**Приложение № 1**

**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

1. **ОБХВАТ:** „Софийска вода“ АД разполага със система за управление на информацията и Събитията, свързани с киберсигурността (SIEM), базирана на IBM Qradar.

Настоящият проект има за основна цел предоставянето на професионални услуги с цел анализ и оптимизиране на системата за управление на информацията и събитията (SIEM) на „Софийска вода“ АД, базирана на IBM Qradar, поради необходимостта от ефективно справяне с множеството генерирани аларми. В обхвата на проекта са включени:

* Анализ на текущо генерирани аларми в SIEM системата, въз основа на правилата, дефинирани по потребителски критерии (приложени на ниво група), с цел идентифициране на мерки за смекчаване на тяхното проявление;
* Проучване и анализ на логиката на десетте най – шумни правила и разработване на предложения за подобрения;
* Внедряване и проверка на промените в логиката на правилата в SIEM след одобрение от „Софийска вода“ АД;
* Предоставяне на препоръки за промени в инфраструктурата (мрежова, сървърна, изчислителна и решения, базирани на Microsoft), която корелира със SIEM, на база на извършения анализ на правилата и генерираните аларми;
* След което в рамките на една работна седмица експерти на „Софийска вода“ АД и избрания Изпълнител трябва да обсъдят конкретни стъпки и действия, необходими за изпълнението на предложените промени в инфраструктурата. Избраният изпълнител трябва да осигури помощ за оптималната интеграция на предложените подобрения. Препоръките за промяна могат да обхванат спектър от дейности, които се отнасят към мрежовата, сървърната и изчислителна инфраструктура, както и към решения, базирани на Microsoft;
* Проследяване на ефективността на промените в правилата в рамките на един месец след тяхното внедряване и прилагане на корекции в случай на необходимост.

Всички дейности по проекта ще се извършват през контролиран отдалечен достъп до системите, осигурен от „Софийска вода“ АД или на място, при възникнала необходимост.

1. **ИЗИСКВАНИЯ КЪМ УЧАСТНИЦИТЕ**:
   1. Участниците трябва да предоставят техническо и ценово предложение, съдържащо следната информация:
      1. Срок за изпълнение на дейностите, попълнен в следната таблица:

|  |  |
| --- | --- |
| Дейност | Работни дни |
| Анализ на текущо генерирани аларми в SIEM системата, въз основа на  правилата, дефинирани по потребителски критерии (приложени на ниво  група), с цел идентифициране на мерки за смекчаване на тяхното  проявление |  |
| Проучване и анализ на логиката на десетте най – шумни правила и  разработване на предложения за подобрения |  |
| Внедряване и проверка на промените в логиката на правилата в SIEM след  одобрение от Софийска вода АД |  |
| Предоставяне на препоръки за промени в инфраструктурата |  |
| Съвместни дейности по прилагане на промени в инфраструктурата |  |
| Извършване на оценка на ефективността на промените в правилата. Предоставяне на доклад на извършените анализ и дейности. |  |

* + 1. Ценово предложение, попълнено в следната таблица:

|  |  |
| --- | --- |
| Дейност | Обща стойност в лв. без ДДС |
| Професионални услуги с цел анализ и оптимизиране на системата за управление на информацията и събитията (SIEM) на Софийска вода, базирана на IBM Qradar, поради необходимостта от ефективно справяне с множеството генерирани аларми. |  |

* 1. **Изисквания към Участниците, при подаване на офертата:**
     1. Участниците следва да притежават валиден, към датата на подаване на офертата, сертификат за внедрена система за управление на качеството, съответстваща на изискванията на стандарт БДС EN ISO 9001:2015. Участниците трябва да предоставят копие на сертификата при подаване на офертата.
     2. Участниците следва да са внедрили успешно поне една система за управление на информацията и събитията (SIEM), базирана на IBM Qradar. Участниците трябва да предоставят доказателство за внедрената система.
     3. Участниците следва да разполагат със следните експерти, като за доказателство трябва да приложат копия от сертификатите. Забележка: един експерт може да притежава повече от един от посочените сертификати:

|  |
| --- |
| Поне един експерт, притежаващ валиден сертификат ITIL Foundation Certificate in IT Service Management Version 4 |
| Поне един експерт, притежаващ валиден сертификат Certified Information Systems Security Professional |
| Поне един експерт, притежаващ валиден сертификат Certified Information Security Manager |
| Поне един експерт, притежаващ валиден сертификат IBM Certified Administrator - Security QRadar SIEM V7.5 |
| Поне един експерт, притежаващ валиден сертификат IBM Certified Deployment Professional – Security QRadar SIEM V7.5 |