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

ДО ЗАИНТЕРЕСОВАНИТЕ ЛИЦА

ОТНОСНО: Изменения в документацията за участие в процедура с предмет: „Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“.

Във връзка с установена техническа грешка в документацията за участие в процедура с предмет: „Закупуване на софтуер за наблюдение, разследване и реагиране на хибридни атаки и инциденти за нуждите на „Информационно обслужване“ АД“ са направени следните изменения:

1. В таблицата от Техническото задание – Приложение № 1 към поканата, количеството по ред 1 е изменено, както следва:

№	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)	4000

2. Образецът на Техническо предложение - Приложение № 3 се изменя съгласно Образец на Техническо предложение – Приложение № 3 (актуализирано).
3. Образецът на Ценово предложение - Приложение № 4 се изменя съгласно Образец на Ценово предложение – Приложение № 4 (актуализирано).

Ivaylo Borisov Filipov
Digitally signed by Ivaylo Borisov Filipov
Date: 2024.04.22 16:43:26 +03'00'

Ивайло Филипов
Изпълнителен директор
„Информационно обслужване“ АД

Приложение № 3

(актуализирано)

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)	4000
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

(актуализирано)

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)	4000		
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.*