Приложение № 2
към рамков договор № 67/24.10.2024 г.

ЗАЯВКА по Рамков договор № 67/24.10.2024 г. (№ ПО-16-3173/24.10.2024 г. на „Информационно обслужване“ АД)	☒
ЗАЯВКА по Рамков договор № 67/24.10.2024 г. (№ ПО-16-3173/24.10.2024 г. на „Информационно обслужване“ АД) (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*17*
Описание на проект съгласно ПГ:	*Система за мрежово откриване, разследване и реагиране на кибер заплахи - NDR*	
CPV код	*48000000*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-11387 / 05.08.2025 г.*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	

Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**, *в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*295 000.00 лв. без ДДС*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на доставката на система за мрежово откриване, разследване и реагиране на кибер заплахи - NDR*
Плащане с акредитив или авансово ДА/НЕ	*НЕ*
Документи за плащане с акредитив или авансово	*НЕ*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*До 4 месеца след подписване на заявката*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Неприложимо*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на доставката на система за мрежово откриване, разследване и реагиране на кибер заплахи - NDR*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Техническа спецификация*

Настоящата заявка да се изпълни при условията на приложените Технически параметри.

ЗАЯВКАТА е ИЗГОТВЕНА ОТ:

Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):	_ __ __ ,	*Подпис:*

[1] Отбелязва се в случай че заявката е актуализирана

ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
Ръководител на договора от страна на БЕНЕФИЦИЕРА:		*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		*Подпис:*

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.*

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ПРИЛОЖЕНИЕ № 1

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА:

„Система за мрежово откриване, разследване и реагиране на кибер заплахи - NDR за нуждите на Министерството на енергетиката“

Гр. София 2025 г.

I. ПРЕДМЕТ

В предмета на заявката се включва доставка система за мрежово откриване, разследване и реагиране на кибер заплахи - NDR за нуждите на Министерство на енергетиката.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Изискванията на Бенефициера относно обхвата и изпълнението на дейностите по доставка на система за мрежово откриване, разследване и реагиране на кибер заплахи - NDR за ME са както следва:

1. Решение за наблюдение, разследване и реагиране на хибридни атаки и инциденти

Минимални технически изисквания	
REQ.1.	Да бъде доставена Network Detection & Response (NDR) система за откриване на 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 500 IP адреса.
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. Механизмите на предложената система за откриване на заплахи да не зависят от правила и сигнатури.
REQ.3.	Системата да може да работи без да е необходима връзка с интернет, например в air-gap среда. Предложената система да не изисква съхранение, обработка и обогатяване на метаданни извън мрежата на Възложителя.
REQ.4.	Системата да предоставя функционалност за извършване на анализ на мрежов трафик, както във вътрешните мрежи на възложителя, така и в облачни мрежи (AWS, GCP, Azure). Системата да осигурява видимост в North-South, East-West трафик.
REQ.5.	Системата да не използва агенти, инсталирани върху крайни станции, за предоставяне на изискваните функционалности.
REQ.6.	Системата да включва функционалност, позволяваща идентифициране на заплахи в криптиран трафик, без да е необходимо неговото декриптиране.
REQ.7.	Системата да включва функционалност, позволяваща генериране на автоматични известия при откриване на заплахи.
REQ.8.	Системата да включва функционалност и механизъм за динамично оценяване на риска на отделните хостове в мрежата на организацията на база тяхното поведение във времето.
REQ.9.	Системата да включва функционалност, позволяваща при откриване на подозрителни събития, повтарящи се на един и същ хост, да обединява откритите в едно общо събитие, като увеличава тежестта на неговия риск, вместо да генерира множество отделни аларми или известия.
REQ.10.	Системата да включва функционалност, позволяваща създаване на Fingerprint на хостовете в мрежата, позволявайки проследяване на поведението на един и същ хост във времето, дори при промяна на неговия IP адрес, така че при проява на индикатори за развитие/напредване на атаката да се увеличава тежестта на риска асоцииран към съответния хост.

REQ.11.	Системата да включва функционалност за идентифициране на индикатори за поведение и действия посредством съпоставяне на случващото се с тактиките и техниките, описани в MITRE ATT&CK framework.
REQ.11.	Системата да включва функционалност да открива заплахи и идентифицира потенциална злонамерена дейност или компрометиране въз основа на контекста на наблюдаваното поведение в хостове, акаунти и услуги.
REQ.12.	Системата да включва функционалност за класифициране на откритите заплахи, използвайки терминология с препратки към Mitre ATT&CK framework.
REQ.13.	Системата да включва функционалност да изгражда модел на взаимодействията между различни потребителски акаунти, хостове и услуги в наблюдаваната мрежа и да търси заплахи свързани с привилегировани акаунти, нетипично използване на акаунти или използване на услуги или промяна на поведението.
REQ.14.	Системата да включва функционалност за сортиране на събитията по важност, включително инструмент за предлагане и създаване на автоматични правила за филтриране на събития.
REQ.15.	Системата да използва пасивна техника за инспекция на трафика без да въвежда латентност в мрежата и да не оказва въздействие върху производителността на съществуващи услуги и приложения в организацията.
REQ.16.	Системата да използва, като основен източник на данни, метаданни от необработен мрежов трафик прихванат от сензорите на предложената система.
REQ.17.	Системата да включва функционалност за категоризация на високорисковите хостове в мрежата на организацията, за да насочва фокуса на анализатора с цел подобряване на времето за откриване и реакция при заплахи. С цел намаляване на шума от нерелевантни аларми при определянето на риска на хостовете, системата да се базира на действия и поведение характерни за атакуващ в мрежата, а не само на база аномалии в поведението на хостовете.
REQ.18.	Системата да включва функционалност, позволяваща събирането на всички засичания на ниво хост и акаунт, и да извежда приоритетно информация за хостове или акаунти, които показват злонамерено поведение.
REQ.19.	Системата трябва да използва технология за машинно обучение работеща със Supervised, Unsupervised и Deep learning алгоритми на обучение, осигуряващи широко покритие за ранно откриване на поведение и техники на нападатели, минимум Command and Control, Hidden tunnels, Reconnaissance, Lateral movement, извличане и ексфилтрация на данни. Предложената система да включва права за обновяване на алгоритмите за машинно обучение и добавяне на нови алгоритми от производителя на системата.
REQ.20.	Системата да включва функционалност да идентифицира и проследява хостове, включително когато се свързват през VPN.
REQ.21.	Системата трябва да може да съхранява отделни аларми в PCAP формат с цел подпомагане на дейностите за разследване.
REQ.22.	Система да включва функционалност, позволяваща събирането на метаданните, извлечени от мрежовия трафик в централно хранилище, където да се подлагат на анализ, базиран на ML модели, с цел търсене за заплахи.
REQ.23.	Система да включва функционалност, позволяваща съхраняваните метаданни да бъдат в криптиран вид, използвайки поне AES-256 алгоритъм.
REQ.24.	Система да включва функционалност, позволяваща търсене на аномалии в поведението на мрежовата среда с цел разпознаване на атаки.

REQ.25.	Система да включва функционалност за визуализация на резултатите от търсенията в метаданните, с цел улеснение на процеса по разследване на инциденти.
REQ.26.	Системата да включва функционалност, позволяваща търсене в събраните метаданни за определени периоди от време или на база на ключови думи.
REQ.27.	Системата да включва функционалност, позволяваща търсене в събраните метаданни чрез филтри, базирани на типовете на метаданните.
REQ.28.	Системата да предоставя възможност за надграждане с функционалност за откриване на заплахи в облачни среди/услуги от AWS, Microsoft Azure, M365.
REQ.29.	Системата да предоставя възможност за надграждане с функционалност, позволяваща разпознаване на уязвимости на база на open-source сигнатури тип IDS, използвайки същите сензори с които се извличат метаданните от мрежовия трафик.
REQ.30.	Системата да предоставя възможност за надграждане с функционалност, позволяваща откриването на атаки, свързани с акаунти от Entra ID (Azure ID)
REQ.31.	Системата да предоставя възможност за надграждане с функционалност, позволяваща корелиране на събития между локални акаунти и акаунти в Entra (Azure ID)
REQ.32.	Системата да включва функционалност, позволяваща откриването на неправомерно ползване на сервизни акаунти
REQ.33.	Системата да включва функционалност, позволяваща откриването на атаки тип Account take-over
REQ.34.	Системата да предоставя възможност за надграждане с функционалност, позволяваща откриването на атаки, таргетираща хранилища на идентичности и/или акаунти, ползвайки техники тип Kerberoasting, DCSYC и не легитимни LDAP заявки.
REQ.35.	Архитектурата на предложената система да е базирана на дистрибутирани в мрежата сензори, които извличат метаданни от мрежовите пакети в реално време и препращат събраните метаданни към централен компонент, който извършва анализа на поведението необходим за откриване на заплахи. За извличане на метаданните сензорите на системата да използват копие на мрежовия трафик. Сензорите на предложената система да могат да получават мрежови трафик минумум от SPAN портове, огледални (mirror) портове, TAPs, брокери на пакети и виртуални комутатори на VMware.
REQ.36.	Предложената система да включва права за използване на виртуални сензори и виртуални централни компоненти за обследване на мрежовия трафик в рамките изискваните IP адреси.
REQ.37.	Системата да включва функционалност за централизирано управление и администриране на всички нейни компоненти.
REQ.38.	Системата да може да съхранява локално записи за откритите заплахи за период не по-малък от 3 месеца.
REQ.39.	Системата да предлага възможност за интеграция с решения за реагиране на инциденти на трети страни посредством API интерфейс.
REQ.40.	Системата да включва RESTful API интеграция с Active Directory, която да позволява ръчно или автоматизирано деактивиране или заключване на акаунти през потребителския интерфейс на системата.

REQ.41.	Системата да включва RESTful API интеграция с EDR решения на трети страни, която позволява ръчно или автоматизирано блокиране на хост.
REQ.42.	Системата да включва интеграция с минимум следните NGFW решения на трети страни - включително Palo Alto Networks, Check Point, Fortinet и Cisco - която да позволява, като минимум изолиране на хост на ниво защитна стена, чрез динамично създаване на правила за блокиране.
REQ.43.	Системата да включва интеграция с минимум следните SIEM решения на трети страни - включително IBM QRadar, Splunk SIEM - с цел обогатяване на SIEM с информация за активни заплахи, неоткрити от останалите решения за сигурност внедрени в организацията.
REQ.44.	Системата да включва интеграция с минимум следните SOAR решения на трети страни - включително IBM SOAR, Palo Alto XSOAR, Splunk Phantom - 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.45.	Системата да включва RESTful API интеграция с NAC решения на трети страни, която да позволява, като минимум преместване на хост в карантинен VLAN.
REQ.46.	Системата да включва отворен API достъпен за администратори и разработчици, поддържащ различни езици за уеб разработка позволяващ достъп и извличане на данни от системата и конфигуриране на системата. Данните предоставяни от системата при отговор през REST API да са в JSON формат.
REQ.47.	Системата да включва функционалност да приема информация от различни канали за разузнаване на заплахи (Threat Intelligence Feeds)
REQ.48.	Софтуерните актуализации на предложената система трябва да бъдат автоматизиран процес, който не изисква човешка намеса.
REQ.49.	Производителят на системата трябва да предоставя регулярни актуализации и ъпдейти на използваните алгоритми адаптиращи системата към постоянно променящите се заплахи.
REQ.50.	Системата да включва функционалност, позволяваща да известява за открити заплахи или подозрителни хостове чрез имейл и syslog.
REQ.51.	Системата да включва функционалност, позволяваща ролеви базиран контрол на достъпа до нейните компоненти.
REQ.52.	Системата да има функционалност, позволяваща изпращане на одитен журнал през syslog за действия като влизане, излизане и промени в настройките, както и такива влияещи върху състоянието на нейната сигурност.
REQ.53.	Системата да включва функционалност, позволяваща автентикация на потребители чрез всеки от следните методи: локална директория, SAML, Radius, TACACS, LDAP
REQ.54.	Централната компонента на предложената система да може да бъде под формата на виртуална машина или специализирано физическо устройство.
REQ.55.	Сензорите на предложената система да могат да бъдат под формата на виртуални машини, специализирани физически устройства или инстанции предназначени за инсталация в AWS или Azure облачна среда.
REQ.56.	Централното хранилище на метаданни да може да приема 95 GB метаданни на ден
Гаранция и поддръжка:	
REQ.57.	Включена поддръжка от производителя на решението за период от минимум 36 месеца

REQ.58.	Гаранционната поддръжка трябва да е от тип: 8x5
REQ.59.	Възможност за обновление на софтуера в периода на поддръжката
REQ.60.	Възможност за обновления на информацията за заплахите от базата данни на производителя

Всички лицензи и права за ползване, осигурени чрез изпълнението на настоящата заявка, следва да са на името на МЕ. Изпълнителят предоставя на МЕ пълната информация относно осигурената осигурените лицензи - всички лицензни файлове, ключове, активационни кодове, данни за достъп до официални сайтове на производителите на софтуерните продукти, когато това е приложимо

III. СРОК НА ИЗПЪЛНЕНИЕ.

1. Срокът на доставката е до 4 месеца след подписване на заявката.

2. Периодът на изпълнение на услугите по техническа поддръжка е 36 месеца, считано от датата на осигуряване.

IV. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Услугите по техническа поддръжка се предоставят отдалечено, при необходимост от оказване на съдействие на място - сградата на Министерство на енергетиката, в гр. София, ул. Триадица № 8

V. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

1. Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

2. Във връзка с мрежовата и информационната сигурност на Възложителя/Бенефициера (МЕУ/МЕ) и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Възложителя/Бенефициера (МЕУ/МЕ), ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Възложителя/Бенефициера (МЕУ/МЕ). За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Възложителя/Бенефициера (МЕУ/МЕ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Възложителя/Бенефициера (МЕУ/МЕ). При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

[2] Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на Възложителя/Бенефициера (МЕУ/МЕ), които са предмет на защита съгласно приложимото законодателство в областта.

(в) определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Възложителя/Бенефициера (МЕУ/МЕ) при възникване на инцидент по МИС.

(г) осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

3. Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Възложителя/Бенефициера (МЕУ/МЕ).

4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.

5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

(а) При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на съответната администрация;

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

(в) При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Възложителя/Бенефициера (МЕУ/МЕ);

(г) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Възложителя/Бенефициера (МЕУ/МЕ), лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на съответната администрация от страна на Възложителя/Бенефициера (МЕУ/МЕ) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.