ОБГРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі послуг згідно з предметом закупівлі: ДК 021:2015 код 72260000-5 «Послуги, пов'язані з програмним забезпеченням» (Послуги у сфері інформатизації з постачання програмного забезпечення для комплексної системи захисту інформації в СІАЗ області на виконання п. 3.6. завдань регіональної програми інформатизації "Дніпропетровщина: цифрова трансформація" на 2023–2025 роки)

1. Замовник

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

2. Підстави закупівлі

Закупівля здійснюється відповідно до пункту 3.6. завдань регіональної програми інформатизації "Дніпропетровщина: цифрова трансформація" на 2023–2025 роки, яку затверджено рішенням сесії Дніпропетровської обласної ради від 14 жовтня 2022 року № 216-13/VIII.

Метою закупівлі є забезпечення програмним продуктом поштового серверного обладнання електронного комунікаційного центру (ЕКЦ) області корпоративної мережі системи інформаційно-аналітичного забезпечення Дніпропетровської облдержадміністрації для захисту електронної пошти відповідно до вимог комплексної системи захисту інформації.

Відповідно до вимог комплексної системи захисту інформації необхідно здійснювати дієві заходи щодо захисту системи електронного листування від проявів шкідливих програмних засобів, забезпечення технічних умов для безперебійного функціонування комп'ютерного обладнання та захисту інформації на них, а саме: забезпечувати багаторівневий захист від усього спектра загроз, що передаються електронною поштою, допомагати виявляти та запобігати атакам через електронну пошту, включаючи спам, фішинг, розсилку шкідливих програм та посилань, заміну відправника та компрометацію корпоративної електронної пошти (BEC).

Одним з найдієвіших заходів для вирішення вищезазначених завдань є встановлення відповідного програмного забезпечення на ЕКЦ області..

Зазначене програмне забезпечення застосовується для захисту веб-застосунків та API (для захисту існуючих сайтів, що функціонують на ЕКЦ області), розрахований на захист від атак вразливостей та загроз "нульового дня", у тому числі з урахуванням рекомендацій щодо першочергових заходів з кібербезпеки (в частині кіберзахисту), направлених листом Держспецзв'язку від 15.06.2023 № 05/05-3129/СЕД.

3. Очікувана вартість предмета закупівлі: 2520000,00 грн з ПДВ (обласний бюджет).

Очікувана вартість сформована з використанням примірної методики визначення очікуваної вартості предмета закупівлі, затвердженої наказом Мінекономіки від 18.02.2020 №275, на підставі запиту безпосередньо до представника виробника програмної продукції, самостійного аналізу цін на аналогічні за технічними характеристиками типи програмної продукції через мережу Інтернет та в електронній системі закупівель Prozorro, а також з урахуванням необхідності забезпечення економії бюджетних коштів в умовах дії правового режиму воєнного стану в Україні.

4. Технічні та якісні характеристики предмета закупівлі

ТЕХНІЧНА СПЕЦИФІКАЦІЯ

Найменування програмного забезпечення	Кількість, од.
Програмне забезпечення Web Application Firewall - virtual appliance for all supported platforms. Supports up to 4 x vCPU core	1
Технічна підтримка: FortiWeb-VM04 1 Year Advanced Bundle (FortiCare Premium plus AV, FortiWeb Security Service, IP Reputation, FortiSandbox Cloud Service, Credential Stuffing Defense Service and Threat Analytics)	1

Найменування	Технічні вимоги
Загальні вимоги	• Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових 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 запропоноване рішення не має бути анонсів end-of-sale та end-of life (EOS/EOL) від виробника • Запропоноване рішення повинно мати чинні експертні висновки Державної служби спеціального зв'язку та захисту інформації України на відповідність вимогам законодавства в галузі захисту інформації або проходити відповідну державну експертизу на момент подання Учасником пропозиції конкурсних торгів
Архітектура та форм-фактор	Система має поставлятись як віртуальна машина (VM), що буде встановлюватися на відповідний сервер з системою віртуалізації, які надаються замовником
Продуктивність (Throughput)	• Кожна одиниця цієї системи (яка може складатись з кластеру) має продуктивність обробки трафіку не менше ніж 500 Mbps
Ліцензування	• Необмежена кількість веб-додатків що захищаються • Ліцензія захисту від botnet, malicious IP, phishing URLs, anonymous proxies, Trojan, ddos sources • Ліцензія для балансування навантаження на сервери на 7 рівні (Load balancing) • Інші ліцензії, що потребують задоволенню наведених функціональних вимог
Резервування, відмовостійкість	• Active / Passive • Active / Active
Режими функціонування	• Зворотний проксі (Reverse Proxy) • Прозорий режим (Transparent / Bridge) • Прозорий проксі режим (Transparent Reverse Proxy) • Офлайн-режим (Non-inline sniffer / Off-line Sniffing) • WCCP
Мережевий функціонал	• Статична маршрутизація (Static routing) • Маршрутизація на основі політик (Policy-based routing) • Трансляція IP-адрес (NAT) • Віртуальні мережі (VLAN - IEEE 802.1Q)

	• Агрегація групи фізичних інтерфейсів в один логічний інтерфейс (LACP - IEEE 802.3ad)
SSL/TLS-обробка	• Обробка SSL/TLS (якщо для цього потрібні додаткові ліцензії, вони мають бути у комплекті поставки) • Дешифрування та інспектування SSL/TLS (SSL off-loading)
Створення еталонної моделі функціонування веб-додатків	• Створення еталонної моделі функціонування веб-додатків шляхом автоматичного навчання (auto learn) або машинного навчання (machine learning), які базуються на основі запитів користувачів до веб-додатків • Підтримка автоматизованого динамічного профілювання веб-додатків • Підтримка автоматизованого внесення змін в еталоную модель при зміні веб-додатків
Комплексний захист від атак OWASP top 10 та перевірка на вразливості	• Виявлення та попередження OWASP top 10 атак (https://www.owasp.org/index.php/Top_10-2017_Top_10) • Наявність вбудованого сканеру вразливостей або інтеграція зі стороннім рішенням даного типу (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічною підтримкою на такий саме термін, що й система захисту веб-серверів)
Захист від DOS/DDOS-атак, Bot-protection	• Виявлення та захист від атак повного перебору на облікові дані користувачів (Brute Force Login) • Захист від DoS-атак на 3/4 рівні OSI (TCP Flood Prevention) • Захист від DoS-атак на 7 рівні OSI (HTTP Flood Prevention) • Розпізнавання підключення до сайту програми (bot) чи людини за допомогою CAPTCHA-запиту (CAPTCHA request) чи з використанням тесту (Real Browser Enforcement / Bot Protection)
Відстеження користувачів та їх пристроїв	• Відстеження користувацьких сесій та поведінки користувачів після їх вдалої автентифікації (User Tracking) • Профілювання та відстеження пристроїв користувачів, визначення їх репутації безпеки на основі порушення ними політик безпеки та автоматизація відповідної реакції у реальному часі (Device Intelligence Service / Device identification tracking)
Функції захисту веб-додатків та веб-сайтів	• Розмежування та обмеження доступу на основі whitelist та blacklist • Захист від Botnet, Anonymous proxy, Phishing, tor, spam, ddos та інше на основі баз IP-репутації (IP Reputation) • Розмежування та обмеження доступу на основі баз IP-геолокації (IP Geolocation) • Перевірка відповідності HTTP RFC (Protocol validation) • Захист від відомих атак на основі сигнатур для веб-сервісів/додатків (Web services signatures) • Створення користувацьких сигнатур для захисту від атак на веб-сервіси/додатки (Custom signatures) • Запобігання витоків важливих даних (DLP signatures) • Додавання системних cookie у HTTP-запити без їх шифрування • Додавання системних cookie у HTTP-запити з їх шифруванням • Міжмережевий екран на 4 рівні OSI або списки керування

	доступу на 4 рівні OSI (Stateful Firewall / Access control lists / IP Filters) • Виявлення та блокування шкідливих програм (Malware detection) завдяки вбудованому антивірусу або завдяки інтеграції зі стороннім рішенням даного типу (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічної підтримкою на такий саме термін, що й WAF) • Аналіз команд протоколу FTP (Allowed / Blocked commands) при доступі до сайту та перевірка на наявність шкідливих програм у файлах що завантажуються “на” чи “з” сервера (upload or download) • Захист на основі бази скомпрометованих облікових даних (Credential Stuffing Defense) (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічної підтримкою на такий саме термін, що й WAF) • Захист на основі алгоритму машинного навчання для виявлення шаблонів атак, та присвоєння їм рівня серйозності (Threat Analytics) (дане рішення має бути включене до пропозиції з необхідним набором ліцензій та технічної підтримкою на такий саме термін, що й WAF)
Інтеграція з системою захисту від цілеспрямованих атак класу sandbox	• Запропоноване рішення повинно мати можливість інтеграції з існуючою у замовника системою захисту класу sandbox (FortiSandbox) від цілеспрямованих атак шляхом відправлення до неї файлів на перевірку та отримання результатів сканування • Запропоноване рішення повинно мати можливість інтеграції з системою захисту від складних атак нульового дня (хмарний сервіс від виробника обладнання - cloud sandbox), шляхом відправлення до неї файли на перевірку та отримання результатів сканування
Визначення логіки, порядку доступу до ресурсів сайту та цілісності структури сайту	• Визначення URL сайту, з якого має розпочинатись доступ до контенту сайту (Start Page Enforcement) • Визначення URL сайту, що мають бути доступні у певній черзі (Page Order Rules) • Дозвіл чи блокування доступу до певних URL сайту (URL access) • Дозвіл чи блокування певних методів доступу HTTP до сайту / URL (Allow / Deny HTTP Method) • Виявлення видалення, додавання чи зміни файлів на веб-сайті та автоматичне відновлення структури та контенту сайту (Web Defacement Protection)
Доставка та маршрутизация контенту додатків	• Переписування або переправлення запитів і відповідей HTTP (URL Rewriting, redirecting) • Маршрутизація запитів до серверів на основі HTTP контенту (HTTP content routing) • Можливість додавання чи зчитування оригінальної IP-адреси ініціатора сеансу з HTTP-заголовку (X-Forwarded-For / X-Real-IP / True-Client-IP) • Балансування навантаження на сервери на 7 рівні (Load balancing) • Перевірка доступності серверів (Health Check) для

	балансування навантаження за допомогою ICMP, TCP, HTTP • Стиснення файлів (Content compression) • Кешування контенту (Content caching) • SSL/TLS off-loading • Модернізація сторінок, що відображають код помилки при порушенні користувачами політик безпеки, недоступності веб-сайту, перевірки captcha
Підтримка та аналіз протоколів	• Підтримка та аналіз протоколів XML, JSON • Підтримка та аналіз протоколів HTTP/2 • Підтримка та аналіз протоколу WebSocket
Автентифікація	• Підтримка протоколів LDAP, RADIUS, TACACS+ • Підтримка 2-факторної автентифікації (two-factor authentication) • Підтримка єдиної автентифікації користувачів (single sign-on) через WAF для доступу до декількох веб-додатків в одному домені • Автентифікація на основі SSL-сертифікатів користувачів • Інтеграція з Public Key Infrastructure (PKI) • Модернізація сторінок автентифікації користувачів
Управління, звітність, інтеграція	• Графічний веб-інтерфейс (Web GUI) • Інтерфейс командного рядка (CLI) • Підтримка системи централізованого керування для декількох пристроїв • Підтримка REST API • Централізоване ведення журналів та звітності (logging and reporting) • Розмежування доступу різних груп адміністраторів, призначаючи їм різні адміністративні привілеї для підмножини політик і захищених імен хостів (Administrative domain / Administrative Partitions / Virtual domain) • Ролевий доступ адміністраторів (RBAC) • Повідомлення про події за допомогою SNMP, Syslog та Email • Пересилання та зберігання журналів подій на виділений пристрій за допомогою FTP/TFTP, Email • Функціонал запису пакетів з мережевого інтерфейсу для подальшого їх аналізу (packet capture) • Функціонал резервного копіювання та відновлення файлів конфігурації на виділений пристрій за допомогою FTP • Графічний інтерфейс відображення інформації щодо працездатності та основних характеристик системи у реальному часі • Підтримка інтеграції з системами типу SIEM • Інтегровані звіти
Технічна сервісна підтримка від виробника	• Запропоноване рішення повинно забезпечуватись технічною сервісною підтримкою від виробника строком не менше ніж 12 місяців з рівнем сервісу 24*7 • Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24*7 • Постійний авторизований доступ до сайту виробника 24*7

	• Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки • Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника • Можливість реєстрації сервісних випадків в режимі 24*7*365 в сервісній службі виробника

Додаткові вимоги:

1. Учасник повинен мати статус зареєстрованого партнера з надавачем послуг.
2. Наявність не менше 1 сертифікованого спеціаліста рівня NSE 2 або аналогічного.
3. Учасник повинен надати копії сертифікатів від надавача послуг.
4. Сертифікати повинні бути дійсними протягом строку надання послуг.
5. Учасник повинен надати документи, що підтверджують партнерські відносини (співпрацю) Учасника з надавачем послуг або з офіційним представництвом надавача послуг, про те що Учасник є авторизованим партнером або офіційним представником надавача послуг з правом реалізації оригінальних послуг відповідно, а саме:

• оригінал або копія листа (завірена Учасником) від надавача послуг /офіційного представництва надавача послуг щодо авторизації Учасника та/або визнання його офіційним представником надавача послуг, а також, що послуги, які пропонує (реалізує) Учасник є оригінальними;

• та/або копія договору (завірена Учасником), що підтверджує партнерські відносини (співпрацю) Учасника та надавача послуг з постачання програмного забезпечення /офіційного представництва постачальника програмного забезпечення.