**Запит на комерційну пропозицію**

**щодо закупівлі програмного забезпечення для впровадження підсистеми керування ідентифікаційними даними та доступом, послуг з її впровадження та підтримки**

**АТ «Концерн Галнафтогаз»**

**ЛЬВІВ 2025**

**ЗАПРОШЕННЯ
до участі в конкурсі**

Компанія «Концерн Галнафтогаз» (www.okko.ua) повідомляє про проведення конкурсу потенційних партнерів по постачанню програмного забезпечення для впровадження підсистеми керування ідентифікаційними даними та доступом, послуг з її впровадження та підтримки для АТ «Концерн Галнафтогаз».

1. **Інформація про компанію**

Компанія «Концерн Галнафтогаз», є оператором мережі АЗК «ОККО» – однієї з найбільших автозаправних мереж в Україні, до складу якої сьогодні входить понад 400 АЗК у всіх регіонах держави. Вона також управляє найбільшою в Україні мережею закладів харчування в дорозі, що працює під брендами A la minute, Pasta Mia, Hot café. У складі мережі «ОККО» працює 10 нафтобаз і 12 акредитованих лабораторій контролю якості нафтопродуктів. Команда «Концерну Галнафтогаз» (далі - «Замовника») налічує майже 10 тисяч працівників.

1. **Предмет закупівлі:**
* Постачання програмного забезпечення для впровадження підсистеми керування ідентифікаційними даними та доступом, терміном на 1 (один) рік (далі – «ПЗ»).
* Надання послуг з впровадження підсистеми керування ідентифікаційними даними та доступом (далі – «Підсистема»).
* Надання послуг з розширеної технічної підтримки Підсистеми строком на 1 (один) рік, починаючи з моменту завершення впровадження Підсистеми.
1. **Регламент проведення конкурсу та терміни**

3.1. Контактна особа з організаційних і технічних питань: Роман Стефанишин, менеджер департаменту інформаційної безпеки, (електронна пошта RStefanyshyn@gng.com.ua).

Додаткова інформація може бути надана на вимогу, якщо вона буде відповідати предмету конкурсу.

3.2. Регламент проведення конкурсу:

* Формування та розсилка Запиту на комерційну пропозицію.
* Отримання комерційних пропозицій.
* Аналіз та оцінка комерційних пропозицій, формування короткого списку.
* На вимогу Замовника проведення презентації комерційної пропозиції учасників “on-line». Час узгоджується індивідуально. Тривалість презентації не більше ніж 2 години. Презентацію пропозиції повинен проводити керівник проекту.
* Проведення редукціону серед учасників, які пройшли кваліфікаційний відбір та надали пропозицію, яка відповідає вимогам тендеру (заплановано багатокроковий редукціон).
* Погодження та підпис договору.
1. **Специфікація програмного забезпечення та послуг**

У рамках конкурсу Учасник повинен надати специфікацію програмного забезпечення та послуг згідно наведених нижче вимог та заповнений Додаток №1.

1. **Вимоги щодо кваліфікації Учасника**

Учасник повинен мати статус авторизованого партнера виробника рішення якого подає пропозицію, що підтверджується авторизаційним листом від виробника програмного забезпечення та/або офіційним представником виробника в Україні.

Учасник повинен мати досвід постачання та надання послуг з впровадження програмного забезпечення для інформаційної безпеки. На підтвердження Виконавець повинен надати не менше 3 (трьох) листів-відгуків про надання аналогічних послуг.

1. **Технічні вимоги:**

|  |
| --- |
| **6.1.**  **До програмного забезпечення**  **підсистеми керування ідентифікаційними даними та доступом:** |
|  | ПЗ має забезпечувати **централізований контроль автентифікації та авторизації** для користувачів, сервісних акаунтів, привілейованих облікових записів та доступу до серверних ОС, баз даних і хмарних застосунків (єдиний інтерфейс керування). |
|  | ПЗ має підтримувати **масштабування** для моніторингу безпеки для **не менше 3000 облікових записів**, із можливістю подальшого розширення. |
|  | ПЗ має підтримувати **захист не менше ніж 150 сервісних облікових записів та 250 привілейованих облікових акаунтів** із автоматичним виявленням та класифікацією (Privileged Access Security, Service Accounts, Cloud Non-Human Identities). |
|  | ПЗ має підтримувати можливість впровадження **багатофакторної автентифікації (MFA) без агентів** на кінцевих системах і пристроях користувачів (agentless MFA). |
|  | ПЗ має забезпечувати MFA та контроль автентифікації у **середовищах з legacy-протоколами** (Kerberos, NTLM, LDAP), які не підтримують сучасні механізми безпеки. |
|  | ПЗ має дозволяти налаштовувати MFA для **будь-якого ресурсу** (сервери, бази даних, VPN, мережеве обладнання), що використовує централізовану автентифікацію. |
|  | ПЗ має підтримувати **політики умовного доступу (Conditional Access)** з урахуванням **ризиків автентифікації** (географія, час, пристрій, підозрілі сесії тощо). |
|  | ПЗ має забезпечувати **захист сервісних акаунтів**, включно з контролем використання лише в заданому контексті та забороною lateral movement. |
|  | ПЗ має дозволяти контролювати та обмежувати **кількість активних сесій сервісних акаунтів**. |
|  | ПЗ має забезпечувати **моніторинг та аудит усіх подій автентифікації у реальному часі**, зберігання логів та їх подальший аналіз. |
|  | ПЗ має підтримувати **сповіщення адміністраторів про підозрілі спроби автентифікації** (Risk Indicators, Threat Indicators). |
|  | ПЗ має інтегруватися з **SIEM та SOAR** для передавання подій автентифікації, інцидентів та ризикових показників у режимі реального часу. |
|  | ПЗ має підтримувати інтеграцію з **Active Directory** (у тому числі керування привілейованими акаунтами). |
|  | ПЗ має підтримувати інтеграцію з **Microsoft Authenticator** для виклику та застосування MFA. |
|  | ПЗ має підтримувати використання **push-сповіщень** як методів MFA для 250  **привілейованих облікових акаунтів** використовуючи існуюче рішення MFA Microsoft Authenticator та через власний Mobile App для 25 **облікових акаунтів** (як резервний варіант). |
|  | ПЗ має дозволяти створення **винятків для критичних сервісних акаунтів** із документованим обґрунтуванням (наприклад, для сценаріїв break-glass). |
|  | ПЗ має забезпечувати **контроль доступу до адміністративних інтерфейсів ОС, баз даних, хмарних сервісів** та виявлення привілейованих входів. |
|  | ПЗ має забезпечувати **централізоване управління політиками доступу через єдиний інтерфейс**, з підтримкою **шаблонів політик** і гнучким налаштуванням (Policy Templates, Custom Policies). |
|  | ПЗ має забезпечувати **Just-In-Time (JIT) доступ** до привілейованих акаунтів із MFA та зазначенням причини доступу, з автоматичним відключенням після завершення сесії. |
|  | ПЗ має забезпечувати **виявлення та блокування атак на рівні автентифікації** (Pass-the-Hash, Pass-the-Ticket, Kerberoasting, NTLM Relay, Golden Ticket, MFA Bombing тощо). |
|  | ПЗ має забезпечувати **Identity Security Posture Management (ISPM)** – виявлення небезпечних налаштувань (unsafe practices), проблем із гігієною облікових записів (наприклад, паролі без експірації, слабке шифрування). |
|  | ПЗ повинно підтримувати розгортання своїх компонентів в Azure Cloud інфраструктурі. |
|  | ПЗ повинно підтримувати інтеграцію з рішеннями Microsoft і наявність офіційної документації від Microsoft що підтверджує таку можливість |
|  | Термін дії ліцензій і технічної підтримки від виробника має становити **не менше 12 місяців**. |
| **6.2.**  **Вимоги до процесу та обсягу послуг з впровадження Підсистеми**  **керування ідентифікаційними даними та доступом:** |
|  | Виконавець має провести обстеження існуючої інфраструктури Замовника та погодити технічне завдання для впровадження Підсистеми керування ідентифікаційними даними та доступом. |
|  | Виконавець повинен здійснити налаштування Підсистеми, провести інтеграцію в інфраструктуру та надати технічну та експлуатаційну документацію, яка складається з:* Паспорт підсистеми
* Інструкція адміністратора
* Інструкція користувача
 |
|  | Виконавець повинен здійснити інсталяцію та налаштування ПЗ. |
|  | Виконавець має провести інтеграцію ПЗ з Active Directory, SIEM та іншими сумісними системами. |
|  | Виконавець має розробити та погодити із Замовником політики захисту аутентифікацій.  |
|  | Виконавець має забезпечити захист щонайменше 150 сервісних акаунтів та 250 привілейованих облікових записів. |
|  | Виконавець має забезпечити можливість впровадження MFA токенів для 25 користувачів. |
|  | Виконавець має розробити та погодити із Замовником рольову модель доступу. |
|  | Виконавець має забезпечити механізм оповіщення відповідальних осіб про інциденти автентифікації. |
|  | Виконавець повинен виконати модифікацію джерел даних та скриптів для дашбордів SOC. |
|  | Виконавець повинен погодити та впровадити як мінімум наступні автоматизовані UseCase на IBM QRadar SIEM для контролів ІБ Системи (5 шт.):* Контроль використання MFA – забезпечення захищеної автентифікації до критичних систем;
* Контроль аномальних дій автентифікації облікових записів (Insights) – виявлення підозрілих сценаріїв автентифікації;
* Контроль сервісних облікових записів – виявлення автентифікації сервісних облікових записів не за призначенням;
* Контроль створення/видалення політик Підсистеми – захист від несанкціонованих змін політик;
* Контроль загроз з Identity Threat Detection – виявлення активних загроз засобами Identity Threat Detection.
 |
|  | Виконавець має запропонувати та погодити із Замовником звіти у вигляді дашбордів реалізованих на Microsoft PowerBI. |
| **6.3.**  **Вимоги до процесу та обсягу послуг з розширеної технічної підтримки Підсистеми**  **керування ідентифікаційними даними та доступом:** |
|  | Виконавець має забезпечити вирішення технічних інцидентів у роботі Підсистеми:* виявлення та інформування Замовника щодо відхилень у роботі Підсистеми;
* діагностика відхилень у роботі Підсистеми;
* збір інформації про причини інциденту та її аналіз;
* внесення змін для вирішення технічних інцидентів;
* опрацювання технічних інцидентів, в т.ч. за запитом Замовника;
* надання Замовнику інформації щодо причин виникнення та шляхів вирішення технічного інциденту.
 |
|  | Виконавець має забезпечити адміністрування Підсистеми:* оновлення компонентів Підсистеми;
* надання рекомендацій при налаштуванні інтеграцій з допомогою існуючих конекторів;
* налаштування базової конфігурації Підсистеми та політик захисту;
* надання консультацій та рекомендацій Замовнику щодо зміни апаратних характеристик компонентів Підсистеми.
 |
|  | Виконавець має забезпечити супровід запитів до вендора/розробника:* реєстрація/закриття запитів;
* виконання рекомендацій згідно відповіді підтримки вендора;
* надання даних для діагностики підтримці вендора.
 |
|  | Виконавець має забезпечити виконання регламентних робіт щодо оновлення компонентів Підсистеми:* підтримка актуальності версії ПЗ (які не передбачають змін архітектури/міграції);
* підтримка актуальності версії додатків.
 |
|  | Виконавець має забезпечити актуалізацію документації:* Опис поточної конфігурації Підсистеми;
* Актуалізація документації після внесення змін;
* Формування супроводжуючої документації за запитом Замовника.
 |
|  | Виконавець має забезпечити аналітичне супроводження Підсистеми:* підтримка переліку критичних облікових записів (далі – «ОЗ») для покриття МFA:
* спільне з Замовником визначення критеріїв критичності ОЗ;
* фіксація критеріїв на технічному рівні в технологічній платформі SOC;
* постійне визначення переліку критичних ОЗ;
* підтримка переліку ОЗ, що покриваються МFA, з урахуванням рівня критичності.
* підтримка переліку високопріоритетних технологічних записів, що потребують моніторингу
* спільне з Замовником визначення переліку критеріїв ризику, що впливають на технічні ОЗ;
* фіксація критеріїв на технічному рівні в технологічній платформі SOC;
* постійне визначення переліку технічних ОЗ, що потребують моніторингу;
* підтримку переліку ОЗ, що покриваються моніторингом, з урахуванням рівня ризику.
* реагування на спрацювання Use Case;
* підтримка ескалації спрацювань контролів Підсистеми;
* аналітика спрацювань Підсистеми.
 |
|  | Виконавець має забезпечити надання звітності:* формування звітності щодо наданих послуг(може бути онлайн дашборд);
* формування звітності щодо стану Підсистеми (може бути онлайн дашборд);
* Участь у щоденних доповідях по інцидентах за участю SOC команди.
 |
|  | Строк надання послуг з розширеної технічної підтримки Підсистеми – 1 (один) рік, починаючи з моменту завершення впровадження Підсистеми. |
|  | Виконавець має забезпечити наступний рівень SLA (в робочі дні з 9-00 до 18-00) реагування на звернення Замовника:* Критичний рівень – 1 година; (в робочі дні з 08-00 до 19-00)
* Високий рівень – 2 години;
* Середній рівень – 4 години;
* Низький рівень – 8 годин;
* Надання консультацій Замовнику – 8 годин.
 |

**Умови та терміни подачі комерційних пропозицій.**

Для участі в тендері потрібно підготувати комерційну пропозицію відповідно до Додатку №1 та надати пакет необхідних документів (згідно вимог ТЗ) та занести дані у відповідні розділи тендерної платформи <https://tpext.gng.com.ua> . Мова надання пропозицій: українська.

**ДОДАТОК №1**

**Комерційна пропозиція для АТ «Концерн Галнафтогаз».**

|  |  |
| --- | --- |
| Назва постачальника | \* |
| Адреса постачальника | \* |
| Телефони | \* |
| e-mail | \* |
| ПІБ особи, відповідальної за комерційну пропозицію | \* |
| Контактна інформація особи, відповідальної за комерційну пропозицію | \* |

\* поле обов’язкове до заповнення

1. **Специфікація**

1.1. Програмне забезпечення для Підсистеми керування ідентифікаційними даними та доступом:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **з/п**  | **Найменування**  | **К-сть**  | **Ціна за одиницю, грн, з ПДВ\***  | **Вартість, грн,** **з ПДВ** |
| 1  | Програмне забезпечення *(назва програмного забезпечення)* |  |  |  |
| **Загальна вартість з ПДВ грн.:**  |  |
| **ПДВ:** |  |

1.2. Послуги з впровадження Підсистеми керування ідентифікаційними даними та доступом:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **з/п** | **Найменування** | **К-сть** | **Ціна за одиницю, грн, з ПДВ** | **Вартість, грн,****з ПДВ** |
| 1 | Послуги з впровадження Підсистеми керування ідентифікаційними даними та доступом: | 1 |  |  |
| **Загальна вартість з ПДВ грн.:**  |  |
| **ПДВ:** |  |

1.3. Послуги з розширеної технічної підтримки Підсистеми керування ідентифікаційними даними та доступом, терміном на 1 (один) рік:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **з/п** | **Найменування** | **К-сть****(кварталів)** | **Ціна за квартал, грн, з ПДВ** | **Вартість****за 1 рік, грн,****з ПДВ** |
| 1 | Послуги з розширеної технічної підтримки Підсистеми керування ідентифікаційними даними та доступом: | 4 |  |  |
| **Загальна вартість з ПДВ грн.:**  |  |
| **ПДВ:** |  |