ОБҐРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, його очікуваної вартості та/або розміру бюджетного призначення в межах закупівлі

UA-2025-06-26-002484-a

Замовник: Державна установа «Урядовий контактний центр» (далі-Центр) (ЄДРПОУ 36521731)

Місцезнаходження замовника: 01001, м. Київ, вул. Еспланадна, буд. 8/10

Категорія замовника: юридична особа, яка забезпечує потреби держави або територіальної громади.

Підстава для публікації: постанова Кабінету Міністрів України «Про ефективне використання державних коштів» від 11 жовтня 2016 р. № 710»

Предмет закупівлі: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки (Послуги з оновлення ліцензійного програмного забезпечення для захисту персональних комп’ютерів та електронної пошти від кіберзагроз) (код ДК 021:2015: 48730000-4 Пакети програмного забезпечення для забезпечення безпеки

Опис закупівлі: Рішення повинно включати доступ до вже діючого в Урядовому контактному центрі програмного забезпечення антивірусного захисту робочих станцій та програмного забезпечення захисту електронної пошти з вбудованою «пісочницею» (програмна продукція Trend Micro Apex One On-premises: New: New, Normal, 251-500, 12 month(s) або еквівалент).

Зазначене програмне забезпечення повинно відповідати наступним обов’язковим функціональним вимогам (Таблиця № 1):

Таблиця № 1

№ з/п	Параметр	Найменування, характеристики
1	Загальні вимоги	- Програмне забезпечення повинна включати можливість встановлення-ПЗ на не менше ніж 251 робочу станцію - Централізована система управління (адміністрування) захистом робочих станцій, підключених до локальної мережі. - Безпека і шифрування команд при віддаленому адмініструванні на основі підпису агент-серверної комунікації цифровими сертифікатами. - Віддалене розгортання, конфігурування і адміністрування клієнтів на робочих станціях. - Відсутність ліцензійних обмежень на розгортання додаткових серверів віддаленого адміністрування. - Можливість створення в системі управління груп керованих комп'ютерів як вручну (на основі імен комп'ютерів), так і автоматично (на основі структури Active Directory або діапазонів IP-адрес). - Наявність функцій централізованого збору статистичної інформації про роботу антивірусного програмного забезпечення на робочих станціях.

		- Можливість експортувати певні журнали та / або події про роботу антивірусного програмного забезпечення на робочих станціях. - Можливість інтеграції з середовищем динамічного аналізу («пісочницями») того ж виробника. - Наявність сканеру файлів. - Можливість формування списків довірених додатків. - Можливість відключення сканування для довірених додатків. - Можливість виключити з перевірки файли і папки з конкретним шляхом. - Наявність поведінкового аналізатора, що дозволяє на підставі поведінки додатка зробити висновок, зловмисне воно чи ні. - Можливість додавати виключення зі сканування для модулю поведінкового аналізу. - Наявність технологій, що дозволяють по репутації файлу, його давності та розповсюдженості виносити вердикт про його зловмисності. - Можливість автоматичної зміни параметрів роботи при старті поза периметром корпоративної мережі. - Наявність резидентного монітору. - Використання евристичних технологій під час сканування та забезпечення захисту в режимі реального часу. - Захист від шпигунського та рекламного ПЗ. - Виявлення руткітів (прихованих файлів / системних аномалій). - Має містити модуль, який при виявленні змін, що були ініційовані зловмисним скриптом – здійснює дії усунення наслідків шкідливого впливу: • Видалення активних файлів-вірусів та троянів; • Видалення завантажених файлів зловмисним ПЗ; • Відновлення файлів, модифікованих троянами; • Зупинку процесів, запущених вірусами; • Видалення створених гілок системного реєстру або їх значень модифікованих зловмисними скриптами; - Система захисту повинна забезпечувати захист від наступних типів загроз: • Віруси • Трояни • Мережеві черв'яки • Рекламні програми • Шпигунські програми • Програми - "дзвонилки" • Програми-жарти • Генератори піратських ключів • Віруси-вимагачі та шифрувальники - Наявність моніторингу подій типу • Появи нової служби; • Поява нового об’єкту у списку автозапуску при старті ОС; • Ін’єкції сторонніх бібліотек у типові системні процеси;

		• Модифікацій системних файлів/процесів; • Появи файлів з іменами, що дублюють системні; • Зміну політик безпеки ОС, і т.п. та можливість задання автоматичної дії при виявленні подібної поведінки з переліку: дозвіл/блокування/запит дії у користувача за потреби. При цьому має бути можливість вказування часу застосування дії автоматично, якщо користувач не відповів на запит щодо дозволу чи блокування підозрілої поведінки. - Захист від експлойтів який забезпечує захист від загроз здатних використовувати уразливості Java, Flash та інших додатків. - Докладне журналювання, формування зведених звітів та звітів щодо кожної робочої станції. - Наявність антивірусної перевірки файлів в архівах форматів ARJ, UPX, MSCOMP, PKLite, ASPAC, DIET, LZEXE, ACE, BZIP, BZIP2, CAB, CHM, GZIP, LHA, RAR, TAR, ZIP, BIN, TD0. - Можливість сканування файлів під час запуску системи. - Можливість сканування за розкладом. - Можливість запуску антивірусного сканування по команді користувача з підзахисної машини або адміністратора з консолі централізованого управління. - Можливість відключення антивірусного захисту або окремих модулів захисту при необхідності. - Автоматична антивірусна перевірка змінних носіїв. - Можливість запуску завдань за розкладом. - Можливість регулювання розподілу ресурсів робочої станції між антивірусом і іншими додатками в залежності від рівня навантаження Центрального Процесора ЕОМ (паузи між скануванням файлів при досягненні порогових значень 20% або 50%). - Наявність захисту від ще невідомих шкідливих програм на основі аналізу їхнього поводження та контролю змін системного реєстру (поведінковий аналіз та модулю прогнозного машинного навчання). - Наявність захисту від ботнетів: виявляти шкідливі програми, аналізуючи їх схеми обміну даними і протоколи. - Розширений сканер пам'яті, який відстежує підозрілі процеси та сканує їх, як тільки вони виникають, що дозволяє запобігти зараженню навіть ретельно зашифрованими та прихованими загрозами, або ж малорозповсюдженими програмами-архіваторами. - Захист від RansomWare – автоматичне створення резервних копій модифікованих (шифрованих) файлів і відновлення їх у разі, якщо їх модифікує шкідлива програма-шифрувальник; - Наявність персонального міжмережевого екрану. - Міжмережевий екран повинен мати можливість блокувати мережевий трафік кінцевої точки не лише за IP, адресою, напрямком, портом призначення та іншими мережевими атрибутами, але і для визначених додатків за шляхом їх

		розміщення у файловій системі, а також за шляхом асоційованих гілок системного реєстру конкретного ПЗ. - Регламентне оновлення виробником системи баз даних загроз та програмних модулів в автоматичному режимі та/або за розкладом не менш ніж 24 рази на добу. - Можливість централізованого оновлення системи антивірусного захисту робочих станцій, підключених до локальної мережі з одного комп'ютера, який розташований в локальній мережі (проміжний сервер оновлень). - Можливість оновлення програмних засобів і антивірусних баз з різних джерел, як по каналах зв'язку, так і зі змінних носів інформації. - Можливість створення дзеркала оновлень та локального репозиторію файлової і веб-репутації для зменшення навантаження на зовнішні канали зв'язку. - Можливість налаштування часу оновлень і сканування в межах заданого терміну. - Наявність ієрархічної системи управління політиками з можливістю успадкування частини політик від батьківських груп. - Сервер адміністрування повинен підтримувати функціонал резервного копіювання та відновлення згідно наданої виробником інструкції. - Наявність антивірусного сканування трафіку за такими протоколами: FTP, HTTP, HTTPs і POP3 трафіку. - Можливість захисту веб-трафіку - перевірка об'єктів, що надходять на комп'ютер користувача при взаємодії з ресурсами мережі Інтернет. - Можливість блокування Інтернет-ресурсів за веб-адресою або IP-адресою. - Можливість захисту від зміни параметрів ПЗ паролем. - Наявність захисту від фішингу: захист від спроб отримати паролів та іншу конфіденційну інформацію, забороняючи доступ до шкідливим веб-сайтів, які приймають вид нормальних веб-сайтів. - Можливість імпорту для виявлення зловмисного ПЗ сигнатур у форматі- OpenIOC. - Наявність функції автоматичного сповіщення адміністраторів системи антивірусного захисту про виявлення шкідливого програмного забезпечення. - Можливість інтеграції з центром безпеки Windows. - Наявність технічного сервісу по надсиланню зразків нового шкідливого програмного забезпечення для проведення аналізу та надання рекомендацій. - Якщо модуль не здатний заблокувати шкідливий файл в автоматичному режимі, повинні бути запропоновані наступні механізми ручного стримування епідемії: • блокування файла по імені; • блокування запису в певні папки; • блокування мережевої взаємодії з певних портів;

		• блокування запису в мережеві папки. - Має бути реалізовано механізм відправки довільних повідомлень на підзахисних комп'ютер для інформування користувача адміністратором.
2	Вимоги до підтримуваних потенційних каналів витоку даних	- Функціонал має бути реалізований засобами єдиного з антивірусним агентом, без необхідності встановлення будь-якого додаткового ПЗ / агенту. - Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються "всередину" і "назовні" корпоративної мережі по протоколам як мінімум: SMTP, HTTP, HTTPS, FTP. - Підсистема захисту від витоків даних повинна бути здатна виявляти передавання конфіденційних даних в клієнтах електронної пошти (як мінімум Microsoft Outlook) та через веб-сторінки онлайн поштових сервісів. - Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються на друк. - Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що записуються на зовнішні накопичувачі: CD/DVD, USB Flash. - Підсистема захисту від витоків даних повинна бути здатна виявляти конфіденційні дані що передаються по локальній мережі - Система повинна підтримувати як мінімум наступні види параметрів, за якими проводиться пошук конфіденційних даних: • Словник (в т.ч. споріднені слова за коренем, кількість входжень, співпадіння від вказаного за порядком символу) • Регулярні вирази • Метадані файлів • Номери банківських карт • Номери паспортів та інших регулярних алфавітно-цифрових комбінацій - Система повинна підтримувати експорт та імпорт налаштувань фільтрації у форматі XML - Система повинна забезпечувати наступні види реакції на виявлення в переданому файлі конфіденційних даних: • Блокування передачі • Фіксація факту передачі в журналі • Повідомлення Користувачу
3	Вимоги до захисту від вразливостей	- Система захисту від вразливостей повинна забезпечувати можливості запобігання вторгненням на рівні мережі, націлених на вразливості як ОС так і стороннього програмного забезпечення встановленого на робочій станції. - Виробник антивірусного продукту має мати власну команду дослідників поширеного ПЗ та ОС на предмет наявності вразливостей, а не лише спиратись на результати досліджень сторонніх організацій. - Система повинна мати модуль захисту від вразливостей без установки окремого від антивіруса агента, щоб уникнути перенавантаження на кінцеві точки.

		- Система захисту повинна бути здатна конфігуруватися з метою активації тільки тих фільтруючих правил, які актуальні для даного комп'ютера або групи комп'ютерів. - Система захисту повинна забезпечувати роботи в режимах: • Inline (в розрив) • TAP (в режимі прослуховування трафіку та фіксації подій) - Система захисту повинна мати можливість вибору попередньо сконфігурованого профілю для захисту, наприклад, оптимізованого з точки зору безпеки або з точки зору продуктивності задля спрощення та прискорення впровадження. - Система має містити розділ з детальною конфігурацією дій щодо джерела з якого походять небезпечні команди, зокрема: • ESTABLISHED Timeout • LAST_ACK Timeout • Cold Start Timeout • UDP Timeout • Maximum TCP Connections • Maximum UDP Connections • Ignore Status Code • Block Same Src-Dest IP Address • Minimum Fragment Offset • Minimum Fragment Size - Перелік правил має містити назву правила, його статус (активовано / деактивовано), тип або сімейство ПЗ до якого правило може бути застосованим, індекс за глобальною класифікацією CVE, Microsoft CVE (якщо вразливість стосується ПЗ Microsoft), ступінь критичності CVSS, дату останнього оновлення правила, та інші.
4	Вимоги до контролю додатків	- Робота модулю повинна налаштовуватися як для окремих користувачів імпортованих з Active Directory (чи груп), так і для комп'ютерів в цілому. - Повинна бути можливість дозволити / заборонити повідомлення користувача про блокування - Підсистема повинна забезпечити наступні критерії визначення додатка: • Контрольна сума SHA1 • Сертифікат цифрового підпису • Розташування файлу • Розробник • Належність певної категорії, типу додатка • Загальний рейтинг довіри (за даними виробника) • Глобальна розповсюдженість - Повинні бути реалізовані наступні можливості контролю сертифікатів додатків: • Довірений сертифікат • Довірений, але застарілий сертифікат • Недовірений сертифікат • Країна емітента • Назва емітента • Організація емітент

		• Інші атрибути емітента - 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 - Система повинна дозволяти визначати як мінімум наступних виробників програмного забезпечення: Microsoft, Adobe, Oracle, Apple та інш. - 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 - Система повинна забезпечувати довільну комбінацію перерахованих вище критеріїв визначення файлів з використанням булевої логіки дозволяючу або блокуючу дію запуску програм. - 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 Windows

5	Вимоги до захисту інфраструктур VDI	- Підсистема захисту інфраструктур VDI повинна безшовно інтегруватися з системою захисту робочих станцій - Підсистема повинна підтримувати наступні платформи віртуалізації: • Citrix XEN • VMware vSphere • Microsoft Hyper-V - Підсистема повинна підтримувати інтеграцію з більш, ніж з одним гіпервізором одночасно - Підсистема повинна дозволяти зробити еталонний образ ОС Windows з вбудованим агентом захисту - Підсистема повинна дозволяти налаштовувати максимальну кількість агентів що одночасно можуть виконувати оновлення компонент - Підсистема повинна дозволяти налаштовувати максимальну кількість агентів що паралельно здійснюють перевірку за розкладом - Система повинна пропонувати такі обов'язкові механізми антивірусної перевірки: • З повною базою (для автономних інфраструктур) • З мінімальною базою і використанням сервісу файлової репутації антивірусного серверу, чи ресурсів виробника
6	Вимоги до захисту робочих станцій на базі macOS	- Система захисту повинна забезпечувати підтримку наступних ОС: • macOS™ 10.15 та вище - Агент повинен пропонувати наступні механізми захисту: • Сигнатурний аналіз по "повній базі" для комп'ютерів, розміщених в автономних мережах • Сигнатурний аналіз по скороченій базі для комп'ютерів, що мають доступ до онлайн-ресурсів виробника • Сигнатурний аналіз по скороченій базі для комп'ютерів, що мають доступ до внутрішнього сервера з копією даних з онлайн-ресурсів виробника • Технології «машинного навчання» для захисту від загроз «нульового дня» - Система захисту повинна підтримувати наступні типи сканування: • У реальному часі (при створенні / зміні файлу) • За запитом користувача • За розкладом - Система захисту повинна мати функціонал контролю пристроїв: • Блокування підключення зовнішніх пристроїв за їх типом • Дозволяти тільки відображення вмісту зовнішніх пристроїв • Повний доступ - Система контролю зовнішніх пристроїв повинна налаштовуватися як для окремих користувачів імпортованих з Active Directory (чи груп), так і для комп'ютерів в цілому.

		- Система контролю зовнішніх пристроїв повинна мати можливість автоматично змінювати параметр роботи в разі роботи комп'ютера поза корпоративної мережею. - Система контролю зовнішніх пристроїв повинна надавати можливість створення виключень як за параметрами самого пристрою (модель, виробник, серійний номер), так і за програмним забезпеченням, яке матиме дозвіл на взаємодію попри глобальну заборону для решти ПЗ. - Система захисту повинна мати функціонал самозахисту - Підсистема повинна забезпечувати належний рівень самозахисту: • Контроль цілісності агента • Запобігання блокування роботи агента • Запобігання доступу непривілейованих користувачів до файлів агента, журналів - Система захисту повинна дозволяти використовувати не тільки локальну антивірусну базу, але і перевіряти репутацію файлів по хмарній базі виробника - Повинна бути можливість розміщення всередині корпоративної мережі копії хмарної репутаційної бази виробника для перевірки файлів та веб-посилань. - Підсистема повинна забезпечувати очищення заражених систем від наслідків зараження - Підсистема повинна забезпечити блокування підключень до шкідливих веб-ресурсів
7	Підтримка операційних систем клієнтської частини	- Windows 10 і новіші - Windows Server версії: починаючи від Microsoft Windows Server 2012 і новіші.
8	Гарантійне обслуговування та сервісна підтрика.	- Гарантійні зобов’язання та технічна підтримка від виробника повинна становити: на програмну продукцію не менше 12 місяців.

Функціональні вимоги до вже діючого в Урядовому контактному центрі програмного забезпечення захисту електронної пошти з вбудованою «пісочницею».(програмне забезпечення Trend Micro Deep Discovery Email Inspector - Advanced Threat and Gateway Modules, SW: New: New, Normal, 1-1000, 12 month(s) або еквівалент.

Зазначене програмне забезпечення повинне відповідати наступним обов’язковим функціональним вимогам (Таблиця № 2):

Таблиця № 2

№ з/п	Параметр	Найменування, характеристики
1	Загальні вимоги	- Програмне забезпечення повинне включати можливість захисту не менше ніж 230 поштових скриньок користувачів - Робота у вигляді програмно-апаратного комплексу (ПАК), або у вигляді віртуальної машини з керуванням через веб-консоль - Робота з копією трафіку у режимах SPAN/TAP, BCC

		- Робота в режимі "логічного розриву" (MTA) із утриманням об'єкта до винесення вердикту - Можливість інтеграції з XDR платформою того ж виробника. - Наявність статичної антивірусної перевірки перед відправкою до модуля «пісочниці». o За базами відомих сигнатур; o За моделями, отриманих на основі алгоритмів машинного навчання задля протидії невідомим загрозам. - Підтримка зміни маршруту для листів у черзі по: MX-запису, IP-адресі чи доменним ім’ям поштового серверу з можливістю вказування пріоритетного маршруту доставки - Можливість обмежувати кількість одночасних вхідних з’єднань - Можливість створення довірених джерел пошти за IP-адресою и маскою підмережі - Можливість блокування джерел пошти за правилом "заборони всіх, окрім явно вказаних" - Можливість заміни адреси отримувача - Аналіз пошти із підтримкою TLS у т.ч. версії TLS 1.3 - Підтримка DKIM, DMARC, SPF - Підтримка технології DANE для вихідних листів - Протидія атакам, націлених на збір реальних адрес користувачів (DHA) за наступними критеріями: o Період аналізу o Відсоток листів з небезпечним вмістом o Загальна кількість листів o Кількістю отримувачів o Кількістю неіснуючих отримувачів з можливістю постійного або тимчасового блокування відправника на заданий проміжок часу - Протидія атакам, що опираються на відправку автовідповідей (Bounce Attack) за наступними критеріями: o Період аналізу o Відсоток листів з небезпечним вмістом o Загальна кількість листів з можливістю постійного або тимчасового блокування відправника на заданий проміжок часу - Можливість вводу лімітів за кількістю відправлених листів від одного відправника за email-адресою та за IP-адресою за певний проміжок часу чи за кількістю листів з блокуванням, тривалість якого можна конфігурувати - Підтримка шифрування надсилання пошти на основі IBE алгоритму власної розробки - Можливість автоматичного застосування шифрування при наявності ключових слів у заголовках, у тілі листа чи у вкладених файлах

		- Можливість застосування дій, якщо фактична адреса відправника не співпадає із зазначеною в полі "від" (захист від спуфінгу) - Можливість окремого налаштування дій за рівнями критичності ризику - Можливість вставляти текстові мітки у заголовки/тему листа при порушеннях політик безпеки - Можливість зберігати оригінальний лист у карантині у випадку коли вкладення не може бути видалено, або перед видаленням вкладення - Можливість пересилання листа, на який зреагувала політика антивірусного захисту, на окремий поштовий сервер по SMTP, або у вигляді прихованої копії (BCC) на окремий поштовий ящик - Можливість пересилання листів на окремий "сервер архівації" для зберігання - Наявність карантину пошти, доступного адміністратору (за всіма загрозами) - Наявність персонального карантину пошти, доступного користувачам (за спамом) - Авторизація користувачів у карантині за доменним обліковим записом - Розсилка консолідованих звітів за утриманими листами у персональному карантині кожному користувачу - Прив'язка політик до користувачів Active Directory / LDAP - Підтримка зовнішніх пісочниць того ж виробника - Підтримка передачі інцидентів по Syslog у форматах CEF, LEEF - Підтримка передачі звітів про інциденти по email - Перезапис/заміна небезпечних посилань усередині листа з перенаправленням на сторінку з повідомленням про небезпеку на самому модулі або довільній сторінці / внутрішньому порталі організації - Створення винятків за словами в URL для застосування правил заміни посилань (запобігання порушенню роботи маркетингових розсилок) - Створення винятків по відправникам та одержувачам для перевірки на СПАМ - Створення винятків по відправникам та одержувачам за: доменом, IP-адресою/підмережею за маскою, email-адресою, типами запису A, AAAA, MX - При додаванні відправника/отримувача у список виключень – антивірусна та контентна фільтрація за типом дозволених об’єктів має залишатись активованою - Підтримка чорних списків відправників (адреси, домени, IP, MX) - Створення винятків за словами URL (захист від порушення роботи списків розсилок) - Підтримка зовнішніх балансувальників для побудови відмовостійкості

		- Підтримка SNMP для моніторингу
2	Вимоги до аналізу поштового трафіку	- Підтримка контентної фільтрації за типами файлів, словами в тілі/заголовках/вкладених файлах, розмірами файлів та з використанням регулярних виразів - Можливість контентного фільтра видаляти активний вміст (наприклад, скрипти, макроси) всередині документів - Наявність механізмів DLP контролю над вихідними листами - Підтримка явної заборони запаролених об'єктів (архівів та документів) - Підтримка антиспам захисту від репутації джерел - Підтримка антиспам захисту на сигнатурній основі - Можливість виявляти та блокувати шкідливий код у файлах, що передаються електронною поштою користувачів - Механізм перезапису посилань з подальшим аналізом кожного переходу по них користувача з метою ретроспективної оцінки компрометації цільових сторінок засобами хмарного Threat Intelligence. - Можливість примусової (ручної) передачі листів для аналізу у форматах EML та MSG. - Відхилення листа від невідомих IP-адрес відправників або доменів - Відхилення листа невідомим корпоративним отримувачам - 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;
3	Додаткові вимоги	- Програмне забезпечення повинно бути сумісною з ПАК (програмно-апаратним комплексом із вбудованим функціоналом пісочниці) з наступними характеристиками: - Підтримка інтегрованих пісочниць не менше 30 віртуальних машин на один пристрій - Наявність можливості встановлення мережних інтерфейсів 10Gbps - Підтримка пісочниць версій ОС: WinXP, Win7, Win8/8.1, Win10/11 (для всіх версій 32/64 біта) - Підтримка пісочниць версій ОС для серверів Win2003, Win2008, Win2012, 2016, 2019, 2022 (для всіх версій 32/64 біта) - Можливість створення пісочниць на основі власних шаблонів ОС із прикладним унікальним ПЗ підприємства та можливістю автоматизованої перевірки коректності образу після його підготовки за допомогою спеціалізованого ПЗ виробника - Підтримка україномовних ОС у пісочниці - Використання унікальних активаційних ключів для Windows, Office та іншого програмного забезпечення пісочниць, що може виступати тригером спрацювання шкідливого ПЗ - Підтримка виходу пісочниць в інтернет через NAT та проксі - Підтримка розкриття та перевірки вмісту запаролених архівів та документів (Office, PDF) за заздалегідь підготовленою словниковою базою

		- Підтримка розкриття та перевірки вмісту запаролених архівів і документів (Office, PDF) шляхом автоматичного вилучення пароля з тіла листа чи теми та застосування його до вкладення (в т.ч. і в іншому/наступному листі) - Можливість повторної перевірки листів з нерозкритими запароленими вкладеннями шляхом ручного введення пароля для відкриття в карантині (з наступною доставкою "безпечного" листа або реагуванням за виявленим ризиком згідно політики безпеки) - Попередні перевірки вмісту за репутаційними базами та евристикою ДО відправки в пісочницю (файли, посилання) - Завантаження вмісту/об’єкту за довільними URL-посиланнями у листі та подальший його аналіз - Завантаження вмісту/об’єкту за посиланнями з хмарних сховищ (Dropox, Google, OneDrive тощо) у листі та подальший його аналіз - Можливість корегувати параметри HTTP(s)-сесій для завантаження об’єктів зі сторонніх ресурсів (тривалість сесії, час завантаження, розмір об’єкту завантаження) – для оптимізації часу обробки листів - Вилучення та аналіз посилань з документів Office та PDF з можливістю перевірки не менше 20 посилань на документ. Кількість повинна бути доступною для редагування - Вилучення та аналіз посилань для контейнерів .MHT - Вилучення та аналіз посилань для файлів усередині архівів - Можливість примусового надсилання листів на вказані теми для аналізу в пісочницях (без репутаційної/евристичної передфільтрації файлів/посилань) - Підтримка розкриття запаролених архівів та документів (Office, PDF) за заздалегідь підготовленою словниковою базою - Можливість розширення списку типів файлів, що перевіряються, в пісочницях за рахунок встановлення необхідного ПЗ всередину образу пісочниці користувачем - Підтримка системи глобального списку «білих додатків» для зниження хибнопозитивних спрацьовувань при обробці в пісочниці - Зіставлення результатів із MITRE ATT&CK - Відображення у звіті сканування схематичної дочірньо-батьківської моделі запуску шкідливих процесів під час аналізу у пісочниці - Підтримка створення винятків за хешами, IP, URL, доменом - Можливість налаштування критеріїв для передачі об'єктів на аналіз у пісочницях (пріоритезовані відправники/отримувачі, розширення файлів обов’язкових для аналізу, тривалість перевірки) - Можливість примусового надсилання певних категорій файлів для аналізу у пісочницях - Можливість пріоритезації відправлення листів до пісочниці на основі відправника/отримувача - Можливість примусового відправлення URL до пісочниці на основі ключових слів у темі листа - Стійкість до техніки обходу пісочниць (в т.ч. з перевірки оточення, MAC адрес та таймерів запуску, можливість

		встановлення довільних драйверів та підключених пристроїв в якості приманок та інших механізмів) - Підтримка повноцінної симуляції в пісочниці для таких типів об'єктів, але не обмежуючись : .svg, .swf, .mov, .htm, .html, .xht, .xhtml, .mht, .mhtml, .jar, .class, .doc, .dot, .docx, .dotx, .pps, .ppsx, .ppt, .pptx, .pub, .xla, .xls, .xlsx, .xlt, .xlm, .cell, .xml, .xlsb, .xltx, .hwp, .hwpx, .jtd, .gul, .msg, .slk, .iqy, .csv, .odp, .ods, .odt, .docm, .dotm, .potm, .ppam, .ppsm, .pptm, .xlam, .xlsm, .xltm, .chm, .lnk, .rtf, .pdf, .bat, .cmd, .js, .jse, .hta, .ps1, .vbe, .vbs, .wsf, .url, .sh, .com, .cpl, .crt, .dll, .drv, .elf, .exe, .ocx, .scr, .sys, .7z, .ace, .alz, .amg, .arj, .hqx, .bz2, .bzip2, .cab, .cpio, .cpgz, .egg, .gzip, .gz, .ics, .lha, .lharc, .lzh, .eml, .email, .msg, .rar, .sit, .sitx, .tar, .tgz, .tnef, .winmail.dat, .win.dat, .iso, .uue, .vcs, .x, .zip, .dmg, .pkg, .o - Виявлення 0-day експлойтів у файлах документів - Підтримка ідентифікації загроз у пісочницях на основі даних моделі машинного навчання - Деталізація результатів аналізу в пісочниці (звіт у форматі .pdf або .html, pcap-файл мережевого дампу, знімки екрану, IOC, підвантажені додаткові компоненти ШПЗ) - Симуляція переходу за посиланнями (у тому числі з перенаправленнями) усередині пісочниць з наступним аналізом вмісту - Симуляція переходу за короткими посиланнями з наступним аналізом вмісту - Виявлення загроз у пісочницях на основі профілів Yara - Побудова зв'язного ланцюжка подій у звіті для візуального представлення результатів розслідування - Робота у форматі віртуальної машини у середовищі VMware, Hyper-V - Без необхідності придбання додаткової ліцензії - Консолідація даних з усіх керованих модулів - Наявність вбудованого репозиторію образів "пісочниць", прошивок, патчів та хотфіксів. - 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). - Централізація оновлень ПЗ за всіма керованими модулями - Централізація поширення/заміни образів "пісочниць" за всіма керованими модулями автоматично за розкладом - Забезпечення реплікації конфігурацій між керованими пристроями - Забезпечення єдиної точки обміну індикаторами компрометації (IoC) на рівні всіх керованих модулів - Забезпечення передачі IoC засобам антивірусного захисту кінцевих точок того самого виробника. - Забезпечення передачі IoC з усіх керованих модулів стороннім системам (CheckPoint, Palo Alto, BlueCoat та ін.) - Публікація списку IoC засобами внутрішнього веб-сервера для спрощення інтеграції з продуктами сторонніх розробників - Єдина система оповіщень у форматі CEF, LEEF, SNMP за подіями від усіх керованих модулів

		- Централізоване розповсюдження профілів Yara по всіх керованих модулях для ідентифікації загроз у "пісочницях" - Централізоване розповсюдження профілів STIX по всіх керованих модулях для ідентифікації загроз у "пісочницях" - Централізоване поширення профілів методом TAXII стороннім системам - Система доступу на основі RBAC - Інтеграція з Active Directory для адміністративних завдань - Централізований "чорний" список об'єктів за всіма керованими модулями - Централізований список виключень об'єктів (хеші, домени, URL, IP) за всіма керованими модулями - Можливості детального пошуку інцидентів щодо широкого спектру параметрів із збереженням пошукового запиту - Можливість збереження деталей інциденту (включаючи звіти, опис, pcap-дампи) - Зіставлення локальних результатів інциденту з даними Global Threat Intelligence - Централізоване керування словниковою базою паролів для розкриття запаролених архівів та документів (Office, PDF) по всіх керованих пристроях з можливістю експорту/імпорту списків.
4	Гарантійне обслуговування та сервісна підтримка.	- Гарантійні зобов’язання та технічна підтримка від виробника повинна становити: на програмну продукцію не менше 12 місяців, на ПАК не менше 24 місяців. Послуги з надання в користування обладнання на термін дії ліцензій, послуги з налаштування та впровадження програмного забезпечення повинні бути включені у вартість пропозиції та здійснюватися кваліфікованими спеціалістами, які сертифіковані виробником та мають рівень «Certified Professional» або аналог (надати копії сертифікатів, щонайменше 2-х співробітників).

Обґрунтування очікуваної вартості предмета закупівлі, розміру бюджетного призначення: Очікувана вартість закупівлі формувалась із середніх цін комерційних пропозицій, наданих суб’єктами господарювання.

Очікувана вартість 2 000 000 грн. з ПДВ