * Повний доступ     * Дозвіл модифікації     * Дозвіл на читання та виконання     * Дозвіл тільки на читання     * Дозвіл тільки на перегляд вмісту кореневого каталогу     * Повне блокування при підключенні до кінцевої точки (без присвоєння системного шляху доступу на рівні ОС) 81. Для пристроїв що підключаються при глобальній політиці блокування має бути можливість створення виключень за назвою виробника, моделлю та серійним номером. 82. Також має бути можливість створення дозволів на роботу з зовнішніми пристроями лише для певних додатків за абсолютним шляхом, або за назвою компанії-власника цифрового підпису додатку.   **Вимоги до модулю протидії витоку даних (DLP)**   1. Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються “всередину” і “назовні” корпоративної мережі по протоколам як мінімум: SMB, SMTP, HTTP, HTTPS, FTP, але не обмежуючись. 2. Функціонал контролю за витоком даних має біти інтегрованим у антивірусний агент без необхідності встановлення додаткового ПЗ. 3. Підсистема захисту від витоків даних повинна бути здатна виявляти передавання конфіденційних даних в клієнтах електронної пошти та через веб-інтерфейс онлайн поштових сервісів. 4. Підсистема захисту від витоків даних повинна бути здатна виявляти наявність конфіденційних даних у буфері обміну ОС. 5. Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що:    * передаються на друк;    * записуються на зовнішні накопичувачі: CD/DVD;    * Передаються на USB Flash накопичувачі з можливістю створення списків виключень за назвою виробника, моделюю, серійним номером накопичувача;    * передаються по локальній мережі;    * передаються до хмарних сервісів збереження інформації. 6. Система повинна підтримувати як мінімум наступні види параметрів, за якими проводиться пошук конфіденційних даних:    * Словник:      + точне/часткове з вказуванням ступеня співпадіння      + всі слова, або хоча б одне      + вказування кількості повторювань слів у тексті    * Регулярні вирази (для опису довільних алфавітно-цифрових комбінацій)    * Метадані файлів 7. Система повинна підтримувати експорт та імпорт налаштувань фільтрації у форматі XML 8. Система повинна забезпечувати наступні види реакції на виявлення в переданому файлі конфіденційних даних:    * Блокування передачі    * Фіксація факту передачі в журналі з/без повідомлення користувачу    * Повідомлення Користувачу про порушення політики    * Повідомлення Користувачу з полем введення, яке дозволяє зафіксувати в централізованому журналі виробничу необхідність для передачі конфіденційної інформації та надати дозвіл на передачу конфіденційних даних після зазначення причини.    * Повідомлення Користувачу з готовими варіантами відповіді, яке дозволяє зафіксувати в централізованому журналі одну із заздалегідь вказаних адміністраторами причин, по якій Користувачу треба було передати конфіденційну інформацію. 9. Проводити періодичне сканування інформації на кінцевих точках у заданих директоріях чи за маскою по типу файлу з ціллю виявлення даних, що порушують встановлені політики зберігання конфіденційної інформації. 10. Консолідована інформація про виявлені порушення політик протидії витокам даних повинна відображатись на головному екрані веб-консолі керування антивірусним комплексом у вигляді таблиць/графіків/діаграм. 11. Журнал подій повинен надавати інструменти поглибленої фільтрації подій за правилом спрацювання, дією, групою або конкретним комп’ютером, каналом передачі тощо… 12. Журнал подій має підтримувати можливість експорту у форматах XML, CSV для подальшого імпорту у сторонні системи звітності.   **Вимоги до захисту від вразливостей на рівні хоста при скануванні мережевого трафіку**   1. Система захисту від вразливостей повинна забезпечувати можливості запобігання вторгненням на рівні мережі, націлених на вразливості як ОС так і стороннього програмного забезпечення встановленого на кінцеві точки. 2. Система повинна мати модуль захисту від вразливостей без установки окремого від антивірусного агента. 3. Підсистема захисту повинна бути здатна конфігуруватися з метою активації тільки тих фільтруючих правил, які актуальні для даного комп'ютера або групи комп'ютерів. 4. Система захисту повинна забезпечувати роботи в режимах:    * Inline (в розрив з можливістю блокування);    * TAP (в режимі лише моніторингу трафіку та фіксації подій). 5. Система захисту повинна мати можливість блокування використання вразливостей. Та для кожного правила мати вказівку на конкретну вразливість CVE. Наприклад:    * CVE-2018-8467    * CVE-2022-26809    * MSCVE-2022-26809 6. Система захисту повинна відображати рівень критичності зазначеної вразливості за загальноприйнятим рейтингом CVSS (від 0 до 10). 7. Система захисту повинна мати можливість вибору попередньо сконфігурованого профілю для захисту, наприклад, оптимізованого з точки зору безпеки або з точки зору продуктивності. 8. Система захисту повинна дозволяти створення виключень зі сканування трафіку конкретних кінцевих точок за IP-адресою. 9. Інструменти реагування модулю захисту від вразливостей має містити наступні можливості:    * Скидання створених з’єднань за таймаутом    * Кількістю одночасних TCP/UDP сесій    * Комбінацією не менше ніж 3х статусів з’єднань для ігнорування подій (створення виключень)    * Блокування пакетів що мають одинакові ІР-адреси відправника та отримувача    * Вибору із заздалегідь створених виробником рівня деталізації запису в журнал подій модулем захисту від вразливостей   **Вимоги до модулю контролю додатків**   1. Модуль має забезпечувати роботу в 2х режимах:    * Блокувати всі окрім дозволених додатків;    * Дозволяти все з можливістю створення переліку окремих заборонених додатків. 2. Правила контролю додатків повинні підтримувати їх застосування для окремих користувачів чи груп Active Directory 3. Має бути доступним режим проведення інвентаризації ПЗ, що використовується в організації, на всіх кінцевих точках, де встановлено антивірусний агент. 4. Підсистема повинна забезпечити наступні критерії визначення додатка:    * Контрольну суму SHA1    * Цифровий сертифікат електронного підпису додатку з диференціацією:      + Тільки довірений дійсний      + Довірений дійсний або прострочений      + Довірений дійсний або прострочений чи недовірений      + Тільки недовірений      + Недовірений або довірений, але "прострочений"      + Недовірений або довірений дійсний, або "прострочений"    * Розташування файлу    * Розробник    * Належність певної категорії, типу додатка    * Загальний рейтинг довіри (за даними виробника)    * Глобальна розповсюдженість 5. Повинні бути реалізовані наступні можливості контролю сертифікатів додатків:    * Країна емітента    * Назва емітента    * Організація емітент    * Інші атрибути емітента 6. Повинні бути реалізовані наступні критерії визначення місця розташування файлу:    * Файл з шляхом, відповідним масці    * Файл з шляхом, відповідним регулярному виразу    * Файл на будь-якому локальному сховищі з шляхом, відповідним масці    * Файл на будь-якому локальному сховищі з шляхом, відповідним регулярному виразу    * Файл на знімному носії з шляхом, відповідним масці    * Файл на знімному носії з шляхом, відповідним регулярному виразу    * Файл на мережевому ресурсі з шляхом, відповідним масці    * Файл на мережевому ресурсі з шляхом, відповідним регулярному виразу 7. Система повинна дозволяти визначати програмне забезпечення наступних категорій:    * Браузери    * Інструменти розробки    * Засоби розподілених обчислень    * Ігри    * Прошивки пристроїв і драйвери    * Потенційно небезпечні програми    * Системи миттєвого обміну повідомленнями    * Інструменти роботи з мультимедіа    * Засоби синхронізації з мобільними пристроями    * Клієнти хмарних сховищ    * Утиліти запису та емулятори оптичних дисків    * Клієнти пірінгових мереж    * Засоби підвищення продуктивності    * Системні утиліти 8. Система повинна забезпечувати довільну комбінацію перерахованих вище критеріїв визначення файлів з використанням булевої логіки дозволяючу або блокуючу дію запуску програм. 9. Сукупність блокуючих і дозволяючих правил повинна динамічно застосовуватися до робочих станцій, згідно довільної комбінації наступних критеріїв з використанням булевої логіки:    * Версія агента    * Домен    * Ім'я робочої станції    * Діапазон IP-адрес    * Належність домену підсистеми антивірусного захисту    * Ім'я користувача    * Група користувача    * Версія ОС   **Вимоги до захисту робочих станцій на базі macOS**   1. Встановлення агенту на macOS 10.15 та вище. 2. Робота агенту з процесорами Apple M1, Apple M2, чи Intel Core 3. Система захисту повинна забезпечувати захист від наступних типів загроз:    * Вірус    * Трояни    * Мережеві черв'яки    * Рекламні програми    * Шпигунські програми    * Програми-жарти    * Генератори піратських ключів    * Віруси-вимагачі та шифрувальники 4. Агент повинен пропонувати наступні механізми захисту:    * Сигнатурний аналіз по "повній базі" для комп'ютерів з обмеженим доступом до мережі Інтернет;    * Сигнатурний аналіз по скороченій базі для комп'ютерів, що мають доступ до онлайн-ресурсів виробника без обмежень;    * Технології «машинного навчання» для захисту від загроз «нульового дня» 5. Система захисту повинна підтримувати наступні типи сканування:    * У реальному часі (при створенні / зміні файлу)    * За запитом користувача    * За розкладом 6. Система захисту повинна мати функціонал контролю пристроїв:    * Блокування запуску додатків з зовнішніх пристроїв    * Дозволяти тільки відображення вмісту зовнішніх пристроїв    * Часткове дозвіл дій із зовнішнім пристроєм: копіювання, переміщення, видалення, зміна, запуск додатків з зовнішніх пристроїв. 7. Модуль контролю пристроїв має дозволяти створення списків виключень за назвою виробника, ідентифікатором пристрою та його серійним номером. 8. Виключення мають дозволяти або повний доступ, або лише право на читання вмісту. 9. Система захисту повинна мати функціонал самозахисту 10. Система захисту повинна дозволяти використовувати не тільки локальну антивірусну базу, але і перевіряти репутацію (розповсюдженість за кількістю екземплярів та давністю – часом від моменту першої фіксації існування) файлів по хмарній базі виробника 11. Підсистема повинна забезпечити блокування підключень до шкідливих веб-ресурсів 12. Можливість налаштування часу і тривалості періодичних сканувань. 13. Можливість налаштування пропуску сканування за розкладом, якщо рівень заряду батареї комп’ютера/ноутбука нижче за певне значення (10%, 20% і т.д.) та кабель живлення від’єднано від мережі. 14. Попередження користувача спливаючим вікном, або його відключенням про чергове періодичне сканування. 15. Можливість надання дозволу певним групам користувачів відключати чи переносити чергове сканування за розкладом. 16. Можливість вказування високого чи низького пріоритету сканування за розкладом чи по команді користувача для оптимального використання апаратних ресурсів кінцевої точки. 17. Можливість створення списку перевірених безпечних файлів, так званого кешу, задля зменшення часу наступних періодичних сканувань. 18. Самозахист файлів та служб агенту шляхом блокування змін сторонніми додатками. 19. Можливість захисту антивірусного агенту від видалення шляхом встановлення спеціального паролю. 20. Можливість створення виключення зі сканування для файлів та директорій. 21. Можливість додавати додатки до списку довірених, якщо під час їх виконання відбуваються хибно-позитивні спрацювання антивірусного агенту.   **Вимоги до проведення розслідувань кіберінцидентів.**   1. Рішення повинно представляти собою самостійний "хмарний" сервіс (SaaS) та всі зазначені вимоги реалізовувати без обов’язкової необхідності інтеграції з будь-яким антивірусним рішенням. 2. Виробник рішення повинен мати сертифікат ISO27001 для підтвердження здатності на достатньому рівні управління безпекою "хмарної" інфраструктури. 3. Рішення повинно мати самостійний окремий агент, встановлення якого не потребує видалення поточного антивірусного рішення що використовується у замовника. 4. Рішення повинно здійснювати кореляцію між метаданими, що отримані з кінцевих точок, пошти та мережевого трафіку за наявності відповідних агентів/сенсорів у інфраструктурі замовника. 5. Рішення має підтримувати встановлення агенту на наступні ОС Windows:  * Desktop   + Windows 10 і вище;  1. Повинні підтримуватися наступні варіанти Linux:  * AlmaLinux 8 та вище; * Amazon Linux, Amazon Linux 2 (x86\_64) та вище; Amazon Linux 2 (AArch64) та вище; * CentOS 6 та вище; * CloudLinux 7 та вище; * Debian 8 та вище; * OracleLinux 6 та вище; * Red Hat Enterprise Linux 7 (x86\_64) та вище, Red Hat Enterprise Linux 8 (AArch64) та вище; * RockyLinux 8 та вище; * SuSE 12 та вище; * Ubuntu 16 (x86\_64) та вище, Ubuntu 18.04 (AArch64) та вище;  1. Повинні підтримуватися наступні варіанти macOS:  * 10.15 та вище;  1. Рішення має інтегруватись з локальною архітектурою Active Directory (on-premises) для опрацювання журналів безпеки, відображення підозрілих подій та реалізації дій по реагуванню на кіберінциденти на рівні AD. 2. Рішення на основі отриманих даних телеметрії повинно бути здатним будувати схематичну дочірньо-батьківську модель взаємодії об’єктів в рамках виявленого кіберінциденту з деталізацією по кожному із залучених об’єктів; 3. Деталізація має також містити інформацію про характер поведінки кожного із залучених об’єктів:    * тип дії – створення/доступ/комунікація;    * створення дочірніх процесів/комунікацій;    * створення/видалення записів у системному реєстрі;    * завантаження/створення/видалення файлів; 4. Відображення дочірньо-батьківської моделі повинно мати режим, в якому можна буде покроково відслідкувати кожен етап інциденту вручну контролюючи процес переходу між значимими подіями на "часовій шкалі". 5. Деталізована інформація щодо інциденту повинна містити розділ з текстовою інтерпретацією (поясненням від імені системи) подій для спрощення та прискорення розуміння про природу та перебіг активності. 6. Розділ з деталізацією інциденту має містити посилання на конкретні "техніки", згідно матриці MITRE, які спостерігаються в рамках конкретної активності; 7. Розділ з деталізацією інциденту має містити перелік усіх хостів, облікових записів та об’єктів, які залучені у поточній активності. 8. Рішення повинно мати можливість інтеграції з SIEM і SOAR системами замовника. 9. Рішення повинно мати можливість інтеграції зі сторонніми програмами через інтерфейс прикладного програмування (API), зокрема підтримувати Restful API. 10. Документація по API має бути у публічному доступі та не вимагати погодження будь-яких додаткових зобов’язань з боку замовника (підписання додаткових угод, придбання прав користування на комерційній основі і тому подібне). 11. Реалізовано розгортання агента з використанням різних підтримуваних процедур. Наприклад, розповсюдження посилання на веб-інсталятор, завантаження полегшеного інсталятора з автоматичним визначенням, завантаженням та запуском файлів інсталяційних дистрибутивів під необхідну версію ОС, завантаження повнофункціонального пакету інсталятора агента для централізованого розгортання засобами корпоративного управління встановлення додатків (SCCM, GPO, тощо). 12. Під час установки агента повинна бути можливість вказання адреси проксі-серверу для зовнішніх комунікацій. 13. Рішення має містити компонент без додаткового ліцензування, який розгортається локально та виконує роль акумулюючого проксі-серверу для передачі телеметрії від локальних агентів без прямого Інтернет-з’єднання до хмарного сервісу кореляції. 14. Агент повинен як передавати телеметрію з кінцевої точки для подальшої кореляції подій, так і здатним виконувати певні команди з консолі управління, що спрямовані на протидію потенційно небезпечній активності, обов’язково, але не обмежуючись:     * ізоляція кінцевої точки;     * додавання знайдених індикаторів компрометації до переліку явно шкідливих об’єктів;     * припинення шкідливих процесів;     * запуск з веб-консолі на віддаленому хості інтерфейсу командного рядка (CLI) для поглибленого розслідування та реагування на кіберінцидент;     * можливість запуску довільних скриптів на віддаленому хості.     * вилучення/копіювання потенційно шкідливих об’єктів із скомпрометованого хоста до веб-консолі керування для подальшого дослідження;     * створення та вивантаження «дампу» оперативної пам’яті з віддаленого комп’ютера (для OS Windows). 15. Відображення кіберінцидентів має містити показник ймовірної фази кібератаки із загальноприйнятого переліку (наприклад: виконання, підвищення привілеїв, горизонтальне переміщення, зв’зок з С&С, вивантаження даних і т.п.) 16. Агент рішення повинен періодично аналізувати операційну систему на предмет наявності вразливих компонент та передавати інформацію до консолі керування із зазначенням та відображенням:     * Загальної кількості наявних унікальних вразливостей за загальноприйнятою системою індексації CVE;     * Середній час між проведенням процедури інсталяції патчів на підзахисній інфраструктурі;     * Середньостатистичний час протягом якого кінцеві точки не мають встановлених найновіших патчів;     * Середньостатистичний показник кількості небезпечних вразливостей на один підзахисний комп’ютер; 17. Рішення повинно підтримувати роботу агентів у середовищі VDI:     * VMware Horizon версії 8.3 та вище     * Azure Virtual Desktop 18. Робота агентів у середовищі VDI повинна бути реалізована в режимах "persistent" та "non-persistent". 19. Повинна бути можливість включити агент системи у базовий образ з якого будуть запускатись "віртуалізовані робочі місця" в рамках VDI. 20. У режимі "persistent " агент повинен мати функціонал визначення вразливостей щонайменше операційної системи та передавати інформацію у хмарний сервіс. 21. Для ефективного використання придбаних ліцензій – має бути реалізовано механізм активації та деактивації агентів у консолі керування без фактичного видалення ПЗ агенту з кінцевої точки. 22. Видалення агенту рішення повинно бути захищеним додатковим механізмом, відключення якого можливе лише шляхом застосування спеціалізованого "токену" з обмеженим терміном дії, що генерується персонально конкретному замовнику. 23. Рішення повинно мати єдину централізовану консоль управління розслідуванням. 24. Рішення повинно забезпечувати функції централізованого управління з точки зору аналізу журналів, аналізу загроз, стану керованих продуктів/пристроїв і розгортання додатків. 25. Рішення повинно забезпечувати деталізовані фільтри пошуку по зібраній телеметрії, щоб користувачі могли визначати свої власні критерії пошуку з використанням логічних операторів "та"/"або"/"ні". 26. Рішення повинно мати можливість виконувати багаторівневий пошук і розслідування на основі окремих параметрів або об'єктів ІоС, файлів OpenIOC і файлів STIX. Параметри пошуку повинні включати:  * Зв'язок: IP-адреса, порт, домен, DNS, назва хоста, URL * Назву шкідливого ПЗ або будь-який файл по:   + хешу SHA1,   + імені файлу,   + шляху до файлу,   + типу файлу. * Діяльність в реєстрі:   + створення,   + редагування,   + видалення. * Активність облікового запису користувача  1. Має бути можливість збереження довільних критеріїв пошуку подій на кінцевих точках та на їх основі створювати правила оповіщення. 2. Рішення повинно забезпечувати централізований огляд виявлення загроз для керованих продуктів / пристроїв. 3. Рішення повинно мати представлення у вигляді дерева або еквівалентне представлення всіх керованих продуктів/пристроїв, включаючи назву продукту / пристрою, IP-адресу, стан підключення, версії додатків тощо. 4. Рішення повинно забезпечувати рольовий контроль доступу для цілей адміністрування, розслідування, а також інших операцій. 5. Рішення повинно забезпечувати функцію журналу аудиту для перегляду історії дій користувачів. 6. Підтримку багатофакторної аутентифікації (MFA) 7. Рішення повинно зберігати метадані з кінцевих точок у централізованій базі даних:    * Інформації про файли/об’єкти,    * дії і важливі системні події,   а також постійно оновлювати цю базу даних для запису факту появи і виконання підозрілих об'єктів.   1. Рішення має надавати можливість користувачу визначати та завантажувати власні правила та індикатори компрометації (ІоС), щоб визначати файли та події для моніторингу. 2. Рішення має надавати можливість користувачу створювати власні правила відслідковування подій, задаючи критерії детектування засобами хмарної платформи. Тобто створювати власні моделі детектування XDR. 3. Рішення повинно мати можливість відстежувати і досліджувати події на кінцевих точках незалежно від їх місця розташування - локально, віддалено або "хмарно". 4. Рішення повинно мати інтерактивні інформаційні панелі для перегляду та аналізу дій системи з плином часу (віджети), оцінки термінів діяльності в масштабі всього підприємства та експорту результатів розслідування. 5. Рішення повинно мати можливість обмінюватися даними про загрози між керованими/інтегрованими продуктами та пристроями того ж виробника, а також продуктами сторонніх виробників, згідно наявного списку інтеграцій у веб-консолі та через застосування АРІ. 6. Інформація про загрози повинна бути сумісна з загальнодоступним стандартом STIX. 7. Рішення повинно мати можливість підключатися до різних серверів TAXII в якості клієнта для отримання аналітичних даних про загрози без додаткового ліцензування. 8. Рішення повинно підтримувати функції клієнта та сервера MISP для отримання/передачі різних індикаторів компрометації без додаткового ліцензування. 9. Рішення повинно містити в собі підписку на звіти розслідувань від виробника з інформацією по шкідливим кампаніям з різних регіонів Світу, зокрема і з України, без додаткової оплати, і можливістю отримання деталізованої довідки по різним шкідливим кампаніям. 10. Рішення має також надавати інформацію про діючі кіберугрупування без додаткового ліцензування, як мінімум про наступне:     * Опис самого кіберугрупування, його спеціалізація та особливі прикмети;     * Посилання на опис Технік, Тактики і Процедур, що застосовуються конкретним кіберугрупуванням;     * Перелік спеціалізованих утиліт/шкідливого ПЗ/характерних вразливостей за CVE, що використовуються конкретним кіберугрупуванням.     * Перелік комп’ютерів з підзахисної інфраструктури де було виявлено відповідні артефакти для прискорення оцінки компрометації інфраструктури. 11. Можливість підключення до сторонніх баз шкідливих кампаній без додаткового ліцензування. 12. Рішення повинно автоматично сканувати наявні метадані з підзахисних об’єктів на предмет присутності індикаторів компрометації із нових шкідливих кіберкампаній ретроспективно та щонайменше, протягом останніх 7 днів від дня отримання/появи у рішенні інформації про активність кіберкампанії. 13. Рішення повинно дозволяти користувачам визначати глобальний список винятків для створення винятків всередині організації і можливість передачі списку винятків іншим продуктам того ж або стороннім виробникам. 14. Рішення повинно забезпечувати виявлення загроз на основі найновіших моделей, створених виробником, без необхідності будь-якого втручання в ручному режимі з боку користувачів. 15. Рішення повинно вміти приорітезувати визначені загрози/інциденти шляхом присвоєння відповідного рівня критичності. 16. У рішення має бути функціонал присвоєння статусу виявлених інцидентів, щонайменше:     * Новий,     * В процесі дослідження,     * Вирішено,     * Закритий як хибнопозитивний. 17. Для інцидентів повинна бути можливість додавання довільних коментарів. 18. Рішення повинно мати можливість ідентифікувати всі хости, заражені однією і тією ж загрозою. 19. Рішення повинно мати можливість ідентифікувати всі хости, які підключалися до шкідливого C&C сервера. 20. Рішення має зберігати метадані в централізованому реєстрі метаданих. 21. У реєстрі метаданих повинні бути дані про активність, а також дані про виявлення. Рішення повинно дозволяти пошук незалежно від того, чи знаходиться машина в мережі або офлайн. 22. Рішення повинно мати налаштування автоматизованих сценаріїв реагування (плейбуків). 23. Запуск плейбуків має бути реалізованим за:     * подією (виявлення за поведінкою XDR, за наявністю шкідливого об’єкта, наявністю вразливості, тощо),     * рівнем критичності події (високий/середній/низький),     * рівнем критичності виявленого об’єкту,     * розкладом, або за командою користувача. 24. Результати виконання дій в рамках плейбуків мають надсилатись визначеним користувачам електронною поштою, або за допомогою надсилання у вигляді "заявки" на зазначений веб-ресурс після проходження авторизації. 25. Рішення має відображати сукупний рівень ризиків ввіреної інфраструктури у вигляді графіку з інформацією щонайменше за останні 30 днів.   Допускається відображення показників у відносних одиницях з певного діапазону, наприклад у діапазоні від 0 до 100 одиниць, де 0 – низький рівень ризиків, а 100 – найвищий.  **Кількісні та якісні характеристики програмного забезпечення**   1. Програмне забезпечення повинно включати в себе всі вищезазначені модулі в активному стані 2. Кількість – 540 3. Всі ліцензії та активні підписки повинні бути не менше, ніж на 12 місяців 4. Має бути зазначеним в Gartner’s Magic Quadrant for Endpoint Protection Platforms за 2022 та 2023 роки | шт | 540 |
| 2 | Програмне забезпечення антивірусна система захисту серверів (подовження) | **Вимоги до антивірусної системи захисту серверів**  ***Загальні вимоги***   1. Захист з використанням агентів для систем під управлінням: Windows/Linux/AIX/Solaris/macOS/OpenShift. 2. Можливість задання конкретних шляхів обов’язкового сканування та виключень зі сканування. 3. Можливість працювати з готовими списками обов’язкових шляхів та виключень з перевірки об'єктів, щоб тиражувати їх для різних підзахисних груп (тиражовані списки). 4. Можливість передачі інформації для проведення розслідувань в системи класу XDR (extended detection & respond) того ж виробника. 5. Можливість інтеграції з середовищами динамічного аналізу ("пісочницями") того ж виробника. 6. Для налаштування довільної системи пріоритезації сповіщень про події - можливість довільного зазначення рівня критичності виявлених подій на основі "бальної" системи для кожного окремого модуля. 7. Підтримка інтеграції з наступними середовищами віртуалізації та хмарними сервісами:    * VMware (vCloud/vCenter);    * Amazon Web Services;    * Microsoft Azure;    * Google Cloud Platform. 8. Можливість управління всіма налаштуваннями з єдиної локальної консолі, не залежно від платформи розгортання агентів/середовища віртуалізації і характеру підзахисних вузлів (віртуальна або фізична машина). 9. Підтримувані платформи (агент) – Windows:    * Версія ОС для робочих станцій Windows 7 (32 і 64 біт) і вище    * Версія для серверних ОС Windows 2008R2 (32 і 64 біт) і вище 10. Підтримувані платформи (агент) – Linux:     * AlmaLinux 8 та вище;     * Amazon Linux, Amazon Linux 2 (x86\_64); Amazon Linux 2 (AArch64)     * CentOS 6 та вище;     * CloudLinux 7 та вище;     * Debian 8 та вище;     * OracleLinux 6 та вище;     * Red Hat Enterprise Linux 7 (x86\_64) та вище, Red Hat Enterprise Linux 8 (AArch64) та вище;     * RockyLinux 8 та вище;     * SuSE 12 та вище;     * Ubuntu 16 (x86\_64) та вище, Ubuntu 18.04 (AArch64) та вище; 11. Підтримувані платформи (агент) – Solaris:     * Solaris 10 і вище 12. Підтримувані платформи (агент) – AIX:     * AIX 6.1 TL 9 і вище 13. Підтримувані платформи (агент) – macOS:     * macOS Catalina 10.15 і вище   **Вимоги до агентів:**   1. Агент повинен поширюватися у вигляді максимально полегшеного ядра (без функціональних модулів). 2. Агент повинен мати можливість підвантаження функціональних модулів з сервера на основі включених захисних функцій і політик. 3. Агент повинен мати можливість обміну даними з сервером як в двосторонньому режимі (як сервер, так і агент можуть ініціювати з'єднання), так і в односторонньому режимі (тільки сервер, або тільки агент може ініціювати з'єднання). 4. Агент повинен мати можливості роботи з повним приховуванням графічної частини. 5. Агент повинен підтримувати управління з командного рядка. 6. Агент повинен мати вбудовані механізми самозахисту, що відключаються тільки з командного рядка (включаючи пароль). 7. Агент повинен мати можливість установки без первинної прив'язки до сервера управління (для включення його в стандартні шаблони віртуальних машин і еталонні образи масового розгортання ОС). 8. Агент повинен мати можливості прив'язки (реєстрації/активації) до сервера управління за допомогою інструментів командного рядка. 9. Агент повинен мати можливості аварійного скидання налаштувань та інформації про керуючий сервер за допомогою інструментів командного рядка.   **Робота з "контейнерами"**   1. Можливість захисту контейнерів Docker, Docker CE, Docker EE. 2. Пошук і захист від вразливостей на хості. 3. Моніторинг цілісності на хості. 4. Моніторинг цілісності в працюючих контейнерах (включаючи конфігурації). 5. Нормалізація подій у журналах. 6. Пошук і захист від вразливостей в працюючих контейнерах. 7. Пошук і захист від шкідливого ПЗ в працюючих контейнерах на всіх рівнях. 8. Контроль запуску додатків на хості.   **Система управління**   1. Система управління повинна бути реалізована як "хмарний" сервіс від виробника рішення та інтегрована у єдину консоль разом з рішенням рослідування і реагувань на кіберінциденти (XDR). 2. Керування має здійснюватись через веб-консоль, підтримувати всі актуальні версії браузерів і не вимагати додаткових компонентів для здійснення адміністративних завдань. 3. Робота з веб-консоллю управління та БД здійснюється по захищеному з'єднанню (SSL). 4. Система управління повинна мати підтримку генерації спеціальних скриптів для автоматичного розгортання агентів під платформи Windows/Linux/AIX/Solaris/macOS/OpenShift. 5. Система управління повинна підтримувати пряму інтеграцію з системою VMware vCenter (з версії 6.5 і вище). 6. Система управління повинна підтримувати роботу з більш, ніж одним VMware vCenter. 7. При роботі з VMware vCenter відстеження всіх змін в інфраструктурі має відбуватися в режимі, близькому до реального часу. 8. Система управління рішенням повинна підтримувати гнучку рольову модель (RBAC) з можливістю детального налаштування областей і прав роботи з ними. 9. Рішення повинно підтримувати режим делегування прав. 10. Рішення повинно відстежувати і фіксувати всі дії адміністраторів при роботі з нею, а також зберігати докладні відомості по кожному з них (наприклад, хто і коли вніс зміни в налаштування чи політики безпеки, після чого виникли проблеми з роботою бізнес-сервісу). 11. Система управління рішенням повинна мати вбудовані засоби оповіщення про загрози та інциденти через пошту. 12. Система управління рішенням повинна мати вбудовані засоби оповіщення про загрози та інциденти в SIEM системи з підтримкою наступних типів форматів: raw syslog, CEF, LEEF. 13. Рішення повинно підтримувати окрему настройку передачі інцидентів в системи кореляції подій (SIEM) для кожного модуля захисту окремо. 14. В системі повинна бути передбачена інтеграція зі сторонніми системами ідентифікації на основі SAML 2.0 (наприклад, ADFS, Okta, Azure AD та ін.). 15. Рішення повинно підтримувати роботу з LDAP для синхронізації даних по машинах та для забезпечення доступу доменних користувачів до системи. 16. Робота з LDAP повинна здійснюватись у захищеному режимі (LDAPS, StartTLS). 17. Система управління рішенням повинна мати відкритий API для інтеграції зі сторонніми системами. 18. Має бути передбачено призначення ролі "серверу оновлень" довільним антивірусним агентам для зниження навантаження на зовнішні канали зв’язку інфраструктури замовника. 19. Система оновлень повинна підтримувати ієрархію для джерел розповсюдження оновлень. 20. Система управління рішенням повинна мати можливості запуску перевірки відкритих портів для модуля міжмережевого екрану (далі - ММЕ). 21. Система управління рішенням повинна мати можливості ручного запуску повної і швидкої антивірусної перевірки на підзахисних хостах. 22. Система управління рішенням повинна мати можливості скидання налаштувань агента (відключення політик, відв'язування від системи управління). 23. Система управління рішенням повинна мати інструменти для об'єднання підзахисних хостів/машин у довільні групи по широкому набору ознак (умов). 24. Рішення повинно мати можливість автоматичного застосування релевантних цільовим підзахисним системам наборів правил захисту на основі розширеного списку умов і подій (машина з'явилася в інфраструктурі, машина перемістилася з хоста на хост, машина включилася, у машини відбулася зміна IP, тощо).   **Модуль антивірусного захисту:**   1. Робота антивіруса з використанням репутаційної оцінки ("легкі агенти"). 2. Перевірка репутації за критеріями глобальної поширеності об'єкта і числу запусків. 3. Робота антивіруса з використанням класичної моделі оцінки загроз за сигнатурами на самих агентах (для ізольованих систем без доступу до мережі Інтернет). 4. Можливість вилучення об'єктів з карантину адміністратором. 5. Антивірусний захист в реальному часі для систем під управлінням Windows/Linux/macOS. 6. Запуск антивірусних перевірок за розкладом або вручну для систем під управлінням Windows/Linux/AIX/Solaris/macOS/OpenShift. 7. Можливість завдання часових меж антивірусної перевірки (як час старту, так і час закінчення). 8. Можливість завдання режимів перевірки в реальному часі (запис/читання, тільки запис, тільки читання). 9. Забезпечення контролю пам'яті при використанні агентів. 10. Поведінковий аналіз для виявлення невідомих загроз за специфічними ознаками. 11. Захист від шифрувальників на основі системного відстеження спроб зашифрувати дані відомим та невідомим способом. 12. Автоматичне створення резервних копій файлів, щодо яких були помічені спроби їх зашифрувати, а також їх відновлення автоматично після очищення системи від слідів вірусу-шифрувальника. 13. Оцінка загроз за моделлю машинного навчання до запуску файлів. 14. Виявлення спроб використання вразливостей в документах. 15. Інтеграція з системою динамічного аналізу ("пісочницею") для передачі підозрілих об'єктів на перевірку і подальшого їх блокування на основі вердикту "пісочниць". 16. Захист від шпигунського ПЗ. 17. Можливість задати максимальний розмір файлів, що перевіряються. 18. Перевірка файлів всередині архівів з вказуванням глибини вкладеності архівів. 19. Можливість задати максимальну кількість добутих з архіву об'єктів для перевірки. 20. Можливість задати максимальний розмір кожного файлу при витяганні з архіву об'єктів для перевірки. 21. Можливість перевірки вбудованих об'єктів всередині документів Office (OLE). 22. Перевірка мережевих папок. 23. Можливість явно задати включаються з перевірки папки і файли. 24. Можливість явно задати виключення з перевірки папки, файли, розширення, процеси. 25. Налаштування максимально споживаного процесорного часу агентом для ручних і планових перевірок. 26. Налаштування багатопоточної антивірусної перевірки.   **Захист зовнішніх веб-комунікацій**   1. Блокування доступу до шкідливих ресурсів на основі репутаційної оцінки. 2. Налаштування порогових значень для регулювання чутливості спрацьовування блокування. 3. Можливість налаштування виведеного повідомлення при блокуванні веб-ресурсів. 4. Можливість вказування портів для моніторингу веб-активностей 5. Можливість ведення "чорних" і "білих" списків по URL (весь домен, URL, за ключовими словами у адресному рядку). 6. Використання як глобального центру для обробки репутаційних запитів, так і робота через локально встановлені проміжні обробники (компонент з локалізованою базою файлової та веб-репутації). 7. Можливість вибору роботи мережевого аналізатора: inline (в розрив) або tap (тільки логування, для тестових задач).   **Міжмережевий екран (ММЕ) рівня вузла. Функціоналом ПЗ повинні бути реалізовані:**   1. Підтримка обробки пакетів на L2 і вище рівнях. 2. Підтримка роботи з заголовками і фреймами. 3. Наявність передвстановлених правил (для оперативного налаштування). 4. Підтримка виявлення розвідки - сканування портів з можливістю вказівки діапазону. 5. Підтримка виявлення розвідки "OS Fingerprint". 6. Підтримка виявлення розвідки-аномальні TCP активності (null scan, SYN FIN scan, Xmax scan). 7. Підтримка виявлення розвідки-можливість створення винятків за джерелами. 8. Можливість налаштування ізоляції інтерфейсів. 9. Підтримка режиму stateful inspection. 10. Можливість роботи ММЕ за розкладом. 11. Можливість збору даних пакетів для розслідування. 12. Можливість вибору режиму роботи мережевого модуля в bypass (fail open) або блокування (fail close). 13. Можливість вибору режиму роботи мережевого модуля в inline або tap (тільки логування, для тестових завдань). 14. Можливість вказівки максимального числа з'єднань (TCP, UDP, ICMP). 15. Можливість задати таймаути для різних станів мережевих сесій і аномалій (SYN\_SENT, CLOSED, CLOSING, ACK STORM, ESTABLISHED та інших). 16. Блокування з'єднань з ідентичними IP для SRC і DST. 17. Можливість налаштування заборони для Null IP. 18. Можливість "тихого" скидання TCP з'єднання (silent). 19. Режим bypass для Cisco WAAS. 20. Можливості налаштування "скидання" з'єднання для пакетів з дублюючими або перекриваються даними (evasive retransmit attack techniques). 21. Можливості перевірки TCP сhecksum. 22. Можливості налаштування мінімальних значень для фрагментів пакета (fragment offset & size). 23. Можливості налаштування мінімальних значень для SSL сесій (time & size). 24. Можливості скидання невідомого протоколу для SSL трафіку. 25. Можливості фільтрації тунелів (IPv4, IPv6). 26. Можливість налаштування для збереження максимального числа фрагментованих IP пакетів. 27. Можливість bypass для MAC адрес, що не відносяться до хосту.   **Наявність модулю запобігання вторгненням на рівні вузла (HostIPS)**   1. Захист від вразливостей у ПЗ та самих ОС Windows/Linux/Solaris (з прив'язкою до конкретних вразливостей і експлойтів) на мережевому рівні, шляхом блокування спроб використання вразливостей непропатчених компонентів – так званий "віртуальний патчинг". 2. Правила виявлення і запобігання вразливостей повинні мати посилання на глобальні бази по вразливостях для зіставлення результатів (наприклад, MITTRE, Microsoft, CVE). 3. Можливість блокування прикладних додатків на мережевому рівні (network application control). 4. Наявність механізмів захисту класу WAF для хостів в складі рішення (захист від XSS, SQL injections) з можливістю налаштування параметрів. 5. Можливість вибору режимів роботи (запобігання або виявлення) на рівні Host IPS (HIPS). 6. Можливість вибору режимів роботи (запобігання або виявлення вторгнень) на рівні окремих правил модуля HIPS. 7. Можливості перевірки (аудиту) підзахисних систем в автоматичному і ручному режимах для виявлення слабких місць і вразливостей в додатках і ОС з можливістю подальшої активації відповідних правил HIPS (або видачі рекомендацій щодо їх використання) для усунення знайдених проблем. 8. Можливість автоматичної прив'язки / відключення правил, отриманих в результаті автоматичного пошуку вразливостей, до цільових підзахисних системам або політикам для них. 9. Робота автоматичного пошуку вразливостей через "планувальник завдань" для оптимізації набору правил виявлення / запобігання вторгнень (відключення правил для вразливостей, вже закритих реальними патчами від виробників систем і додатків; включення актуальних правил під нові знайдені вразливості, що ще не закриті реальними патчами від виробників).   **Контроль цілісності підзахисних систем.**   1. Можливість роботи контролю цілісності за допомогою агента. 2. Наявність механізмів моніторингу цілісності:    * файлів і папок,    * ключів реєстру,    * служб,    * портів. 3. Можливість відстеження змін в режимах:    * реального часу,    * heartbeat,    * ручному режимі. 4. Використання еталонних джерел для формування набору довірених змін (локальні машини, глобальні бази "білих додатків"). 5. Можливість вибору типу хешу (SHA-1 або SHA-256). 6. Можливість вибору атрибутів для контролю сутностей. 7. Можливості перевірки (аудиту) підзахисних систем в автоматичному і ручному режимах для підбору релевантних правил контролю цілісності і можливістю подальшої активації цих правил (або видачі рекомендацій по їх включенню). 8. Можливість автоматичної прив'язки / відключення правил, отриманих в результаті автоматичного пошуку, до цільових підзахисних систем або політикам для них.   **Контроль подій на рівні журналів ОС**   1. Механізми роботи модуля вилучення і нормалізації даних журналів для стандартних типів систем (event log, snort, syslog та інші). 2. Робота правил модуля вилучення і нормалізації даних журналів на основі синтаксису OSSEC. 3. Можливість роботи з готовим набором декодерів даних (regex). 4. Можливість створення свого набору декодерів даних (regex). 5. Можливість створення правил через спрощені рядкові значення або засобами regex. 6. Можливості перевірки (аудиту) підзахисних систем в автоматичному і ручному режимах для підбору релевантних правил модуля вилучення і нормалізації даних журналів і можливістю подальшої активації цих правил (або видачі рекомендацій по їх включенню) 7. Можливість автоматичної прив'язки / відключення правил, отриманих в результаті автоматичного пошуку, до цільових підзахисних систем або політикам для них.   **Контроль додатків**   1. Можливість роботи модуля контролю додатків за допомогою агента (Windows/Linux). 2. Автоматичне створення переліку довірених додатків. 3. Режим роботи в режимі "білого списку" (блокування/логування запуску всіх додатків, що не входять в "білий" список). 4. Режим роботи в режимі вибіркової заборони. 5. Функціонал створення критеріїв довірених додатків за:    * Цифровим сертифікатом підписанта,    * Місцем розташування файлу, тощо. 6. Підтримка технологічних "вікон" (дозвіл на запуск і установку об'єктів, пов'язаних з оновленням систем і додатків) - безстроково або на обмежений період часу. 7. Можливість заборони або дозволу запуску з журналу подій модуля контролю додатків.   **Вимоги до проведення розслідувань кіберінцидентів.**   1. Рішення повинно представляти собою самостійний "хмарний" сервіс (SaaS) та всі зазначені вимоги реалізовувати без обов’язкової необхідності інтеграції з будь-яким антивірусним рішенням. 2. Виробник рішення повинен мати сертифікат ISO27001 для підтвердження здатності на достатньому рівні управління безпекою "хмарної" інфраструктури. 3. Рішення повинно мати самостійний окремий агент, встановлення якого не потребує видалення поточного антивірусного рішення що використовується у замовника. 4. Рішення повинно здійснювати кореляцію між метаданими, що отримані з кінцевих точок, пошти та мережевого трафіку за наявності відповідних агентів/сенсорів у інфраструктурі замовника. 5. Рішення має підтримувати встановлення агенту на наступні ОС Windows:  * Server   + Windows Server 2012 і вище;  1. Повинні підтримуватися наступні варіанти Linux:  * AlmaLinux 8 та вище; * Amazon Linux, Amazon Linux 2 (x86\_64) та вище; Amazon Linux 2 (AArch64) та вище; * CentOS 6 та вище; * CloudLinux 7 та вище; * Debian 8 та вище; * OracleLinux 6 та вище; * Red Hat Enterprise Linux 7 (x86\_64) та вище, Red Hat Enterprise Linux 8 (AArch64) та вище; * RockyLinux 8 та вище; * SuSE 12 та вище; * Ubuntu 16 (x86\_64) та вище, Ubuntu 18.04 (AArch64) та вище;  1. Повинні підтримуватися наступні варіанти macOS:  * 10.15 та вище;  1. Рішення має інтегруватись з локальною архітектурою Active Directory (on-premises) для опрацювання журналів безпеки, відображення підозрілих подій та реалізації дій по реагуванню на кіберінциденти на рівні AD. 2. Рішення на основі отриманих даних телеметрії повинно бути здатним будувати схематичну дочірньо-батьківську модель взаємодії об’єктів в рамках виявленого кіберінциденту з деталізацією по кожному із залучених об’єктів; 3. Деталізація має також містити інформацію про характер поведінки кожного із залучених об’єктів:    * тип дії – створення/доступ/комунікація;    * створення дочірніх процесів/комунікацій;    * створення/видалення записів у системному реєстрі;    * завантаження/створення/видалення файлів; 4. Відображення дочірньо-батьківської моделі повинно мати режим, в якому можна буде покроково відслідкувати кожен етап інциденту вручну контролюючи процес переходу між значимими подіями на "часовій шкалі". 5. Деталізована інформація щодо інциденту повинна містити розділ з текстовою інтерпретацією (поясненням від імені системи) подій для спрощення та прискорення розуміння про природу та перебіг активності. 6. Розділ з деталізацією інциденту має містити посилання на конкретні "техніки", згідно матриці MITRE, які спостерігаються в рамках конкретної активності; 7. Розділ з деталізацією інциденту має містити перелік усіх хостів, облікових записів та об’єктів, які залучені у поточній активності. 8. Рішення повинно мати можливість інтеграції з SIEM і SOAR системами замовника. 9. Рішення повинно мати можливість інтеграції зі сторонніми програмами через інтерфейс прикладного програмування (API), зокрема підтримувати Restful API. 10. Документація по API має бути у публічному доступі та не вимагати погодження будь-яких додаткових зобов’язань з боку замовника (підписання додаткових угод, придбання прав користування на комерційній основі і тому подібне). 11. Реалізовано розгортання агента з використанням різних підтримуваних процедур. Наприклад, розповсюдження посилання на веб-інсталятор, завантаження полегшеного інсталятора з автоматичним визначенням, завантаженням та запуском файлів інсталяційних дистрибутивів під необхідну версію ОС, завантаження повнофункціонального пакету інсталятора агента для централізованого розгортання засобами корпоративного управління встановлення додатків (SCCM, GPO, тощо). 12. Під час установки агента повинна бути можливість вказання адреси проксі-серверу для зовнішніх комунікацій. 13. Рішення має містити компонент без додаткового ліцензування, який розгортається локально та виконує роль акумулюючого проксі-серверу для передачі телеметрії від локальних агентів без прямого Інтернет-з’єднання до хмарного сервісу кореляції. 14. Агент повинен як передавати телеметрію з кінцевої точки для подальшої кореляції подій, так і здатним виконувати певні команди з консолі управління, що спрямовані на протидію потенційно небезпечній активності, обов’язково, але не обмежуючись:     * ізоляція кінцевої точки;     * додавання знайдених індикаторів компрометації до переліку явно шкідливих об’єктів;     * припинення шкідливих процесів;     * запуск з веб-консолі на віддаленому хості інтерфейсу командного рядка (CLI) для поглибленого розслідування та реагування на кіберінцидент;     * можливість запуску довільних скриптів на віддаленому хості.     * вилучення/копіювання потенційно шкідливих об’єктів із скомпрометованого хоста до веб-консолі керування для подальшого дослідження;     * створення та вивантаження «дампу» оперативної пам’яті з віддаленого комп’ютера (для OS Windows). 15. Відображення кіберінцидентів має містити показник ймовірної фази кібератаки із загальноприйнятого переліку (наприклад: виконання, підвищення привілеїв, горизонтальне переміщення, зв’зок з С&С, вивантаження даних і т.п.) 16. Агент рішення повинен періодично аналізувати операційну систему на предмет наявності вразливих компонент та передавати інформацію до консолі керування із зазначенням та відображенням:     * Загальної кількості наявних унікальних вразливостей за загальноприйнятою системою індексації CVE;     * Середній час між проведенням процедури інсталяції патчів на підзахисній інфраструктурі;     * Середньостатистичний час протягом якого кінцеві точки не мають встановлених найновіших патчів;     * Середньостатистичний показник кількості небезпечних вразливостей на один підзахисний комп’ютер; 17. Рішення повинно підтримувати роботу агентів у середовищі VDI:     * VMware Horizon версії 8.3 та вище     * Azure Virtual Desktop 18. Робота агентів у середовищі VDI повинна бути реалізована в режимах "persistent" та "non-persistent". 19. Повинна бути можливість включити агент системи у базовий образ з якого будуть запускатись "віртуалізовані робочі місця" в рамках VDI. 20. У режимі "persistent " агент повинен мати функціонал визначення вразливостей щонайменше операційної системи та передавати інформацію у хмарний сервіс. 21. Для ефективного використання придбаних ліцензій – має бути реалізовано механізм активації та деактивації агентів у консолі керування без фактичного видалення ПЗ агенту з кінцевої точки. 22. Видалення агенту рішення повинно бути захищеним додатковим механізмом, відключення якого можливе лише шляхом застосування спеціалізованого "токену" з обмеженим терміном дії, що генерується персонально конкретному замовнику. 23. Рішення повинно мати єдину централізовану консоль управління розслідуванням. 24. Рішення повинно забезпечувати функції централізованого управління з точки зору аналізу журналів, аналізу загроз, стану керованих продуктів/пристроїв і розгортання додатків. 25. Рішення повинно забезпечувати деталізовані фільтри пошуку по зібраній телеметрії, щоб користувачі могли визначати свої власні критерії пошуку з використанням логічних операторів "та"/"або"/"ні". 26. Рішення повинно мати можливість виконувати багаторівневий пошук і розслідування на основі окремих параметрів або об'єктів ІоС, файлів OpenIOC і файлів STIX. Параметри пошуку повинні включати:  * Зв'язок: IP-адреса, порт, домен, DNS, назва хоста, URL * Назву шкідливого ПЗ або будь-який файл по:   + хешу SHA1,   + імені файлу,   + шляху до файлу,   + типу файлу. * Діяльність в реєстрі:   + створення,   + редагування,   + видалення. * Активність облікового запису користувача  1. Має бути можливість збереження довільних критеріїв пошуку подій на кінцевих точках та на їх основі створювати правила оповіщення. 2. Рішення повинно забезпечувати централізований огляд виявлення загроз для керованих продуктів / пристроїв. 3. Рішення повинно мати представлення у вигляді дерева або еквівалентне представлення всіх керованих продуктів/пристроїв, включаючи назву продукту / пристрою, IP-адресу, стан підключення, версії додатків тощо. 4. Рішення повинно забезпечувати рольовий контроль доступу для цілей адміністрування, розслідування, а також інших операцій. 5. Рішення повинно забезпечувати функцію журналу аудиту для перегляду історії дій користувачів. 6. Підтримку багатофакторної аутентифікації (MFA) 7. Рішення повинно зберігати метадані з кінцевих точок у централізованій базі даних:    * Інформації про файли/об’єкти,    * дії і важливі системні події,   а також постійно оновлювати цю базу даних для запису факту появи і виконання підозрілих об'єктів.   1. Рішення має надавати можливість користувачу визначати та завантажувати власні правила та індикатори компрометації (ІоС), щоб визначати файли та події для моніторингу. 2. Рішення має надавати можливість користувачу створювати власні правила відслідковування подій, задаючи критерії детектування засобами хмарної платформи. Тобто створювати власні моделі детектування XDR. 3. Рішення повинно мати можливість відстежувати і досліджувати події на кінцевих точках незалежно від їх місця розташування - локально, віддалено або "хмарно". 4. Рішення повинно мати інтерактивні інформаційні панелі для перегляду та аналізу дій системи з плином часу (віджети), оцінки термінів діяльності в масштабі всього підприємства та експорту результатів розслідування. 5. Рішення повинно мати можливість обмінюватися даними про загрози між керованими/інтегрованими продуктами та пристроями того ж виробника, а також продуктами сторонніх виробників, згідно наявного списку інтеграцій у веб-консолі та через застосування АРІ. 6. Інформація про загрози повинна бути сумісна з загальнодоступним стандартом STIX. 7. Рішення повинно мати можливість підключатися до різних серверів TAXII в якості клієнта для отримання аналітичних даних про загрози без додаткового ліцензування. 8. Рішення повинно підтримувати функції клієнта та сервера MISP для отримання/передачі різних індикаторів компрометації без додаткового ліцензування. 9. Рішення повинно містити в собі підписку на звіти розслідувань від виробника з інформацією по шкідливим кампаніям з різних регіонів Світу, зокрема і з України, без додаткової оплати, і можливістю отримання деталізованої довідки по різним шкідливим кампаніям. 10. Рішення має також надавати інформацію про діючі кіберугрупування без додаткового ліцензування, як мінімум про наступне:     * Опис самого кіберугрупування, його спеціалізація та особливі прикмети;     * Посилання на опис Технік, Тактики і Процедур, що застосовуються конкретним кіберугрупуванням;     * Перелік спеціалізованих утиліт/шкідливого ПЗ/характерних вразливостей за CVE, що використовуються конкретним кіберугрупуванням.     * Перелік комп’ютерів з підзахисної інфраструктури де було виявлено відповідні артефакти для прискорення оцінки компрометації інфраструктури. 11. Можливість підключення до сторонніх баз шкідливих кампаній без додаткового ліцензування. 12. Рішення повинно автоматично сканувати наявні метадані з підзахисних об’єктів на предмет присутності індикаторів компрометації із нових шкідливих кіберкампаній ретроспективно та щонайменше, протягом останніх 7 днів від дня отримання/появи у рішенні інформації про активність кіберкампанії. 13. Рішення повинно дозволяти користувачам визначати глобальний список винятків для створення винятків всередині організації і можливість передачі списку винятків іншим продуктам того ж або стороннім виробникам. 14. Рішення повинно забезпечувати виявлення загроз на основі найновіших моделей, створених виробником, без необхідності будь-якого втручання в ручному режимі з боку користувачів. 15. Рішення повинно вміти приорітезувати визначені загрози/інциденти шляхом присвоєння відповідного рівня критичності. 16. У рішення має бути функціонал присвоєння статусу виявлених інцидентів, щонайменше:     * Новий,     * В процесі дослідження,     * Вирішено,     * Закритий як хибнопозитивний. 17. Для інцидентів повинна бути можливість додавання довільних коментарів. 18. Рішення повинно мати можливість ідентифікувати всі хости, заражені однією і тією ж загрозою. 19. Рішення повинно мати можливість ідентифікувати всі хости, які підключалися до шкідливого C&C сервера. 20. Рішення має зберігати метадані в централізованому реєстрі метаданих. 21. У реєстрі метаданих повинні бути дані про активність, а також дані про виявлення. Рішення повинно дозволяти пошук незалежно від того, чи знаходиться машина в мережі або офлайн. 22. Рішення повинно мати налаштування автоматизованих сценаріїв реагування (плейбуків). 23. Запуск плейбуків має бути реалізованим за:     * подією (виявлення за поведінкою XDR, за наявністю шкідливого об’єкта, наявністю вразливості, тощо),     * рівнем критичності події (високий/середній/низький),     * рівнем критичності виявленого об’єкту,     * розкладом, або за командою користувача. 24. Результати виконання дій в рамках плейбуків мають надсилатись визначеним користувачам електронною поштою, або за допомогою надсилання у вигляді "заявки" на зазначений веб-ресурс після проходження авторизації. 25. Рішення має відображати сукупний рівень ризиків ввіреної інфраструктури у вигляді графіку з інформацією щонайменше за останні 30 днів.   Допускається відображення показників у відносних одиницях з певного діапазону, наприклад у діапазоні від 0 до 100 одиниць, де 0 – низький рівень ризиків, а 100 – найвищий.  **Кількісні та якісні характеристики програмного забезпечення**   1. Програмне забезпечення повинно включати в себе всі вищезазначені модулі в активному стані 2. Кількість – 60 3. Всі ліцензії та активні підписки повинні бути не менше, ніж на 12 місяців 4. Має бути зазначеним в Gartner’s Magic Quadrant for Endpoint Protection Platforms за 2022 та 2023 роки | шт | 60 |
| 3. | Програмне забезпечення система захисту від цільових атак у електронній пошті (подовження) | **Вимоги до системи системи захисту від цільових атак у електронній пошті**  ***Загальні вимоги***  1. Робота у вигляді програмно-апаратного комплексу (ПАК), або у вигляді віртуальної машини з керуванням через веб-консоль  2. Робота з копією трафіку у режимах SPAN/TAP, BCC  3. Робота в режимі "логічного розриву" (MTA) із утриманням об'єкта до винесення вердикту  4. Можливість інтеграції з XDR платформою того ж виробника.  5. Наявність статичної антивірусної перевірки перед відправкою до модуля «пісочниці» (за її наявності).  - За базами відомих сигнатур;  - За моделями, отриманих на основі алгоритмів машинного навчання задля протидії невідомим загрозам.  6. Підтримка зміни маршруту для листів у черзі по: MX-запису, ІР-адресі чи доменним ім’ям поштового серверу з можливістю вказування пріоритетного маршруту доставки  7. Можливість обмежувати кількість одночасних вхідних з’єднань  8. Можливість створення довірених джерел пошти за ІР-адресою и маскою підмережі  9. Можливість блокування джерел пошти за правилом "заборони всіх, окрім явно вказаних"  10. Можливість заміни адреси отримувача  11. Аналіз пошти із підтримкою TLS у т.ч. версії TLS 1.3  12. Підтримка DKIM, DMARC, SPF  13. Підтримка технології DANE для вихідних листів  14. Протидія атакам, націлених на збір реальних адрес користувачів (DHA) за наступними критеріями:  - Період аналізу  - Відсоток листів з небезпечним вмістом  - Загальна кількість листів  - Кількістю отримувачів  - Кількістю неіснуючих отримувачів  з можливістю постійного або тимчасового блокування відправника на заданий проміжок часу  15. Протидія атакам, що опираються на відправку автовідповідей (Bounce Attack) за наступними критеріями:  - Період аналізу  - Відсоток листів з небезпечним вмістом  - Загальна кількість листів  з можливістю постійного або тимчасового блокування відправника на заданий проміжок часу  16. Можливість вводу лімітів за кількістю відправлених листів від одного відправника за email-адресою та за ІР-адресою за певний проміжок часу чи за кількістю листів з блокуванням, тривалість якого можна конфігурувати  17. Підтримка шифрування надсилання пошти на основі IBE алгоритму власної розробки  18. Можливість автоматичного застосування шифрування при наявності ключових слів у заголовках, у тілі листа чи у вкладених файлах  19. Можливість застосування дій, якщо фактична адреса відправника не співпадає із зазначеною в полі "від" (захист від спуфінгу)  20. Можливість окремого налаштування дій за рівнями критичності ризику  21. Можливість вставляти текстові мітки у заголовки/тему листа при порушеннях політик безпеки  22. Можливість зберігати оригінальний лист у карантині у випадку коли вкладення не може бути видалено, або перед видаленням вкладення  23. Можливість пересилання листа, на який зреагувала політика антивірусного захисту, на окремий поштовий сервер по SMTP, або у вигляді прихованої копії (ВСС) на окремий поштовий ящик  24. Можливість пересилання листів на окремий "сервер архівації" для зберігання  25. Наявність карантину пошти, доступного адміністратору (за всіма загрозами)  26. Наявність персонального карантину пошти, доступного користувачам (за спамом)  27. Авторизація користувачів у карантині за доменним обліковим записом  28. Розсилка консолідованих звітів за утриманими листами у персональному карантині кожному користувачу  29. Прив'язка політик до користувачів Active Directory / LDAP  30. Підтримка зовнішніх пісочниць того ж виробника  31. Підтримка передачі інцидентів по Syslog у форматах CEF, LEEF  32. Підтримка передачі звітів про інциденти по email  33. Перезапис/заміна небезпечних посилань усередині листа з перенаправленням на сторінку з повідомленням про небезпеку на самому модулі або довільній сторінці / внутрішньому порталі організації  34. Створення винятків за словами в URL для застосування правил заміни посилань (запобігання порушенню роботи маркетингових розсилок)  35. Створення винятків по відправникам та одержувачам для перевірки на СПАМ  36. Створення винятків по відправникам та одержувачам за: доменом, ІР-адресою/підмережею за маскою, email-адресою, типами запису А, АААА, МХ  37. При додаванні відправника/отримувача у список виключень – антивірусна та контентна фільтрація за типом дозволених об’єктів має залишатись активованою  38. Підтримка чорних списків відправників (адреси, домени, IP, МХ)  39. Створення винятків за словами URL (захист від порушення роботи списків розсилок)  40. Підтримка зовнішніх балансувальників для побудови відмовостійкості  41. Підтримка SNMP для моніторингу  Вимоги до аналізу поштового трафіку  42. Підтримка контентної фільтрації за типами файлів, словами в тілі/заголовках/вкладених файлах, розмірами файлів та з використанням регулярних виразів  43. Можливість контентного фільтра видаляти активний вміст (наприклад, скрипти, макроси) всередині документів  44. Наявність механізмів DLP контролю над вихідними листами  45. Підтримка явної заборони запаролених об'єктів (архівів та документів)  46. Підтримка антиспам захисту від репутації джерел  47. Підтримка антиспам захисту на сигнатурній основі  48. Можливість виявляти та блокувати шкідливий код у файлах, що передаються електронною поштою користувачів  49. Механізм перезапису посилань з подальшим аналізом кожного переходу по них користувача з метою ретроспективної оцінки компрометації цільових сторінок засобами хмарного Threat Intelligence  50. Можливість примусової (ручної) передачі листів для аналізу у форматах EML та MSG  51. Відхилення листа від невідомих IP-адрес відправників або доменів  52. Відхилення листа невідомим корпоративним отримувачам  53. Наявність захисту від "схожих" з відомими, або корпоративними доменами, коли заміна символів у адресі може вводити в оману отримувача листа. Захист повинен дозволяти регулювати ступінь "схожості" шляхом зміни коефіцієнтів тотожності  **Система керування**  54. Робота у форматі віртуальної машини у середовищі VMware, Hyper-V  55. Без необхідності придбання додаткового ПЗ  56. Консолідація даних з усіх керованих модулів  57. Можливість створення завдань щодо поширення оновлень ПЗ, встановлення патчів, хотфіксів та образів "пісочниць" по всіх керованих модулях та автоматичне виконання їх за розкладом (дата, години, хвилини).  58. Централізація оновлень ПЗ за всіма керованими модулями  59. Централізація поширення/заміни образів "пісочниць" за всіма керованими модулями автоматично за розкладом  60. Забезпечення реплікації конфігурацій між керованими пристроями  61. Забезпечення єдиної точки обміну індикаторами компрометації (IoC) на рівні всіх керованих модулів  62. Забезпечення передачі IoC засобам антивірусного захисту кінцевих точок того самого виробника.  63. Забезпечення передачі IoC з усіх керованих модулів стороннім системам (CheckPoint, Palo Alto, BlueCoat та ін.)  64. Публікація списку IoC засобами внутрішнього веб-сервера для спрощення інтеграції з продуктами сторонніх розробників  65. Єдина система оповіщень у форматі CEF, LEEF, SNMP за подіями від усіх керованих модулів  66. Централізоване поширення профілів методом TAXII стороннім системам  67. Система доступу на основі RBAC  68. Інтеграція з Active Directory для адміністративних завдань  69. Централізований "чорний" список об'єктів за всіма керованими модулями  70. Централізований список виключень об'єктів (хеші, домени, URL, IP) за всіма керованими модулями  71. Можливості детального пошуку інцидентів щодо широкого спектру параметрів із збереженням пошукового запиту  72. Можливість збереження деталей інциденту (включаючи звіти, опис, pcap-дампи)  73. Зіставлення локальних результатів інциденту з даними Global Threat Intelligence  74. Централізоване керування словниковою базою паролів для розкриття запаролених архівів та документів (Office, PDF) по всіх керованих пристроях з можливістю експорту/імпорту списків.  **Кількісні та якісні характеристики програмного забезпечення**  75. Програмне забезпечення повинно включати в себе всі вищезазначені модулі в активному стані  76. Кількість – 540  77. Всі ліцензії та активні підписки повинні бути не менше, ніж на 12 місяців | шт. | 540 |
| 4. | Програмне забезпечення система динамічного аналізу в ізольованому середовищі | **Вимоги до системи система динамічного аналізу в ізольованому середовищі**  ***Основні функції аналізу***   1. Динамічний аналіз об'єктів: здійснює поведінковий аналіз підозрілих файлів, URL-адрес та інших об'єктів у ізольованому віртуальному середовищі. 2. Підтримка різних типів об'єктів: аналіз файлів, URL-адрес, скриптів, документів та інших потенційно небезпечних об'єктів. 3. Інтеграція з іншими модулями: можливість надсилання об'єктів на аналіз з таких модулів, як Workbench, Observed Attack Techniques та Search App.   ***Методи подання об'єктів***   1. Ручне подання: через інтерфейс Sandbox Analysis App або за допомогою публічного API. 2. Автоматичне подання: з інтегрованих продуктів Trend Micro Vision One endpoint security (Essentials, Pro), Deep Discovery Email Inspector та інших. 3. Подання через API: використання публічного API для інтеграції з внутрішніми системами та автоматизації процесу подання об'єктів.   ***Звіти та результати аналізу***   1. Детальні звіти: надання інформації про поведінку об'єкта, виявлені загрози, використані техніки атак та інші релевантні дані. 2. Інтеграція з Virtual Analyzer: результати аналізу можуть бути отримані від Virtual Analyzer (VA) та відображаються в Sandbox Analysis App. 3. Візуалізація результатів: інтерфейс надає зручну візуалізацію результатів аналізу для швидкого розуміння загроз.   ***Інтеграція з іншими продуктами***   1. Підтримка інтеграції: з такими продуктами, як Trend Micro Vision One endpoint security (Essentials, Pro), Deep Discovery Email Inspector 2. Сумісність з API: можливість інтеграції з внутрішніми системами через публічний API для автоматизації процесів. 3. Підтримка сторонніх продуктів: інтеграція з продуктами інших виробників, такими як Fortinet, Palo Alto Networks, Splunk та іншими   ***Безпека та конфіденційність***   1. Ізольоване середовище: аналіз об'єктів проводиться в безпечному віртуальному середовищі, що запобігає впливу на реальну інфраструктуру. 2. Конфіденційність даних: забезпечується захист даних, що передаються на аналіз, відповідно до політик безпеки Trend Micro. 3. Контроль доступу: можливість налаштування прав доступу до модуля та результатів аналізу для різних користувачів.   ***Технічні вимоги***   1. Підключення до Інтернету: необхідне для взаємодії з хмарним середовищем аналізу. 2. Сумісність з продуктами: підтримка інтеграції з різними продуктами Trend Micro для забезпечення автоматичного подання об'єктів. 3. Використання API: можливість інтеграції з внутрішніми системами через публічний API для автоматизації процесів.   **Кількісні та якісні характеристики програмного забезпечення**   1. Програмне забезпечення повинно включати в себе всі вищезазначені модулі в активному стані 2. Кількість – 540 3. Всі ліцензії та активні підписки повинні бути не менше, ніж на 12 місяців | Шт. | 540 |
|  | Програмне забезпечення система розширеного виявлення та реагування в мережевому трафіку (XDR for Networks) | **Вимоги до системи система розширеного виявлення та реагування в мережевому трафіку (XDR for Networks)**  ***Основні функції***   1. Розширене виявлення загроз: автоматичне виявлення аномалій, підозрілих дій та складних атак у мережевому трафіку. 2. Кореляція подій: об'єднання даних з різних джерел для повного розуміння ланцюга атаки. 3. Візуалізація атак: графічне відображення етапів атаки для полегшення аналізу та реагування. 4. Інтеграція з іншими модулями: можливість об'єднання з іншими продуктами Trend Micro для покращення загальної безпеки.   ***Пропускна здатність***   1. Пропускна здатність: до 500 Мбіт/с аналізованого мережевого трафіку. 2. Ліцензія: передбачає підписку на 12 місяців для одного блоку пропускної здатності (500 Мбіт/с).   ***Зберігання та обробка даних***   1. Термін зберігання: стандартно 30 днів, з можливістю розширення до 180 днів за додаткову плату. 2. Обсяг зберігання: приблизно 2,3 ТБ на 1 Гбіт/с трафіку, тобто близько 1,15 ТБ для 500 Мбіт/с . 3. Формат зберігання: дані зберігаються у форматі, оптимізованому для швидкого пошуку та аналізу   ***Інтеграція та сумісність***   1. Підтримка інтеграції: з такими продуктами, як Trend Micro Vision One endpoint security (Essentials, Pro), Deep Discovery Email Inspector та іншими. 2. Сумісність з API: можливість інтеграції з внутрішніми системами через публічний API для автоматизації процесів. 3. Підтримка сторонніх продуктів: інтеграція з продуктами інших виробників, такими як Fortinet, Palo Alto Networks, Splunk та іншими.   ***Безпека та конфіденційність***   1. Ізольоване середовище: аналіз об'єктів проводиться в безпечному віртуальному середовищі, що запобігає впливу на реальну інфраструктуру. 2. Конфіденційність даних: забезпечується захист даних, що передаються на аналіз, відповідно до політик безпеки Trend Micro. 3. Контроль доступу: можливість налаштування прав доступу до модуля та результатів аналізу для різних користувачів.   ***Технічні вимоги***   1. Підключення до Інтернету: необхідне для взаємодії з хмарним середовищем аналізу. 2. Сумісність з продуктами: підтримка інтеграції з різними продуктами Trend Micro для забезпечення автоматичного подання об'єктів. 3. Використання API: можливість інтеграції з внутрішніми системами через публічний API для автоматизації процесів.   **Кількісні та якісні характеристики програмного забезпечення**   1. Програмне забезпечення повинно включати в себе всі вищезазначені модулі в активному стані 2. Кількість – 2 3. Всі ліцензії та активні підписки повинні бути не менше, ніж на 12 місяців | Шт. | 2 |

**Додатково:**

1. Учасник повинен у складі своєї Пропозиції надати документ, що підтверджує статус Учасника як офіційного представника (партнера) виробника в Україні, а саме - авторизаційний лист від виробника (дилера, дистриб’ютора) щодо можливості постачання предмету даної закупівлі. Лист має бути адресований замовнику торгів та містити ідентифікатор закупівлі, назву предмету закупівлі. Повноваження дилера/дистриб’ютора повинні бути підтверджені шляхом надання копії документу, який свідчить про передачу повноважень від виробника представляти його інтереси на території України.

**У разі, якщо пропозиція учасника не відповідає умовам технічної специфікації та іншим вимогам щодо предмета закупівлі встановленим даною тендерною документацією, або учасник не в змозі виконати умови які визначені Замовником в даній тендерній документації, пропозиція відхиляється.**