ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

ПОКАНА

„Информационно обслужване" АД, със седалище и адрес на управление: гр. София, ул. „Панайот Волов" № 2, тел. 02/9420340, e-mail: office@is-bg.net, представлявано от **Ивайло Филипов – Изпълнителен директор**, Ви кани да участвате в процедура за избор на доставчик, при следните условия:

1. **Предмет на процедурата:**

„Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване" АД".

Количествената и техническа спецификация на софтуера за наблюдение, разследване и реагиране на хибридни атаки и инциденти е посочена в Техническо задание – Приложение №1.

2. **Срок за изпълнение:**

2.1. Срок за доставка на лицензите за софтуера - до 10 (десет) работни дни, считано от датата на сключване на договор.

2.2. Срок на валидност на лицензите - 3 (три) години, считано от датата на приемо-предавателния протокол за доставка.

3. **Критерии за оценка на предложенията:** „най-ниска предложена цена".

Участниците се класират според предложената от тях обща цена в лева без ДДС. На първо място се класира участникът, предложил най-ниска цена. Оценката на предложенията се извършва съгласно Методика за оценка на предложенията, приложена към настоящата покана (Приложение № 2).

4. **Списък на документите, които кандидатите следва да представят:**

4.1. Документи за идентификация и квалификация:

4.1.1. Документ/оторизация от производителя на софтуерното решение, удостоверяващ, че кандидатът е оторизиран доставчик за корпоративни клиенти.

4.1.2. Декларация по образец – Приложение № 5.

4.2. Техническо предложение, изготвено по образец - Приложение № 3.

4.3. Ценово предложение, изготвено по образец - Приложение № 4.

5. Начин на плащане: извършва се по банков път, на три равни годишни вноски в срок до 30 (тридесет) дни след:

5.1. подписване на приемо-предавателен протокол и приемане без възражения и забележки от Възложителя и издадена фактура от Изпълнителя (за първата годишна вноска);

5.2. издадена фактура от Изпълнителя (за втората и третата годишна вноска).

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

6. **Максимална обща цена** – кандидатите следва да предложат цена, която не надвишава определената максимална обща цена от **420 000 (четиристотин и двадесет хиляди) лв. без ДДС**.

   Кандидат, предложил по-висока от максималната обща цена, ще бъде отстранен от участие в процедурата.

7. **Срок на валидност на предложението** - срокът на валидност да бъде не по-малко от 60 (шестдесет) календарни дни, считано от датата на представяне на предложението.

8. **Подаване на предложението:**

8.1. Срок, място и начин:

Предложението следва да бъде подадено по електронен път в срок **до 12:00 часа на 30.04.2024 г.**, на следния адрес на електронна поща: office@is-bg.net.

8.2. Изисквания към подаване на предложението:

Техническото предложение (Приложение № 3), Ценовото предложение (Приложение № 4) и Декларацията (Приложение № 5) се съставят като електронни документи във формат .pdf и се подписват с квалифициран електронен подпис.

Ако към предложението е необходимо да бъде представен документ, който е издаден на хартиен носител, същият се представя сканиран и заверен с квалифициран електронен подпис.

В случай, че обстоятелства от документите за идентификация и квалификация са достъпни чрез публичен безплатен регистър или информацията е публично достъпна на друг официален адрес, кандидатите могат да посочат електронен адрес, на който тази информация е налична и достъпна.

Електронното съобщение, с което се подава предложението в настоящата процедура, следва да съдържа данни за:

1. наименованието на участника;
2. телефон и електронен адрес;
3. наименованието на процедурата, за която се подават документите.

За дата и час на получаване на предложението се приемат датата и часа на получаване на предложението на посочения в т. 8.1 адрес на електронна поща за подаване на предложения.

„Информационно обслужване“ АД използва инструменти за осигуряване на сигурността на информацията, предавана по електронна поща, които могат да забавят получаването на електронни съобщения, поради което е препоръчително предложенията в настоящата процедура да се изпращат най-малко 30 минути преди крайния срок по т. 8.1.

9. **Лице за контакти с „Информационно обслужване” АД**

Симеон Кърцелянски, ръководител, отдел Киберсигурност, отдел „Оперативен център за киберсигурност“, мобилен: +359 877 469 169, e-mail: s.kartselyanski@is-bg.net.

10. **Участници в процедурата**

В процедурата могат да участват и кандидати, до които не е изпратена изрична покана.

ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

11. Приложения:

11.1. Техническо задание – Приложение № 1;
11.2. Методика за оценка на предложенията – Приложение № 2;
11.3. Техническо предложение – образец - Приложение № 3;
11.4. Ценово предложение – образец - Приложение № 4;
11.5. Декларация – образец – Приложение № 5;
11.6. Указания за участие в процедурата – Приложение № 6.

Ivaylo Borisov Filipov
Digitally signed by Ivaylo Borisov Filipov
Date: 2024.04.17 11:24:44 +03'00'

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ” АД

Приложение № 1

ТЕХНИЧЕСКО ЗАДАНИЕ

с

Количествена и техническа спецификация за
„Софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“

№	Продукт	Описание	Количество
Софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти			
1.	Software/licence	Detect for Network software subscription and support, per active IP - (3Y)	1
2.	Software/licence	Recall (GB/Day) - 2 WKS	90
3.	Software/licence	Detect for M365 subscription and support, per internal account (3Y)	700
4.	Software/licence	Detect for Azure AD subscription and support, per internal account (3Y)	700

Технически и функционални изисквания	
Софтуер за реагиране и обработка на хибридни атаки	
REQ.1.	Да бъде доставена система за откриване на хибридни заплахи, на база поведенчески анализ на данните от мрежовия трафик. Участникът да достави всички необходими лицензи с права за ползване на всички изисквани функционалности, за период от минимум 36 (тридесет и шест) месеца.
REQ.2.	Системата да предоставя функционалност за откриване на заплахи в реално време в мониторираните мрежи на Възложителя въз основа на идентифициране на поведение и действия типични при атака.
REQ.3.	Системата да може да извършва анализ на мрежов трафик във вътрешните мрежи на възложителя и в облачни мрежи. Системата да осигурява видимост в North-South, East-West трафик.
REQ.4.	Системата включва функционалност за откриване на заплахи в облачни услуги Microsoft Azure AD и Microsoft 365 за потребителски идентичности.
REQ.5.	Системата да предоставя възможност за надграждане с функционалност за откриване на заплахи в облачна среда/услуги в Amazon AWS.
REQ.6.	Системата да не изисква използването на агенти за предоставяне на изискваните функционалности.
REQ.7.	Системата да може да идентифицира заплахи в криптиран трафик.

REQ.8.	Системата да включва функционалност за генериране на автоматични известия при откриване на заплахи.
REQ.9.	Системата да разполага с механизъм за динамично оценяване на риска на отделните хостове в мрежата на организацията на база тяхното поведение във времето.
REQ.10.	При откриване на подозрително поведение, повтарящо се на един и същ хост, системата да добавя откритите събития в едно общо събитие, като увеличава тежестта на неговия риск, вместо да генерира множество отделни аларми или известия.
REQ.11.	Системата да може да открива и обединява на едно място информация за подозрителни активности в поведението на различни хостове водещи до обща заплаха, например C2C комуникация, с цел предоставяне на изглед от едно място върху напредъка и разпространението на заплахата в мрежата на организацията. Всички открити подозрителни активности да са придружени с описание за модела на тяхното засичане и описание на поведението.
REQ.12.	Системата да включва функционалност за извличане на минимум 90GB метаданни на ден от мрежовия трафик и тяхното препращане за съхранение за минимум 14 дни в облачно приложение и хранилище на производителя с цел извършване на задълбочен анализ и лов на заплахи.
REQ.13.	Системата да може да открива заплахи на база идентифициране на индикатори за поведение и действия типични за атакуващите и посредством съпоставянето им с техниките по MITRE ATT&CK framework.
REQ.14.	Системата да може да открива заплахи и идентифицира потенциална злонамерена дейност или компрометиране въз основа на контекста на наблюдаваното поведение в хостове, акаунти и услуги.
REQ.15.	Системата да може да изгражда модел на взаимодействията между различни потребителски акаунти, хостове и услуги в наблюдаваната мрежа на база, на който да може да засича аномалии и да открива злоупотреба с привилегировани акаунти, като нетипично използване на потребителски акаунт на различни устройства или използване на услуги на хостове, които обикновено потребителя не използва.
REQ.16.	Предложената система да включва централизирано управление и администриране на всички нейни компоненти.
REQ.17.	Системата да включва функционалност за сортиране на събитията по важност, включително инструмент за предлагане и създаване на автоматични правила за филтриране на събития, които с голяма вероятност са в резултат на нормална комуникация в инфраструктурата на организацията.
REQ.18.	Системата да използва пасивна техника за инспекция на трафика, да не въвежда латентност в мрежата и да не оказва въздействие върху производителността на съществуващи услуги и приложения в организацията.
REQ.19.	Системата да използва, като основен източник на данни, метаданни от необработен мрежов трафик прихванат от предложената система.
REQ.20.	Интерфейсът на системата да включва табло с информация за високорисковите хостове в мрежата на организацията за да насочва фокуса на анализатора с цел подобряване на времето за откриване и реакция на заплахи.
REQ.21.	Системата трябва да идентифицира хостове и акаунти, засегнати от конкретна кампания за атака, позволявайки на анализаторите да идентифицират всички засегнати хостове и акаунти и да разберат първоизточника на атаката и последователността от събития.

REQ.22.	Системата трябва да може да идентифицира и проследява хостове, включително когато се свързват през VPN. Да проследява страничното движение на нападатели и всички засегнати хостове, да изгражда и предоставя изглед на цялата кампания на атаката, и да добавя информация за взаимовръзките между засегнатите хостове, акаунти и използвани услуги.
REQ.23.	Системата да предлага възможност за бъдещо надграждане с функционалност за изпращане на извлечени и обогатени от нея метаданни за мрежовия трафик към външен Data Lake и SIEM решения.
Изисквания за управление на логове и интеграция	
REQ.24.	Системата да може да съхранява локално записи за откритите заплахи за период не по-малък от 3 месеца.
REQ.25.	Системата да предлага възможност за интеграция с решения за реагиране на инциденти на трети страни посредством API интерфейс.
REQ.26.	Системата да включва интеграция с Active Directory, която да позволява ръчно или автоматизирано деактивиране или заключване на акаунти през потребителския интерфейс на системата.
REQ.27.	Системата да включва RESTful API интеграция с EDR решения на трети страни, която позволява ръчно или автоматизирано блокиране на хост.
REQ.28.	Системата да включва интеграция с NGFW решения на трети страни, която да позволява, като минимум изолиране на хост на ниво защитна стена, чрез динамично създаване на правила за блокиране.
REQ.29.	Системата да включва интеграция със SIEM, с цел обогатяване на SIEM с информация за активни заплахи, неоткрити от останалите решения за сигурност внедрени в организацията.
REQ.30.	Системата да включва интеграция със SOAR, с цел обогатяване на SOAR с информация за активни заплахи за стартирането на автоматизирани процеси, като отваряне на инцидент, автоматизиран процес за реакция при инцидент и т.н.
REQ.31.	Системата да може да приема информация от различни канали за разузнаване на заплахи (Threat Intelligence Feeds)

Приложение № 2

Методика за оценка на предложенията,

подадени в процедура за избор на доставчик с предмет:

„Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“

1. Предложенията се оценяват за съответствие с техническите изисквания в Техническото задание - Приложение № 1.

2. Предложенията, отговарящи на изискванията по т. 1, се оценяват по критерия „най-ниска предложена цена“, като се сравнява предложената обща цена в лева без ДДС.

3. На първо място се класира участникът, предложил най-ниска цена, като участниците се подреждат по възходящ ред.

Приложение № 3

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ“ № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

за

участие в процедура за избор на доставчик с предмет:

„Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“

След запознаване с поканата за участие в процедура за избор на доставчик с предмет: „Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“, с настоящото Техническо предложение правим следните обвързващи предложения:

1. Срок за изпълнение:
   1.1. Декларираме, че ще доставим лицензите за софтуера в срок до ……..…./……./ работни дни (*не повече от 10 /десет/ работни дни*), считано от датата на сключване на договор.
   1.2. Срокът на валидност на лицензите е 3 (три) години, считано от датата на приемо-предавателния протокол за доставка.
2. Приемаме да изпълним предмета на процедурата, съгласно всички условия и изисквания, посочени от Възложителя в поканата за участие в настоящата процедура и Техническото задание - Приложение № 1.
3. Приемаме да осигурим възможност за обновяване по всяко време на софтуерното решение до последна версия за целия период на валидност на лицензите.
4. Предложението е със срок на валидност …….. / ……/ календарни дни *(не по-малко от 60 /шестдесет/ календарни дни)*, считано от датата на представяне на предложението.

5. Приемаме да доставим софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти, със следната количествена и техническа спецификация:

№	Продукт	Описание	Количество
Софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти			
1.	Software/licence	Detect for Network software subscription and support, per active IP - (3Y)	1
2.	Software/licence	Recall (GB/Day) - 2 WKS	90
3.	Software/licence	Detect for M365 subscription and support, per internal account (3Y)	700
4.	Software/licence	Detect for Azure AD subscription and support, per internal account (3Y)	700

Технически и функционални изисквания	
Софтуер за реагиране и обработка на хибридни атаки	
REQ.1.	Да бъде доставена система за откриване на хибридни заплахи, на база поведенчески анализ на данните от мрежовия трафик. Участникът да достави всички необходими лицензи с права за ползване на всички изисквани функционалности, за период от минимум 36 (тридесет и шест) месеца.
REQ.2.	Системата да предоставя функционалност за откриване на заплахи в реално време в мониторираните мрежи на Възложителя въз основа на идентифициране на поведение и действия типични при атака.
REQ.3.	Системата да може да извършва анализ на мрежов трафик във вътрешните мрежи на възложителя и в облачни мрежи. Системата да осигурява видимост в North-South, East-West трафик.
REQ.4.	Системата включва функционалност за откриване на заплахи в облачни услуги Microsoft Azure AD и Microsoft 365 за потребителски идентичности.
REQ.5.	Системата да предоставя възможност за надграждане с функционалност за откриване на заплахи в облачна среда/услуги в Amazon AWS.
REQ.6.	Системата да не изисква използването на агенти за предоставяне на изискваните функционалности.
REQ.7.	Системата да може да идентифицира заплахи в криптиран трафик.
REQ.8.	Системата да включва функционалност за генериране на автоматични известия при откриване на заплахи.
REQ.9.	Системата да разполага с механизъм за динамично оценяване на риска на отделните хостове в мрежата на организацията на база тяхното поведение във времето.
REQ.10.	При откриване на подозрително поведение, повтарящо се на един и същ хост, системата да добавя откритите събития в едно общо събитие, като увеличава тежестта на неговия риск, вместо да генерира множество отделни аларми или известия.

REQ.11.	Системата да може да открива и обединява на едно място информация за подозрителни активности в поведението на различни хостове водещи до обща заплаха, например C2C комуникация, с цел предоставяне на изглед от едно място върху напредъка и разпространението на заплахата в мрежата на организацията. Всички открити подозрителни активности да са придружени с описание за модела на тяхното засичане и описание на поведението.
REQ.12.	Системата да включва функционалност за извличане на минимум 90GB метаданни на ден от мрежовия трафик и тяхното препращане за съхранение за минимум 14 дни в облачно приложение и хранилище на производителя с цел извършване на задълбочен анализ и лов на заплахи.
REQ.13.	Системата да може да открива заплахи на база идентифициране на индикатори за поведение и действия типични за атакуващите и посредством съпоставянето им с техниките по MITRE ATT&CK framework.
REQ.14.	Системата да може да открива заплахи и идентифицира потенциална злонамерена дейност или компрометиране въз основа на контекста на наблюдаваното поведение в хостове, акаунти и услуги.
REQ.15.	Системата да може да изгражда модел на взаимодействията между различни потребителски акаунти, хостове и услуги в наблюдаваната мрежа на база, на който да може да засича аномалии и да открива злоупотреба с привилегировани акаунти, като нетипично използване на потребителски акаунт на различни устройства или използване на услуги на хостове, които обикновено потребителя не използва.
REQ.16.	Предложената система да включва централизирано управление и администриране на всички нейни компоненти.
REQ.17.	Системата да включва функционалност за сортиране на събитията по важност, включително инструмент за предлагане и създаване на автоматични правила за филтриране на събития, които с голяма вероятност са в резултат на нормална комуникация в инфраструктурата на организацията.
REQ.18.	Системата да използва пасивна техника за инспекция на трафика, да не въвежда латентност в мрежата и да не оказва въздействие върху производителността на съществуващи услуги и приложения в организацията.
REQ.19.	Системата да използва, като основен източник на данни, метаданни от необработен мрежов трафик прихванат от предложената система.
REQ.20.	Интерфейсът на системата да включва табло с информация за високорисковите хостове в мрежата на организацията за да насочва фокуса на анализатора с цел подобряване на времето за откриване и реакция на заплахи.
REQ.21.	Системата трябва да идентифицира хостове и акаунти, засегнати от конкретна кампания за атака, позволявайки на анализаторите да идентифицират всички засегнати хостове и акаунти и да разберат първоизточника на атаката и последователността от събития.
REQ.22.	Системата трябва да може да идентифицира и проследява хостове, включително когато се свързват през VPN. Да проследява страничното движение на нападатели и всички засегнати хостове, да изгражда и предоставя изглед на цялата кампания на атаката, и да добавя информация за взаимовръзките между засегнатите хостове, акаунти и използвани услуги.
REQ.23.	Системата да предлага възможност за бъдещо надграждане с функционалност за изпращане на извлечени и обогатени от нея метаданни за мрежовия трафик към външен Data Lake и SIEM решения.

Изисквания за управление на логове и интеграция	
REQ.24.	Системата да може да съхранява локално записи за откритите заплахи за период не по-малък от 3 месеца.
REQ.25.	Системата да предлага възможност за интеграция с решения за реагиране на инциденти на трети страни посредством API интерфейс.
REQ.26.	Системата да включва интеграция с Active Directory, която да позволява ръчно или автоматизирано деактивиране или заключване на акаунти през потребителския интерфейс на системата.
REQ.27.	Системата да включва RESTful API интеграция с EDR решения на трети страни, която позволява ръчно или автоматизирано блокиране на хост.
REQ.28.	Системата да включва интеграция с NGFW решения на трети страни, която да позволява, като минимум изолиране на хост на ниво защитна стена, чрез динамично създаване на правила за блокиране.
REQ.29.	Системата да включва интеграция със SIEM, с цел обогатяване на SIEM с информация за активни заплахи, неоткрити от останалите решения за сигурност внедрени в организацията.
REQ.30.	Системата да включва интеграция със SOAR, с цел обогатяване на SOAR с информация за активни заплахи за стартирането на автоматизирани процеси, като отваряне на инцидент, автоматизиран процес за реакция при инцидент и т.н.
REQ.31.	Системата да може да приема информация от различни канали за разузнаване на заплахи (Threat Intelligence Feeds).

Прилагаме като неразделна част към настоящото предложение всички необходими документи, както следва:

1. …….
2. …….
3. …….

/Описват се подробно приложените документи, съгласно т. 4 от поканата, както и допълнителни документи, представени по преценка на кандидата/

[дата]

ПОДПИС

[име и фамилия]

[качество на представляващия участника]

Забележка: *Техническото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 4

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ” № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ЦЕНОВО ПРЕДЛОЖЕНИЕ
за
участие в процедура за избор на доставчик с предмет:

„Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“

След запознаване с поканата за участие в процедура за избор на доставчик с предмет: „Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“ и Техническото задание на Възложителя, ние предоставяме следното Ценово предложение:

1. Предлагаме да доставим софтуера, предмет на горецитираната процедура, в съответствие с Техническото задание на Възложителя – Приложение № 1 и представеното от нас Техническо предложение – Приложение № 3 **при обща цена в размер ……..…….. (словом: ……..) лева без ДДС**, формирана както следва:

№	Продукт	Описание	Кол.	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
Софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти					
1.	Software/licence	Detect for Network software subscription and support, per active IP - (3Y)	1		
2.	Software/licence	Recall (GB/Day) - 2 WKS	90		
3.	Software/licence	Detect for M365 subscription and support, per internal account (3Y)	700		
4.	Software/licence	Detect for Azure AD subscription and support, per internal account (3Y)	700		

2. Декларираме, че в предложената цена са включени всички разходи за изпълнение на дейностите, предмет на процедурата, включени в Техническото задание на Възложителя и представеното от нас Техническо предложение.

3. Начин на плащане – извършва се по банков път, на три равни годишни вноски в срок до 30 (тридесет) дни след:

3.1. подписване на приемо-предавателен протокол и приемане без възражения и забележки от Възложителя и издадена фактура от Изпълнителя (за първата годишна вноска);

3.2. издадена фактура от Изпълнителя (за втората и третата годишна вноска).

[дата]

ПОДПИС
[име и фамилия]
[качество на представляващия участника]

Забележка: *Ценовото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 5

Образец

ДЕКЛАРАЦИЯ

От.....,

представляващ ..... – кандидат в процедура с предмет: „Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“, в качеството ми на .....,

ДЕКЛАРИРАМ, че представляваното от мен дружество:

1. Не е обявено в несъстоятелност и не е в производство за обявяване в несъстоятелност;
2. Не е в производство по ликвидация.

ДЕКЛАРИРАМ, че:

3. Не съм лишен от правото да упражнявам търговска дейност;
4. Не съм осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, включително изпиране на пари, по чл. 253 – 260 от НК, за подкуп по чл. 301 – 307 от НК, участие в организирана престъпна група по чл. 321 и чл. 321а от НК, както и за престъпление против собствеността по чл. 194 – 217 от НК или против стопанството по чл. 219 – 252 от НК.

ДЕКЛАРАТОР:

Забележки:

1. Декларацията се представя в електронен вид във формат .pdf, подписана с квалифициран електронен подпис.

2. Декларацията се подписва задължително от управляващия и представляващ дружеството. Когато управляващите дружеството са повече от едно лице, декларацията се подписва от всички лица, вписани в Търговския регистър като представляващи и се представя в отделен екземпляр за всяко представляващо лице.

Приложение № 6

УКАЗАНИЯ

за участие в процедура за избор на доставчик с предмет:

„Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“

1. Кандидатите изготвят и окомплектоват предложенията си съгласно изискванията, посочени в поканата и приложенията към нея.
2. Не по-късно от 11:00 ч. на 26.04.2024 г. всеки кандидат може да поиска от Възложителя писмено разяснения по документацията. Възложителят изпраща разяснението до всички кандидати, които са получили документация за участие и са посочили адрес за кореспонденция и го публикува на интернет-страницата на „Информационно обслужване” АД.
3. Предложенията се приемат по начина и в срока, посочени в поканата. Приемат се и предложения на кандидати, които не са поканени с изрична покана.
4. Предложение, получено след изтичане на крайния срок, не се разглежда от Възложителя. В този случай до кандидата се изпраща уведомление.
5. Изборът на доставчици се извършва въз основа на подадените предложения.
6. Изпълнителният директор на „Информационно обслужване” АД назначава комисия за разглеждането и оценяването на подадените предложения.
7. Комисията отстранява от процедурата кандидат, който:
   - е обявен в несъстоятелност/ е в производство по ликвидация / е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - управител или член на управителните органи на кандидат, а в случай, че членове са юридически лица – за техните представители в съответния управителен орган е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - не е изготвил и окомплектовал предложението си съгласно изискванията, посочени в документацията за участие;
   - е представил непълно техническо или ценово предложение.
8. Възложителят може да изиска от кандидатите да представят допълнително документи, с които да докажат икономическото и финансовото си състояние, техническите възможности и/или квалификацията им.
9. След разглеждане на получените предложения, Възложителят може еднократно да поиска от кандидатите да представят подобрено ценово предложение.

10. Кандидатите са длъжни в процеса на провеждане на процедурата да уведомяват за всички настъпили промени в обстоятелствата, за които са представили декларация по образец (Приложение № 5 към поканата) - в 7-дневен срок от узнаването им.
11. Лице, което е дало съгласие и фигурира като подизпълнител в офертата на друг кандидат, не може да представя самостоятелна оферта.
12. Когато при изпълнението на договора кандидатът ще използва подизпълнител, предложението трябва да съдържа изискваните документи за идентификация и квалификация и за подизпълнителя.
13. Когато кандидат за участие в процедурата е обединение на юридически лица (консорциум) за всеки от участниците в консорциума се представят документите за идентификация и квалификация, изисквани от участниците в процедурата.
14. Всички кандидати се уведомяват за резултатите от процедурата в срок от три работни дни, считано от датата на решението на Съвета на директорите, с което се одобрява изборът на доставчик, като на избрания за изпълнител кандидат се предлага да сключи договор при условията на подаденото предложение.
15. Когато избраният за изпълнител кандидат откаже, не представи изискваните документи или по друга причина договорът с него не може да бъде подписан, изпълнителният директор предлага на класирания на следващо място кандидат да сключи договор при условията на подаденото предложение или прекратява тази и насрочва нова процедура за избор на доставчик.
16. При подписване на договора кандидатът, определен за изпълнител, представя електронно свидетелство за съдимост за удостоверяване на обстоятелствата, заявени с декларация по образец (Приложение № 5 към поканата). При невъзможност за представяне на електронно свидетелство за съдимост кандидатът представя свидетелство за съдимост или друг еквивалентен документ – сканирани и заверени с квалифициран електронен подпис. Представените документи не се съхраняват от „Информационно обслужване“ АД.