**ОБҐРУНТУВАННЯ ТЕХНІЧНИХ ТА ЯКІСНИХ ХАРАКТЕРИСТИК ПРЕДМЕТА ЗАКУПІВЛІ, РОЗМІРУ БЮДЖЕТНОГО ПРИЗНАЧЕННЯ, ОЧІКУВАНОЇ ВАРТОСТІ ПРЕДМЕТА ЗАКУПІВЛІ**

(відповідно до пункту 41 постанови КМУ від 11.10.2016 № 710 «Про ефективне використання державних коштів» (зі змінами))

**1. Найменування, місцезнаходження та ідентифікаційний код замовника в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань, його категорія:** ДЕРЖАВНА УСТАНОВА "ЦЕНТР ІНФРАСТРУКТУРИ ТА ТЕХНОЛОГІЙ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ"; 03151, Україна, м. Київ, вул. Володимира Сікевича, 28; категорія замовника – бюджетна неприбуткова установа.

## 2. Назва предмета закупівлі із зазначенням коду за Єдиним закупівельним словником (у разі поділу на лоти такі відомості повинні зазначатися стосовно кожного лота) та назви відповідних класифікаторів предмета закупівлі і частин предмета закупівлі (лотів) (за наявності): Закупівля програмної продукції для створення та впровадження системи кіберзахисту за кодом CPV за ЄЗС ДК 021:2015: 48730000-4 - Пакети програмного забезпечення для забезпечення безпеки

**3. Ідентифікатор закупівлі: —** UA-2023-12-07-017965-а

**4. Обґрунтування технічних та якісних характеристик предмета закупівлі**: Закупівля програмної продукції для створення та впровадження системи кіберзахисту за кодом CPV за ЄЗС ДК 021:2015: 48730000-4 - Пакети програмного забезпечення для забезпечення безпеки

**ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

##  [Закупівля програмної продукції для створення та впровадження системи кіберзахисту за кодом CPV за ЄЗС ДК 021:2015: 48730000-4 - Пакети програмного забезпечення для забезпечення безпеки](https://www.dzo.com.ua/tenders/17227183)

|  |
| --- |
| **ТЕХНІЧНІ ВИМОГИ** |
| **№** | **Назва параметру** | **Вимога** |
| Вимоги до підсистеми керування вразливостями |
|  | Загальні вимоги | Рішення повинно підтримувати пошук вразливостей не менше ніж для 100 робочих станцій та серверів та не менш ніж 8 зовнішніх доменів та ІР адрес |
|  | Строк дії підписки не менше ніж 12 місяців |
|  | Рішення повинно включати можливість активного та пасивного сканування для повної видимості активів, вразливостей та конфігурацій |
|  | Рішення повинно визначати пріоритет для вразливості на основі ризиків |
|  | Пропозиція з рішення повинна включати технічну підтримку 24/7/365 |
|  | Рішення повинно включати автоматичне оновлення нових перевірок на вразливості кожні 24 години |
|  | Рішення повинно мати ліцензію на основі активів, враховуючи інші параметри мережі, крім IP, у випадку, якщо пристрій має 2 IP |
|  | Рішення не повинно покладатися на IP-адреси, як єдиний засіб відстеження ліцензування активу |
|  | Рішення повинно враховувати IP-адресу, тип обладнання, операційні системи, UUID BIOS, MAC-адресу, ім’я NetBIOS, повне доменне ім’я для визначення активу |
|  | Рішення повинно мати можливість привласнювати декілька IP-адрес одному активу, для пристроїв, які мають кілька IP-адрес одночасно |
|  | Рішення повинно забезпечувати еластичну модель ліцензування, щоб забезпечити безперервне функціонування продукту, коли тимчасово перевищено ліцензійне обмеження |
|  | Рішення повинно дозволити тимчасово перевищити ліцензію у разі необхідності сканувати додаткові ресурси |
|  | Всі компоненти, модулі сканування повинні постачатися тим же виробником, що і основна система |
|  | Архітектура | Рішення повинно забезпечувати інтегровану модель зберігання, яка не покладається на сторонні продукти баз даних |
|  | Рішення повинно забезпечувати комплексне хмарне сканування, що включає видимість, оцінку та порівняльний аналіз веб-служб Microsoft Azure |
|  | Рішення повинно мати можливість постійного моніторингу мережевого трафіку для виявлення та оцінки систем які знаходяться короткий час в мережі та важко скануючих пристроїв, таких як чутливі системи OT та IoT |
|  | Рішення повинно забезпечувати повний і повністю задокументований API для автоматизації процесів та інтеграції зі сторонніми додатками |
|  | API повинен надаватися без додаткових витрат і бути частиною єдиної підписки |
|  | Рішення має масштабуватися до мільйонів активів |
|  | Рішення повинно включати опцію для агентів, які забезпечують виявлення вразливостей та оцінку конфігурації безпеки кінцевого пристрою |
|  | Рішення повинно мати можливість використовувати групу сканерів в одному скануванні |
|  | Рішення повинно мати можливість сканувати об’єкти у внутрішніх мережах, а також об’єкти, які є зовнішніми та загальнодоступними |
|  | Сканерами повинна керувати платформа, наприклад, оновлення для виявлення вразливостей, код та інші оновлення |
|  | Рішення повинно забезпечувати можливість розгортання необмежених повнофункціональних пасивних сканерів без додаткових витрат |
|  | Рішення повинно забезпечувати можливість розгортання необмежених повнофункціональних активних сканерів без додаткових витрат |
|  | Рішення повинно забезпечувати можливість розгортання необмежених повнофункціональних агентів без додаткових витрат |
|  | Загальна кількість повнофункціональних сканерів, агентів та пасивних сканерів має бути необмеженою |
|  | Всі модулі сканування повинні постачатися одним виробником |
|  | Усі повнофункціональні агенти, активні сканери, пасивні сканери повинні бути частиною єдиної підписки |
|  | Рішення повинно надавати можливість розгортання віртуального пристрою для єдиної точки комунікації з SaaS платформою всіх підключених сенсорів розгорнутих локально. Сенсори повинні надсилати інформацію до віртуального пристрою, який централізовано передає до SaaS платформи інформацію про вразливості, а не кожний сенсор напряму |
|  | Повністю функціональний віртуальний пристрій для централізованої комунікації з SaaS платформою повинен надаватися без додаткових витрат |
|  | Агент повинен мати можливість підключатися до консолі через проксі-сервер |
|  | Сканери повинні мати можливість підключатися до консолі через проксі-сервер |
|  | Агент повинен мати можливість встановлюватися за допомогою сторонніх рішень, таких як Active Directory або SCCM |
|  | Управління доступом | Рішення повинно забезпечувати рольову модель доступу (RBAC) для контролю прав користувачів над певними наборами даних та функціональних можливостей |
|  | Рішення повинно надавати можливість приймати або змінювати ризик вразливостей, при цьому така функціональність обмежується роллю користувача і будь-яке прийняття ризику вразливості повинне бути задокументоване |
|  | Рішення повинно мати можливість визначати та керувати групами користувачів, включаючи обмеження функцій сканування та доступу до звітів |
|  | Рішення повинно мати можливість гарантувати, що певні IP-адреси або порти можуть бути заблоковані від сканування |
|  | Рішення повинно мати двофакторну автентифікацію |
|  | Сканування | Рішення повинно підтримувати різні платформи для механізму сканування, які включають Windows, Linux, а також віртуальні пристрої |
|  | Рішення повинно надавати безкоштовні регіональні хмарні сканери від виробника для використання їх під час створення та запуску сканування без необхідності використовувати власні локальні сканери |
|  | Рішення повинно підтримувати кілька географічно розподілених механізмів сканування, керованих центральною консоллю |
|  | Рішення повинно включати можливість заборони сканування в визначені години |
|  | Рішення повинно передбачати можливість конфігурування портів, протоколів та служб для підключення до сканерів, розгорнутих у мережі |
|  | Рішення повинно мати можливість налаштовувати навантаження на кінцеві станції для планового сканування, щоб дозволяти регулювати сканування для запобігання генерації трафіку, який може порушити нормальну роботу мережевої інфраструктури |
|  | Рішення повинно передбачати можливість введення та безпечного зберігання облікових даних користувачів, включаючи локальні облікові записи Windows та домени, а також Unix su та sudo через SSH |
|  | Рішення повинно забезпечувати можливість підвищення привілеїв сканера на цільових системах із звичайного доступу користувача до адміністраторського доступу |
|  | Рішення повинно підтримувати індивідуальне планування сканування, включаючи можливість запускати сканування у визначений час із заздалегідь визначеною частотою |
|  | Рішення повинно мати можливість виконувати пошук конфіденційних даних в системах Windows, Unix та Linux |
|  | Рішення повинно включати в модель ліцензування «автоматичне старіння», щоб активи які не скануються протягом 90 днів, більше не враховувались у ліцензії |
|  | Система повинна дозволяти користувачам запускати сканування на перевірку усунення вразливостей, щоб переконатися, що вони виправлені, без необхідності налаштовувати параметри сканування |
|  | Виявлення активів | Продукт повинен підтримувати можливість виявлення активів, які не враховуються в ліцензуванні |
|  | Продукт повинен забезпечувати можливість пасивного моніторингу мережі для виявлення активів |
|  | Продукт повинен підтримувати можливість отримувати видимість активів в режимі реального часу та проводити інвентаризацію загальнодоступних хмарних активів, коли хмарні екземпляри вмикаються або виводяться з експлуатації |
|  | Рішення повинно мати можливість виявляти мобільні пристрої та інтегруватися з декількома різними системами управління мобільними пристроями (MDM) |
|  | Рішення повинно забезпечувати виявлення служб Інтернету та баз даних |
|  | Рішення повинно мати можливість виявлення служб, що працюють на нестандартних портах |
|  | Рішення повинно мати можливість виявлення служб, налаштованих не відображати банери з’єднання |
|  | Рішення повинно мати можливість тестувати кілька екземплярів однієї і тієї ж служби, що працює на різних портах |
|  | Рішення повинно мати можливість сканувати мертві хости (пристрої, які не реагують на ICMP запити) |
|  | Рішення повинно підтримувати використання netstat для швидкого та точного перерахування відкритих портів у системі при наданні облікових даних |
|  | Рішення повинно підтримувати використання SMB та WMI для сканування систем Windows |
|  | Рішення повинно мати можливість автоматичного запуску віддалених служб реєстру в системах Windows під час виконання сканування, а потім автоматично зупиняти служби після завершення сканування |
|  | Сканер повинен підтримувати безпечне з’єднання(ssh) з можливістю підвищення привілеїв для сканування на наявність вразливостей і аудиту конфігурацій в системах Unix |
|  | Рішення повинно забезпечувати можливість налаштування політики сканування для мінімального впливу на мережі та цілі сканування |
|  | Продукт повинен забезпечувати активне та пасивне виявлення бездротових точок доступу (WAP) |
|  | Групування активів на основі тегів | Рішення повинне надавати можливість створювати статичні групи активів на основі тегів. |
|  | Рішення повинне надавати можливість створювати динамічні групи активів на основі тегів за допомогою написання правил. |
|  | Рішення повинне надавати можливість створювати теги за шаблоном Категорія: Значення |
|  | Рішення повинне надавати можливості створення правил тегів за допомогою фільтрів або мови запитів |
|  | Панель створення правил тегів повинна містити як мінімум такі фільтри: Asset ID; Has Plugin Results; IPv4; FQDN; Last Licensed Scan; Type; Deleted; First Seen; BIOS ID; Cloud Provider; Hosting Provider; Is Unsupported; Is Auto Scale; Name; Open Ports; Region; Resource Category; SSL/TLS; Tags; Public; Operating System; Record Type |
|  | Рішення повинне надавати можливість додавати/видаляти активи в тегах |
|  | Рішення повинне надавати можливість обирати теги під час створення скану |
|  | Пасивне сканування | Пасивний сканер повинен включати можливість сканування вразливостей шляхом моніторингу мережевого трафіку без активного сканування |
|  | Пасивний сканер повинен відображати вразливості в режимі реального часу, виявлені в трафіку. Ці дані слід застосовувати до додатків, портів, протоколів, загроз та інших мережевих пристроїв з можливістю аналізу трафіку під час розслідування |
|  | Пасивний сканер повинен надавати інформацію про окрему мережу, всю мережу або будь-яку групу хостів |
|  | Пасивний сканер повинен мати можливість аналізувати трафік та повідомляти про зміни відповідно до певних граничних змін значень |
|  | Пасивний сканер повинен виявляти потенційно небезпечні програми в мережевому трафіку (шкідливе програмне забезпечення, ботнет, тимчасова мережа) |
|  | Пасивний сканер повинен постачатися тим же виробником, що і основна система |
|  | Пасивний сканер повинен мати можливість аналізувати трафік та надавати інформацію про вразливі місця без підключення до Інтернету |
|  | Оцінка вразливості | Продукт повинен забезпечувати як аутентифіковане, так і неаутентифіковане мережеве сканування цільових систем |
|  | Рішення не повинне покладатися на будь-які сторонні сканери для сканування на вразливість |
|  | Рішення повинно мати можливість як автентифікованого, так і неавтентифікованого сканування для виявлення вразливостей, без необхідності встановлення клієнтського агента на цільовому пристрої |
|  | Рішення повинно мати можливість сканування агентом для локального виявлення вразливостей без додаткової плати |
|  | Рішення повинно надавати сканери, що розміщуються у хмарі, для сканування периметра мережі |
|  | Рішення повинно мати можливість відстежувати зміни DHCP, пов’язуючи результати сканування однієї і тієї ж системи в випадку зміни IP |
|  | Рішення повинно виявляти проблеми, ризики та вразливості. Він також повинен надавати детальну інформацію щодо характеру вразливості та рекомендації щодо її усунення |
|  | Рішення повинно включати детальний висновок щодо результатів сканування, включаючи таку інформацію, як знайдені версії DLL |
|  | Рішення повинно бути сумісним з CVE та забезпечувати оцінкою CVE щонайменше 10 років |
|  | Рішення повинно передбачати аудит виправлення для операційних систем та програм Microsoft, що включає Windows XP, Windows 7, Windows 8 / 8.1, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Internet Explorer, Microsoft Edge, Microsoft Office, IIS, Exchange та багато іншого |
|  | Рішення повинно передбачати аудит виправлень для всіх основних операційних систем Unix, включаючи Linux та багато іншого |
|  | Рішення повинно виявляти вразливості в сторонніх програм, таких як Java та Adobe. |
|  | Рішення повинно забезпечувати інтеграцію із системами управління виправленнями для аудиту виправлень та створення звітів щодо результатів сканування, таких як IBM Tivoli Endpoint  |
|  | Рішення повинно забезпечувати інтеграцію з продуктами управління мобільними пристроями (MDM), такими як Microsoft Intune для виявлення вразливостей та аудиту мобільних пристроїв |
|  | Система повинна забезпечувати пріоритизацію вразливостей з використанням аналітики загроз в реальному часі і алгоритмів машинного навчання для оцінки вразливостей і прогнозування того, які з них з найбільшою ймовірністю будуть використані в найближчому майбутньому |
|  | Система повинна забезпечувати пріоритизацію вразливостей, яка допомагає користувачам зрозуміти ключові фактори, що впливають на кожну оцінку вразливості (наприклад, новизну загрози, зрілість коду використання, категорії джерел Intel). Рішення також повинно включати оцінку вразливості відповідно до Загальної системи оцінки вразливості версії 3 (CVSS v3) |
|  | Рішення повинно надавати інформацію про вразливість із сторонніх джерел, таких як Core Impact, Metasploit та Canvas |
|  | Рішення повинно містити інформацію про наявність експлойтів для вразливості, включаючи короткий опис вразливих місць, які можуть використовуватися шкідливим програмним забезпеченням для зараження активів |
|  | Рішення повинно розумно вибирати тести для виявлення вразливостей та конфігурацій в активі на основі інформації, отриманої в результаті первинного сканування цього активу |
|  | Рішення повинно відстежувати історичні дати виявлення вразливості, які можуть бути використані для фільтрації та складання звітів з часовими фільтрами |
|  | Рішення повинно дозволяти вмикати або вимикати тести на виявлення вразливості та змінювати конфігурації для планового сканування |
|  | Рішення повинно підтримувати сканування IPv6 з пасивним виявленням цілей IPv6 |
|  | Рішення має аналізувати загальнодоступні хмарні ресурси на предмет неправильної конфігурації та наявність вразливостей за допомогою активного сканування та агентів |
|  | Рішення повинно відстежувати активи та їх вразливості, включаючи високодинамічні ІТ-ресурси, такі як мобільні пристрої, віртуальні машини та хмарні ресурси |
|  | Сканування вразливостей для сучасних веб-додатків | Рішення повинно мати можливість сканувати як внутрішні, так і зовнішні веб-програми |
|  | Рішення повинно вміти визначати частини критично важливих веб-додатків, які безпечно сканувати, та визначати інші частини, які ніколи не слід сканувати, щоб запобігти затримці роботи або порушенням |
|  | Рішення повинно мати можливість сканувати веб-програми HTML5, AJAX, HTML |
|  | Рішення повинно мати можливість звітувати про всі вразливості в веб-додатках - як внутрішніх, так і зовнішніх - в одній єдиній інформаційній панелі |
|  | Рішення повинно мати можливість сканувати веб-програми за допомогою: облікових даних для автентифікації на основі сервера HTTP, автентифікації за допомогою форми входу, автентифікації за допомогою файлів cookie, автентифікації за допомогою Selenium |
|  | Рішення повинно мати можливість регулювати навантаження для сканування |
|  | Рішення повинно мати можливість обирати тести, які будуть використовуватися для сканування |
|  | Рішення має ідентифікувати та класифікувати проблеми, ризики та вразливості. Він також повинен надавати детальну інформацію про ризики, вразливості та рекомендації щодо їх мінімізації |
|  | Рішення повинно відстежувати дату виявлення вразливості |
|  | Рішення повинно мати можливість розгортання локального сканера веб-додатків для виявлення вразливостей у веб-програмах, недоступних з мережі Інтернет |
|  | Рішення повинно забезпечувати можливість розгортання локального сканера веб-додатків без додаткових витрат |
|  | Сканер веб-додатків повинен надавати той самий виробник. |
|  | Рішення повинно мати власний сканер у хмарі для виявлення вразливостей у веб-додатках, до яких можна отримати доступ через мережу інтернет |
|  | Рішення повинно мати можливість імпортувати сценарій Selenium, який містить один або кілька сценаріїв для відтворення дій сканера на певних сторінках для оцінки |
|  | Рішення має оцінювати веб-програми і специфічні компоненти в веб-додатках та класифікувати вразливості по OWASP Top 10 |
|  | Рішення повинно бути простим у використанні та масштабуватися, щоб включати всі веб-додатки організації |
|  | Рішення повинно сканувати та виявляти вразливості в API |
|  | Рішення повинно перевіряти реалізацію SSL / TLS в веб-додатках |
|  | Сканування зовнішньої поверхні атаки | Система повинна мати можливість отримання інформації про зовнішню поверхню атаки для одного домену верхнього рівня, а саме, визначати, які активи та сервіси вашої організації мають доступ до Інтернету та можуть бути доступні ззовні для зловмисників без проведення активного сканування. |
|  | Система повинна отримувати видимість метаданих, що відносяться до хоста, типу запису, IP-адреси, ASN та порту. |
|  | Система має оновлювати інформацію про зовнішню поверхню атаки щоквартально |
|  | Система повинна мати можливість виявляти зовнішні активи у 10-кратній кількості ліцензованих активів |
|  | Інформаційно-консультаційні послуги щодо впровадження «підсистеми керування вразливостями» | Визначення підмереж для встановлення активних сканерів |
|  | Визначення підмереж (критичних та некритичних) для встановлення пасивного сканера для сканування копії трафіку |
|  | Визначення кінцевих точок для установки агентів (опціонально) |
|  | Затвердження структури та графіка виконання робіт |
|  | Створення матриці ролей усередині компанії, вказівка вимог щодо наявності прав доступу до системи управління вразливістю |
|  | Створення та затвердження остаточної схеми встановлення рішення (High-Level Design), включаючи всі керуючі та службові компоненти |
|  | Виділення ресурсів та підготовка інфраструктури для впровадження |
|  | Реєстрація в клієнтському порталі для огляду та керування ліцензією, контактами, кейсами |
|  | Огляд та завантаження необхідних образів |
|  | Консоль управління: активація ліцензії та отримання доступу до консолі |
|  | Сканер веб-додатків: встановлення компонента в обраній підмережі |
|  | Сканер веб-додатків: базові налаштування образу |
|  | Активний сканер: встановлення компонента у вибраних підмережах (до 5 сканерів) |
|  | Активний сканер: базові налаштування образів (до 5 сканерів) |
|  | Пасивний сканер: встановлення компонента у вибраних підмережах та надання SPAN від замовника (до 3 сканерів) |
|  | Пасивний сканер: базові налаштування образів (до 3 сканерів) |
|  | Агенти: встановлення агентів та підключення (до 100 агентів) |
|  | Створення додаткових користувачів системи |
|  | Налаштування підключення до проксі-серверу для оновлення баз даних про вразливості в активному сканері |
|  | Налаштування підключення до проксі-серверу для оновлення баз даних про вразливості в пасивному сканері |
|  | Підключення активних сканерів до консолі керування |
|  | Підключення пасивних сканерів до консолі керування |
|  | Підключення сканеру веб-додатків до консолі керування |
|  | Створення окремих зон сканування для кожної підмережі, де встановлено сканер |
|  | Налаштування двофакторної аутентифікації для користувачів |
|  | Створення мереж для розподілу сканерів |
|  | Налаштування відображення пріорититної оцінки CVSS згідно версії (CVSSv2/CVSSv3) |
|  | Створення груп користувачів для розподілу прав доступу (до 2 груп) |
|  | Налаштування тегів, що поєднують активи згідно заданих критеріїв (до 5 тегів) |
|  | Налаштування прав доступу для роботи з виділеними активами в системі (до 3 варіантів прав доступу) |
|  | Створення та налаштування сканування з політикою інвентаризації активів |
|  | Створення та налаштування сканування з політикою базового мережевого сканування |
|  | Створення та налаштування сканування з політикою сканування агентами |
|  | Створення та налаштування сканування з політикою поверхневого огляду веб-додатку |
|  | Створення та налаштування сканування з політикою комплексної оцінки веб-додатку на вразливості |
|  | Створення та налаштування сканування з політикою сканування API веб-додатку |
|  | Додавання облікових даних для сканування з аутентифікацією (до 5 записів) |
|  | Створення шаблонів сканувань на основі кастомізованих політик активного сканування |
|  | Створення шаблонів сканувань на основі кастомізованих політик сканування агентами |
|  | Створення шаблонів сканувань на основі кастомізованих політик  сканування веб-додатків (до 2 шаблонів) |
|  | Налаштування виключень, щоб обмежити сканування певних хостів на основі вибраного розкладу |
|  | Створення кастомних тек для упорядковування існуючих та нових сканів |
|  | Тестування сканування за створеними політиками |
|  | Аналіз результатів сканування з використанням інструментів пошуку |
|  | Аналіз отриманих результатів моніторингу зовнішньої поверхні атаки  |
|  | Створення інформаційних панелей за вимогами замовника з наявних шаблонів (до 3 дашбордів) |
|  | Кастомізація інформаційних панелей за вимогами замовника на основі вразливостей (до 3 дашбордів) |
|  | Створення звітів за вимогами замовника з наявних шаблонів (до 3 звітів) |
|  | Кастомізація звітів за вимогами замовника на основі отриманих даних (до 3 звітів) |
|  | Створення запитів на основі клієнтських фільтрів для пошуку вразливостей, створення звітів, повідомлень та завдань (до 5 запитів) |
|  | Проведення експлуатаційних тестів системи |
|  | Створення та налаштування проекту усунення вразливостей згідно заданих фільтрів та назначення крайньої дати чи кількості виділених днів |
|  | Створення та налаштування інструменту встановленої цілі для відстеження програми закриття вразливостей згідно обраних фільтрів |
|  | Передача знань при роботі з сервісними порталами вендора:Support Portal, Community Portal, Documentation Portal |
|  | Тренінг по роботі з системою та її компонентами (до 3 осіб) |
| Вимоги до підсистеми аудиту дій користувачів |
|  | Загальні вимоги | Адміністрування системи має відбуватися через веб-консоль |
|  | Управління налаштуваннями та щоденна робота з рішенням має здійснюватися виключно через веб-інтерфейс |
|  | Управління базою користувачів має здійснюватися тільки через веб-інтерфейс |
|  | Система повинна мати механізм протидії атакам з підбору пароля на веб-інтерфейс |
|  | Система повинна мати централізовану панель для перегляду сесій з різних інсталяцій незалежних між собою. |
|  | Система має підтримувати можливість входу на веб-консоль через облікові записи Active Directory, локально та через SSO (Single-Sign-On) |
|  | Система має мати веб-інтерфейс користувача та адміністратора українською мовою  |
|  | Система повинна підтримувати можливість розподілення веб-консолі на декілька адміністративних гілок управління незалежних між собою. Для кожної з них встановлюється відповідальний адміністратор який буде керувати власними налаштуваннями. Дані що обробляються в кожній з гілок повинні зберігатися централізовано на 1 інсталяції. |
|  | Система повинна мати рольове управління з наступними можливостями:* Розмежування прав доступу для налаштування безпосередньо системи для аудиту дій користувачів
* Призначення відповідальних офіцерів безпеки на окремі сегменти робочих станцій та серверів
* Призначення відповідальних офіцерів безпеки на аудит певних агентів.
 |
|  | Система має надавати можливість перегляду офіцером безпеки будь-якої активної сесії для контролю дій користувачів |
|  | Система має базуватися на агентному методі |
|  | Система повинна базуватися на архітектурі клієнт-сервер |
|  | Система має забезпечити можливість встановлення агентів віддалено через веб-консоль як в доменну інфраструктуру, так і на локальні кінцеві точки. |
|  | Система повинна підтримувати автоматичне оновлення агентів на кінцевих робочих станціях відразу при оновленні серверної частини |
|  | Агенти рішення не повинні залежати від IP Address кінцевих точок та від облікових записів користувачів – «плаваючі ліцензії». |
|  | Рішення повинно покрити наступний об’єм кінцевих точок:Сервер управління - 1 штРобочі станції (Windows, Linux) – 100 шт |
|  | Строк дії підписки не менше ніж 12 місяців |
|  | Система повинна легко масштабуватися до кількох тисяч агентів |
|  | Зв'язок між агентом та сервером управління має бути захищений за допомогою симетричного або асиметричного шифрування з ключем AES-256 або подібним  |
|  | Система повинна використовувати криптостійкий сертифікат (наприклад,  SHA-2 та подібні) для захисту збережених даних, за замовчуванням, або з можливістю використання власного сертифіката клієнта |
|  | Система повинна мати можливість сповіщати користувача про те, що всі його дії записуються при вході на робочу станцію |
|  | Система повинна мати можливість сповіщавати користувачів про запис сесії в процесі роботи користувача |
|  | Система повинна мати механізм ознайомлення користувача з політиками використання корпоративних ресурсів після входу в систему |
|  | Система повинна мати можливість показувати повідомлення користувачам на робочій станції під час входу в ОС |
|  | Система повинна мати можливість переглядати сесії користувачів як наживо, так і в записі |
|  | Система повинна записувати дії користувачів (знімки екранів + метадані) та у вигляді відеозапису. |
|  | Система має забезпечувати перевірку результатів моніторингу для гарантування цілісності даних які контролюються |
|  | Записані сесії повинні мати механізм захисту їх цілісності |
|  | Система повинна записувати локальні сесії |
|  | Система повинна записувати віддалені сесії (RDP, SSH та інші) |
|  | Система повинна мати можливість приховання реальних ідентифікаторів (анонімізація) співробітників для відповідності міжнародним стандартам по GDPR |
|  | Система повинна мати можливість ідентифікувати користувача, який використовує спільний обліковий запис |
|  | Запис сесій повинен відбуватися як у кольоровому, так і у чорно-білому режимах |
|  | Система повинна підтримувати  запис дій тільки активних вікон для економії сховища даних |
|  | Система повинна мати можливість записувати тільки визначені додатки |
|  | Система повинна підтримувати моніторинг відвідування сайтів |
|  | Система повинна мати  моніторинг буфера обміну |
|  | Система має визначати весь текст буфера обміну, при цьому дані мають бути збережені в хешованому вигляді |
|  | Система повинна мати можливість відображення сесії співробітника який працював одночасно на двох або більше моніторах |
|  | Система повинна мати можливість записувати тільки окремі URL або записувати всі URL, крім виокремлених |
|  | Система повинна мати можливість збирати тільки метадані, без відеозапису сесії користувача |
|  | Система має виявляти підключення пристроїв по USB, моніторити  USB носії та мати можливість блокувати носії, що не внесені у списки дозволенних (білі списки) для використання на кінцевих точках |
|  | Система повинна мати можливість контролювати та блокувати окремі USB пристрої (миші, клавіатури, аудіопристрої і т.д.) |
|  | Система повинна надавати\забороняти доступ до сесії (локальної чи віддаленої) на основі груп AD |
|  | Система повинна мати можливість віддаленого блокування користувача з консолі адміністратора системи. |
|  | Система має надавати можливість дозволити або закрити доступ користувачу до систем |
|  | Впродовж активної сесії рішення повинно забезпечити можливість заблокувати користувача для подальшого розслідування інциденту |
|  | Система має надавати доступ кінцевим користувачам тільки за обов’язковим коментарем (представлення необхідної інформації адміністратору системи) та дозволом адміністратора системи |
|  | Система повинна підтримувати можливість припинення запису сесії при відсутності активності на комп’ютері |
|  | Система повинна продовжувати запис дій навіть після втрати з’єднання з сервером управління (оффлайн режим)  |
|  | Дані, що зберігаються в оффлайн режимі, мають бути збережені локально та з обмеженням доступу         |
|  | Система має забезпечувати можливість архівування результатів моніторингу та перегляд даних з архіву |
|  | Система має підтримувати експортування окремих сесій та їх епізодів в зашифрованому вигляді |
|  | Система має забезпечувати перевірку результатів експорту даних для гарантування цілісності даних |
|  | Система повинна мати можливість завантажити з веб-консолі журнал подій агентів в разі розслідування неналежної роботи агента |
|  | Система має підтримувати аудит використання системи, аудит змін в середині системи, аудит має бути захищений від будь-яких модифікацій |
|  | Логування всіх дій користувачів та моніторинг результатів з можливістю фільтрації даних |
|  | Система повинна забезпечувати можливість пошуку по зібраним даним:* Мульти-параметри при пошуку в результатах  моніторингу
* (Моніторинг віддалених ІР, з яких здійснювався доступ до моніторингової системи. Фільтрування сесій моніторингу по віддалених IP адресах і т.д.)
* Можливість фільтрації користувачів під час моніторингу
* Можливість фільтрації додатків або веб сайтів під час моніторингу
* Можливість моніторингу активності користувачів під час конкретного інтервалу часу
 |
|  | Система повинна мати попередньо-встановленні шаблони політик для виявлення інцидентів безпеки |
|  | Система повинна мати можливість створювати політики сповіщень на основі даних, зібраних з агентів. |
|  | Сповіщення повинні надходити в режимі реального часу |
|  | Система повинна мати механізм взаємодії з користувачем у реальному часі  у випадку порушення політик безпеки, із можливістю інформування користувача про порушені політики або блокування дій, або примусового переривання його сесії |
|  | Система повинна мати можливість блокування роботи користувача у випадку спрацювання правила |
|  | Система повинна  виявляти та зупиняти завантаження файлів на веб ресурси |
|  | Система має виявляти та зупиняти активність з файлами при переміщені на  хмарні сховища. |
|  | Можливість блокування користувача як автоматично так і в ручному режимі при виявленні протиправних дій |
|  | Система повинна мати змогу виконувати наступні автоматичні дії:* Надіслати повідомлення користувачу про порушення ним політик безпеки без блокування його дій
* Надіслати повідомлення користувачу про порушення ним політик безпеки з блокуванням його дій
* Закриття веб сайту
* Закриття додатку
* Блокування користувача на всіх робочих точках,  де встановлений агент
 |
|  | Можливість відключення протиправних (не дозволених) процесів на робочій станції за допомогою системи алертів |
|  | Система повинна мати можливість пакетного імпорту-експорту правил сповіщень. |
|  | Система повинна мати можливість повідомлення адміністратора у випадку порушення політик безпеки та потенційного витоку даних |
|  | Система повинна мати вбудований модуль аналізу поведінки користувачів в режимі реального часу. |
|  | Система повинна мати вбудовану систему звітності |
|  | Звіти повинні відправлятися обраним користувачам за розкладом |
|  | Система повинна мати можливість підтримки режиму Multi-tenant для всіх видів підтримуваних операційних систем з можливістю створення окремих користувачів тенанта які не матимуть доступ до інших тенантів, клієнтів, конфігурацій, правил сповіщення, репортів та іншого |
|  | Система повинна підтримувати можливість роботи на кластерах бази даних в режимі високої доступності (High Availability) |
|  | Архітектура системи має підтримувати паралельний збір даних з агентів за рахунок розгортання декількох серверів додатків та підтримувати роботу з системою балансування навантаження. |
|  | В разі зміни адреси сервера додатків, агенти повинні мати можливість переключитися на іншу адресу сервера без втручання адміністратора.  |
|  | Система повинна підтримувати централізовано роботу з розгалуженими (distributed) серверами в різних географічних місцях |
|  | Система не повинна змінювати топологію мережі чи змінювати звичний спосіб автентифікації користувачів |
|  | Система має забезпечити шифрування конфіденційної інформації в базі даних |
|  | Система повинна підтримувати можливість зберігання записів сесій на файлових серверах |
|  | **Вимоги до Windows систем** | Система повинна збирати наступні дані на ОС Windows:* Назву запущеного додатку
* Назви заголовків вікон
* URL
* Назви веб сайтів
* Назви запущених процесів
* Відстеження скопійованого тексту наступними методами:
* Натискання правої кнопки миші в контекстному меню «Копіювати», «Вирізати», «Вставити»
* Виклик через меню додатку Змінити > Копіювати, Змінити > Вирізати>Вставити
 |
|  | Система повинна мати наступні можливості налаштування політик запису на ОС  Windows:* Записувати лише обраних користувачів
* Виключити з запису обраних користувачів
* Система повинна записувати обраних користувачів на основі груп AD
* Моніторити певні ІР адреси віддалених підключень
* Записувати лише обрані додатки
* Виключити з запису обрані додатки
* Записувати лише мета дані, без запису екрану
* Записувати лише обрані/виключені URL
* Починати запис екрану після введення “ключового” слова.
 |
|  | Система повинна мати модуль контролю та логування натискання клавіш з клавіатури на сайтах та додатках |
|  | Система повинна мати захист від призупинення / зупинки процесу Агента та зміни / видалення Агента навіть для користувачів із правами адміністратора |
|  | **Вимоги до Linux систем** | Рішення повинно збирати наступні дані на ОС Linux та Unix* Ім’я команди
* Параметри команди
* Виведення команди
* Системні виклики – (реалізовано через запис екрану)
* Змінні середовища
* Всі активності в командній оболонці (shell), незалежно від типу підключення (SSH, Telnet, локальний доступ)
* Як вхідний, так і вихідний потік терміналу
* Системні виклики (реалізовано через запис екрану)
 |
|  | Система повинна відстежувати завантаження файлів через популярні браузери та мессенджери |
|  | Система повинна забезпечувати можливість відстежувати виконання команд Linux та Unix за допомогою алертів та екстрено завершити їх у разі необхідності, у тому числі і що виконуються всередині скриптів |
|  | Система повинна забезпечувати відстеження виконання команд sudo/su на Linux/Unix системах. |
|  | Система повинна мати модуль контролю та логування натискання клавіш з клавіатури на сайтах та додатках |
|  | Система повинна записувати всі команди, що виконуються на Linux ОС, у тому числі що запущені за допомогою скриптів |
|  | Система повинна мати механізм екстреного завершення обраних команд та атрибутів |
|  | Система має підтримувати пошук у вихідних даних сеансу Linux |
|  | Можливість запису сесій на Linux з використанням графічних інтерфейсів (GUI) |
|  | **Вимоги до підтримуваних систем** | Система повинна підтримувати збір, аналіз та аудит дій на сервери та робочі станції з підтримкою наступних ОС:Для серверів:* Windows Server 2012 (32-bit та 64-bit)
* Windows Server 2016 (32-bit та 64-bit)
* Windows Server 2019 (32-bit та 64-bit)
* Windows Server 2022 (32-bit та 64-bit)
* Terminal Server – Windows
* Ubuntu 14.04 і вище
* CentOS 6, 7
* Debian 7 і вище

Для робочих станційь: * Windows 7 (32-bit і 64-bit)
* Windows 8 (32-bit і 64-bit)
* Windows 8.1 (32-bit і 64-bit)
* Windows 10 (32-bit і 64-bit)
* Windows 11
* Ubuntu 14.04 і вище
* CentOS 6, 7
 |
|  | **Загальні функціональні вимоги** | Сервісна підтримка повинна надаватися від виробника |
|  | Сервісна підтримка не менше, ніж 12 місяців з можливістю звернення телефоном або через Інтернет (електронна пошта) |
|  | Доступ до технічної документації |
|  | Перша лінія підтримки має бути наявна в Україні від розробника або його офіційного представника |
|  | Система має підтримувати режим відновлення після технічних проблем |
|  | Система повинна мати вбудовану систему моніторингу стану своїх компонентів та агентів |
|  | Система повинна мати моніторинг ресурсів та розміру бази даних з можливістю повідомлення через електронну пошту про проблеми. |
|  | Система повинна підтримувати наступні версії баз даних як сховища інформації:* SQL Server 2012/2014/2017/2019 і вище
* PostgreDB 10.1 і вище
 |
|  | Система повинна підтримувати можливість роботи на кластерах бази даних в режимі високої доступності (High Availability) |
|  | Система має підтримувати можливість незалежного адміністрування та підтримку бази даних (дефрагментація, реіндексація, shadow backup, shadow copy, shrink) офіційними інструментами обслуговування бази даних поза рішенням і не впливати на його функціонал.  |
|  | Система має підтримувати інтеграцію з Active Directory |
|  | Система повинна інтегруватися із LDAP системами |
|  | Система має підтримувати інтеграцію з SIEM IBM QRadar |
|  | Система має підтримувати надсилання логів у форматах CEF та LEEF. |
|  | Система повинна мати можливість передачі даних через протокол syslog |
|  | Система повинна мати можливість інтеграції з системами підтримки користувачів (ServiceNow або аналогами).  |
|  | Система повинна мати відкритий API |
|  | Система повинна мати можливість вивантаження інформації через API або іншими способами для майбутнього написання конекторів в сторонні системи під потреби адміністратора. |
|  | **Інформаційно-консультаційні послуги щодо впровадження «підсистеми аудиту дій користувачів»** | Консультація і підготовка інфраструктури замовника до впровадження системи аудиту дій користувачів |
|  | Надати вимоги для встановлення системи аудиту дій користувачів |
|  | Встановити систему аудиту дій користувачів |
|  | Надати рекомендації по налаштуванню інформаційних систем |
|  | Налаштувати інформаційні системи самостійно або разом з відповідальним адміністратором |
|  | Надати перелік прав для облікових записів які будуть використовуватися при роботі з ними |
|  | Надати перелік портів та протоколів для роботи системи аудиту дій користувачів |
|  | Налаштувати зберігання інформації для системи аудиту дій користувачів |
|  | Налаштувати архівацію даних |
|  | Підключити систему аудиту дій користувачів до інформаційних систем |
|  | Налаштувати правила сповіщень |
|  | Налаштувати автоматичне отримування звітів |
|  | Супроводжувати систему аудиту дій користувачів протягом 2 тижнів з моменту встановлення |
|  | Впровадження та налаштування опції відмовостійкості системи аудиту дій користувачів |
|  | Консультації щодо найкращих практик UEBA (User and Entity Behavior Analytics) |
|  | Консультація по роботі з сповіщеннями та панелі керування системи аудиту дій користувачів |
|  | Супровід по роботі з технічної документацією по системи аудиту дій користувачів |
|  | Надання документації по роботі з системою аудиту дій користувачів |
|  | Консультація «How to» щодо характеристик і функцій продуктів в системі аудиту дій користувачів |
|  | Допомога в оновленні, виправлення помилок та міграції системи аудиту дій користувачів |
|  | Гарантія якості розгортання та рекомендації щодо найкращих практики використання системи аудиту дій користувачів |
|  | Поглиблені рекомендації щодо вдосконалення, засновані на висновках системи аудиту дій користувачів |
|  | Розробка та надання звіту по впровадженню системи аудиту дій користувачів в інфраструктуру |
|  | Базове продуктове навчання для спеціалістів замовника |
|  | Поглиблене продуктове навчання для спеціалістів замовника |
|  | Локальна сервісна підтримка 8 годин на день, 5 робочих днів на тиждень |
| Вимоги до підсистеми захисту кінцевих точок від шкідливого програмного забезпечення |
|  | Загальні вимоги | Забезпечення захисту не менше ніж для 100 робочих станцій та серверів |
|  | Строк дії підписки не менше ніж 12 місяців |
|  | Забезпечення отримання основних та проміжних релізів програмного забезпечення через сайт Виробника, підтримка програмних кодів у актуальному стані відповідно до рекомендацій Виробника протягом 12 місяців |
|  | Забезпечення застосування Cisco Advanced Malware Protection з підтримкою актуальності (оновлення) захисту протягом 12 місяців для 100 робочих станцій та серверів |
|  | Підтримка моніторингу шкідливого коду на рівні робочої станції |
|  | Виявлення та запобігання складному шкідливому коду (malware), атакам нульового дня та цільовим атакам або без використання, або з мінімальним використанням бази даних сигнатур |
|  | Вендор послуги захисту безпеки повинен мати окремий підрозділ безпеки, що фокусується на дослідженнях шкідливого коду (malware) |
|  | Функціональні вимоги | Підтримка робочих станцій та серверів |
|  | Можливість інтерактивної та прозорої інсталяції |
|  | Наявність єдиної графічної консолі керування, моніторингу та налаштування |
|  | Підтримка наступних операційних систем:* + Windows;
	+ Linux.
 |
|  | Можливості аналізу на підозрілих станціях та серверах:* + Послідовний та хронологічних запис подій, з деталями, що включає хост, ім’я користувача, IP, клієнтські додатки;
	+ Деталі, що включають інформацію про те, який файл чи процес постраждав.
 |
|  | Відслідковування на мережевому рівні і візуалізація системи і користувачів, що постраждали: користувач, метод та точка входу |
|  | Можливість видачі інформації про шкідливий код (malware), який був невідомий на момент його проходження через систему з можливістю отримання звіту про джерело, приймача і автоматичне блокування спроб передачі його в майбутньому (cloud recall) |
|  | Рішення повинно підтримувати моніторинг шкідливого коду як на рівні мережі, так і на рівні робочої станції, повинно виявляти та запобігати складному malware, атакам нульового дня та цільовим атакам або без використання, або з мінімальним використанням бази даних сигнатур |
|  | Рішення повинно виявляти та блокувати підозрілі файли:* + Виявлення та блокування всіх видів malware, як відомого, так і невідомого;
	+ Аналіз всіх файлів, включаючи формати PDF, Flash, RTF, MS Office, Multimedia, архіви (при наявності розширеної ліцензії).
 |
|  | Рішення повинно підтримувати можливість проведення безперервного аналізу файлів, виявлення причини зараження для подальшої класифікації інцидентів безпеки:* + Можливість видачі інформації про malware, яке було невідомо на момент його проходження через систему з можливістю отримання звіту про джерело, отримувача і автоматичне блокування спроб передачі його в майбутньому (при наявності розширеної ліцензії);
	+ Можливість відправити malware на додатковий аналіз в «пісочницю» як автоматично, так і вручну (при наявності розширеної ліцензії)
 |
|  | Рішення повинно підтримувати можливість проведення розслідувань, що включають (але не обмежують) наступне:* + Джерело інфекції на аналіз причин виникнення загроз malware;
	+ Масштаби загрози, що включають звіти по кількості і типах машин, що були атаковані, первинне виявлення і детальна історія malware, включаючи профіль вузлів, а також інша підозріла діяльність на вузлах (підключення до C&C тощо);
	+ Візуальна репрезентація руху malware по мережі та по робочих станціях
 |
|  | Аналіз файлів в захищеній пісочниці для швидкого виявлення malware та підозрілої поведінки файлів (при наявності розширеної ліцензії) |
|  | Блокування можливих підключень до серверів керування ботнетами і активності дроперів, а також стримання розповсюдження malware |
|  | Функціонал на робочих станціях та серверах для реагування на інциденти повинен включати (але не обмежувати) наступне:* + Відслідковування та захоплення файлів на підозрілій машині;
	+ Блокування підозрілих файлів/процесів/сервісів, що показують шкідливу поведінку;
	+ Виявлення дроперів та блокування завантажень з URL/вузлів;
	+ Відправлення підозрілих файлів для аналізу (при наявності розширеної ліцензії)
 |
|  | Динамічний аналіз в реальному часі для виявлення malware нульового дня чи цільових атак (при наявності розширеної ліцензії) |
|  | Виведення результатів аналізу в формі графічної панелі або звіту, що показує деталі поведінки загрози і повинно як мінімум включати наступне:* + Операції ОС системного рівня;
	+ API виклики - Роботи процесів/потоків;
	+ Криптографічні операції;
	+ Можливості по захисту від debuggers;
	+ Можливості протидії “засинанню” malware чи затримці часу;
	+ Модифікації файлової системи;
	+ Модифікації реєстру;
	+ Мережеві порти та протоколи;
	+ Визначення Command and Control connections;
	+ Характеристики протоколів;
	+ Аналіз наступних файлів: Microsoft Office, Executable Files (exe, com, dll), PDF, Flash, Shockwave, Java JDK і JRE, Windows Media Player, Multimedia, Microsoft .NET framework, Microsoft Visual C++ redistributable, Microsoft Silverlight, Microsoft VMScript (при наявності розширеної ліцензії).
 |
|  | Сервісна підтримка | Сервісна підписки повинна мати строк дії не менше ніж на 12 місяців |
|  | Умови розширеної гарантії повинні включати в себе можливість реєстрації сервісних випадків в режимі 24х7х365, оновлення мікрокоду системи і версій встановленого програмного забезпечення |
|  | Надання консультацій по телефону, електронній пошті та на сайті підтримки виробника по питаннях установки, конфігурування і експлуатації обладнання з понеділка по неділю з 00.00 до 24.00 годин цілодобово |
|  | Постійний (24х7) авторизований доступ до сайту виробника |
| Вимоги до підсистеми розвідки загроз з відкритих джерел та Dark Web |
|  | Архітектура та форм-фактор | Система має бути у вигляді SaaS та розміщена на потужностях виконавця або виробника |
|  | Система має включати увесь зазначений функціонал в єдиному web-інтерфейсі |
|  | У комплекті поставки мають бути всі необхідні доступи та підключення до джерел інформації (сервера, СУБД, тощо) та ліцензії для повнофункціональної роботи системи |
|  | Якщо таких систем або елементів системи, для виконання вимог ТЗ, повинно бути декілька, вони усі мають входити до комплекту поставки рішення |
|  | Система повинна мати власну базу даних інформації щодо скомпрометованих облікових записів електронних систем |
|  | Система повинна мати власну базу даних інформації про вразливості у системах та сервісах, що використовують задля скоєння кібератак та кіберзлочинів |
|  | Система повинна мати власну базу даних інформації щодо суб'єктів, що планують, здійснюють, готують, та надають сервісні або технічні засоби задля скоєння кібератак та кіберзлочинів |
|  | Система має надавати технічну можливість для спільного ведення розслідування або дослідження декількома аналітиками в рамках одного провадження |
|  | Система має надавати можливість замовникові, при необхідності за допомогою виробника, додавати власні набори даних для наповнення Бази даних виробника, але з доступом до цієї інформації виключно лише для виробника системи та замовника |
|  | Система має містити Базу даних з інформацією щодо акаунтів, що мають відношення до кіберзлочинів та приближених до них осіб |
|  | Ліцензування | Система має бути ліцензована для прийому не менш ніж 3000 запитів до Бази даних на місяць з кожного аккаунта, що ліцензовано в системі для роботи окремого аналітика |
|  | Система має бути ліцензована для доступу до UI |
|  | Система має бути ліцензована для одночасної роботи не менше ніж 2 аналітиків |
|  | Система має бути ліцензована для отримання від виробника всієї наявної у Базі даних виробника інформації у відкритому вигляді про будь-який суб'єкт або об'єкт дослідження, що є в наявності у виробника системи |
|  | Системна архітектура | Система має бути реалізована на основі масштабованої, розподіленої архітектури на потужностях виробника |
|  | Система має складатись з: бази даних системи, веб-додатку, що здійснює (обробку, аналітику, експорт, імпорт інформації тощо) |
|  | Система повинна підтримувати можливості масштабування на потужностях виробника у обсягу необхідному для пошуку та обробки інформації у режимі реального часу |
|  | Система повинна підтримувати можливості збільшення обсягу Бази даних без обмеження |
|  | Система повинна надавати доступ для користувачів Замовника через канали Всесвітньої мережі Інтернет з використання шифрування не нижче TLS.v.1.1 |
|  | Система повинна зберігати дані у закриптованих сховищах |
|  | Система має забезпечувати веб-інтерфейс та доступ для аналітиків 24\*7 |
|  | Система повинна підтримувати можливість експорту даних у .json, .csv, тощо форматах |
|  | Функціональність | Система повинна мати наступний функціонал щодо облікових записів:* Пошук у відкритих джерелах інформації, щодо скомпрометованих облікових записів систем, що належать Замовникові;
* Пошук має відбуватися на підставі доменних імен, що належать Замовникові та додано у систему;
* Отримання паролів у відкритому вигляді з хеш-значень паролів, що було отримано під час пошуку інформації, про скомпрометовані акаунти, що належать Замовникові;
* Додавання та видалення доменних імен та окремих адрес електронної пошти, що належать Замовникові, та інформацію, щодо компрометації яких має шукати Виконавець;
* Відображення наступної інформації, щодо скомпрометованого аккаунта:
1. адреса електронної пошти,
2. дата отримання інформації Виконавцем,
3. джерело отримання інформації Виконавцем.

Система повинна підтримувати можливість експорту даних у .json, .csv, тощо форматах; |
|  | Система має містити наступну інформацію, щодо вразливостей в системах та сервісах:- Перелік CVE (Critical Vulnerabilities and Exploitations - https://cve.mitre.org/) , що на момент доступу до системи з боку Замовника є актуальними\*\*\* та використовуються зловмисниками для скоєння кібер атак та/або є доступними у комерційних та/або безкоштовних версіях ПЗ для пошуку вразливостей, тестування на проникнення та різноманітних “exploit-packs”, “exploit frameworks”, що розробляються зловмисниками для скоєння кібер-атак та можуть розповсюджуватись в Dark/Deep Net;\*\*\* - (період часу - сьогодні, останні 24 години, цього тижня - останні 7 днів, цього місяця)- Перелік АРТ-груп, АРТ-груп з державною підтримкою, хактивістських груп та/або інших об'єднаннях громадян або індивідуально певними особами, які можуть готувати, скоювати або в інший спосіб бути причетними до кібер-атак;- Інформація про дату та/або час, коли Виконавцем було зафіксовано використання, або готування до використання, або наявність відповідного програмного коду або файлу, що виконується для експлуатації вразливостей, що зареєстровано як CVE, або можуть бути не зареєстровані, як CVE, але характеризується як вразливості нульового дня (Zero-Day);- Інформацію про ПЗ, що є вразливим до вразливостей, що зареєстровано як CVE, або можуть бути не зареєстровані, як CVE, але характеризується як вразливості нульового дня (Zero-Day) із зазначенням версій ПЗ, що є вразливими;- Інформацію про патчі-виправлення для ПЗ, що усувають вразливості в ПЗ, що є вразливим, та/або інформацію про варіанти використання додаткових шарів захисту для  усунення можливості використання вразливостей в ПЗ без використання патчів-виправлень. |
|  | Система повинна мати функціонал пошуку по власній базі даних за наступними критеріями:- За CVE ідентифікатором, повне або часткове співпадіння;- За датою та/або часом фіксації інформації в системі Виконавця;- За назвою ПЗ або системи, що є вразливою;- За приналежністю до АРТ-груп, АРТ-груп з державною підтримкою, хактивістських груп та/або інших об'єднаннях громадян або індивідуально певними особами, які можуть готувати, скоювати або в інший спосіб бути причетними до кібер-атак; |
|  | Система повинна мати функціонал пошуку по Базі даних за наступними критеріями:- За мережевим псевдонімом суб`єкта і об`єкта дослідження;- За адресою електронної скриньки суб`єкта і об`єкта дослідження;- За номером телефону суб`єкта і об`єкта дослідження;- За IP-адресою суб`єкта і об`єкта дослідження;- За зашифрованим засобом доступу суб`єкта і об`єкта дослідження;- За доменом суб`єкта і об`єкта дослідження;- За псевдонімом у системах обміну повідомленнями суб`єкта і об`єкта дослідження;- За ключовими словами тощо; |
|  | Повинна надавати доступ до інформації про небезпечні з'єднання (TOR, PROXY, VPN). Підсистема повинна підтримувати рознесену модель для кореляції даних з усіх джерел збору інформації. Повинна забезпечувати зберігання подій протягом тривалого періоду часу (щонайменше 12 місяців) для можливості подальших розслідувань і надання розширеної інформації за запитом Замовника. |
|  | Повинна бути можливість отримання додаткової інформації про IP-адресу, що може містити загрозу для інформаційної системи Замовника;Повинна забезпечувати фільтрацію даних, а також показувати через користувацький інтерфейс усі актуальні події;Повинна надавати можливість аналізу подій, зібраних протягом певного періоду часу. |
|  | Інформація щодо IP-адрес, що можуть містити загрозу для інформаційної системи Замовника, має формуватися виробником на підставі власних даних або збирання інформації власними інструментами із зовнішніх джерел;Інформація має бути оновлений у режимі реального часу;Підсистема повинна надавати інформацію про підстави включення IP-адреси до складу списку, що можуть містити загрозу для інформаційної системи Замовника. |
|  | Система повинна мати вбудований (Built-in) функціонал задля кореляції інформації щодо суб`єкта або об`єкта дослідження; |
|  | Система повинна мати графічні панелі візуалізації (Built-in Dashboards) для аналізу інформації щодо скомпрометованих аккаунтів, а також її пошуку; |
|  | Система повинна мати систему звітів, щодо завершених досліджень та тих, що в процесі проведення (Built-in); |
|  | Система повинна мати вбудовану рейтингову систему щодо інформації з бази даних, та надавати можливість сортування за цими рейтингами; |
|  | Система повинна підтримувати вбудовані механізми створення і обробки нотаток аналітиків щодо суб`єкта або об`єкта дослідження або розслідування; (Built-in notes system). |
|  | Система повинна мати вбудовану рейтингову систему щодо джерел інформації з Бази даних, та надавати можливість фільтрації за цими рейтингами; |
|  | Система має мати аналітичне відображення кількості скомпрометованих акаунтів, що було знайдено Виконавцем; |
|  | Система повинна мати систему сповіщень по налаштованих критеріях шляхом відправки електронного листа на адресу Замовника; |
|  | Система повинна мати можливість експорту даних у форматі .txt та/або .json та/або .csv шляхом прямого експорту через функціонал Системи; |
|  | Відмовостійкість та резервування | Резервування системи та інформації, що в ній оброблюється має відбуватися в режимі реального часу на боці виробника системи; |
|  | Система має бути розгорнутою на потужностях хмарного дата-центру та мати резервування основних потужностей для збору, зберігання та обробки даних, а також систем охолодження, електропостачання, каналів зв`язку тощо; |
|  | Резервування та відновлення конфігурації системи має відбуватися прозоро для замовника на боці виконавця; |
|  | Відновлення бази даних системи після збоїв має відбуватися прозоро для замовника на боці виконавця або вендора (такі збої не мають впливати на працездатність системи для замовника та перешкоджати процесу дослідження та/або розслідування) |
|  | Захищеність системи | Обмеження доступу до даних і інтерфейсу управління на основі ролей (RBAC); |
|  | Підтримка обов’язкового використання 2FA (Two-factor authentication); |
|  | Ведення журналу обліку доступу до Системи на боці Виконавця; |
|  | Ведення журналу обліку змін об'єктів, що ініційовані користувачами; |
|  | Ведення журналу обліку змін об'єктів, що ініційовані системними компонентами; |
|  | Безпечні протоколи передачі даних між компонентами системи (HTTPS, TLS версії не менш ніж 1.1). |
|  | Пошук інформації на основі домену або адреси електронної пошти; |
|  | Пошук інформації в режимі реального часу; |
|  | Зберігання даних протягом різного періоду часу, без видалення інформації з попередніх періодів незалежно від дати її отримання, додавання до Бази даних системи, або періодам до якого ця інформація віднесена згідно дати та часу (timestamp); |
|  | Виробник повинен заповнювати систему щомісячно; |
|  | Управління розслідуваннями, дослідженнями і даними | Нормалізація інформації, що завантажується від замовника для додання у Базу даних виробника задля інтеграції в систему у повному обсязі; (інформація, що додається має бути приведена у відповідність до вимог бази даних фахівцями виконавця або вендора) |
|  | Відображення інформації про суб'єкти, що є в Базі даних, розподілена по окремих категоріях; |
|  | Дедуплікація ідентичної інформації, що була отримана з різних джерел (об'єднання однакових значень); |
|  | Фільтрація інформації, з метою проведення кореляції з різних джерел (об`єднання інформації з різних джерел, але поєднаної за спільними критеріями, наприклад однаковий  e-mail, номер телефону, псевдонім, ip-адреса та інші категорії); |
|  | Пошук інформації на основі ключових слів та/або атрибутів; |
|  | Пошук інформації в режимі реального часу (великі запити до пошукової системи повинні бути оброблені не довше ніж за 600 секунд, незалежно від складності запиту та обсягу інформації, в якій здійснюється пошук); |
|  | Зберігання даних протягом різного періоду часу, без видалення інформації з попередніх періодів незалежно від дати її отримання, додавання до Бази даних системи, або періодам до якого ця інформація віднесена згідно дати та часу (timestamp); |
|  | Виробник повинен доповнювати систему щомісячно, незалежно від того, чи було надано інформацію з боку замовника чи ні; |
|  | Виробник повинен самостійно знаходити інформацію з джерел  щодо осіб, що можуть здійснювати кібератаки та/або скоювати кіберзлочини для додавання до Бази даних системи; |
|  | Підтримка завантаження різних форматів баз даних, що замовник надає виробникові для завантаження до Бази даних системи (замовник та виробник узгоджують технічне завдання, щодо інформації яку необхідно додати до Бази даних системи); |
|  | Відображення мапи та Geo інформації, щодо ip-адрес, які фігурують в дослідженнях та розслідуваннях; |
|  | Відображення інформації про належність датасета, що фігурують в дослідженнях та розслідуваннях; |
|  | Візуалізація і аналітика | Фільтрація по категоріях, regex; |
|  | Повнотекстовий пошук по ключових словах; |
|  | Візуалізація кросс-зв`язків по різних джерелах, суб`єктах та об`єктах, що фігурують в дослідженнях та розслідуваннях; |
|  | Управління дослідженнями та розслідуваннями | Система повинна підтримувати механізми аналітики та управління дослідженнями та розслідуваннями; |
|  | Ведення картки дослідження або розслідування; |
|  | Можливість додавання інформації до дослідження або розслідування з будь яких результатів пошуку у системі; |
|  | Система повинна підтримувати можливість ведення спільного дослідження або розслідування кількома аналітиками одночасно; |
|  | Система повинна підтримувати можливості надання інформації до дослідження або розслідування аналітиком в ручному режимі; |
|  | Система повинна підтримувати ведення дослідження або розслідування одним аналітиком; |
|  | Можливість видалення помилкової інформації, що було додано до дослідження або розслідування; |
|  | Можливість експорту результатів дослідження або розслідування в форматі .json, .csv; |
|  | Технічна сервісна підтримка | Технічна сервісна підтримка не менше ніж 12 місяців з рівнем підтримки у робочі дні по телефону або шляхом електронного листування; |
|  | Усі ліцензії повинні мати строк дії не менше ніж 12 місяців Постійний доступ до центру технічної підтримки постачальника електронною поштою або за телефоном |
| Вимоги до підсистеми двостороннього захисту Інтернет-трафіку |
|  | Загальний функціонал | Система захищає від кіберзагроз, має можливість блокувати доступ до зловмисних доменів, пов’язаних із фішингом, шкідливим програмним забезпеченням, програмами-вимагачами, інфраструктурою командних серверів шкідливого програмного забезпечення тощо |
|  | Система використовує систему доменних імен (DNS) та аналізує запити, зроблені пристроями в мережі, і блокує будь-які запити до шкідливих доменів |
|  | Система використовує вдосконалені канали розвідки, алгоритми машинного навчання та аналіз поведінки для виявлення та блокування шкідливих доменів у режимі реального часу |
|  | Система  є простим у впровадженні та управлінні, з простим процесом налаштування та інтуїтивно зрозумілим інтерфейсом користувача, який забезпечує видимість і контекст як на високому, так і на деталізованому рівнях |
|  | Рішення включає:* доступ до інтерфейсу користувача, сповіщення електронною поштою, розширені запити, збагачення інформації геоданими
* виявлення уражених пристроїв, інтеграцію, стандартне звітування, підтримку клієнтів, роумінг користувачів
 |
|  | Захист DNS | Рішення виявляє та запобігає атакам до того, як вони відбудуться, незалежно від протоколу, для пристроїв у мережі та за її межами. Впровадження повинно підтримувати WFH\гібридні робочі моделі та захищати всі типи пристроїв (інтернет речей, сервери, мобільні пристрої, стаціонарні ЕОМ тощо) |
|  | Видимість загроз | Система:* забезпечує розширене виявлення зловмисної інфраструктури і використовує штучний інтелект для захисту мережі користувача;
* забезпечує високоефективне сповіщення про загрозу, щоб зменшити хибні спрацювання і покращити мережеву аналітику;
* виявляє та блокує атаки низького та повільного рівня, атаки на ланцюги поставок та інші вторгнення, замасковані у мережевому трафіку;
* уникає програм-вимагачів, фішингу та компрометації ланцюга поставок;
* зупиняє атаки, гарантуючи, що користувачі, пристрої чи сервери випадково не зв’яжуться з інфраструктурою зловмисників;
* аналізує DNS, щоб збільшити наявні інструменти кібербезпеки за допомогою інтеграції API;
* рішення забезпечує можливість швидко та легко інтегрувати через API існуючі рішення SIEM, SOAR, брандмауери та кінцеві точки;
* блокує комунікації шкідливих програм із командними серверами (C2);
* підтримує WFH / гібридні робочі моделі та захищає всі типи пристроїв (IoT, сервери, мобільні пристрої, стаціонарні ЕОМ, тощо);
* підтримує нескінченне масштабування;
* надає інформацію про джерело заблокованої загрози;
* здійснює аналіз шаблонів комунікації;
* використовує поєднання історичних даних домену продовж попереднього часу існування із аналізом комунікаційних шаблонів у реальному часі
 |
|  | Термін підписки | Підписка 36 місяців |
|  | Пакет підписки має такі розгортання | Резолвер HYASАгент HYAS (Windows, Android)Спеціалізована підтримка з доступом до порталу та системи продажу tickets |
|  | Вимоги до архітектури рішення | Система має можливість впровадження і як хмарне рішення безпеки Protective DNS, і через інтеграцію API з існуючими системами кібербезпеки Система має можливість обмінюватися даними з клієнтською мережею хмарними DNS-перетворювачами для рекурсивного вирішення, аналізу ризиків і процесу прийняття рішень на основі вердикту |
|  | Вимоги відповідності до операційної системи та програмного забезпечення настільного клієнта (робочої станції) | Рішення для моніторингу мережі на рівні DNS із використанням хмарних рекурсивних резолверів DNS |
|  | Вимоги відповідності  корпоративної мережі | Система має можливість здійснити підключення до відкритої глобальної мережі «Інтернет» і підтримувати можливість підключення до спеціалізованих служб, необхідних для рішення Protective DNS.Система використовує один або декілька з наведених нижче портів і/або служб, щоб запустити рішення в експлуатацію:* порт 53 UDP/TCP;
* DOH – DNS через HTTPS (порт 443);
* DOT – DNS через TLS (порт 853)
 |
|  | Вимоги до функціональності захисту | Система має у своєму складі необхідний функціонал для блокування шкідливого трафіку DNS за замовчуванням від виробника. Показники підтверджені дослідженнями AV-TEST, або іншою незалежною організацією яка оцінює антивірусне програмне забезпечення та програмне забезпечення безпеки  |
|  | Система забезпечує безпеку та блокує комунікації із командними серверами шкідливих програм (C2), програмами-вимагачами, фішингом і атаками на ланцюжки поставок,  при цьому надає інтелектуальні дані на вимогу для покращення існуючого стека безпеки та ІТ-керування. Усуває загрози у режимі реального часу |
|  | Вимоги до аналітики | Система містить:* доступ до інтерфейсу користувача, сповіщення електронною поштою, розширені запити;
* виявлення заражених машин, інтеграцію, стандартні звіти, підтримку та роумінг користувачів;
* вбудовану підтримку виявлення алгоритму створення домену (DGA), DNSSEC, DNS через HTTPS і DNS через TLS;
* висновки та аналіз даних DNS за допомогою аналізу журналів у реальному часі;
* блокування по репутації реєстранта домену, геолокації, IP та CIDR, NS та ASN;
* оцінювання рівня складності атаки - звичайна чи направлена;
* функціонал Sinkholing та подальший аналіз на основі хендшейку;
* блокування доменів на основі ризиків (домен не має MX-запису, сервер імен у небажаному регіоні, активність C2 тощо);
* підтримка RESTFUL API interface для отримання фільтрованих журналів та керування правилами блокування
 |
|  | Кількість користувачів | Доступ на 100 користувачів |
|  | Рівень доступності | Платформа системи доступна щонайменше у  99,9 % часу |
|  | Вимога до підтримки | * Захист 24/7;
* спеціалізована підтримка з доступом до порталу виробника;
* ввідний інструктаж, адаптація та підтримка користувачів;
* навчання та тренінги без обмежень і додаткової плати від виробника;
* щоквартальний звіт про успіх користувача;
* можливість щоквартальних зустрічей з технічною командою виробника для будь-яких питань / обговорень щодо роботи та функціоналу продукту;
* виробник поділиться знаннями, заснованими на досвіді інших клієнтів (успішними USE-cases)
 |

Учасник якого визначено переможцем процедури закупівлі, перед укладанням договору проводить науково-технічну експертизу та/або експертну оцінку та/або незалежну оцінку вартості послуг, за результатом аукціону, вказаних в Додатку 5 до тендерної документації та надає Замовнику документ що підтверджує вартість вказаних послуг. У разі надання документу де вартість послуг буде нижча ніж зазначив Учасник за результатом аукціону, Учасник-Переможець укладає разом із договором додаткову угоду на зменшення вартості за одиницю послуг (надати у складі тендерної документації гарантійний лист).

**5. Обґрунтування розміру бюджетного призначення:** розмір бюджетного призначення визначено Законом України «Про Державний бюджет України на 2023 рік» за КПКВК 1001050 «Реалізація державної політики у сфері внутрішніх справ, забезпечення виконання завдань і функцій органів, установ та закладів Міністерства внутрішніх справ України» відповідно до бюджетного запиту на 2023 рік.

**6. Очікувана вартість предмета закупівлі:** 10 622 028,86 грн. (десять мільйонів шістсот двадцять дві тисячі двадцять вісім гривень 86 коп.) з ПДВ.

**7. Обґрунтування очікуваної вартості предмета закупівлі:** Очікувана вартість визначена відповідно до частини 1 та 2 пункту 1 Розділу ІІІ «Методи визначення очікуваної вартості» Примірної методики визначення очікуваної вартості предмета закупівлі затвердженої Наказом Міністерства розвитку економіки, торгівлі та сільського господарства України 18.02.2020 № 275 та розрахована, як середньоарифметичне значення масиву отриманих даних, що розраховується за такою формулою: Цод = (Ц1 +… + Цк) / К.

**8. Процедура закупівлі:** Застосовується процедура відкритих торгів з особливостями.