Виконуючому обов'язки
директора Спеціалізованого
комунального підприємства
«Київтелесервіс»

Чернікову Павлу Олександровичу

Заступника директора з ІТ
Голуба Ігоря Павловича

СЛУЖБОВА ЗАПИСКА

місто Київ «17» вересня 2021 року

Конкретна назва предмета закупівлі - **Створення, впровадження та супроводження операційного центру кібербезпеки (48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника)**

Обґрунтування доцільності закупівлі:

З метою створення та розвитку сучасного операційного центру кібербезпеки для захисту міської ІТ-інфраструктури від кіберзагроз, а також відповідно до пункту 16.22. «Створення та впровадження операційного центру кібербезпеки, його технічне обслуговування, сервісна підтримка, розширення та дооснащення» напрямів діяльності та заходів Комплексної міської цільової програми «Електронна столиця на 2019 - 2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512., вважаю за доцільне провести закупівлю.

Обґрунтування обсягів закупівлі:

Відповідно до поточних потреб необхідно забезпечити придбання наступної програмної продукції для функціонування операційного центру кібербезпеки:

1) Програмна продукція **Підсистеми керування мережевими пристроями безпеки** для забезпечення керування 390 пристроїв безпеки строком дії не менше ніж 12 місяців – **1 комплект**.

2) Програмна продукція **Підсистеми оркестрування, автоматизації та реагування на інциденти безпеки** для забезпечення роботи не менш ніж 3 (трьох) аналітиків строком дії не менше ніж 12 місяців – **1 комплект**.

3) Програмна продукція **Підсистеми пошуку вразливостей в рамках циклу розробки програмного забезпечення /SDLC** для забезпечення роботи не менш ніж в 10 (десяти) одночасних проектах строком дії не менше ніж 12 місяців – **1 комплект.**

4) Програмна продукція **Підсистеми моніторингу ІТ-сервісів** у складі:
   - примірник програмної продукції для забезпечення моніторингу ІТ-сервісів, що розміщені в інфраструктурі із загальним обсягом оперативної пам'яті не менш ніж 384 GB строком дії не менше ніж 12 місяців – **1 комплект**;
   - примірник програмної продукції для забезпечення контролю якості взаємодії користувачів із ІТ сервісами та моніторингу не менш ніж 1 000 000 сесій реальних

користувачів строком дії не менше ніж 12 місяців – **1 комплект.**

5) Програмна продукція **Підсистеми моніторингу та контролю дій привілейованих користувачів** для забезпечення одночасної роботи з відповідними контрольованими (цільовими) системами не менш ніж 20 (двадцять) привілейованих користувачів в межах існуючої у Замовника інсталяції строком дії не менше ніж 12 місяців – **1 комплект.**

6) Програмна продукція **Підсистеми адаптивної мережевої автоматизації** у складі:
   - примірник програмної продукції для забезпечення одночасної роботи не менше ніж 1 (одного) адміністратора строком дії не менше ніж 12 місяців – **1 комплект;**
   - примірник програмної продукції для забезпечення покриття не менш ніж 250 мережевих пристроїв включаючи функціональність Change management (або аналог згідно вимог) строком дії не менше ніж 12 місяців – **1 комплект.**
   - примірник програмної продукції для забезпечення покриття не менш ніж 250 мережевих пристроїв включаючи функціональність Application Assurance (або аналог згідно вимог) строком дії не менше ніж 12 місяців – **1 комплект.**

7) Програмна продукція **Підсистеми керування процесом пошуку та мінімізації впливу вразливостей ІТ-інфраструктури** для забезпечення роботи підсистеми у відповідності до технічних вимог строком дії не менше ніж 12 місяців – **1 комплект.**

Обґрунтування якісних характеристик закупівлі:

Предмет закупівлі повинен відповідати технічним, якісним та кількісним вимогам, наданим у Додатку 1.

Технічні вимоги до предмета закупівлі рекомендовані протоколом № 41 засідання робочої групи з розробки та погодження технічних вимог до закупівель робіт, товарів і послуг при виконанні заходів Комплексної міської цільової програми «Електронна столиця» на 2019 – 2022 роки у 2021 – 2022 роках від 13 вересня 2021 року.

Очікувана вартість предмета закупівлі, згідно проведеного Ініціатором закупівлі (відповідальним за розробку технічних вимог) моніторингу цін, становить 27 030 000,00 грн (двадцять сім мільйонів тридцять тисяч гривень 00 копійок) з ПДВ.

Джерело фінансування закупівлі – місцевий бюджет, КЕКВ 2610 Субсидії та поточні трансферти підприємствам (установам, організаціям).

Процедура закупівлі – відкриті торги з публікацією англійською мовою.

Вид предмету закупівлі – програмна продукція з супутніми послугами з її встановлення та налаштування.

Кількість товару – 10 комплектів.

Місце поставки товару – 04070, місто Київ, вулиця Фролівська, будинок 1/6 А.

Строки поставки товарів – по 31 грудня 2021 року.

Додатки:

1. Додаток 1. Інформація про необхідні технічні, якісні та кількісні характеристики предмета закупівлі (Технічні вимоги) на 56 арк.
2. Додаток 2. Кваліфікаційні критерії до учасників на 2 арк.
3. Додаток 3. Підтвердження очікуваної вартості предмета закупівлі (моніторинг цін) на 6 арк.

Ініціатор закупівлі _____ **І. П. Голуб**

«ПОГОДЖЕНО»:

Головний бухгалтер _____ **Г. А. Букша**

Начальник загально-правового відділу _____ **В. В. Тихонов**

Заступник директора з впровадження
та інформаційного супроводу ІТ рішень _____ **В. Є. Іцкович**

Заступник директора з технічних питань _____ **О. Ф. Поліщук**

Додаток 1

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ (ТЕХНІЧНІ ВИМОГИ).

Предмет закупівлі: Створення, впровадження та супроводження операційного центру кібербезпеки
(48150000-4 Пакети програмного забезпечення для керування виробничими процесами за ДК 021:2015 Єдиного закупівельного словника).

На виконання пункту 16.22. «Створення та впровадження операційного центру кібербезпеки, його технічне обслуговування, сервісна підтримка, розширення та дооснащення» напрямів діяльності та заходів Комплексної міської цільової програми «Електронна столиця на 2019 - 2022 роки, затвердженої рішенням Київської міської ради від 18.12.2018 № 461/6512.

На підтвердження відповідності пропозиції технічним, якісним та кількісним характеристикам предмета закупівлі у складі своєї тендерної пропозиції (Учасник) повинен надати інформацію про можливість постачання Товару Замовнику з урахуванням вимог, наведених нижче.

Учасник має право запропонувати еквівалент конкретної торговельної марки чи фірми, патенту, конструкції або типу предмета закупівлі, джерела його походження або виробника, які можливо вживаються в документації конкурсних торгів, за умови, що такий еквівалент відповідатиме вимогам, встановленим у цій документації.

З метою встановлення джерела постачання та наявності гарантій виробника на Товар, що пропонується до постачання, Учасником у складі тендерної пропозиції надається:

Авторизаційний лист (авторизаційна форма, тощо) від виробника (або від його офіційного представника виробника на території України) програмного забезпечення, що пропонується до постачання Учасником, який засвідчує наявність в учасника статусу партнера та права учасника здійснювати продаж запропонованого програмного забезпечення, адресований на ім'я Замовника із посилання на процедуру закупівлі.

1. Мета та задачі створення Центру

Центр керування та моніторингу компонентів ІТ-інфраструктури та Кіберзахисту (далі – Центр) призначений для:

1) створення умов для систематичного автоматизованого спостереження за параметрами функціонування ІТ-систем у встановлених межах, оперативного виявлення, попередження та усунення збоїв в їх роботі;
2) Забезпечення безперервного процесу виявлення та відповідної реакції на подій, що прямо або опосередковано здатні вплинути на інформаційну безпеку організації, аналіз та швидке усунення наслідків інцидентів кібербезпеки та застосування відповідних заходів щодо запобігання їх повторення в подальшому.

Задачами Центру є:

- Збір, обробка та зберігання даних про різноманітні параметри функціонування ІТ-систем
- Прогнозування, реагування та вживання попереджувальних заходів для недопущення збоїв в роботі ІТ-систем
- Автоматичне оповіщення та виконання визначених дій у випадках виявлення проблем в роботі ІТ-систем
- Контроль якості обслуговування ІТ-систем
- Підвищення рівня керованості та спостереженості існуючої ІТ-інфраструктури за рахунок впровадження методики та практик автоматизації процесів повсякденного супроводу та експлуатації з метою підвищення ефективності роботи

обслуговуючого технічного персоналу.

- Запобігання інцидентам кібербезпеки шляхом активного(ї): безперервного аналізу (ручного та автоматизованого) загроз; обстеження та оцінки стану захищеності активів шляхом сканування мережевої інфраструктури та кінцевих хостів з метою пошуку відомих вразливостей; координації розгортання контрзаходів щодо інцидентів кібербезпеки; побудови та реалізації політик інформаційної безпеки.
- Моніторинг, виявлення та аналіз потенційних вторгнень в реальному часі та в ретроспективі з боку джерел даних, що мають відношення до кібербезпеки: автоматизація використання ідентифікаторів компрометації, які надходитимуть від зовнішніх та внутрішніх джерел (інформаційні, телекомунікаційні та інформаційно-телекомунікаційні системи, програмні, програмно-апаратні засоби та інше), технологічних партнерів, глобального Treat Intelligence виробників; автоматизована аналітична діяльність з обробки масивів даних про кіберінциденти.
- Своєчасне реагування на підтверджені інциденти кібербезпеки, координуючи ресурси та направляючи своєчасні, та відповідні потребам контрзаходи, включаючи оперативне, та стратегічне управління, моделювання, прогнозування розвитку подій.
- Надання інформації щодо ситуаційної обізнаності та звітування про стан захищеності інформаційних активів, інцидентів і тенденцій поведінки потенційних зловмисників, відповідно до галузевої специфіки.
- Обстеження та оцінка стану захищеності активів, підготовка, та надання відповідних рекомендацій в частині вдосконалення засобів захисту.

2. Загальні вимоги

Відповідно до поточних потреб Замовника Центр включатиме але не обмежуватиметься наступними підсистемами, в рамках яких очікується досягнення наступних завдань:

8) Підсистема керування мережевими пристроями безпеки
   - Забезпечити продовження технічної підтримки згідно технічних вимог на існуюче рішення строком на 12 місяців;
   - Провести дооснащення існуючого рішення до наявних потреб (з урахуванням планового розширення).
9) Підсистема оркестрування, автоматизації та реагування на інциденти безпеки;
   - забезпечити узгодження роботи (оркестрація) систем кібербезпеки, а також управління реагуванням на інциденти в режимі реального часу;
   - оптимізувати базові / рутинні операції CSOC (прийом повідомлень, визначення пріоритетів в залежності від рівня ризиків і розподіл завдань), що в свою чергу дозволить знизити навантаження (трудовитрати) на персонал, а також знизити ризик помилок і недогляду в зв'язку з людським фактором;
   - надати для IRT (зовнішньої і / або штатної) інструментарій для організації процесу управління реагуванням на інциденти;
   - знизити ризики схильності інфраструктури Замовника до можливих критичних інцидентів ІБ.
10) Підсистема пошуку вразливостей в рамках циклу розробки програмного забезпечення /SDLC;
   - Впровадити процес аналізу нових поставок ПО на наявність вразливостей;
   - Розробити та провадити процедури для розробників щодо їх усунення;
   - Підвищити якість поставок ПЗ в майбутньому за рахунок реалізації контролю вихідного коду;
   - Знизити ризики схильності впроваджуваних сервісів/ застосувань до можливих

критичних інцидентів ІБ.

11) Підсистема моніторингу ІТ-сервісів, яка призначена для моніторингу веб-додатків, додатків та контролю якості взаємодії користувачів із ІТ сервісами;
   - Забезпечення контролю продуктивності ІТ-сервісів (щонайменше критичних, з можливістю подальшого масштабування);
     - Визначення причин виникнення помилок в роботі зазначених ІТ-сервісів;
     - Прискорення процесу реакції на інциденти і усунення їх наслідків;
   - Забезпечення аналізу активності користувачів для ключових ІТ-систем:
     - можливість аналізу кожної сесії користувача включаючи можливість її відтворення;
     - можливість отримання розширеної інформації про ступінь впливу помилок в продуктивності ІТ-систем на користувачів;
     - можливість оцінки рівня задоволеності користувачів ІТ-системами;
     - можливість роботи з Synthetic tests для зниження репутаційних ризиків при Canary tests;
   - Розробити та описати процес моніторингу додатків, процес реакції на виникаючі інциденти, описати зони відповідальності команд, описати групи нотифікацій та розробити чіткі інструкції по реакції на інциденти.
12) Підсистема моніторингу та контролю дій привілейованих користувачів;
   - Організувати єдину платформу для управління доступом адміністраторів і зовнішніх підрядників (з єдиною «точкою входу») в мережах існуючої ІТ-інфраструктури Замовника включаючи забезпечення покриття процесом систем, які функціонують за допомогою СА (поточний інструментарій).
     - Створити контрольований і керований процес надання доступу для привілейованих користувачів;
     - Виявляти порушення політик безпеки в процесі роботи привілейованих користувачів;
     - Знизити ризик інсайдерських загроз;
     - Розширити контроль і управління протоколами віддалених доступів (додатковий контроль за буфер обміну, клавіатурою, активностями миші, каналами передачі даних в розрізі різних протоколів);
     - Прискорити і автоматизувати процес надання доступів до критичних систем;
     - Прискорити процес надання доступом в разі термінової необхідності отримати доступ до критичних систем;
     - Прискорити процес розслідування виявлених загроз як в режимі реального часу, так і в історичній ретроспективі;
     - Налаштувати політики підключення до кінцевих систем відповідно вимог ISO / IEC 27001;
     - Спростити способи підключень співробітників до кінцевих систем не навантажуючи локальні робочі станції непотрібним ПЗ;
     - Розмежування управління і адміністрування кінцевих критичних систем різними адміністратора з різними бізнес ролями відповідно до політик RBAC та обмежити доступ в різні підмережі різних групам адміністраторів відповідно їх повноважень;
   - Масштабувати процес виявлення порушення політик безпеки в процесі роботи привілейованих користувачів на КТЗ;
   - Забезпечити безперешкодне впровадження(інтеграцію) рішення в існуючу КСЗІ зі збереженням профілю захищеності за рахунок наявності у запропонованого рішення чинного експертного висновку ДССЗЗІ.
13) Підсистема адаптивної мережевої автоматизації;
   - впровадження методики та практик автоматизації (за рахунок застосування додаткових інструментів) процесів технічного супроводу мережевої

інфраструктури з метою підвищення якості роботи обслуговуючого персоналу;

- значно прискорити процес пошуку, діагностування, локалізації і усунення інцидентів/відмов, включаючи аналіз причин їх виникнення і надання рекомендацій, що виключають та/або мінімізують виникнення подібних інцидентів/відмов в майбутньому;
- оптимізувати базові/ рутінні операції NOC (за рахунок динамічних карт, RunBook'ов, ...), що в свою чергу дозволить знизити навантаження (трудовитрати) на персонал, а також знизити ризик помилок і недогляду в зв'язку з «людським фактором»;
- впровадити процес контрольованого внесення змін до конфігурації мережевої інфраструктури з урахуванням таких критеріїв (але не обмежуючись цим):
  - зміни, що впливають на роботу сервісів і їх доступності кінцевим споживачам;
  - зміни, що впливають на архітектуру побудови мережевої інфраструктури та/або її компонентів;
  - зміни, за рівнем критичності і складності їх виконання
- Забезпечити процес підтримки актуального стану робочої документації на існуючу мережеву інфраструктуру.

14) Підсистема керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури;

- Систематизувати процес виявлення і усунення потенційно шкідливих вразливостей;
- Знизити ризики схильності інфраструктури Замовника до можливих критичних інцидентів ІБ;
- Підвищити зрілість інфраструктури Замовника (в контексті CyberSecurity) розробивши планові регламенти відповідного процесу.
- Проведення випробувань інформаційних ресурсів (веб-додатків) та IT-інфраструктури Замовника на вразливості (Penetration Testing).

Підсистеми повинні мати можливості для подальшого розширення функціоналу та кількості компонентів IT-систем, що контролюються в Системі, без внесення суттєвих змін до існуючої IT-інфраструктури.

Зазначене програмне забезпечення Системи повинно розгортатися на обладнані Замовника, з вже встановленими на ньому операційними системами та базами даних.

№ з/п	Найменування технічні характеристики та вимоги		Одиниця виміру	Кіль-кість
1.	Програмна продукція **підсистеми керування мережевими пристроями безпеки** для забезпечення керування 390 пристроїв безпеки строком дії не менше ніж 12 місяців.		**комплект**	**1**
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:			
	Загальні вимоги	- Якщо відповідно до функціональності запропонованого рішення або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки; - Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення;		

		- На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника
	Архітектура та форм-фактор	- Запропоноване рішення має мати можливість бути реалізовано у вигляді віртуалізованого або програмно-апаратного рішення; ▪ Якщо запропоноване рішення являє собою віртуальну машину, то вона буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником (заздалегідь має погоджуватися обсяг необхідних ресурсів); ▪ Якщо така система являє собою програмно-апаратний комплекс (ПАК), то всі елементи рішення мають бути у комплекті поставки; – Повинна забезпечуватися можливість створення окремих ізольованих між собою адміністративних доменів для розподілення між ними пристроїв (як фізичних так і віртуальних пристроїв) та відповідних адміністраторів (Multi-Tenancy); – Запропоноване рішення має забезпечувати відмовостійкість (high availability): ▪ Підтримка об'єднання декількох фізичних пристроїв в один логічний кластер для відмовостійкості; ▪ Active/Passive кластер; ▪ Синхронізація конфігурацій та системних баз з Active до Passive вузлів кластеру.
	Ліцензування та підтримка існуючої мережевої інфраструктури	– Запропоноване рішення повинно бути ліцензоване для підтримки не менше ніж 390 пристроїв мережевої безпеки (фізичних, віртуальних); – Запропоноване рішення повинно підтримувати та забезпечувати повноцінне керування існуючими у замовника мережевими пристроями безпеки (Fortinet FortiGate).
	Функціональні вимоги	– Централізоване налаштування мережевих пристроїв безпеки повинно забезпечуватися: ▪ Шляхом застосування конфігураційних пакетів (templates); ▪ Шляхом безпосередньої конфігурації пристроїв через WEB-інтерфейс; ▪ Шляхом запуску сценаріїв (scripts). – Додавання пристроїв до системи повинно здійснюватися одним з наступних варіантів: ▪ Помічник (wizard) адміністратора системи для додавання та реєстрації пристроїв у системі керування; ▪ Відправлення запитів з самих пристроїв до системи щодо централізованого керування ними; ▪ Додавання пристроїв, що вже підключені до мережі та тих, що будуть підключені (pre-provision). – При роботі з конфігураційними файлами запропоноване рішення має забезпечувати:

		▪ Централізоване сховище конфігураційних файлів пристроїв, що знаходяться під керуванням; ▪ Централізоване розповсюдження нових конфігураційних файлів на пристрої; ▪ Ведення бази змін конфігураційних файлів, відображення хто и коли робив ці зміни, а також які зміни були внесені (аудит конфігураційних змін); ▪ Ведення журнальних записів, що фіксують які конфігурації зміни завантажились на пристрій та чи мали місце під час цього процесу помилки або попередження; ▪ Перегляд (review) конфігураційних налаштувань та підтвердження (commit) їх встановлення на пристрої, що знаходяться під керуванням системи; ▪ Повернення (revert) функціонування пристрою до попередньої редакції (revision) конфігураційного файлу; ▪ Синхронізація конфігураційних файлів між пристроями та централізованою системою; ▪ Автоматичне оновлення конфігурації пристроїв при їх підключенні до мережі (перехід з стану offline- до online-); ▪ Підтримка функціоналу гарантування цілісності та коректності інсталяції конфігураційних змін на пристрої; ▪ Підтримка функціоналу повернення до попередньої робочої конфігурації на пристроях, якщо під час інсталяції оновленої конфігурації виникли помилки; ▪ Підтримка функціоналу інсталяції оригінального конфігураційного файлу пристрою, що вийшов з ладу, на новий підмінний пристрій. – При роботі з Конфігураційними пакетами (templates) запропоноване рішення має забезпечувати: ▪ Формування конфігураційних пакетів (templates), які містять налаштування для пристроїв (profiles), що будуть знаходитись чи знаходяться під керуванням системи; ▪ Застосування цих конфігураційних пакетів до одного або декількох пристроїв одночасно; ▪ Імпорт та експорт цих конфігураційних пакетів між різними адміністративними доменами. – Запропоноване рішення має забезпечувати підтримку роботи зі сценаріями (scripts): ▪ Запуск CLI-based та TCL-based сценаріїв для змін у конфігураціях; ▪ Імпорт та експорт сценаріїв; ▪ Запуск сценаріїв у реальному часі та за розкладом. – Має забезпечуватися можливість групування пристроїв у системі для спрощення застосування однакових дій для декількох пристроїв одночасно (виконання сценаріїв, оновлення

		програмного забезпечення та застосування змін конфігурації, тощо); – Запропоноване рішення має надавати можливість обмеження одночасного конфігурування системи, а саме: ▪ Обмеження одночасного конфігурування системи різними адміністраторами для того, щоб не виникало конфліктів у конфігураційних файлах; ▪ Блокування одночасної зміни конфігурації (lock mode) декількома адміністраторами на рівні адміністративних доменів, конкретного пристрою, пакету політик безпеки, тощо; ▪ Режим розподілення обов'язків по конфігуруванню системи одним адміністратором та схвалення цих конфігурацій іншим адміністратором. – При роботі з глобальними політиками безпеки та об'єктами має забезпечуватися можливість: ▪ Створення глобальних пакетів політик безпеки, що містять правила безпеки (firewall policy) які можуть призначатись різним адміністративним доменам; ▪ Застосування пакетів політик безпеки як до фізичних, так і віртуальних пристроїв; ▪ Клонування пакетів політик безпеки; ▪ Створення глобальних об'єктів для політик безпеки які являють собою IP-адреси, мережі, сервіси, профілі безпеки, користувачі, пристрої, тощо та застосування цих глобальних об'єктів у політиках безпеки; ▪ Зіставлення для одного об'єкта (інтерфейс, мережа, тощо) унікальних значень, які він може приймати при використанні на різних пристроях (динамічні об'єкти); ▪ Пошук та видалення об'єктів, що не використовуються системою (unused objects); ▪ Пошук та об'єднання (merge) всіх об'єктів, які мають ідентичні значення (duplicate); ▪ Збереження поточного стану набору пакетів політик безпеки та об'єктів як резервної копії (revision); ▪ Порівняння та виявлення відмінностей між такими копіями; ▪ Завантаження попередньої копії у систему (revert); ▪ Налаштування автоматичного видалення старих копій (revision); ▪ Блокування (lock revision) певних копій (revision) від автоматичного видалення; ▪ Централізоване керування політиками безпеки, об'єктами та підключеннями VPN: централізоване налаштування та керування різними топологіями IPSec VPN (mesh, star, тощо).

		– Має забезпечуватися можливість відображення точного географічного розташування пристроїв на Google Maps шляхом введення координат або переміщенням на карті; – Має забезпечуватися можливість централізованого завантаження, зберігання та оновлення ПЗ, перевірка ліцензування, а також завантаження, зберігання та розповсюдження сигнатур та баз безпеки (antivirus, IPS, web-filtering, тощо) на пристроях, що знаходяться під керуванням. – Вимоги до функціоналу керування, налаштування та моніторингу: ▪ Керування через графічний веб-інтерфейс (Web GUI) з використанням HTTPS або CLI з використанням SSH-підключення; ▪ Конфігурування політик стійкості паролів (password policy) для локальних записів (local accounts); ▪ Автентифікація адміністраторів на основі локальної бази, LDAP, Raduis, Tacacs+, PKI; ▪ Централізоване керування, налаштування та моніторинг пристроїв мережевої безпеки (NGFW), мережевих комутаторів та бездротових точок доступу, що контролюються пристроями мережевої безпеки (NGFW); ▪ Моніторинг стану системи (status та health), часткою використаних апаратних ресурсів та використанням мережі (resource monitoring and network usage); ▪ Створення шаблонів політик для швидкого додавання нових пристроїв у систему керування; ▪ Статична маршрутизація; ▪ JavaScript Object Notation (JSON) API та eXtensible Markup Language (XML) API. – Вимоги до забезпечення резервного копіювання та відновлення системи (Backup та restore): ▪ Резервне копіювання конфігураційних файлів та системних баз на вимогу та за розкладом; ▪ Збереження/відновлення конфігураційних файлів та системних баз з використанням паролів; ▪ Збереження/відновлення конфігураційних файлів та системних баз на адміністративній станції або на мережевому сервері з використанням протоколів FTP, SCP, SFTP; ▪ Міграція конфігураційних файлів та системних баз с однієї апаратної платформи на іншу; ▪ Резервне копіювання та відновлення лог-файлів та звітів. – Вимоги до спостереження за роботою системи: ▪ Відображення стану системних завдань, що виконуються адміністраторами у системі;

		▪ Фільтрація серед списку цих завдань за статусом чи станом їх виконання; ▪ Відміна (delete) виконання певних завдань; ▪ Ведення журналу подій (event log) які виникають під час роботи системи; ▪ Відображення подій з заданим рівнем важливості (severity); ▪ Збереження журналу подій для подальшого аналізу; ▪ Фільтрація та пошук у журналі подій за різними критеріями. – Вимоги до можливостей процесу пошуку ти виявлення несправностей (troubleshooting): ▪ Відображення завантаження та використання основних апаратних елементів (cpu, memory, hdd, тощо) системи; ▪ Ведення crash log файлу для аналізу та виявлення неполадок з системою у разі її збою; ▪ Наявність packet sniffer для виявлення неполадок шляхом збору та аналізу мережевого трафіку; ▪ Перевірка та відновлення файлової системи; ▪ Перевірка та відновлення коректності бази даних системи. – Забезпечення можливості роботи з програмно-визначеними (SDN) архітектурами: ▪ Забезпечення централізованого розгортання, конфігурування та моніторингу SD-WAN; ▪ Забезпечення конфігурування SD-WAN як на рівні окремого пристрою так і на рівні адміністративного домену; ▪ На рівні адміністративного домену створення елементів конфігурації SD-WAN, що мають бути доступні кожному з пристроїв цього домену ▪ Конфігурування елементів SD-WAN, що мають бути доступні як фізичним, так і віртуальним пристроям; ▪ Формування та застосування конфігураційних пакетів SD-WAN (templates), які містять налаштування для мережевих пристроїв.
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою із показниками не гірше ніж 8x5xNBD (8 робочих годин, 5 днів на тиждень, заміна – Next Business Day) строком не менше ніж **1 рік**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт, електронною поштою або за телефоном для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ Можливість реєстрації сервісних випадків в режимі 24x7 в системі підтримки Виробника.

2.	Програмна продукція **Підсистеми оркестрування, автоматизації та реагування на інциденти безпеки** для забезпечення роботи не менш ніж 3 (три) аналітика строком дії не менше ніж 12 місяців.	**комплект**	**1**
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:		
	Загальні вимоги	– Якщо відповідно до функціональності запропонованого рішення або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки; – Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення; – На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника	
	Архітектура та форм-фактор	– Запропоноване рішення має мати можливість бути реалізовано у вигляді віртуалізованого або програмно-апаратного рішення; ▪ Якщо запропоноване рішення являє собою віртуальну машину, то вона буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником (заздалегідь має погоджуватися обсяг необхідних ресурсів); ▪ Якщо така система являє собою програмно-апаратний комплекс (ПАК), то всі елементи рішення мають бути у комплекті поставки; – Запропоноване рішення має забезпечувати відмовостійкість (high availability): ▪ Підтримка об'єднання декількох систем в один логічний кластер для відмовостійкості; ▪ Можливість створення Active/Active та Active/Passive кластеру.	
	Ліцензування	– Запропоноване рішення повинно бути ліцензоване для підтримки роботи не менше ніж 3 аналітиків та підтримувати збільшення кількості аналітиків, що будуть працювати у системі при додатковому ліцензуванні;	
	Функціональні вимоги	– Запропоноване рішення повинно забезпечувати можливість реалізації наступних процесів: ▪ Інтеграції з зовнішніми системами та існуючою інфраструктурою Замовника; ▪ Прийом сповіщень про підозрілу діяльність (alerts) з сторонніх систем; ▪ Розслідування інцидентів / фактичних порушень безпеки (incident investigation); ▪ Реагування на інциденти / фактичні порушення безпеки (incident responce)	

		▪ Автоматизацію робочого процесу роботи центру кіберзахисту; ▪ Надання звітності (reporting); ▪ Threat Intelligence Management. – Вимоги щодо складу запропонованого рішення відповідно до процесів: ▪ Інформаційні панелі системи (dashboards) ▪ Модуль взаємодії (workflow) аналітиків з сповіщеннями (alerts) та інцидентами (incidents) та реагування на них (incident response); ▪ Модуль інтеграції з зовнішніми системами (connectors); ▪ Модуль формування автоматизації (automation), що включає різнопланові сценарії реагування; ▪ Модуль звітності (reporting), що включає наявні звіти та дозволяє конфігурувати нові звіти; ▪ Модуль системних налаштувань (system settings).
	Вимоги до функціоналу інформаційних панелей	– Наявність попередньо налаштованих інформаційних панелей: Overview Dashboard, System Dashboard, Executive Dashboard, Analyst Dashboard та Admin Dashboard – Можливість створення власних інформаційних панелей; – Модифікація, клонування та імпорт/експорт інформаційних панелей; – Графічний конструктор інформаційних панелей (dashboard builder), який має забезпечувати можливість гнучко та легко створювати необхідні аналітику панелі; – Можливість використовувати інструментарій віджетів (widgets).
	Вимоги до модуля взаємодії (workflow) аналітиків	– Прийом сповіщень про підозрілу діяльність (alerts); – Набір інцидентів / фактичних порушень безпеки (incident); – Набір завдань, що здійснюються як аналітиком, так і автоматизованою реакцією при реагуванні на інциденти (tasks); – Набір записів/даних, що ідентифікують загрозу пов'язану з інцидентом (indicators); – Набір потенційно шкідливих електронних листів з заголовками (email); – База MITRE ATT&CK framework (тактик, прийомів та методів, що використовуються кіберзлочинцями); – Має забезпечуватися керування чергами завдань (Queue Management): ▪ Створення черг обробки сповіщень, інцидентів та завдань (alerts, incidents, tasks); ▪ Додавання членів команд та окремих аналітиків до обробки цих черг; ▪ Додавання сповіщень, інцидентів та завдань до цих черг вручну або автоматично (через playbook);

		▪ Перегляд призначень по чергам або по аналітикам / командам.
	Вимоги до модуля інтеграції з зовнішніми системами	– Інтеграція з сторонніми системами з використанням системних вбудованих конекторів (використовуючи API цих систем або стандартні протоколи - IMAP, Exchange, Syslog, тощо); – Отримання сповіщень про підозрілу діяльність від систем, що інтегруються; – Збагачення вже отриманих даних через конектори шляхом запиту додаткової інформації; – Збагачення даних в автоматичному режимі від систем, що інтегровані; – Збагачення даних від систем, що інтегровані за розкладом; – Збагачення даних від систем, що інтегровані з використанням встановлених на них add-on/plug-in; – Виконання автоматизованих дії на системах, що інтегровані через конектори; – Перегляд, пошук, встановлення, оновлення та видалення конекторів у системі; – Розробка власних конекторів (використовуючи SDK, Python); – Наявність разом з конекторами наборів автоматизованих дій (playbooks) для отримання даних з систем, що інтегруються; – Обов'язкова інтеграція з існуючим у замовника обладнанням: FortiGate, FortiAnalyzer, FortiMail; – Інтеграція з SIEM системами, наприклад: Splunk, IBM Qradar, ArcSight, FortiSIEM тощо; – Інтеграція з системами класу "ticketing system": JIRA, Zendesk, Foresight, Salesforce, ConnectWise Manage, RSA Archer, тощо
	Функції модуля формування автоматизації (сценаріїв реагування)	– Системний репозиторій сценаріїв реагування (playbooks) на інциденти безпеки; – Модифікація системних сценаріїв реагування; – Створення власних сценаріїв реагування на інциденти безпеки при виникненні певних умов; – Графічний конструктор сценаріїв реагування на інциденти безпеки, який дозволяє аналітикам створювати їх у стилі блок-схеми; – Сценарії реагування мають містити логіку прийняття рішень та багато типів кроків ▪ створити/оновити/видалити запис; ▪ виконати кроки прийняття рішення (decision, approval, manual input, тощо); ▪ виконайте дію певного конектора або фрагмент програмного коду; ▪ виконати інший playbook; ▪ надіслати повідомлення (через email або конектор); ▪ інше.

	Функції модуля звітності	– Створення різнопланових звітів; – Планувальник звітів (report scheduler), який регулярно запускає звіти; – Відправка запланованих (scheduled) звітів одержувачам електронною поштою (report notifications); – Збереження історії нещодавно запущених звітів (report history); – Графічний конструктор звітів, який має забезпечувати можливість гнучко та легко створювати звіти та підтримувати діаграми, показники, записи, коментарі, тощо.
	Функції Threat Intelligence	– Отримання інформації щодо загроз з сповіщень, завантажених файлів, поштових повідомлень та зовнішніх джерел аналізу загроз (TI). – Зберігання інформації щодо загроз у БД для використання іншими модулями системи. – Інтеграція з системами класу “threat intelligence” та репутаційними сервісами: McAfee TIE, Facebook Threat Exchange, Intel 471, Recorded Future, MISP, Darktrace, Anomali Threatstream, BluVector,VirusTotal, AbuseIPDB, Whois, тощо.
	Автентифікація та рольовий доступ	– Внутрішня автентифікація користувачів (internal), LDAP та SSO (SAML) – Двофакторна автентифікація (2FA) на основі SMS або токенів; – Надання аналітикам системи доступу до певних модулів/функцій системи на основі їх рольових дозволів (Role Based Access Control/ Role Permissions) – Наявність попередньо налаштованих (preconfigured) ролей у системі, щонайменше: Security Administrator, Application Administrator, Application User та Playbook Administrator; – Налаштування (customization) попередньо налаштованих ролей у системі; – Створення власних ролей; – Рольові дозволи (Role Permissions) мають включати можливість створення, читання, оновлення та видалення даних у модулях/функціях системи.
	Вимоги до супутніх послуг з інтеграції рішення в інфраструктуру Замовника	– Розробка цільової архітектури впроваджуваного рішення; – Розробка процесу. Process Design Document (PDD). SECURITY OPERATIONS. IRP/SOAR (включаючи PlayBook'и); – Розгортання комплексу; – Реалізація цільового процесу автоматизації розслідування та реагування; – Налаштування звітності та моніторинг роботи сервісу та метрік ефективності CSOC; – Передача знань за впровадженим рішенням; – Консультативний супровід на стадії поставки запропонованого рішення;

		– Консультування Замовника з виникаючих питань в процесі експлуатації.		
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою із показниками не гірше ніж 8x5xNBD (8 робочих годин, 5 днів на тиждень, заміна – Next Business Day) строком не менше ніж **1 рік**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт, електронною поштою або за телефоном для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ - Можливість реєстрації сервісних випадків в режимі 24x7 в системі підримки Виробника.		
3.	Програмна продукція **Підсистеми пошуку вразливостей в рамках циклу розробки програмного забезпечення /SDLC** для забезпечення роботи в не менш ніж 10 (десяти) одночасних проектах строком дії не менше ніж 12 місяців.		**комплект**	**1**
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:			
	Загальні вимоги	– Якщо відповідно до функціональності запропонованого рішення або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки; – Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення; – На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника		
	Вимоги до архітектури	– Запропоноване рішення повинно підтримувати зашифровану комунікацію між власними компонентами/модулями (за наявності); – Запропоноване рішення повинно зберігати результати сканування і оцінку активів в локальній базі даних для можливості підготовки звітів і відслідковування хронології змін. База даних запропонованого рішення має відповідати таким критеріям: ▪ забезпечувати відокремлене зберігання даних сканування у відокремлених сховищах в залежності від результату (типи вразливостей, груп ресурсів, тощо) при здійсненні аналізу, або запиту даних, для об'єднання результатів у будь-якій комбінації;		

		▪ забезпечити можливість зберігання журналів даних програмного забезпечення протягом визначеного та налаштованого терміну, після чого автоматично очищати базу даних (БД) від застарілої інформації. – Запропоноване рішення повинно забезпечувати просте, швидке масштабування за кількісними показниками та розширення функціоналу за необхідності; – Запропоноване рішення повинно зберігати результати сканування (отримані події, вразливості коду та ін.), не менше ніж 90 днів, при наявності доступного вільного простору на інфраструктурі Замовника, де воно буде розташоване. – Запропоноване рішення повинно забезпечувати підтримку веб-інтерфейсу через наступні браузери: Google Chrome – 62 або пізніша версія, Mozilla Firefox – 56 або пізніша версія. – Платформа повинна мати відкритий та задокументований API для інтеграції із іншими системами.
	Ліцензування	– Запропоноване рішення повинно включати усі необхідні ліцензії та підписки для забезпечення можливості сканування коду в не менш ніж 10 (десяти) одночасних проектах згідно зазначених даних технічних вимог.
	Функціональні вимоги	Вимоги до процесу сканування: – Запропоноване рішення повинно реалізовувати можливості: ▪ сканування вихідного коду без компіляції; ▪ сканування фрагментів вихідного коду, які неможливо скомпілювати в силу їх неповноти; ▪ інкрементальне сканування проектів (сканування тільки внесених після останнього сканування змін); ▪ в єдиному скануванні коду проекту, що містить код який - написаний на різних мовах програмування; ▪ можливість асинхронного сканування; ▪ можливість порівняння сканувань. – Запропоноване рішення повинно мати можливість запуску сканування за розкладом. – Запропоноване рішення повинно мати шаблон пошуку для кожної підтримуваної мови програмування та платформ. – Запропоноване рішення повинно відображувати знайдені помилки або вразливості шляхом виділення відповідних фрагментів тексту в коді. – Модуль сканування повинен встановлюватися, як мінімум, на операційну систему MS Windows. – Запропоноване рішення повинно дозволяти користувачам створення та використання власних типів перевірок під час сканування. – Запропоноване рішення повинно мати засоби мінімізації кількості спрацювань False Positives і False Negatives.

		– Вимоги до ідентифікації та керування вразливостями: – Запропоноване рішення повинно забезпечувати можливість перевірки відповідності кращим практикам (забезпечувати можливість контролю відповідності стандартам програмування за рахунок налаштувань запитів), включаючи: ▪ OWASP Top 10; ▪ PCI DSS; ▪ CWE. – Запропоноване рішення повинно забезпечувати можливість виявлення зв'язку між вразливостями; – Запропоноване рішення повинно забезпечувати можливість виконувати операції з вразливостями; – Запропоноване рішення повинно забезпечувати можливість класифікації виявлених вразливостей за типом та ступенем критичності; – Запропоноване рішення повинно надавати можливість візуалізації векторів потенційних атак; – Запропоноване рішення повинно забезпечувати можливість виявлення зв'язку між однотипними вразливостями; – Запропоноване рішення повинно мати можливість рекомендувати способи усунення виявлених вразливостей; – Запропоноване рішення повинно візуалізувати виявлені помилки і / або уразливості шляхом виділення відповідних фрагментів тексту в коді.
	Вимоги до технічних характеристик для забезпечення роботи з інфраструкту-рою Замовника	– Запропоноване рішення повинно підтримувати, як мінімум, наступні мови програмування для сканування: Java, J2SE, J2EE, JSP, JavaScript, VBScript, PL \ SQL, HTML5, .Net додаток C # та VB.Net (.Net Core, .Net Standard ASP.NET з можливістю підтримки .NET Framework версії не нижче 4.7.2), JavaScript, PL \ SQL, HTML5, SP, JavaScript, VBScript, PL \ SQL, HTML5, Python, C / C ++: C / C ++, PHP, JavaScript, Java, Kotlin, Objective-C.
	Візуалізація даних та звітність	– Запропоноване рішення повинно мати вбудований набір панелей для візуалізації даних (Інформаційні панелі даних або аналогічне), які повинні: ▪ мати функцію автоматичного оновлення даних, що на них відображені; ▪ надавати можливість перегляду результатів сканування та сортування даних по щонайменше за датою сканування, датою завершення сканування, назвою проекту або оцінкою рівня ризику. – Запропоноване рішення повинно надавати звітність по всім скануванням в одному інтерфейсі різного ступеню деталізації; – У звіті повинно надавати можливість переходу за посиланням на розгорнуту інформацію про вразливості, які було знайдено;

		– Запропоноване рішення повинно мати можливість порівняння звітів одного і того ж проекту; – Запропоноване рішення повинно мати засоби для створення звітів по задачам та проектам; – Запропоноване рішення повинно мати можливість отримувати звіти у наступних форматах: ▪ Xml; ▪ Rtf; ▪ Pdf.
	Можливості інтеграції	– Запропоноване рішення повинно мати плагіни, як мінімум, до наступних інтегрованих середовищ розробки (IDE): Eclipse, Visual Studio, IntelliJ. – Запропоноване рішення повинно мати можливість інтеграції з, як мінімум, такими інструментами автоматизації процесу складання програмного продукту: Apache Ant, Maven, Gradle. – Запропоноване рішення повинно підтримувати репозиторії вихідного коду, як мінімум: TFS, SVN, GIT. – Запропоноване рішення повинно підтримувати сервера збірки, як мінімум: GitLab, Jenkins, Bamboo. – Запропоноване рішення повинно мати можливість інтеграції з дефект-трекінг системою Atlassian Jira.
	Автентифікація та рольовий доступ	– Запропоноване рішення повинно інтегруватися із стороннім ПЗ служби каталогів (LDAP, AD) для забезпечення автентентифікації та авторизації внутрішніх користувачів; – ПЗ має підтримувати чітке розподілення на основі ролей та прав доступу користувачів, надаючи, або забороняючи наступне: ▪ здійснення будь-якого сканування; ▪ керування обліковими записами користувачів; ▪ доступ до перегляду даних про вразливості; ▪ створення і спільне використання списків проектів; ▪ можливість створювати оповіщення; ▪ можливість видалення проектів та сканувань ▪ створення і спільне використання політик сканування.
	Вимоги до супутніх послуг з інтеграції рішення в інфраструктуру Замовника	– Аудит існуючого процесу пошуку вразливостей в рамках циклу розробки програмного забезпечення: ▪ документування поточного процесу управління поставками ПЗ; ▪ визначення місця процедури сканування в процесі поставки ПЗ; ▪ визначення відповідального за процедуру сканування коду. – Розробка цільової архітектури впроваджуваного рішення (за необхідності внесення змін до існуючої архітектури у Замовника);

		– Розробка процесу. Process Design Document (PDD). Automation. DecSecOps. (включаючи PlayBook'и та інструкції по роботі з результатами сканування); – Розгортання комплексу; – Реалізація цільового процесу в рамках впроваджуваного рішення; – Передача знань за впровадженим рішенням: ▪ навчання роботі з платформою відповідальних за сканування співробітників; ▪ проведення тестових сканувань і практичне відпрацювання інструкцій. – Консультативний супровід на стадії поставки запропонованого рішення; – Консультування Замовника з виникаючих питань в процесі експлуатації.
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **1 рік**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт або електронною поштою для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ Можливість реєстрації сервісних випадків в режимі 24x7 в системі підтримки Виробника.
4.	Програмна продукція **Підсистеми моніторингу IT-сервісів** у складі: **- примірник програмної продукції** для забезпечення моніторингу IT-сервісів, що розміщені в інфраструктурі із загальним обсягом оперативної пам'яті не менш ніж 384 GB строком дії не менше ніж 12 місяців – **1 комплект**; **- примірник програмної продукції** для забезпечення контролю якості взаємодії користувачів із IT сервісами та моніторингу не менш ніж 1 000 000 сесій реальних користувачів строком дії не менше ніж 12 місяців – **1 комплект**;	
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:	
	Загальні вимоги	– Якщо відповідно до функціональності пристроїв/ систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки; – Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення; – На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника

	Архітектура та форм-фактор	– Запропоноване рішення має мати можливість бути реалізовано у вигляді віртуалізованого або програмно-апаратного рішення; ▪ Якщо запропоноване рішення являє собою віртуальну машину, то вона буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником (заздалегідь має погоджуватися обсяг необхідних ресурсів); ▪ Якщо така система являє собою програмно-апаратний комплекс (ПАК), то всі елементи рішення мають бути у комплекті поставки; – Запропоноване рішення має забезпечувати відмовостійкість (high availability): ▪ Підтримка об'єднання декількох систем в один логічний кластер для відмовостійкості; ▪ Можливість створення Active/Active та Active/Passive кластеру.
	Ліцензування	– Запропоноване рішення повинно бути ліцензоване для підтримки роботи не менше ніж 3 аналітиків та підтримувати збільшення кількості аналітиків, що будуть працювати у системі при додатковому ліцензуванні;
	Функціональні вимоги	– Має забезпечувати моніторинг взаємодії користувачів із IT сервісом через наступні канали: веб, мобільна версія сайту, мобільний застосунок; – Запропоноване рішення повинно мати вбудований механізм автоматичного виявлення всіх компонентів сервісу, та будувати зв'язки між ними через весь IT-стек: хости, процеси, сервіси і застосунки; – Запропоноване рішення повинно автоматично виявляти всі процеси, які виконуються на хості, незалежно від технології, яка використовується; – має автоматично інтегрувати метрики моніторингу застосунків, хостів, CPU, мережі, дискової підсистеми, віртуалізації, ЦОД в єдину модель даних; – Запропоноване рішення повинно збирати інформацію із лог-файлів та мати вбудований механізм для централізованого їх зберігання; – Запропоноване рішення повинно забезпечувати проактивний моніторинг роботи IT сервісу, із можливістю швидкого виявлення проблем, аналізу їх впливу на взаємодію користувачів із IT сервісом та інформування про причину такої проблеми; – Запропоноване рішення повинно мати вбудовані механізми пріоритезації проблем, в залежності від рівня їх впливу на роботу IT сервісу та взаємодії користувачів із ним – За рахунок вбудованих алгоритмів кореляції запропоноване рішення повинно виявляти причину(и) проблем в роботі IT сервісу;

		– має показувати всі операції між компонентами IT сервісу, а також взаємодію цих компонентів їх зовнішніми сервісами; – Запропоноване рішення повинно будувати графіки та звіти на базі даних, що зібрано під час моніторингу IT сервісу; – Запропоноване рішення повинно мати вбудований механізм автоматичного розрахунку «базової лінії» (baseline) для метрик моніторингу; – Запропоноване рішення повинно давати можливість створювати панелі моніторингу (dashboards) із різним рівнем доступу і деталізації даних; – Запропоноване рішення повинно автоматично визначати та візуалізувати топологію на рівні ЦОД, хостів, процесів, сервісів, застосунків; – Запропоноване рішення повинно мати функціональність автоматичної ідентифікації наявності Docker Farm на хості та автоматичної інсталяції в Docker-контейнери, що запускаються без модифікації скриптів завантаження контейнерів; – Запропоноване рішення повинно мати вбудовану функціональність моніторингу дій реальних користувачів у застосунках; – Запропоноване рішення повинно мати вбудовану функціональність виявлення та аналізу вразливостей програмних елементів застосунку; – Запропоноване рішення повинно аналізувати та виконувати пріоритизацію вразливостей в залежності від критичності впливу за допомогою штучного інтелекту; – Запропоноване рішення повинно мати вбудований механізм налаштування та моніторингу показників SLO; – Запропоноване рішення повинно автоматично будувати шлях проходження транзакції (синхронної і асинхронної) з розбивкою за часом, витраченому на кожному з компонентів, які брали участь в транзакції; – Запропоноване рішення повинно надавати дані про методи, класи або API в рамках всієї транзакції, за принципом end-to-end; – Запропоноване рішення повинно мати можливість об'єднувати розрізнені повідомлення про помилки в єдину сутність, з консолідованою інформацією про кореневі причини виникнення помилок, кількості користувачів, що постраждали від інциденту і проблемних компонентів IT сервісу додатків; – Запропоноване рішення повинно мати можливість візуального відтворювати процес розповсюдження проблеми по компонентам IT сервісу; – Запропоноване рішення повинно мати можливість ретроспективного аналізу проблеми з роботою сервісу з прив'язкою помилок і подій до часових проміжків і топології сервісів;

		– Запропоноване рішення повинно мати механізм автоматичного тегування об'єктів моніторингу; – Запропоноване рішення повинно мати вбудовану функціональність для централізованого збору та зберігання лог-файлів додатків з об'єктів моніторингу, з можливістю пошуку за подіями; – Запропоноване рішення повинно мати можливість надавати параметри методів і параметри SQL-запитів; – Запропоноване рішення повинно підтримувати автоматичний збір трейсів в Java у разі виявлення проблеми з продуктивністю компонентів додатку; – Запропоноване рішення повинно мати вбудовані механізми очищення, деперсоналізації і маскування чутливих даних, які можуть бути зібрані в процесі моніторингу; – Запропоноване рішення повинно мати можливість побудови звітів про доступність сервісів; – Запропоноване рішення повинно підтримувати можливість відправки звітів про стан сервісу за розкладом; – Запропоноване рішення повинно мати можливість графічного зображення даних компонентів моніторингу в режимі реального часу; – Запропоноване рішення повинно підтримувати функціональність створення довільно налаштованих графічних зображень даних моніторингу; – Запропоноване рішення повинно мати можливість організації рольового доступу до замаскованих даних, що зібрані в процесі моніторингу; – Запропоноване рішення повинно надавати деталізований доступ до інтерфейсу, з можливістю налаштування прав користування для кожної з ролей та для кожного із компонентів;
	Вимоги до архітектури	– Запропоноване рішення повинно мати єдиний веб-інтерфейс для взаємодії з усіма її компонентами і функціями; – Запропоноване рішення не повинно встановлювати більше одного агента на хост, моніторинг якого вона здійснює; – Агент моніторингу повинен бути універсальним для всіх технологій Замовника і однією інсталяцією має встановлювати всі необхідні компоненти IT сервісу: мережева взаємодія, ОС, лог-файли, процеси, служби, транзакції, застосунки, дії користувачів; – Агенти відразу після встановлення мають автоматично визначати які служби і процеси запущені на хості, визначити взаємозв'язки між ними і почати виконувати їх моніторинг; – Запропоноване рішення повинно містити механізми штучного інтелекту, що автоматично знаходять компоненти, що

		викликають проблеми та ідентифікують першопричини їх виникнення; – Запропоноване рішення повинно мати власний мобільний застосунок з функцією push для повідомлень у разі виникнення проблем; – Агент повинен мати можливість автоматично визначати такі типи змін в додатку: перезапуск процесу, новий реліз, зміна файлів релізу; – Агент повинен виконувати читання записів з журналів подій додатків, служб або процесів на тому хості, на якому він встановлений; – Управління, оновлення, чи зміна конфігурацій агентів має відбуватися централізовано з основного інтерфейсу управління, без необхідності будь-яких дій на хостах моніторингу; – Запропоноване рішення повинно підтримувати інтеграцію з системами рівня ServiceDesk для автоматичного відкриття / модифікації / закриття інцидентів; – Оновлення системи мають встановлюватися автоматично; – Запропоноване рішення повинно підтримувати роботу в кластері для високої доступності та балансування навантаження даних від агента; – Робота в режимі високої доступності має будуватися виключна за принципом active-active та будуватися виключно на вбудованих механізмах в середині системи, без необхідності використання чи конфігурування будь-якого стороннього ПЗ; – Запропоноване рішення повинно використовувати власну сховище для зберігання всіх даних моніторингу, без використання будь-якого стороннього ПЗ; – Платформа повинна мати відкритий та задокументований API для інтеграції із іншими системами.
	Вимоги до технічних характеристик для забезпечення роботи з інфраструкту-рою Замовника	– Агент має підтримувати моніторинг веб-серверів MS IIS, NGNIX та Apache HTTP; – Агент має підтримувати можливість автоматичної інструментації застосунків без необхідності змін на рівні коду застосунків; – Агент має підтримувати моніторинг застосунків на Java; – Запропоноване рішення повинно підтримувати збір даних щодо стану хостів віртуалізації безпосередньо з Vmware vCenter; – Запропоноване рішення повинно ідентифікувати помилки javascript з деталізацією до рівня опису помилки та можливістю аналізу minifield файлів в веб-інтерфейсі; – Запропоноване рішення повинно підтримувати моніторинг баз даних Oracle та MySQL; – Агент моніторингу має автоматично збирати дані про стан хоста Docker;

		– Агент моніторингу має автоматично виявляти контейнери, що запускаються на хості Docker та автоматично виконувати інструментацію об'єктів всередині контейнера, без будь-яких додаткових конфігурації на хості Docker; – Агенти моніторингу мають автоматично встановлюватись в нові Docker контейнери, що запускаються на хості Docker, без будь-яких додаткових конфігурацій чи скриптів в середовищі Docker; – Моніторинг сервісів застосунка, що виконуються в контейнерах Docker повинен реалізовуватись без необхідності запуску додаткових контейнерів в цьому середовищі; – Моніторинг Kubernetes/OpenShift кластеру повинен бути реалізований за допомоги універсального агенту без додаткової конфігурації кластеру та без змін на рівні застосунку; – Можливість збору та візуалізації додаткових даних з Kubernetes/OpenShift та Docker за допомоги API; – Запропоноване рішення повинно підтримувати моніторинг Docker for Windows та Docker for Linux; – Запропоноване рішення повинно підтримувати автоматичний збір трейсів з Java, Golang, Node.js, PHP в разі виникнення проблеми в роботі компонента IT сервісу; – Агент моніторингу має працювати на ОС Windows та Linux; – Агент моніторингу має підтримувати моніторинг компонентів на Golang, .Net та ASP.NET, Java, PHP; – Агент моніторингу має підтримувати автоматичну інсталяцію агентів в контейнерних середовищах на Docker, CRIO, Garden; – Запропоноване рішення повинно повинна ідентифікувати користувачів у сесіях, якщо вони пройшли ідентифікацію в застосунку; – Функціональність моніторингу дій реальних користувачів повинна реалізовуватись через технологію javascript, без необхідності використання даних мережевого трафіку; – Запропоноване рішення повинно мати можливість діставати бізнес-метрики із технологічних транзакцій. – Запропоноване рішення повинно підтримувати автоматичне додавання агенту javascript у веб-сторінку застосунку для моніторингу дій реальних користувачів; – Автоматичне додавання агенту javascript у веб-сторінку повинно підтримуватись для Java, Node.js, Apache HTTP Server, MS IIS, NGINX; – Автоматичне додавання агенту javascipit для технології Apache не повинно потребувати ручної зміни чи конфігурації налаштувань httpd.conf та/або ручного створення додаткових файлів конфігурацій Apache; – - Автоматичне додавання агенту javascript для технології NGNIX не повинно потребувати додаткових змін чи конфігурації модулів NGNIX.

	Вимоги до моніторингу і контролю якості взаємодії користувачів із IT сервісами	– Запропоноване рішення повинно мати вбудований механізм запису та емуляції дій користувачів у застосунку; – Запропоноване рішення повинно мати механізм моніторингу дій реальних користувачів у застосунку; – В запропонованому рішенні має бути передбачений механізм повного візуального відтворення сесій реальних користувачів на веб-сайті, із можливістю покрокового аналізу кожної дії; – Запропоноване рішення повинно мати можливість візуального відтворення сесій кожного окремого користувача в додатку; – Моніторинг дій реальних користувачів у застосунку має включати логування всіх дій користувача під час його сесії, із прив'язкою до часу цієї дії та технологічними транзакціями, що виникли після цієї дії між компонентами IT сервісу; – Запропоноване рішення повинно мати можливість ідентифікації сесій окремих користувачів використовуючи їх унікальні ідентифікатори під час моніторингу користувачів; – Запропоноване рішення повинно мати можливість аналізувати дії користувачів в мобільних додатках iOS і Android; – Запропоноване рішення повинно мати вбудовану функцію штучних перевірок доступності веб-додатків, з можливістю запису послідовності дій і подальшого періодичного відтворення операцій користувачів в інтерфейсі; – Запропоноване рішення повинно виявляти гнівні кліки незадоволених користувачів у веб-застосунку; – Запропоноване рішення повинно мати вбудований алгоритм скорінгу дій користувача: в залежності від його досвіду взаємодії із застосунком. – Всі дані дій користувачів мають зберігатися в інфраструктурі Замовника;
	Вимоги до супутніх послуг з інтеграції рішення в інфраструктуру Замовника	– Аудит існуючого процесу моніторингу IT-сервісів та контролю якості взаємодії користувачів із IT сервісами; – Розробка цільової архітектури впроваджуваного рішення (за необхідності внесення змін до існуючої архітектури у Замовника); – Розробка процесу. Process Design Document (PDD). Performance. APM (включаючи PlayBook'и): Сбір інформації про середовище моніторингу; розробка моделі зон відповідальності; розробка процесу реакції на інцидент(play book); опис принципів роботи з групами нотифікацій. – Реалізація цільового процесу в рамках впроваджуваного рішення: ▪ Інсталяція додаткових компонентів платформи; ▪ Конфігурація параметрів системи.; ▪ Встановлення додаткових агентів; ▪ Налаштування механізму визначення додатків; ▪ Налаштування моніторингу fron-end технологій;

		▪ Налаштування функціонлу Session Replay; ▪ Налаштування політик безпеки; ▪ Налаштування функціонлу Synthetic monitoring; ▪ Створення групп нотифікацій; ▪ Налаштування правил нотфікацій. Підключення каналів нотифікацій. ▪ Налаштування мобільного додатку; ▪ Налаштування функціоналу SLO Monitoring. – Передача знань за впровадженим рішенням; – Консультативний супровід на стадії поставки запропонованого рішення; – Консультування Замовника з виникаючих питань в процесі експлуатації.		
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **1 рік**, що включає: ▪ можливість оновлення та модернізації програмного забезпечення за допомогою автоматичних завантажень із серверів Виробника, не рідше ніж 1 раз на місяць; ▪ Інтернет-доступ до документації та технічних ресурсів, бази знань на офіційному веб-сайті компанії Виробника (розробника), при чому всі його загальнодоступні сторінки мають бути відкритими для користувачів із України; ▪ дистанційну підтримку від Виробника (розробника) за допомогою телефону чи Інтернет з необмеженою кількістю заявок; ▪ Постійний (24x7) доступ для від1C25 9205 CD22 CE48 DFAA F6F2 E624 EFF5 F1A3 A9BСкриття заявок на надання технічної підтримки в персональному кабінеті, закріпленого за Замовником на офіційному веб-сайті компанії Виробника (розробника) програмного забезпечення віртуалізації; ▪ сервіс, що пропонується, не повинен залежати від Виробника інфраструктури (від наявності підтримки), на якій буде встановлено та працюватиме запропоноване рішення (у випадку програмної продукції); ▪ гарантований час первинної реакції на звернення рівня Critical в рамках критичної проблеми має бути не більше 4 (чотирьох) годин;		
5.	Програмна продукція **Підсистеми моніторингу та контролю дій привілейованих користувачів** для забезпечення одночасної роботи з відповідними контрольованими (цільовими) системами не менш ніж 20 (двадцять) привілейованих користувачів в межах існуючої у Замовника інсталяції строком дії не менше ніж 12 місяців.		**комплект**	**1**
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:			

	Загальні вимоги	– Якщо відповідно до функціональності запропонованого рішення або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки; – Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення; – На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника
	Вимоги до архітектури	– Запропоноване рішення повинно поставлятися від одного виробника у вигляді програмно-апаратного комплексу або у вигляді віртуального пристрою та повинно бути виконаним у вигляді єдиної платформи, що не потребує використання будь-якого стороннього системного або прикладного програмного забезпечення (операційних систем, програмних додатків, систем керування базами даних тощо) для його впровадження; – Запропоноване рішення має включати всі необхідні компоненти для побудови комплексу технічних засобів та програмного забезпечення (далі КТЗ) з високою доступністю: забезпечувати функціонування комплексу в цілому при виході з ладу будь-якого компонента, за рахунок механізмів автоматичного балансування навантаження та побудови кластеру(ів) високої доступності; – Запропоноване рішення має забезпечувати можливість розгортання КТЗ як на базі апаратних серверів так і у віртуальному середовищі VMware або Hyper-V поточних (підтримуваних виробником) версій; – Під час роботи, рішення повинно бути захищено від впливу інших систем, включаючи зміни та оновлення. – Запропоноване рішення повинно мати вбудований механізм захисту від несанкціонованого доступу до інформації що зберігається у КТЗ. Даний захист повинен забезпечувати використання спеціального ключа захисту (пароля або апаратного ключа) під час кожного запуску КТЗ (після вимкнення або перезавантаження). – Запропоноване рішення має забезпечувати вбудоване захищене сховище для збереження записаних сесій привілейованих користувачів, реквізитів доступу (логін, пароль, ключі, доменні імена тощо) до КТЗ і цільових систем, журналів подій. – Запропоноване рішення має забезпечувати можливість розгортання КТЗ без необхідності інтеграції з корпоративною службою каталогів (AD), тобто забезпечувати функціонування компонент КТЗ незалежно від функціонування корпоративного каталогу.

		– Запропоноване рішення має забезпечувати наявність окремого веб-порталу або додатку для налаштування та адміністрування. – Запропоноване рішення має забезпечувати можливість створення відмовостійких конфігурацій КТЗ на базі вбудованих технологій, використання сторонніх (зовнішніх) засобів для побудови таких (відмово стійких) конфігурацій – не допускається. – Запропоноване рішення має забезпечувати можливість створення резервних копій що мають включати в себе всі параметри та налаштування КТЗ, а також записані сесії привілейованих користувачів. Резервні копії мають створюватися з використанням шифрованих (захищених) протоколів обміну даними (наприклад, на базі пари відкритого та приватного SSH ключа). Створені резервні копії повинні бути захищені від несанкціонованого перегляду даних що в них зберігаються та несанкціонованого відновлення. – Запропоноване рішення має забезпечувати підтримку розширених мережевих налаштувань для серверів КТЗ, що виконують такі функції: ▪ підтримка віртуальних мереж (VLAN); ▪ агрегація мережевих каналів; ▪ налаштування статичної маршрутизації для окремих мереж. – Запропоноване рішення має обов'язково забезпечувати можливість створення безпечних (шифрованих) каналів зв'язку на основі сертифікатів SSL між привілейованими користувачами і Системою та між Системою і цільовими системами. – Запропоноване рішення має забезпечувати можливість налаштування таких безпечних (шифрованих) каналів зв'язку по наступним параметрам: ▪ на основі само підписних сертифікатів (за допомогою пари «відкритий»-«приватний» ключі) ▪ на основі сертифікатів центру сертифікації (CA). – Схема кластеризації повинна надавати можливість взаємодії користувачів та інтеграцію в режимі Active-Active для всіх вузлів кластеру. – Записи привілейованих сесій не мають зберігатись у форматі відео або знімків екрану. – Рішення повинно записувати файли, що передаються через SFTP або буфер обміну в RDP підключеннях з можливістю відновлення їх у початковому вигляді. – Запропоноване рішення повинно мати експертний висновок Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів з технічного захисту інформації.
	Ліцензування	– Запропоноване рішення повинно включати усі необхідні ліцензії та підписки для забезпечення можливості одночасної роботи з

		відповідними контрольованими (цільовими) системами не менш ніж 50 (п'ятдесяти) привілейованих користувачів.
	Функціональні вимоги	– Запропоноване рішення має забезпечувати підтримку не менше двох одночасних систем зовнішньої автентифікації привілейованих користувачів та адміністраторів Системи – серверів служби каталогів користувачів AD та LDAP; – Запропоноване рішення має забезпечувати можливість задавати пріоритет використання кожного серверу каталогу користувачів (AD або LDAP), по відношенню до інших таких серверів; – Запропоноване рішення має забезпечувати можливість налаштування наступних параметрів пошуку користувачів у службах каталогів користувачів: ▪ ім'я та пароль користувача що має доступ на читання груп користувачів на сервері каталогу користувачів AD та LDAP; ▪ організаційна група (OU) в каталозі користувачів в якій потрібно шукати привілейованих користувачів; ▪ адресу (FQDN або IP) та порт серверу каталогу користувачів; ▪ можливість використання шифрованого (безпечного) з'єднання за допомогою сертифікатів. – Запропоноване рішення має забезпечити можливість включення/виключення доступу до буфера обміну на основі параметрів: ▪ час підключення; ▪ членство користувача в групі AD; ▪ IP-адреса робочої станції користувачів чи кінцевого сервера підключення. – Запропоноване рішення має забезпечувати можливість використання облікових записів з паролями для підключення до цільових систем що зберігаються в сторонніх (зовнішніх) сховищах паролів. – Запропоноване рішення має забезпечувати автоматичне надання окремим групам привілейованих користувачів доступу до пулу цільових систем на базі заданої групи на сервері каталогу користувачів (AD або LDAP). – Запропоноване рішення має забезпечувати веб-портал(-и) для доступу до контрольованих (цільових) систем. Використання даного порталу повинно бути опціональним (не обов'язковим), тобто КТЗ повинна забезпечувати доступ до контрольованих (цільових) систем в тому числі й без такого порталу (за допомогою використання спеціалізованих додатків: Putty, Kitty, SecureCRT, Windows RDP client, Royal TSX на Mac OS X, тощо). – Кожен веб-портал для привілейованих користувачів повинен надавати привілейованим користувачам наступні можливості: ▪ перелік доступних для підключення цільових систем з можливістю відкриття сесій за допомогою стандартних клієнтів (для RDP, VNC та SSH протоколів);

		▪ перелік адрес (FQDN або IP) цільових систем; ▪ тип протоколу що використовується для підключення до цільової системи; ▪ перегляд паролю до цільової системи (в разі якщо такі права надані привілейованому користувачу відповідною парольною політикою). – Запропоноване рішення має забезпечувати можливість додавання привілейованих користувачів такими способами: ▪ в ручному режимі; ▪ синхронізація з існуючого каталогу користувачів (AD/LDAP); – Для кожного облікового запису привілейованого користувача повинна бути підтримка одночасно кількох способів автентифікації, щонайменше: ▪ за допомогою статичного паролю що зберігається в захищеному сховищі Системи; ▪ одноразового паролю що генерується зовнішніми сервісами (наприклад, RADIUS-сервером); ▪ за допомогою зовнішнього каталогу користувачів (AD/LDAP); ▪ за допомогою SSH ключа; – Запропоноване рішення має забезпечувати функціональність додавання цільових систем, в процесі чого мають підтримуватися наступні можливості: ▪ додавання цільових серверів по одному (за IP-адресою або FQDN, мережевою маскою та портом); ▪ групового додавання цільових систем (за допомогою мережевої маски накладеної на діапазон IP-адрес). – Запропоноване рішення має забезпечувати роботу з цільовими системами, автентифікація привілейованих користувачів на яких виконується наступним чином: ▪ за допомогою введення локального облікового запису; ▪ за допомогою введення доменного облікового запису; ▪ за допомогою SSH-ключа. – Запропоноване рішення має забезпечувати наступні можливості роботи з реквізитами доступу (логіни, паролі, ім'я домену, ключі SSH тощо) що використовуються привілейованими користувачами для підключення до цільових систем: ▪ ручне створення та збереження реквізитів доступу в захищеному сховищі Системи; ▪ використання зовнішніх систем автентифікації (в тому числі – зовнішніх спеціалізованих сховищ паролів); – Запропоноване рішення має забезпечувати функціонал додаткової (повторної) примусової автентифікації на цільових системах навіть в разі якщо реквізити доступу привілейованих

		користувачів на Систему та на цільових системах повністю співпадають. – Запропоноване рішення має забезпечувати можливість примусової зміни паролів на окремих цільових системах за заданою парольною політикою для окремо заданих облікових записів привілейованих користувачів. Така парольна політика повинна забезпечувати можливості управління вимогами до: ▪ довжини паролю; ▪ складності паролю (в тому числі, вимоги до великих літер, цифрових символів, спеціальних символів); ▪ частоти зміни паролю. – Примусова зміна паролів відповідно до заданої парольної політики повинна підтримуватися щонайменше на таких цільових системах: ▪ Unix/Linux-based операційні системи (через SSH); ▪ Windows операційні системи (через WMI); – Запропоноване рішення має забезпечувати функціональність керування різноманітними об'єктами такими як користувачі, цільові системи, способи підключення як локально (за допомогою веб-порталу) так й віддалено (за допомогою відкритих API-інтерфейсів). – Запропоноване рішення має забезпечувати можливість вибору нумерації портів по яким підключаються привілейовані користувачі та портів по яким виконується підключення до цільових систем, тобто, адміністратор Системи повинен мати можливість примусової зміни портів підключення для привілейованих користувачів для кожної окремої або групи цільових систем.
	Функціонал контролю привілейованих користувачів	– Запропоноване рішення має забезпечувати запис дій привілейованих користувачів вбудованими засобами без необхідності встановлення буд-якого компоненту (агенту, сервісу, драйверу тощо) як на кінцеві робочі точки привілейованих користувачів, так й на системи до яких підключаються привілейовані користувачі (цільові системи). – Запропоноване рішення має забезпечувати можливість підтвердження незмінності записаних сесій привілейованих користувачів за допомогою спеціалізованих ключів/сертифікатів від довірених постачальників таких ключів/сертифікатів. – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу RDP, в тому числі – в режимах Enhanced RDP Security (TLS), SSH, Telnet, VNC. – Запропоноване рішення має забезпечувати можливість роботи зі стандартом X11 через протокол SSH, в тому числі – можливість відтворення графіки через X11.

		– Запропоноване рішення має забезпечувати можливість примусового обмеження чи запису файлових операцій (заборону протоколів файлового обміну SFTP та SCP). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколу Telnet у вигляді відеозапису або текстового журналу дій (команд користувача та відповідей цільової системи на такі команди). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколу RDP, SSH (або X11), VNC у вигляді відеозапису, та забезпечувати можливість: ▪ перегляду відеозаписів вбудованими засобами; ▪ експорту збережених відеоматеріалів (відеозаписів) в зовнішні відео формати в AVI або WEBM форматі, з заданою роздільною здатністю. – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу HTTP та HTTPS (з підтримкою стандартів SSLv2 та SSLv3). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколам HTTP та HTTPS у вигляді записаного текстового журналу дій (методи передачі даних POST/GET, посилання URL, контент (крім конфіденційних даних), відповіді серверів, дані cookies тощо). – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем по протоколу ICA (з підтримкою стандартів SSLv2 та SSLv3). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколу ICA у вигляді відеозапису або текстового журналу дій (команд користувача та відповідей цільової системи на такі команди). ПЗ має забезпечувати можливість експорту збережених текстових журналів в зовнішні формати з текстовою структурою. – Запропоноване рішення має забезпечувати контроль привілейованих користувачів що підключаються до цільових систем для роботи з додатками, які використовують службові протоколи підключення до MS SQL (з підтримкою стандартів TDS - Tabular Data Stream). – Запропоноване рішення має забезпечувати запис дій привілейованих користувачів що підключаються до цільових систем по протоколам MS SQL у вигляді текстового журналу дій

		(команд користувача та відповідей цільової системи на такі команди). – Запропоноване рішення має забезпечувати можливість створення політик щодо команд які вводять привілейовані користувачі під час роботи з цільовими системами. ПЗ має забезпечувати підтримку синтаксису регулярних виразів на базі PCRE. – Запропоноване рішення має забезпечувати можливість налаштування щонайменше наступних правил реагування на спрацювання таких політик: повідомлення відповідальної особи, роз'єднання сесії. – Запропоноване рішення має забезпечувати можливість створення політик щодо часових інтервалів в які привілейовані користувачі мають можливість доступу до цільових систем. – Запропоноване рішення має забезпечувати можливість налаштування щонайменше наступних правил для таких політик: дні тижня в які привілейовані користувачі можуть підключатися до цільових систем, час коли привілейовані користувачі можуть підключатися до цільових систем, інтервал дії такої політики (з вказівкою початкових та кінцевих дат та часу). – Запропоноване рішення має забезпечувати можливість примусового запиту причини підключення до цільової системи привілейованим користувачем з відображенням відповідного поля для відповіді користувача. – Запропоноване рішення має забезпечувати можливість повідомлення зацікавлених сторін, якщо під час сеансу виявлено нетипову поведінку користувача – Запропоноване рішення має забезпечувати можливість налаштування додаткового підтвердження (схвалення) підключення до цільової системи привілейованих користувачів збоку адміністратора цільової системи. – Запропоноване рішення має забезпечувати можливість налаштування відправки повідомлень за допомогою каналів електронного зв'язку (email) адміністратора цільової системи щодо дії привілейованих користувачів (підключення до цільової системи, відключення від цільової системи, приєднання до сесії іншої особи, спрацювання заданої політики). – Запропоноване рішення має забезпечувати можливість повного примусового припинення роботи сесій привілейованих користувачів відповідальними особами в режимі реального часу. Також ПЗ має забезпечувати можливість налаштування блокувати обліковий запис привілейованого користувача сесія якого припиняється, одночасно з припиненням сесії привілейованого користувача.
	Візуалізація даних та звітність	– Запропоноване рішення має забезпечувати функціональність перегляду активних сеансів в режимі реального часу з можливістю його переривання.

		– Запропоноване рішення має забезпечувати вбудований фунціонал збереження та обробки подій в вигляді журналів що зберігаються в захищеному сховищі. Всі журнали подій повинні бути захищені від видалення, в тому числі адміністраторами Системи з найвищими рівнями доступу (правами). Журнали подій повинні включати щонайменше наступну інформацію: ▪ події пов'язані з працездатністю КТЗ (в тому числі – журнали налагоджувань); ▪ події пов'язані з роботою привілейованих користувачів на цільових системах; ▪ події пов'язані з адмініструванням КТЗ. – Запропоноване рішення має забезпечувати функціональність автоматичної передачі таких подій в зовнішні системи обробки подій в реальному часі за допомогою стандартних протоколів, таких як syslog, тощо. – Запропоноване рішення має забезпечувати можливість експорту повного або часткового журналу подій в зовнішній файл текстового формату. Частковий експорт повинен здійснюватися за різноманітними критеріями, за такими як обліковий запис привілейованого користувача(-ів), тип події, ім'я цільової системи, дата тощо. – Запропоноване рішення має забезпечувати вбудовані механізми перегляду результатів дій привілейованих користувачів, а саме – перегляд записаних сесій, команд що вводилися та відповідей цільової системи на такі команди. Перегляд результатів повинен забезпечуватися в веб-порталі адміністрування без необхідності встановлення буд-яких засобів (програмних додатків, плагінів тощо). – Запропоноване рішення має забезпечувати наявність вбудованих фільтрів пошуку результатів дій привілейованих користувачів за різноманітними критеріями, щонайменше за ім'ям привілейованого користувача або користувачів, введеними командами, типом протоколу, ім'ям цільової системи, а також в заданому діапазоні дат. – Запропоноване рішення має забезпечувати можливість створення звітів на базі отриманих результатів за заданими фільтрами. Такі звіти повинні мати можливість бути експортовано в вигляді файлів формату не меньше ніж: CSV форматі. – Запропоноване рішення має забезпечувати можливість перегляду відповідальними особами сесій привілейованих користувачів в режимі реального часу без будь-якого явного інформування привілейованих користувачів під час такого перегляду. Додатково має забезпечуватися можливість надавати відповідальній особі інформацію щодо сесії: ім'я та IP-адресу

		цільової системи, ім'я привілейованого користувача, тип протоколу що використовується, час початку сесії.
	Можливості інтеграції	– Запропоноване рішення має мати можливість інтеграції з іншими системами, в тому числі: CyberArk, Lieberman, Duo, Inwebo, Okta, Splunk, YubiKey, TPAM, ServiceNow, Remedy, Azure MFA, Azure AD, Azure KeyVault, AWS SecretsManagerVault, HashiCorpVault, Jenkins, Kubernetes. – Запропоноване рішення повинно мати інтерфейс для автоматизованого запиту паролей та доступу через REST API.
	Атентифікація та рольовий доступ	– Запропоноване рішення має забезпечувати рольову модель керування та нагляду за привілейованими користувачами. ПЗ має підтримувати наступні розмежування прав на базі різних облікових записів: ▪ повні права адміністрування – в тому числі – можливість конфігурування Системи; ▪ частково обмежені права адміністрування – буд-які дії крім конфігурування Системи; ▪ обмежені права адміністрування – можливість налаштувань та подальшого нагляду за конкретно заданими цільовими системами та привілейованими користувачами; ▪ права користувача - можливість тільки підключення до заданих цільових систем без можливості адміністрування (read only). – Запропоноване рішення має забезпечувати функціональність додавання адміністраторів з можливістю вибору ролі, строку дії облікового запису та способу автентифікації адміністратора. Для кожного облікового запису адміністратора повинна бути підтримка одночасно кількох способів автентифікації, щонайменше: ▪ за допомогою статичного паролю що зберігається в захищеному сховищі Продукту; ▪ за допомогою зовнішнього каталогу користувачів (AD/LDAP); ▪ за допомогою SSH ключа. – Повинна забезпечуватися підтримка аутентифікації користувачів через GSSAPI, Kerberos і Agent Forwarding в SSH сесіях. – Запропоноване рішення має забезпечувати можливість створення політик доступу на перегляд окремими привілейованими користувачами паролю(-ей) до цільових систем до яких вони підключаються, в разі якщо такий пароль їм невідомий. – - Запропоноване рішення має забезпечувати вбудовані механізми перегляду таких паролів за будь-який потрібний час (в минулому) в разі якщо вони (паролі) змінювались за допомогою відповідного функціоналу ПЗ (парольної політики).

	Вимоги до супутніх послуг з інтеграції рішення в інфраструктуру Замовника	– Аудит поточних процесів організації доступу привілейованих користувачів: ▪ доступ адміністраторів; ▪ доступ зовнішніх підрядників. – Розробка цільової архітектури впроваджуваного рішення (за необхідності внесення змін до існуючої архітектури у Замовника); – Розробка процесу. Process Design Document (PDD). SECURITY SERVICES. Privileged Access Management. (включаючи PlayBook'и та інструкції по підключенню для зовнішніх підрядників, внутрішніх адміністраторів та для співробітників, що відповідають за надання доступів). – Реалізація цільового процесу в рамках впроваджуваного рішення: ▪ Розгортання та налаштування системи контролю прівілейованого доступу; ▪ Побудова «єдиного сейфа» паролів для технічних облікових записів всіх критичних об'єктів інфраструктури; ▪ Налаштування порталу запиту доступу для зовнішніх підрядників; ▪ Визначення відповідального співробітника в процесі узгодження доступу; ▪ Заведення всіх наявних систем в Комплекс. – Передача знань за впровадженим рішенням; – Консультативний супровід на стадії поставки запропонованого рішення; – Консультування Замовника з виникаючих питань в процесі експлуатації.
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **1 рік**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт або електронною поштою для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ Можливість реєстрації сервісних випадків в режимі 24x7 в системі підтримки Виробника.
6.	Програмна продукція **Підсистеми адаптивної мережевої автоматизації** у складі: **- примірник програмної продукції** для забезпечення одночасної роботи не менше ніж 1 (одного) адміністратора строком дії не менше ніж 12 місяців – **1 комплект**; **- примірник програмної продукції** для забезпечення покриття не менш ніж 250 мережевих пристроїв включаючи функціональність Change management (або аналог згідно вимог) строком дії не менше ніж 12 місяців – **1 комплект**.	

	- примірник програмної продукції для забезпечення покриття не менш ніж 250 мережевих пристроїв включаючи функціональність Application Assurance (або аналог згідно вимог) строком дії не менше ніж 12 місяців – **1 комплект**.	
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:	
	Тип платформи	– Набір віртуальних машин, що розгортаються в середовищі віртуалізації VMWare vSphere з вимогами до апаратної частини не більше ніж: ▪ 8 ядер процесора; ▪ 32 ГБ оперативної пам'яті; ▪ - 500ГБ дискового простору (може змінюватися від глибини збереження історії).
	Архітектура системи	– Модульна; – З можливістю активувати модулі з необхідною функціональністю та подальшим розширенням за необхідності, як в частині збільшення покриття, так і функціональності;
	Функціональні вимоги	– Візуалізація і аналіз мережевих даних шляхом інтеграції з апаратним, програмним забезпеченням обладнання різних виробників, а також, з системами віртуалізації; – Запропоноване рішення повинно мати можливість масштабуватися в мережевих інфраструктурах операторського рівня на щонайменше 100 000 вузлах; – Динамічна візуалізація карти мережі у вигляді багаторівневої схеми з відображенням мережевих пристроїв, їх назв і атрибутів, а також, шляхів проходження трафіку через них, на підставі всебічного аналізу конфігурації всіх мережевих пристроїв. – При побудові шляху проходження трафіку від IP-адреси джерела до призначення, запропоноване рішення має вміти: ▪ додавати як L2 так і L3 пристрої до свого середовища; ▪ Виділяти асиметричну маршрутизацію між вихідним та зворотним трафіком; ▪ Конфігуруватися з урахування протоколів та портів; ▪ Дозволяти обирати для аналізу real-time або історичні дані із можливістю показу порівняння; ▪ Показувати шляхи проходження трафіку через традиційні мережі та мережі SDN. – Дозволяти виконувати автоматичний пошук пристроїв в мережі; – Забезпечувати можливість (на періодичній основі, інструмент планування) отримувати та аналізувати інформацію про конфігурацію з мережевих пристроїв для відображення логічних топологію мережі на різних рівнях (L2, L3, VPN тощо), включаючи MPLS, маршрутизацію, конфігурації VLAN, списки доступу тощо в залежності від поточних потреб адміністратора системи;

		– Підтримка забезпечення видимості наступних сегментів LAN, WAN, DC, SDN (SD-DC, SD-WAN), платформ віртуалізації та публічних хмар; – Можливість експорту карти мережі в зовнішні формати (як мінімум Microsoft Visio, Microsoft Word); – Можливість нанесення на карту мережі додаткової інформації; – Можливість створення runbook (послідовності дій) з певним і заданим переліком мережевого обладнання для вирішення певних завдань (наприклад, виконання певних команд на обладнанні зі збором результатів виконання); – Наявність готових шаблонів команд і наборів команд, класифікованих за призначенням, для використання в рамках створення runbook-сценаріїв; – Збір, аналіз і візуалізація результатів виконання команд з виконуваних runbook; – Автоматизація завдань конфігурації обладнання та діагностики за допомогою інструменту runbook; – Можливість інтеграції з зовнішніми системами управління та моніторингу, системами управління заявками на зміни і іншими системами за допомогою зовнішнього відкритого API; – Наявність інструментів, що забезпечують процес внесення змін (Change management) в конфігурацію мережевих пристроїв, а саме: наявність попередньо визначеного шаблону процесу внесення змін, що включає фазу підготовки змін конфігураційних файлів, фазу збору конфігурації пристроїв і мережевих даних перед внесенням змін, фазу затвердження внесення змін, фазу виконання змін (як в ручному, так і в автоматичному режимі, з можливістю створення розкладу на старт процесу змін), фазу збору конфігурації пристроїв і мережевих даних після внесення змін, фазу порівняння зібраної інформації до і після внесення змін; – Можливість виконання повернення до попередньої конфігурації; – Можливість проведення інвентаризації мережі з можливістю експорту звіту про інвентаризацію; – Можливість перевірки шляху проходження трафіку додатків з візуалізацією цього шляху на карті мережі; – Можливість завдання оптимального шляху проходження трафіку; – Можливість повідомлення про відхилення шляху проходження трафіку від оптимального; – Можливість визначення блокуючих трафік додатків мережевих пристроїв і причину блокування; – Можливість створення workflow для задач пошуку і усунення несправностей і діагностики мережі; – Можливість здійснення загального аналізу продуктивності як на рівні пристрою (завантаженість процесорів, використання

		пам'яті), так і на рівні інтерфейсу (затримки, використання смуги пропускання); – Можливість інтеграції з програмно-керованими рішеннями побудови мережі ЦОД/ SD-DC (наприклад, Cisco ACI або vmWare NSX) на рівні API ▪ Можливість візуалізації underlay-топології; ▪ Можливість візуалізації внутрішньої логічної структури, включаючи EPG, L3 Out, L2Out, контракти; ▪ Можливість аналізу Traffic Flow всередині фабрики; ▪ Можливість запуску діагностичних Runbook (workflow) за подією, що генерується контролерами. – Можливість інтеграції з VMWare vCenter через API; – Візуалізація параметрів віртуальних мереж VMWare vShpere – Підтримка TACACS та Active Directory для організації доступу до системи на основі RBAC моделі; – Повинен надавати можливість доступу до історичних даних мережі для порівняння та аналізу змін протягом щонайменше 4 (чотири) місяці для всіх зібраних даних; – Можливість визначення бажаного стану для параметрів пристроїв та відстеження змін від цього стану; – Можливість створення карт та маршрутів для Multicast трафіку; – Можливість підтримки multitenancy; – Можливість розгортання рішенні у розподіленій, відмовостійкій та високодоступній топології; – Автоматичне знаходження всіх пристроїв у мережі за допомогою: SNMP, CLI, RESTful API; – Підтримувати інтеграцію з Ansible; – Можливість спільного використання та передачі результатів виконання команд з пошуку несправностей між інженерами; – Можливість створення звіту про аналіз змін для будь-якого пристрою, карти або шляху, що показує, зміни між різними моментами часу. Рішення повинно мати можливість відображати зміни в реальному часі, наприклад зміни в таблицях маршрутизації або MAC, а не лише зміни в конфігурації; – Можливість пошуку для визначеної IP -адреси кінцевого пристрою та відображення, до якого комутатору та порту підключений цей пристрій, з можливістю створення карти; – Можливість створення типових (baseline) параметрів мережі з попередженням про зміни цих параметрів в мережі; – Можливість автоматичного створення карти на основі тригерів з інших систем, наприклад таких як Service Now та Splunk; – наявність вбудованого середовища візуального програмування, що дозволяє розширювати рішення та обробляти інформацію для різноманітних аспектів пристрою за допомогою програм швидкої автоматизації (QApps);

		– наявність можливість відстеження якості роботи мережі (так як це заплановано адміністратором) за відповідних тригерів (network intents), наприклад, використання каналу збільшується вище певного порогового значення тощо. – можливість перевірки відповідності конфігурації мережевих пристроїв до корпоративних політик та кращих практик.
	Вимоги до супутніх послуг з інтеграції рішення в інфраструктуру Замовника	– Аудит поточних процесів технічного супроводу: ▪ процес контролю внесення змін до мережевого обладнання інфраструктури; ▪ типових сценаріїв проведення пошуку та усунення несправностей; ▪ наявної документації на мережеву інфраструктуру, та її підтримання в актуальному стані. – Розробка цільової архітектури впроваджуваного рішення (загальний опис системи та її компонентів); – Розробка процесу. Process Design Document (PDD). AUTOMATION. Change Management. Network Troubleshooting. Documentation. (включаючи PlayBook'и); – Розгортання та налаштування системи (інсталяція) ▪ Базове налаштування системи; ▪ Внесення атрибутів доступу до бази запропоновного рішення; ▪ Discovery мережевих пристроїв та систем; ▪ Налаштування SNMP (в кінцевих системах); ▪ Інтеграція запропонованого рішення з існуючими системами моніторингу (щонайменше з Solarwind); ▪ Інтеграція запропонованого рішення р існуючої Ticketing системою; ▪ Налаштування функціональності Change Management модуля згідно технічних вимог; ▪ Налаштування функціональності Application Assurance модуля згідно технічних вимог; ▪ Налаштування динамічних схем візуалізації топології мережевої інфраструктури; ▪ Налаштування та типовізація шаблонів документації із завданням необхідних регламентів. – Реалізація цільового процесу автоматизації процесів технічного супроводу (1- пошуку та усунення несправностей, 2- внесення змін до мережевої інфраструктури та 3- розробки документації); – Передача знань за впровадженим рішенням (включаючи проходження відповідних імітованих процесів технічного супроводу; – Консультативний супровід на стадії поставки запропонованого рішення; – Консультування Замовника з виникаючих питань в процесі експлуатації.

	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **1 рік**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт або електронною поштою для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ - Можливість реєстрації сервісних випадків в режимі 24x7 в системі підтримки Виробника.		
7.	Програмна продукція **Підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури** для забезпечення роботи підсистеми у відповідності до технічних вимог строком дії не менше ніж 12 місяців.		**комплект**	**1**
	З технічними характеристиками та вимоги до підсистеми не гірше ніж:			
	Загальні вимоги	– Якщо відповідно до функціональності запропонованого рішення або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки; – Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення; – На обладнання не має бути анонсів end-of-sale та end-of life (EOS/EOL) від Виробника		
	Вимоги до архітектури	– Запропоноване рішення повинно поставлятися від одного виробника у вигляді програмно-апаратного комплексу або у вигляді віртуального пристрою та повинно бути виконаним у вигляді єдиної платформи, що не потребує використання будь-якого стороннього системного або прикладного програмного забезпечення (операційних систем, програмних додатків, систем керування базами даних тощо) для його впровадження; – Всі компоненти запропонованого рішення мають встановлювались локально та не потребувати підключення до мережі інтернет. – Запропоноване рішення повинно мати центральну консоль для всіх своїх компонентів, яка розгортається локально, щоб збирати, управляти і аналізувати інформацію про вразливості, не відправляючи їх в хмару. – Запропоноване рішення повинно мати можливість локально встановлювати активні сканера в мережі та підключати їх до центральної консолі		

		– Запропоноване рішення повинно мати можливість локально встановлювати агенти на кінцеві точки та підключати їх до центральної консолі – Запропоноване рішення повинно мати можливість локально встановлювати пасивні сканера та підключати їх до центральної консолі. – Запропоноване рішення повинно централізувати і повністю автоматизувати щоденне оновлення бази вразливостей від постачальника. – Запропоноване рішення повинно підтримувати автономний процес оновлення без доступу в інтернет. – Запропоноване рішення повинно забезпечувати інтегровану модель зберігання даних, яка не залежить від третьо стороннього продукту, який надає базу даних. – Запропоноване рішення повинно мати комплексний, відкритий REST API для автоматичного створення сценаріїв сканування і експорту даних з безпеки, без додаткових витрат. – - Запропоноване рішення повинно мати експертний висновок Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів з технічного захисту інформації.
	Функціонал сканування	– Запропоноване рішення повинно включати в себе інтегровану можливість активного та пасивного сканування для повної видимості вразливостей і відповідності стандартам; – Запропоноване рішення повинно забезпечувати сканування без агентів і на основі агентів; – Запропоноване рішення повинно підтримувати різні платформи для розміщення сканера, включаючи Windows, Linux, macOS, а також віртуальні і апаратні пристрої. – Запропоноване рішення повинно підтримувати різні платформи для розміщення агента, включаючи Windows, Linux, macOS – Додатковий віртуальний образ модулів сканування і консолі повинен бути доступний без додаткових витрат. – Запропоноване рішення повинно підтримувати кілька географічно або логічно розподілених механізмів сканування, керованих центральною консоллю. – Запропоноване рішення повинно підтримувати балансування навантаження і перемикання між декількома сканерами шляхом динамічного розподілу навантаження сканування між сканерами в залежності від доступності сканера протягом всього завдання сканування. – Запропоноване рішення повинно надавати клієнтам можливість розгортати додаткові сканера в своєму середовищі без додаткових витрат.

		– Запропоноване рішення повинно надавати клієнтам можливість розгортати додаткові агенти в своєму середовищі без додаткових витрат. – Запропоноване рішення повинно надавати клієнтам можливість розгортати додаткові пасивні сканери в своєму середовищі без додаткових витрат. – Загальна кількість повнофункціональних сканерів, повнофункціональних агентів і пасивних сканерів для виявлення активів має бути необмежена. – Запропоноване рішення повинно забезпечувати можливість підключення хмарних сканерів і запуску сканування зовнішньої мережі організації з використанням єдиного системного інтерфейсу, розташованого локально, без додаткових витрат. – Запропоноване рішення повинно забезпечувати можливість настройки портів, протоколів і служб для підключень до сканерів, розгорнутим по всій мережі. – Запропоноване рішення повинно налаштовуватись, щоб регулювати сканування, для запобігання генерації трафіку, достатнього для порушення нормальної роботи мережевої інфраструктури. – Запропоноване рішення повинно забезпечувати можливість підтримки автономного сканування і імпорту результатів на сервер. – Запропоноване рішення повинно дозволяти введення і безпечне зберігання облікових даних користувачів, включаючи локальні і доменні облікові записи Windows, а також su і sudo для Unix систем з доступом по ssh. – Запропоноване рішення повинно забезпечувати можливість підвищення привілеїв для цілей зі звичайних користувачів до адміністратора. – Запропоноване рішення повинно підтримувати необмежену кількість облікових даних «ssh». – Запропоноване рішення повинно інтегруватися з рішеннями управління привілейованим доступом, такими як CyberArk, BeyondTrust, Thycotic і Lieberman для управління обліковими даними. – Запропоноване рішення повинно підтримувати сканування з аутентифікацією і без аутентифікації для локального і віддаленого виявлення вразливостей без необхідності установки агента на стороні клієнта на цільовому пристрої. – Запропоноване рішення повинно забезпечувати сканування цільових систем як з аутентифікацією, так і без аутентифікації. – Запропоноване рішення повинно покладатися на сторонні сканери для сканування вразливостей.

		– Запропоноване рішення повинно вміти відслідковувати зміни DHCP, пов'язуючи результати сканування з іменами пристроїв в системі. – Запропоноване рішення повинно підтримувати можливість збереження результатів сканування неактивних кінцевих станцій протягом налаштованого періоду часу. – Запропоноване рішення повинно включати детальні дані відносно результатів сканування, включаючи таку інформацію, як знайдені версії DLL. – Запропоноване рішення повинно повідомляти про відомі недоліки в заданій цілі, виявленої консультативними організаціями з безпеки (наприклад, база даних Common Vulnerabilities and Exposures (CVE), База даних вразливостей з відкритим вихідним кодом (OSVDB), SecurityFocus Bugtraq (BID) або будь-яке їх поєднання). – Запропоноване рішення повинно підтримувати сканування вразливостей на відповідність PCI. Система повинна включати попередньо визначені профілі сканування PCI, які відповідають поточним критеріям PCI DSS для сканування мережі. Повинна існувати функція для фільтрації всіх інших вразливостей, що не відносяться до PCI. – Запропоноване рішення повинно забезпечувати аудит виправлень для операційних систем і додатків Microsoft, таких як 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 і інші. – Запропоноване рішення повинно забезпечувати аудит виправлень для всіх основних операційних систем Unix, включаючи macOS, Linux, Solaris, IBM AIX, HP-UX та інші. – Запропоноване рішення повинно забезпечувати аудит виправлень для мережевої інфраструктури, включаючи Cisco, Juniper і інші. – Запропоноване рішення повинно підтримувати сканування SCADA пристроїв. – Запропоноване рішення повинно вміти збирати/імпортувати і відображати дані про вразливості IT і OT мереж для єдиної візуалізації вразливостей в об'єднаних мережах IT/OT. – Запропоноване рішення повинно забезпечувати сканування сторонніх додатків, таких як Java і Adobe. – Запропоноване рішення повинно забезпечувати інтеграцію з системами управління виправленнями для аудиту виправлень і створення звітів про зміни результатів сканування, таких як Microsoft WSUS / SCCM, Red Hat Satellite, IBM BigFix (раніше IBM Tivoli Endpoint Manager), Symantec Altiris, VMWare Go.

		– Запропоноване рішення повинно забезпечувати інтеграцію з менеджерами мобільних пристроїв (MDM) для виявлення та аудиту мобільних пристроїв. – Запропоноване рішення повинно забезпечувати можливості аудиту пристроїв і мереж SCADA. – Запропоноване рішення повинно надавати звіти про репутацію загроз, виявлених шкідливих програм і бот-мереж. – Запропоноване рішення повинно 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. – Запропоноване рішення повинно забезпечувати пріоритизацію вразливостей, яка допомагає користувачам зрозуміти ключові фактори, що впливають на кожну оцінку вразливості (наприклад, новизну загрози, зрілість коду використання, категорії джерел Intel). – Запропоноване рішення повинно включати оцінку вразливості відповідно до загальної системи оцінки вразливостей (CVSS). – Запропоноване рішення повинно забезпечувати налаштовуваний механізм оцінки вразливостей, що базується на прийнятих в галузі стандартах, таких як CVSS. – Запропоноване рішення повинно надавати інформацію про використання вразливостей з Core Impact, Metasploit і Canvas. – Запропоноване рішення повинно надавати інформацію про використання шкідливих програм на кінцевому пристрої. – Запропоноване рішення повинно дозволяти вибирати тести на основі інформації, отриманої при первинному скануванні, щоб проводити подальше тестування на основі отриманої інформації про даний пристрій або кінцеву точку. – Запропоноване рішення повинно відслідковувати життєвий цикл вразливостей стосовно окремих кінцевих пристроїв, а також середовищ, включаючи дату першого виявлення, останнього спостереження і усунення вразливості. – Запропоноване рішення повинно підтримувати сканування серверів VMware на вразливості і відповідність вимогам за допомогою власного API VMware. – Запропоноване рішення повинно дозволяти сканувати пристрої за розкладом. – Запропоноване рішення повинно дозволяти включати або відключати перевірки на певні вразливості під час сканування. – У запропонованому рішенні має бути передбачена можливість відключення потенційно шкідливих перевірок. – Запропоноване рішення повинно автоматично запускати і зупиняти сканування за розкладом без втручання користувача.

		– Запропоноване рішення повинно дозволяти припиняти і відновлювати сканування вручну. – Запропоноване рішення повинно дозволяти запускати сканування, незавершене у встановлений термін, або переносити на наступний запланований період. – Запропоноване рішення повинно мати можливість приймати цілі сканування в різних форматах, включаючи імена DNS, діапазони IP-адрес і класи IP, а також попередньо визначені списки активів. Наприклад, 10.0.1.1 - 10.0.1.100. Також повинен підтримуватися імпорт списку IP-адрес, що містяться в файлі. – Запропоноване рішення повинно підтримувати сканування IPv6 з пасивним виявленням активів IPv6. – Запропоноване рішення повинно забезпечувати можливість відключення сканування периферійних пристроїв, наприклад принтерів. – Запропоноване рішення повинно забезпечувати можливість пасивного сканування: ▪ Пасивний сканер повинен включати можливість виявлення нових активів шляхом моніторингу мережевого трафіку без активного сканування. ▪ Пасивний сканер повинен відображати виявлені в трафіку активи в реальному часі. ▪ Пасивний сканер повинен надавати інформацію про окрему мережу, мережі в цілому або будь-якої конкретної групи хостів. ▪ Пасивний сканер повинен мати можливість відправляти події, пов'язані з трафіком, через системний журнал в системи кореляції подій. ▪ - Пасивний сканер повинен поставлятися тим же виробником, що і основна система.
	Функціонал роботи з активами	– Запропоноване рішення повинно підтримувати можливість виявлення активів, що не використовують ліцензію. – Запропоноване рішення повинно забезпечувати можливість активного сканування і пасивного моніторингу мережі для виявлення активів. – Запропоноване рішення повинно вміти виявляти мобільні пристрої. – Запропоноване рішення не повинно покладатися на сторонні сканери для виявлення активів, сканування портів або ідентифікації ОС. – Запропоноване рішення повинно забезпечувати виявлення веб-служб і служб баз даних. – Запропоноване рішення повинно вміти виявляти служби, що працюють на нестандартних портах.

		– Запропоноване рішення повинно вміти виявляти служби, в яких не відображаються банери підключення. – Запропоноване рішення повинно бути здатна тестувати кілька примірників однієї й тієї ж служби, що працює на різних портах. – Запропоноване рішення повинно вміти сканувати «мертві» кінцеві точки (пристрої, що не відповідають на ICMP запити). – Запропоноване рішення повинно підтримувати необов'язкове використання netstat для швидкого і точного перерахування відкритих портів в системі при наданні облікових даних. – Запропоноване рішення повинно підтримувати використання SMB і WMI для сканування систем Windows. – Запропоноване рішення повинно мати можливість автоматично запускати служби віддаленого реєстру в системах Windows при виконанні сканування з обліковими даними, а потім автоматично зупиняти службу після завершення сканування. – Запропоноване рішення повинно підтримувати безпечне з'єднання(ssh) з можливістю підвищення привілеїв для сканування вразливостей і аудиту конфігурації в системах Unix. – Запропоноване рішення повинно мати можливість збирати/ імпортувати і відображати дані про активи IT і OT мереж в єдиній консолі. – Запропоноване рішення повинно забезпечувати можливість налаштування політик сканування для мінімального впливу на мережі і цілі сканування. – Запропоноване рішення повинно забезпечувати виявлення точок бездротового доступу (WAP) за допомогою активного і пасивного сканування. – Запропоноване рішення повинно забезпечувати можливість виявлення нових пристроїв і відправки попереджень за допомогою електронної пошти, системного журналу або консольним повідомленнями. – Запропоноване рішення повинно забезпечувати можливість автоматичного запуску сканування нових пристроїв. – Запропоноване рішення повинно підтримувати використання агента для аудиту SCAP. – Запропоноване рішення повинно мати можливість виявляти всі активи, не використовуючи ліцензії, а потім мати можливість вибирати, які активи сканувати на вразливості.
	Вимоги до Агентів	– Агент повинен збирати та відправляти дані на центральну консоль для зменшення навантаження на мережу та кінцевий пристрій – Агенти можуть бути підключені та управлятися як через локальну консоль, так і хмарну – Агент повинен мати можливість встановлюватися у хмарних середовищах, таких як AWS та Azure.

		- Агент повинен надавати можливість регулювати власне навантаження на кінцеву точку, для запобігання порушення робочих процесів. - Агент повинен мати можливість з'єднуватись з консоллю через проксі сервер. - Агент повинен мати можливість встановлюватись через сторонні рішення такі як Active Directory або SCCM. - Запропоноване рішення повинно мати можливість створювати групи агентів для автоматизації процесу виявлення вразливостей. - Запропоноване рішення повинно надавати інформацію відносно статусу агентів. - Агент повинен мати унікальний ідентифікатор для виявлення одного і того пристрою в різних підмережах.
	Вимоги до функціоналу аудиту на відповідність	– Запропоноване рішення повинно підтримувати аудит на відповідність як з автентифікацією, так і без автентифікації, з або без необхідності встановлення агента на стороні клієнта на кінцевій точці. – Запропоноване рішення не повинно покладатися на сторонні сканери для аудиту/оцінки конфігурації безпеки. – Запропоноване рішення повинно надавати єдине представлення про всі результати аудиту вразливостей і відповідності вимогам. – Запропоноване рішення повинно забезпечувати аудит конфігурацій для відповідності нормативним вимогам та іншим галузевим стандартам і стандартам кращої практики постачальників. – Запропоноване рішення повинно забезпечувати аудит конфігурації, що базується на кращих практиках для таких постачальників, як Microsoft, Cisco і VMware. – Запропоноване рішення повинно забезпечувати аудит VMWare ESXi і vCenter за допомогою VMWare SOAP API. – Запропоноване рішення повинно забезпечувати аудит операційних систем Microsoft для перевірки параметрів безпеки і конфігурацій. – Запропоноване рішення повинно забезпечувати аудит всіх основних операційних систем Unix для перевірки параметрів безпеки і конфігурацій. – Запропоноване рішення повинно забезпечувати аудит баз даних для перевірки параметрів безпеки і конфігурацій таких як: PostgreSQL, MongoDB, Microsoft SQL, DB2, Sybase, Oracle, MySQL – Запропоноване рішення повинно забезпечувати аудит додатків для перевірки параметрів безпеки і конфігурацій таких як: Internet Explorer, Microsoft Edge, Google Chrome, Microsoft Office и т.д.

		– Запропоноване рішення повинно забезпечувати аудит мережевої інфраструктури для перевірки параметрів безпеки і конфігурацій таких як: Cisco, Arista, HP, F5 і т.д. – Запропоноване рішення повинно забезпечувати аудит певних продуктів безпеки кінцевих точок на предмет статусу установки і оновлення. – Запропоноване рішення повинно забезпечувати аудит особистої інформації (PII) і іншого конфіденційного контенту. – Запропоноване рішення повинно дозволяти налаштовувати політики аудиту відповідно до потреб організації. – Запропоноване рішення повинно надавати можливість проведення аудитів на відповідність стандартам CIS. – - Запропоноване рішення повинно надавати можливість проведення аудитів на відповідність стандартам DISA STIG.
	Візуалізація даних та звітність	– Запропоноване рішення повинно включати налаштовуванні графічні панелі і створені шаблони панелей для відображення вразливостей і стану безпеки. – Запропоноване рішення повинно забезпечувати налаштовуваний тренд результатів сканування на інформаційних панелях з використанням відфільтрованих результатів для визначення декількох ліній тренда на одному графіку. – Запропоноване рішення повинно дозволяти кожному користувачеві створювати кілька користувальницьких інформаційних панелей. – Елементи інформаційної панелі повинні легко змінюватись шляхом фільтрації, для відображення даних на основі списку активів, перевірок вразливостей або відповідностей, часу, пошуку за ключовими словами, IP-адреси і т.д. – Частота оновлення інформаційних панелей повинна налаштовуватись, для оновлення за розкладом. – Запропоноване рішення повинно забезпечувати можливість імпорту / експорту шаблонів інформаційних панелей. – Запропоноване рішення повинно надавати можливість додавати різні персоналізовані візуальні елементи для налаштування інформаційних панелей, включаючи кругові діаграми, гістограми, матриці і тенденції. – Запропоноване рішення повинно надавати користувачам можливість спільно використовувати інформаційні панелі. – Запропоноване рішення повинно надавати інтернет ресурс для завантаження інформаційних панелей, який включає шаблони: присвячені різним рівням користувачів, стандартам відповідності та засобів управління безпекою. – Запропоноване рішення повинно підтримувати налаштування параметрів шаблону і форматування інформаційних панелей.

		– Запропоноване рішення повинно підтримувати створення звітів, що налаштовуються з використанням шаблонів, наданих постачальником, або без шаблонів. – Запропоноване рішення повинно забезпечувати можливість фільтрації результатів в звітах по різним критеріям, включаючи, але не обмежуючись списками активів, репозиторіями, адресами, типами вразливостей, необробленим текстом і полями дат. – Запропоноване рішення повинно надавати вбудовані звіти про сканування та журнали системи. – Запропоноване рішення повинно забезпечувати можливість повної автоматизації звітів, включаючи виконання і відправлення за розкладом, а також відправлення звітів після сканування. – Запропоноване рішення повинно забезпечувати можливість перегляду результатів в консолі, незалежно від процесу створення звітів. – Запропоноване рішення повинно підтримувати можливість створення звітів в наступних форматах: PDF, CSV, RTF. – Запропоноване рішення повинно забезпечувати можливість налаштовувати та відображати тенденції результатів сканування в звітах на одному графіку. – Запропоноване рішення повинно надавати матричні таблиці, підсумовуючи числа по різним фільтрованим наборам результатів. – Запропоноване рішення повинно забезпечувати автоматичне відправлення звітів для аналітика безпеки на відповідність стандартам. – Запропоноване рішення повинно надавати звіти про відповідність нормативним вимогам без додаткових витрат. – Звіти повинні мати можливість включати імена пристроїв (NetBIOS, DNS) разом з IP-адресами. – Запропоноване рішення повинно забезпечувати можливість шифрування і захисту звітів паролем. – Запропоноване рішення повинно забезпечувати можливість автоматичної відправки звітів по електронній пошті. – Запропоноване рішення повинно забезпечувати можливість відправки звітів за допомогою служб веб-публікації. – Запропоноване рішення повинно дозволяти завантажувати та додавати зображення для створення звіту. – Запропоноване рішення повинно надавати звіти високого рівня щодо показників безпеки і відповідностей стандартам.
	Автоматизація	– Запропоноване рішення повинно забезпечувати повну автоматизацію сканування, створення звітів і попереджень. – Запропоноване рішення повинно мати окремі панелі для відображення вразливостей виявлених: активно, скануванням на відповідність і в мобільних пристроях.

		– Запропоноване рішення повинно об'єднувати результати окремих сканувань вразливостей з можливістю фільтрації, щоб забезпечити можливість деталізації та проведення аналізу. – Запропоноване рішення повинно мати окремі представлення активних і усунених вразливостей з автоматичним перенесенням вразливостей з активних на усунуті після того, як сканування визначає, що вразливості більше немає. – Запропоноване рішення повинно мати можливість відзначати вразливість як раніше усунуту, але яка з'явилася знову, це може статися, коли система відновлюється з резервної копії або стара копія віртуальної машини повертається в оперативний режим. – Запропоноване рішення повинно забезпечувати комплексну фільтрацію виявлених вразливостей з можливістю деталізації по наступним параметрам, але не обмежуватись ними: IP адреса, ідентифікатор агента, актив, аудит файл, ідентифікатор CCE, ідентифікатор CVE, оцінка CVSS v2, оцінка CVSS v3, Ім'я DNS, доступність експлойта, порт, протокол, рівень критичності, дата першого виявлення, дата останнього виявлення, текст вразливості. – В запропонованому рішенні має бути можливість додавати теги до активів, політик, облікових даних або запитів з налаштованим описом для поліпшення фільтрації та управління об'єктами. – Запропоноване рішення повинно мати панель для аналітика безпеки, яка автоматично встановлює пріоритети та оптимізує рішення для виправлення вразливостей, а саме надає відсоткове значення зменшення ризиків, при закритті вразливостей на групі пристроїв. – Запропоноване рішення повинно надавати користувачам можливість запускати сканування на предмет виправлення вразливості, щоб переконатися, що вона усунута без необхідності налаштування параметрів сканування. – Запропоноване рішення повинно забезпечувати можливість автоматичного групування кінцевих точок, тобто створення динамічних списків активів, що базується на результатах сканування, по наступним критеріям, але не обмежуватись ними: IP адреса, ім'я DNS, тип ОС, рівень критичності вразливості, порт, доступність експлойту, дата першого виявлення, дата останнього виявлення, текст вразливості. – Запропоноване рішення повинно дозволяти користувачеві приймати ризик (робити виняток) з налаштованими датами закінчення терміну дії виявленої вразливості або змінювати рівень ризику (критичності) до рівня, що відрізняється від того, який постачальник визначив для цієї вразливості. – Запропоноване рішення повинно забезпечувати функцію створення задач та можливість інтеграції зі сторонніми системами для відслідковування задач.

		– Запропоноване рішення повинно підтримувати призначення задач окремим користувачам. – Запропоноване рішення повинно забезпечувати можливість сповіщення про вразливість і подію. – - Запропоноване рішення повинно підтримувати створення сповіщень на основі результатів сканування вразливостей або аудиту конфігурації. Сповіщення має включати: налаштовуваний електронний лист з декількома змінними контексту, створення задач, запуск сканування, створення події в системному журналі, створення звіту та повідомлення користувачів.
	Автентифікація та рольовий доступ	– Запропоноване рішення повинно забезпечувати управління доступом на основі ролей, щоб контролювати доступ користувачів до певних наборів даних і функцій, доступним цим користувачам. – Запропоноване рішення повинно дозволяти адміністраторам визначати ролі в залежності від посадових обов'язків і відповідних рівнів доступу до функцій. – Запропоноване рішення повинно мати можливість інтеграції з LDAP для аутентифікації користувача. – Запропоноване рішення повинно підтримувати кілька серверів LDAP для аутентифікації. – Запропоноване рішення повинно підтримувати Security Assertion Markup Language (SAML), щоб забезпечити кілька варіантів єдиного входу / аутентифікації, таких як Shibboleth і Okta. – Запропоноване рішення повинно мати докладний звіт щодо активності користувачів. – Запропоноване рішення повинно дозволяти адміністраторам обмежувати доступ для окремих користувачів або груп до певних списків активів, політикам сканування і репозиторіїв вразливостей. – Запропоноване рішення повинно дозволяти адміністраторам призначати ресурси для кожного користувача або групи, наприклад політики сканування, списки активів, запити та облікові дані. – Запропоноване рішення повинно дозволяти адміністраторам обмежувати дозвіл на проведення: повного сканування, сканування з використанням певних політик. – У запропонованому рішенні має бути передбачена можливість планування часу, щоб запобігти сканування в заборонені години. – Запропоноване рішення повинно підтримувати створення організацій з повним поділом даних між цими організаціями в межах однієї консолі. – Запропоноване рішення повинно надавати можливість визначати обмеження для діапазону IP-адрес для кожної організації.

		– Запропоноване рішення повинно забезпечувати можливість прийняття та зміни ризику вразливостей.
	Вимоги до супутніх послуг з інтеграції рішення в інфраструктуру Замовника	– Аудит поточного процесу пошуку та мінімізації впливу вразливостей IT-інфраструктури, включаючи: ▪ аудит існуючих регламентів та типових сценаріїв проведення пошуку вразливостей, а також відповідних дій щодо їх мінімізації; ▪ аудит існуючого рішення Tenable.sc™ Continuous View, щодо коректності реалізації, налаштувань та їх відповідності процесу; o Діагностика стану конфігурацій поточної реалізації; o Перевірка доступу для оновлення системи; o Оновлення системи та баз вразливостей до актуальної версії; o Оновлення встановлених сенсорів до актуальних версій; o Визначення підмереж/кінцевих точок для встановлення додаткових сканерів/агентів/моніторів; o Створення матриці ролей, щодо надання прав доступу до системи управління вразливостями. – Проведення випробувань інформаційних ресурсів (веб-додатків) та IT-інфраструктури Замовника на вразливості (Penetration Testing) у наступному обсязі: ▪ Завдання: Пошук вразливостей інформаційних систем Замовника. ▪ Об'єкти: Об'єкти аналізу надаються Виконавцю у відповідному запиті на надання послуг. ▪ Кількість об'єктів аналізу: Щонайменше 600 людино/годин роботи команди Виконавця, щодо тестування інфраструктури Замовника, а саме: o щонайменше 255: ip-адрес, o 5: веб-додатків o 6: бездротових мереж ▪ Методи аналізу: випробування на проникнення інформаційної системи (тестування на проникнення) здійснюється по зовнішньому телекомунікаційному каналу за принципом чорного або сірого ящику. Після проведення випробування Виконавець готує звіт та надає спеціалістам Замовника консультації (роз'яснення) щодо усунення виявлених недоліків. ▪ Періодичність: протягом строку надання Послуг відповідно до умов Договору, на підставі надходження запитів від Замовника. ▪ Порядок надання послуг:

		○ Замовник надає Виконавцеві письмовий дозвіл щодо початку проведення робіт з тестування відповідно з Договором. ○ Виконавець готує та надає Замовникові План тестування. - При здійсненні тестування Виконавець може використовувати автоматизовану перевірку та обов'язково ручний пошук і експлуатацію вразливостей. ○ Виконавець повинен виконати оцінку можливості отримання несанкціонованого доступу в процесі моделювання атак. ○ Виконавець повинен знайти максимальну кількість вразливостей виходячи з наявної інформації, знань та можливостей інструментальних засобів. ○ При проведенні тестування на проникнення Виконавець повинен провести випробування за принципом чорного або сірого ящику, тобто може отримувати від Замовника інформацію про конфігурацію об'єктів тестування. ○ При виконанні тестування спеціалісти повинні здійснити щонайменьше наступні кроки: a) Збір інформації про інфраструктуру Замовника з відкритих джерел у пасивний та активний спосіб; b) Проведення сканування мереж та систем у інфраструктурі Замовника, що включено у перелік цілей для тестування; c) Випробування на вразливості знайдених активів та сервісів під час попередніх етапів тестування; d) Аналіз результатів випробувань з метою пріоритезації подальшого ходу тестування; e) Класифікація вразливостей і вибір неявних вразливостей для перевірки, оцінка вразливостей відповідно до галузевого стандарту CVSS; f) Документування вразливостей та збір доказів перевірки; g) Аналіз результатів перевірки вразливостей; h) Підготовка звіту з тестування з рекомендаціями, щодо усунення знайдених вразливостей та недоліків безпеки в IT-інфраструктурі Замовника. ○ Всі послуги з тестування на проникнення повинні проводитись тільки після отримання Виконавцем від Замовника офіційного листа та/або електронного повідомлення на дозвіл таких послуг. ○ У випадку можливості виходу з ладу або погіршення показників роботи елементів інфраструктури Замовника в результаті виконання випробувань, такі випробування повинні бути припинені до отримання дозволу від

		Замовника на продовження саме такого виду випробувань. o У випадку отримання доступу до конфіденційної інформації в інформаційній системі Замовника, випробування відносно цієї системи повинні бути припинені до отримання дозволу від Замовника на продовження випробувань відносно цієї системи. ▪ Вимоги до оформлення результатів: o За результатами аналізу Виконавець надає Замовнику звіт за результатами тестування. o Звіт повинен містити наступну інформацію: a) Резюме. Стисле викладення результатів випробувань; b) Мета тестування. Опис цілей проведення випробувань; c) Область дії. Визначення області дії випробувань; d) Опис методики. Методики та інструменти, що були використані Виконавцем в ході тесту та його окремих етапів; e) Результати випробувань. Детальні результати тестування та рекомендації, які повинні містити наступну інформацію: назву вразливості; перелік вразливих систем (сервісів); статус вразливостей (дійсна/не дійсна/потенційна); рівень ризику; опис вразливостей; дії щодо перевірки вразливості (опис виконаних атак); докази перевірки; рекомендації з усунення. o Звіти щодо проведених сканувань об'єктів тестування долучаються у вигляді додатків до основного Звіту. o Звіти з тестування повинні бути підготовлені в письмовій формі українською мовою. ▪ Послуги повинні бути надані з урахуванням вимог, які викладені у наступних документах: o ISECOM OSSTMM 3 (Open Source Security Testing Methodology Manual); o OWASP (OWASP Testing Guide v3.0) - індустріальний стандарт; o Penetration Testing Model (BSI); o ISACA IS auditing procedure "P8 Security Assessment - Penetration testing and vulnerability analysis; o NIST 800-115 (Technical Guide to Information Security Testing and Assessment). ▪ Звіти передаються Замовнику електронними поштовими повідомленнями та/або офіційним листом.

		– Розробка цільової архітектури впроваджуваного рішення (за необхідності внесення змін до існуючої архітектури у Замовника); – Розробка процесу. Process Design Document (PDD). SECURITY SERVICES. Vulnerability managemen. (включаючи PlayBook'и); – Розгортання та налаштування системи (інсталяція) ▪ Базове налаштування системи; ▪ встановлення компонентів (сканерів/агентів/моніторів) у вибраних підмережах і надання SPAN, а також підключення до впроваджуваного рішення; ▪ Створення окремих репозиторіїв для: o Сканувань без автентифікації; o Сканувань з автентифікацією; o Агентного сканування; o Сканувань на відповідність стандартам. ▪ Створення окремих зон сканування для кожної підмережі де встановлений сканер; ▪ Створення окремих організацій для розмежування доступів; ▪ Створення користувачів і груп користувачів для поділу ролей в середині організації; ▪ Налаштування терміну зберігання даних у системі для: o Результатів сканування; o Закритих задач; o Створених звітів. ▪ Налаштування політик сканування, щонайменше: o Host discovery scan; o Basic Network scan; o Agent Scan; o Custom scan. ▪ Створення сканувань на основі створених політик і визначення графіка сканування; ▪ Тестування сканування з політики і розподіленого сканування; ▪ Налагодження та кастомізація інформаційних панелей за вимогами замовника на основі вразливостей (напр. Vulnerability summary, Mitigation summary, Understanding risk); ▪ Налагодження та кастомізація звітів за вимогами замовника на основі отриманих даних (напр. Host discovery, Mitigation summary report, Event Analysis); ▪ Створення запитів на основі клієнтських фільтрів для пошуку вразливостей і подій, створення звітів, повідомлень та задач; ▪ Налаштування сповіщень за вимогами замовника. (налаштування повідомлення користувача, генерація логів, присвоювання задачі, запуск сканування); ▪ Проведення експлуатаційних тестів системи.

		– Реалізація цільового процесу процесу пошуку та мінімізації впливу вразливостей IT-інфраструктури; – Передача знань за впровадженим рішенням: ▪ навчання персоналу задіяного в процесі (адміністраторів системи та аналітикіи з безпеки); ▪ Проходження відповідних імітованих процесів пошуку/реагування/… згідно розробленого процесу. – Консультативний супровід на стадії поставки запропонованого рішення; – Консультування Замовника з виникаючих питань в процесі експлуатації.
	Технічна підтримка та гарантії	– Запропоноване рішення повинно бути забезпечене сервісною підтримкою строком не менше ніж **1 рік**, що включає: ▪ Постійний (24x7) доступ до центру технічної підтримки Виробника через сайт або електронною поштою для отримання консультацій; ▪ Отримання всіх необхідних оновлень для функціонування системи, включаючи основні та проміжні версії програмного забезпечення; ▪ Постійний (24x7) авторизований доступ до сайту Виробника; ▪ Можливість реєстрації сервісних випадків в режимі 24x7 в системі підтримки Виробника.

У разі використання в тендерній документації посилання на стандартні характеристики, технічні регламенти та умови, вимоги, умовні позначення та термінологію, пов'язані з товарами, роботами чи послугами, що закуповуються, передбачені існуючими міжнародними, європейськими стандартами, іншими спільними технічними європейськими нормами, іншими технічними еталонними системами, визнаними європейськими органами зі стандартизації або національними стандартами, нормами та правилами, після такого посилання слід читати вираз "або еквівалент".

У разі використання в тендерній документації посилання на конкретні марку чи виробника або на конкретний процес, що характеризує продукт чи послугу певного суб'єкта господарювання, чи на торгові марки, патенти, типи або конкретне місце походження чи спосіб виробництва, після такого посилання слід читати вираз "або еквівалент".

Ініціатор закупівлі **І. П. Голуб**

Додаток 2

ІНФОРМАЦІЯ ТА ДОКУМЕНТИ, ЩО ПІДТВЕРДЖУЮТЬ ВІДПОВІДНІСТЬ УЧАСНИКА КВАЛІФІКАЦІЙНИМ КРИТЕРІЯМ

№	Кваліфікаційний критерій	Способи документального підтвердження інформації, про відповідність Учасника кваліфікаційним критеріям (документи, які надає Учасник)
1	**Наявність обладнання, матеріально-технічної бази та технологій**	Довідка в довільній формі про наявність обладнання, матеріально-технічної бази та технологій, необхідних для надання супутніх послуг до поставки товару, визначених у технічних вимогах, із зазначенням найменування, кількості та правової підстави володіння/користування. На підтвердження інформації стосовно наявності матеріально-технічної бази (адміністративні приміщення та/або склад та/або транспорт), зазначеної в довідці, учасник має надати документи/документ, на підтвердження права власності/володіння/користування відповідним майном. При цьому договір найму (оренди) транспортного засобу за участі фізичної особи, а також договір найму будівлі або іншої капітальної споруди (їхньої окремої частини) строком на три роки і більше, у разі їх надання учасником, мають бути засвідчені нотаріально/
2	**Наявність працівників відповідної кваліфікації, які мають необхідні знання та досвід**	Довідка в довільній формі за підписом уповноваженої особи Учасника та завірена печаткою (у випадку використання печатки Учасником в своїй господарській діяльності та при оформленні документів), що підтверджує наявність в Учасника торгів спеціалістів відповідної кваліфікації, які мають необхідні знання та досвід і будуть залучені до виконання умов договору (не менше семи кваліфікованих фахівців) з підтвердженою кваліфікацією (шляхом надання копій зазначений нижче сертифікатів, тощо) за наступними напрямками: - Фахівець з тестування на проникнення (pentester), підтвердження кваліфікації - Certified Ethical Hacker (CEH) та/або Certified Information Security Systems Professional (CISSP) та/або Licensed Penetration Tester Master (LPT Master) та/або Offensive Security Certified Professional (OSCP) або аналогічних; - Інженер з реагування на інциденти (incident response), підтвердження кваліфікації - EC-Council Certified Incident Handler (ECIH) та/або EC-Council Certified Security Analyst (ECSA) або аналогічних; - Аудитор з інформаційної безпеки, підтвердження кваліфікації - Сертифікат ISO 27001:2013 Lead Auditor Провідний Аудитор Систем Менеджменту ISO 27001:2013 або аналогічних; - Фахівець з інформаційної безпеки: впровадження/ security deployment (1 людина), експлуатація/ security operations (1 людина), підтвердження кваліфікації: - EC-Council CSA (Certified SOC Analyst) та/або Cisco Certified Network Associate (CCNA Security) та/або Cisco Certified Network Professional (CCNP Security) та/або Linux Certification Practice Tests (LPIC) або аналогічних.

<table>
<tr><td></td><td></td><td>- Інженер інформаційних систем /телекомунікації, підтвердження кваліфікації: Cisco Certified Network Associate (CCNA Enterprise) та/або Certified Network Professional (CCNP Enterprise) або аналогічних.
- Керівник проекту направлення кібербезпеки /архітектор, підтвердження кваліфікації: з досвідом управління проектною командою не менше 3-х років та дизайну рівня Associate/Professional Cisco Certified Design Associate/Professional (CCDA/CCDP) та/або мережевої безпеки рівня Professional/Expert (CCNP Security/ CCIE Security) або аналогічних.
Сертифікати, свідоцтва, дипломи чи інші документи, що підтверджують отримання знань чи проходження навчання та які видані на іноземній мові, повинні мати переклад тексту документу на українську мову, виконаний бюро перекладів з нотаріально засвідченим підписом перекладача</td></tr>
<tr><td>3</td><td>Наявність документально підтвердженого досвіду виконання аналогічного (аналогічних) за предметом закупівлі договору (договорів)</td><td>Інформація (довідка або лист) за підписом уповноваженої особи Учасника, завірена печаткою (у разі використання), на фірмовому бланку (у разі використання) про наявність досвіду виконання аналогічного (аналогічних) за предметом закупівлі договору (договорів) у вигляді наступної таблиці:
<table>
<tr><th>№ п/п</th><th>Замовник (найменування, код ЄДРПОУ, адреса, ПІБ та телефон підписанта)</th><th>Предмет договору</th><th>Сума договору</th><th>Дата укладання і строк дії договору</th></tr>
</table>
На підтвердження виконання аналогічного (аналогічних) за предметом закупівлі договору (договорів), який(і) зазначений(і) в довідці , надається:
– копія виконаного договору,
– копія (-ї) акту (-ів) виконаних робіт або копія (-ї) видаткової (-их) накладної (-их), або інші документи, що підтверджують його виконання.</td></tr>
</table>

У разі участі об'єднання учасників підтвердження відповідності кваліфікаційним критеріям здійснюється з урахуванням узагальнених об'єднаних показників кожного учасника такого об'єднання на підставі наданої об'єднанням інформації.

Ініціатор закупівлі **І. П. Голуб**

iIT Trading
Phone: +38 (044) 33 999 77
E-mail: info@iitt.com.ua
Website: iitt.com.ua

Вих.№15/09/21-4

15.09.2021

Комерційна пропозиція

Доброго дня. Пропонуємо до вашої уваги комерційну пропозицію на поставку ліцензійного програмного забезпечення:

№	Підсистема	Назва	Вартість грв
1	Програмна продукція підсистеми керування мережевими пристроями безпеки .	Fortinet FortiManager/ FortiAnalyzer	2 520 000,00
2	Програмна продукція Підсистеми оркестрування, автоматизації та реагування на інциденти безпеки .	Fortinet FortiSOAR	4 165 000,00
3	Програмна продукція Підсистеми пошуку вразливостей в рамках циклу розробки програмного забезпечення.	Fortify Static Code Analyzer	3 080 000,00
4	Програмна продукція Підсистеми моніторингу IT-сервісів.	UP Dynamics	4 144 000,00
5	Програмна продукція Підсистеми моніторингу та контролю дій привілейованих користувачів.	One Identity Safeguard	1 624 000,00
6	Програмна продукція Підсистеми адаптивної мережевої автоматизації.	NetBrain Network Automation	1 960 000,00
7	Програмна продукція Підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури	GFI Languard	3 304 000,00
	Вартість грв (без ПДВ)		**20 797 000,00**

Вартість впровадження та налаштування **6 280 000,00 грв з ПДВ**

Загальна вартість **27 077 000,00 грв**

*Вартість та склад запропонованого рішення може корегуватися після більш ретельного обстеження.

Директор _____/Казачук І.В.

Київська міська державна адміністрація
Спеціалізоване комунальне підприємство
"КИЇВТЕЛЕСЕРВІС"
Вхідний № 80/09-2021
Від 15 09 2021 р.

ТОВ «ВІ ЄМ ДЖІ»
ЄДРПОУ 40844268
+380 96 001 01 61
info@wmgroup.com.ua
wmgroup.com.ua

_____№_____

Комерційна пропозиція

Компанія **ТОВ «ВІ ЄМ ДЖІ»** висловлює Вам свою вдячність за звернення та відповідно до отриманого запиту № **131-09/2021** від 13 вересня 2021 року, щодо опрацювання питання орієнтовної вартості закупівлі пакетів програмного забезпечення для керування виробничими процесами, пропонуємо Вам розглянути нашу комерційну пропозицію, на побудову (створення, впровадження та супровід) Операційного центру кібербезпеки в рамках Комплексної міської цільової програми «Електронна столиця на 2019 - 2022 роки».

Детально ознайомившись з наданим проектом Технічних вимог до створюваного Комплексу пропонуємо розглянути наступні можливі проектні рішення що відповідають цільовим потребам, а саме:

1. *Підсистема*: керування мережевими пристроями безпеки
   Рішення: **Fortinet FortiManager**
   Цінність:
   - Своєчасне отримання оновлень програмного забезпечення;
   - Забезпечення необхідного рівня покриття централізованою системою управління та моніторингу.

2. *Підсистема*: оркестрування, автоматизації та реагування на інциденти безпеки
   Рішення: **Fotinet FortiSOAR Enterprise**
   Цінність:
   - забезпечення узгодження роботи (оркестрація) систем кібербезпеки, а також управління реагуванням на інциденти в режимі реального часу;
   - оптимізація базових / рутинних операцій CSOC;
   - забезпечення можливості надання для IRT (зовнішньої і / або штатної) інструментів для організації процесу реагуванням на інциденти кібербезпеки;
   - зниження ризикіи схильності інфраструктури Замовника до можливих критичних інцидентів ІБ.

3. *Підсистема*: пошуку вразливостей в рамках циклу розробки програмного забезпечення /SDLC
   Рішення: **Checkmarx Software Security Platform**
   Цінність:
   - Забезпечення можливості аналізу нових поставок ПО на наявність вразливостей;
   - Підвищення якості поставок ПЗ в майбутньому за рахунок реалізації контролю вихідного коду;

- Зниження ризиків схильності впроваджуваних сервісів/ застосувань до можливих критичних інцидентів ІБ.

4. *Підсистема*: Підсистема моніторингу IT-сервісів
   Рішення: **Dynatrace software intelligence platform**
   Цінність:
   - Забезпечення контролю продуктивності IT-сервісів (щонайменше критичних, з можливістю подальшого масштабування);
   - Забезпечення аналізу активності користувачів для ключових IT-систем;

5. *Підсистема*: Моніторингу та контролю дій привілейованих користувачів
   Рішення: **One Identity Safeguard (PAM)**
   Цінність:
   - Створення єдиної платформи для управління доступом адміністраторів і зовнішніх підрядників (з єдиною «точкою входу») в мережах існуючої IT-інфраструктури Замовника включаючи забезпечення покриття процесом систем;
   - Забезпечення впровадження (інтеграцію) рішення в існуючу КСЗІ зі збереженням профілю захищеності.

6. *Підсистема*: Адаптивної мережевої автоматизації
   Рішення: **NetBrain Network Automation Platform**
   Цінність:
   - підвищення якості роботи обслуговуючого персоналу за рахунок впровадження методики та практик автоматизації процесів технічного супроводу мережевої інфраструктури;
   - прискорення процесів пошуку, діагностування, локалізації і усунення інцидентів/відмов;
   - оптимізація базових операції NOC та зниження навантаження (трудовитрати) на персонал;
   - впровадження процесу контрольованого внесення змін до конфігурації мережевої;
   - підтримання актуального стану робочої документації на існуючу мережеву інфраструктуру.

7. *Підсистема*: Керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури
   Рішення: **Tenable.sc™ Continuous View, а також долучення зовнішньої експертизи з кібербезпеки**
   Цінність:
   - Систематизація процесу виявлення і усунення потенційно шкідливих вразливостей;

- Зниження ризику схильності інфраструктури Замовника до можливих критичних інцидентів ІБ;
- Підвищення зрілості інфраструктури Замовника в контексті кібербезпеки.
- Проведення практичних випробувань інформаційних ресурсів (веб-додатків) та IT-інфраструктури Замовника на вразливості.

Табл. 1. Перелік запропонованих рішень та послуг

№	Найменування	Вартість
1	(#MNTR_SEC) Fortinet FortiManager	
2	(#CSOC_SOAR) Fortinet FortiManager	
3	(#DevSecOps) Checkmarx Software Security Platform	
4	(#APM) Dynatrace software intelligence platform	
5	(#SEC_PAM) One Identity Safeguard	
6	(#OPT_ChM,TSHOOT,DOC) NetBrain Network Automation Platform	
7	(#SEC_VM) Tenable.sc™ Continuous View	
8	Супутні послуги з інтеграції запропонованих рішення в інфраструктуру Замовника	

Загалом: 27 350 000,00 UAH

Загальна вартість пропозиції вказана станом на 15.09.2021 р. є оціночною та складає: 27 350 000,00грн. (двадцять сім мільйонів триста п'ятдесят тисяча грн. 00 коп.)

З повагою,

комерційний директор

ТОВ «Ві Єм Джі»

Комар Олександр Леонідович

LLC BELINTECH UKRAINE
56 Valeriia Lobanovskoho ave.,
Kyiv, 03037, Ukraine
Tel: (044) 222 82 93
www.bitech.com.ua

Вих. № 15/09-3 від 15.09.2021

В.о. директора
СКП "КИЇВТЕЛЕСЕРВІС"
П. Чернікову

Щодо запиту
цінової пропозиції

Шановний пане Черніков!

На Ваш запит від 13.09.2021 року за № 130-09/2021 щодо придбання Пакетів програмного забезпечення для керування виробничими процесами, ТОВ «БІЛІНТЕХ УКРАЇНА» повідомляє про наступне.

Згідно наданих технічних вимог надаємо розрахунок вартості Пакетів програмного забезпечення для керування виробничими процесами:

№ п/п	Найменування	Вартість грн без ПДВ	Вартість грн з ПДВ
1	Програмне забезпечення*	21 245 000,00	21 245 000,00
2	Послуги з налаштування	4 265 000,00	5 118 000,00
3	Послуги з навчання	250 000,00	300 000,00
Загальна вартість, грн з ПДВ			26 663 000,00

* Відповідно до пункту 26[1] підрозділу 2 розділу XX Перехідних положень Податкового кодексу України тимчасово, з 1 січня 2013 року до 1 січня 2023 року, звільняються від оподаткування податком на додану вартість операції з постачання програмної продукції.

Зазначаємо, що детальний розрахунок вартості програмного забезпечення наведено у додатку 1 до цього листа.

З повагою
Генеральний директор **В.В. Шахов**

ТОВ «БІЛІНТЕХ УКРАЇНА»
Юр. адреса: 03037, м. Київ,
Проспект Валерія Лобановського, буд. 56
Тел: (044) 222 82 93
www.bitech.com.ua
sales@bitech.com.ua

ЄДРПОУ 37962954
ІПН 379629526571
Св-во ПДВ № 200046963
п/р UA623006140000026009500220903
в АТ "КРЕДІ АГРІКОЛЬ БАНК"
МФО № 300614

LLC BELINTECH UKRAINE
56 Valeriia Lobanovskoho ave.,
Kyiv, 03037, Ukraine
Tel: (044) 222 82 93
www.bitech.com.ua

Додаток 1
До листа № 15/09-3 від 15.09.2021р.

Розрахунок вартості програмного забезпечення.

№ п/п	Підсистема	Од. виміру	К-ть	Вартість грн (без ПДВ)
1	Програмна продукція (Fortinet; FortiManager/ FortiAnalyzer) підсистеми керування мережевими пристроями безпеки для забезпечення керування 390 пристроїв безпеки строком дії не менше ніж 12 місяців.	Комплект	1	2 460 000,00
2	Програмна продукція (Fortinet FortiSOAR) підсистеми оркестрування, автоматизації та реагування на інциденти безпеки для забезпечення роботи не менш ніж 3 (три) аналітика строком дії не менше ніж 12 місяців.	Комплект	1	4 365 000,00
3	Програмна продукція (Fortify Static Code Analyzer) підсистеми пошуку вразливостей в рамках циклу розробки програмного забезпечення. для забезпечення роботи в не менш ніж 10 (десяти) одночасних проектах строком дії не менше ніж 12 місяців.	Комплект	1	2 630 000,00
4	Програмна продукція (Dynatrace) підсистеми моніторингу IT-сервісів: -примірник програмної продукції для забезпечення моніторингу IT-сервісів, що розміщені в інфраструктурі із загальним обсягом оперативної пам'яті не менш ніж 384 GB строком дії не менше ніж 12 місяців; -примірник програмної продукції для забезпечення контролю якості взаємодії користувачів із IT сервісами та моніторингу не менш ніж 1 000 000 сесій реальних користувачів строком дії не менше ніж 12 місяців.	Комплект Комплект	1 1	3 120 000,00 1 220 000,00
5	Програмна продукція (One Identity Safeguard) підсистеми моніторингу та контролю дій привілейованих користувачів. для забезпечення одночасної роботи з відповідними контрольованими (цільовими) системами не менш ніж 20 (двадцять) привілейованих користувачів в межах існуючої у Замовника інсталяції строком дії не менше ніж 12 місяців.	Комплект	1	1 490 000,00
6	Програмна продукція (One Identity Safeguard) підсистеми адаптивної мережевої автоматизації: -примірник програмної продукції для забезпечення одночасної роботи не менше ніж 1 (одного) адміністратора строком дії не менше ніж 12 місяців; -примірник програмної продукції для забезпечення покриття не менш ніж 250 мережевих пристроїв включаючи функціональність Change management строком дії не менше ніж 12 місяців; -примірник програмної продукції для забезпечення покриття не менш ніж 250 мережевих пристроїв включаючи функціональність Application Assurance строком дії не менше ніж 12 місяців.	Комплект Комплект Комплект	1 1 1	940 000,00 970 000,00 920 000,00
7	Програмна продукція (Tenable) підсистеми керування процесом пошуку та мінімізації впливу вразливостей IT-інфраструктури для забезпечення роботи підсистеми у відповідності до технічних вимог строком дії не менше ніж 12 місяців.	Комплект	1	3 130 000,00
Загальна вартість грн, без ПДВ				**21 245 000,00**

ТОВ «БІЛІНТЕХ УКРАЇНА»
Юр. адреса: 03037, м. Київ,
Проспект Валерія Лобановського, буд. 56
Тел: (044) 222 82 93
www.bitech.com.ua
sales@bitech.com.ua

ЄДРПОУ 37962954
ІПН 379629526571
Св-во ПДВ № 200046963
п/р UA623006140000026009500220903
в АТ "КРЕДІ АГРІКОЛЬ БАНК"
МФО № 300614