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-2026 г.:	*№ по ред от ПГ*	*12*
Описание на проект съгласно ПГ:	*Осигуряване на решение за защита на крайни устройства*	
CPV код	*48760000-3*	
Рег. номер на писмо от МИДТ за утвърждаване на проекта /становище по проекта	*МИДТ Рег.№ 04-03-63/07.08.2026*	
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*	*36 500,00 евро 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 осигуряването на решение за защита на крайни устройства*
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 осигуряването на решение за защита на крайни устройства*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.	
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:	

[1] Отбелязва се в случай че заявката е актуализирана

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

„Осигуряване на решение за защита на крайни устройства за нуждите на Министерството на енергетиката“

Гр. София 2026 г.

I. ПРЕДМЕТ

В предмета на заявката се включва осигуряване на решение за защита на крайни устройства за период от 12 (дванадесет месеца) месеца.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Изпълнителят следва да осигури решение за защита на крайни устройства със следните минимални изисквания:

Минимални технически изисквания	
REQ. 1.	Предложеното решение трябва да е с включени лицензи за 280 крайни точки (230 работни станции и 50 сървъра). Предложените лицензи трябва да са с валидност и включена поддръжка за период от 12 месеца.
REQ. 2.	Решението трябва да има централизирана конзола, внедрена като софтуер като услуга (SaaS). Достъпът до конзолата трябва да бъде осигурен чрез уеб-базиран потребителски интерфейс и чрез REST API интерфейс.
REQ. 3.	Решението трябва да бъде изцяло предоставено от един производител. Не е допустимо отделни функционални звена на платформата на решението да бъдат реализирани чрез отделни решения от различни производители.
REQ. 4.	Платформата на решението трябва да осигурява минимално следните механизми за сигурност на потребителските акаунти: -Многофакторно удостоверяване с помощта на TOTP токени -Възможност за интеграция с външен доставчик на идентичност чрез SAML 2.0 -Автоматично излизане от акаунта след определен период на неактивност на потребителя -Контрол на достъпа, базиран на роли (RBAC)
REQ. 5.	Платформата на решението трябва да позволява дефинирането на потребителски акаунти с различни нива на разрешения, включително минимално: -Пълен контрол над платформата -Контрол върху отделните функционални модули на платформата -Достъп само за четене на информация
REQ. 6.	Инсталирането на агента на решението не трябва да изисква рестартиране на операционната система на крайните точки.
REQ. 7.	Агентът на решението трябва да може да провери коректността на използван сертификат за връзка по време на установяване на връзка с платформата, за да се предпази от атаки от типа „човек по средата“.
REQ. 8.	Агентът на решението трябва да разполага със защитни механизми, които предотвратяват деактивирането му или засягането на правилното му функциониране, дори от потребители с повишени привилегии.
REQ. 9.	Процесът по деинсталирането на агента трябва да може да бъде защитен с уникална парола за всяка защитена работна станция, за да се предотврати деинсталирането на агента дори от потребители с повишени привилегии.
REQ. 10.	Агентът на решението трябва да поддържа инсталиране и деинсталиране чрез общи инструменти за внедряване като SCCM, Ansible, Jamf.
REQ. 11.	Агентът на решението трябва да поддържа инсталационни токени, които предпазват от неконтролирани инсталации.
REQ. 12.	Агентът на решението трябва да поддържа токен за деинсталиране, който трябва да може да бъде свързан с отделен хост.
REQ. 13.	Агентът на решението за Windows, MacOS и Linux системи трябва да

	събира и изпраща до платформата минимално следните телеметрични данни: -Създаване на нов процес и прекратяване на процеса -Операции с мрежови сокети за TCP и UDP протоколи -Файлови операции -Данни от операции по вписване -Операции с регистри (поне за Windows системи)
REQ. 14.	При инсталиране на агента на решението трябва да има опция за задаване на етикет на агента, който да не може да бъде премахнат и който да може да се използва като атрибут за групиране на крайни точки.
REQ. 15.	По време на инсталирането на агента на решението трябва да има опция за задаване на специален прокси сървър, който агентът да използва за свързване с платформата.
REQ. 16.	Агентът на решението трябва да може да открива и блокира опити за деактивиране на услугата за копиране на дялове (VSS) и други опити за повреждане на моментни извадки за състоянието на VSS бекъпираните данни (snapshots).
REQ. 17.	Агентът на решението трябва да може да осигури защита срещу атаки от типа „Bring Your Own Vulnerable Driver“ (BYOVD), като да може да открива и блокира опитите за зареждане на уязвими драйвери.
REQ. 18.	Агентът на решението трябва да осигурява защита срещу известни и неизвестни злонамерени двоични файлове директно на защитената крайна точка, минимално по следните начини: -Проверка на репутацията на файла в базата данни за информация за заплахи на производителя -Локален статичен анализ, базиран на машинно самообучение (Machine Learning)
REQ. 19.	Агентът на решението трябва да осигурява защита срещу известни и неизвестни злонамерени макроси във файлове на Microsoft Word и Microsoft Excel, минимално по следните начини: -Проверка на репутацията на макроса в базата данни за разузнаване на заплахите на производителя -Локален статичен анализ, базиран на машинно самообучение (Machine Learning)
REQ. 20.	Агентът на решението трябва да има възможността да премахва злонамерени макроси, открити във файлове на Microsoft Word и Microsoft Excel.
REQ. 21.	Агентът на решението трябва да има всеобхватни възможности за откриване на зловреден софтуер, използвайки както сигнатурни, така и поведенчески методи за идентифициране на известни и неизвестни заплахи. Трябва да има редовни актуализации на вирусните дефиниции и евристики.
REQ. 22.	Агентът на решението трябва да осигурява защита срещу криптиране на дискове и файлове от зловреден софтуер от тип криптовируси.
REQ. 23.	Агентът на решението трябва да може да извърши анализ на двоични файлове, след като те са били записани във файловата система на крайните точки.
REQ. 24.	Агентът на решението трябва да осигурява защита срещу известни и неизвестни уязвимости.
REQ. 25.	Агентът на решението трябва да има конфигурируема опция за поставяне под карантина на злонамерени файлове.
REQ. 26.	Агентът на решението трябва да може автоматично да извърши сканиране за заплахи на преносими устройства за данни, веднага щом те

	бъдат свързани към USB порт.
REQ. 27.	Агентът на решението, чрез анализ на сложни причинно-следствени вериги от събития и откриване на техники и тактики, използвани от киберпрестъпниците, трябва да може да осигури защита срещу атаки от типа „Living of the land“, които използват легитимни системни инструменти по злонамерен начин.
REQ. 28.	Агентът на решението трябва да осигурява защита срещу атаки, насочени към кражба на потребителски идентификационни данни.
REQ. 29.	Агентът на решението трябва да има способността автоматично да отстранява сложни атаки, минимално чрез: справяне със злонамерени процеси, поставяне на файлове под карантина, премахване на планирани задачи и изтриване на записи в системния регистър.
REQ. 30.	Агентът на решението трябва да може да се интегрира с Центъра за защита на Windows.
REQ. 31.	Решението трябва да поддържа минимално следните нива на критичност на предупрежденията: информационно, ниско, средно, високо и критично.
REQ. 32.	Решението трябва да може автоматично да групира свързани сигнали, за да улесни по-бързото и лесно сортиране и анализ на инциденти.
REQ. 33.	Решението трябва да може автоматично да създава причинно-следствени вериги за групирани сигнали в рамките на инцидент, представляващи връзките между процесите, използвани по време на атака и свързаните телеметрични данни, за да се улесни минимално: -Анализ на използваните техники -Определяне на обхвата на атаката -Идентифициране на целта и обхвата на атаката -Проверка дали целта е постигната
REQ. 34.	Решението трябва да позволява управление на инциденти минимално в следния обхват: -Възлагане на инцидент на анализатор -Промяна на състоянието на инцидента: разследване, фалшиво положителен, истински положителен, дублиран инцидент, инцидент от проведено тестване -Добавяне на бележки към инцидента
REQ. 35.	Решението трябва да може да съпоставя сигналите с рамката MITRE ATT&CK.
REQ. 36.	Решението трябва да позволява преглед на отчет от модул sandbox за файлове, свързан с инцидента, с възможност за експортиране на отчета.
REQ. 37.	Решението трябва да има възможност за конфигуриране на ръчни и автоматични актуализации на агента за определени групи крайни точки. Политиката за автоматично конфигуриране на агента трябва да позволява минимално: -Посочване на деня от седмицата и времевия диапазон, в който актуализацията няма да се извършва -Определяне на броя на крайните точки, които ще бъдат актуализирани -Дефиниране на версията: последна версия, последна предишна версия или статично зададена версия
REQ. 38.	Решението трябва да има възможност за записване в лог файл на всички промени по политиките за сигурност.
REQ. 39.	Решението трябва да позволява създаването на правила за изключения за системата за машинно самообучение.
REQ. 40.	Решението трябва да позволява създаването на правила за изключения за функцията за поведенческо сканиране.

REQ. 41.	Решението трябва да позволява установяване на отдалечена конзолна връзка с крайна точка, защитена от агента, предлагайки минимално следните функции: -Преглед на изпълняваните процеси -Преглед на файлови системи -Преглед на състоянието на мрежовия сокет -Прекратяване на определен процес -Изпълнение на скрипт от библиотека -Изтегляне на файл от крайната точка -Качване на файл към крайната точка -Дъмп на паметта на процесите -Дъмп на паметта на операционната система -Изключване и рестартиране на системата -Списък на мрежовите връзки -Премахване на файл -Извличане на файл с опция за криптиране му преди това с използване на парола, дефинирана от потребителя на решението -Стартиране на изпълним файл -Добавяне/премахване на споделени мрежови ресурси -Списък на локалните потребители на крайната точка
REQ. 42.	Решението трябва да позволява създаването на библиотека със скриптове и тяхното дистанционно изпълнение на дадена крайна точка или на група от крайни точки. Необходима е поддръжка минимално на следните скриптови езици: -за Windows системи: PowerShell -за Linux системи: Bash скриптове -за MacOS системи: Zsh скриптове
REQ. 43.	Решението трябва да позволява отдалечена мрежова изолация на крайната точка, задействана чрез потребителски интерфейс и чрез API. По време на мрежовата изолация, целият мрежов трафик, с изключение на връзките към платформата на решението и DHCP протокола, трябва да може да бъде блокиран.
REQ. 44.	Решението трябва да позволява създаване на IP-базирани изключения за ограничаване на мрежата.
REQ. 45.	Решението трябва да има възможността да изпълнява пълно сканиране на крайната точка при поискване и в отговор на регистрирано предупреждение.
REQ. 46.	Решението трябва да позволява директна интеграция с услугата на VirusTotal за информация за заплахи.
REQ. 47.	Решението трябва да позволява глобално и групово блокиране на крайни точки за изпълнението на двоични файлове чрез задаване на техния SHA256 хеш.
REQ. 48.	Решението трябва да разполага с възможността да изгражда персонализирани правила за откриване и предотвратяване на заплахи, базирани минимално на дефиницията на причинно-следствена верига от процеси, заедно със специфицирането на параметри на командния интерфейс на крайните точки.
REQ. 49.	Решението трябва да може да изгражда свои собствени списъци с индикатори за компрометиране под формата на имена на домейни, IPv4 и IPv6 адреси и SHA256 и MD5 хешове минимално чрез: -Импортиране на индикатори от файл -Ръчно добавяне на индикатори -Добавяне на индикатори програмно чрез API

REQ. 50.	Решението трябва да позволява дефиниране на персонализирани табла (конзоли), използвайки предварително дефинирани контроли за визуализация на данни (widgets) и контроли за визуализация на данни, които са дефинирани чрез заявки към телеметрични данни.
REQ. 51.	Решението трябва да позволява търсене на всички телеметрични данни от крайните точки с помощта на подсказки или ръчно със заявки. Заявките трябва да позволяват комбиниране на телеметрични данни от различни източници, както и филтриране и трансформиране на резултатите. Правилата за създаване на заявки трябва да бъдат описани в системната документация на производителя.
REQ. 52.	Решението трябва да позволява запазване на заявка към телеметрични данни от крайни точки в глобална библиотека, достъпна за всички останали потребители на платформата.
REQ. 53.	Решението трябва да позволява изпълнение на заявка към телеметрични данни от крайни точки и четене на резултатите от нея чрез API.
REQ. 54.	Решението трябва да позволява извличане на резултатите от заявка за телеметрични данни от крайни точки под формата на текстов файл.
REQ. 55.	Решението трябва да позволява циклично изпълнение на заявка според зададен график или еднократно в определено време и изпращане на имейл известие до посочени имейл адреси с прикачен текстов файл, съдържащ резултатите от заявката.
REQ. 56.	Решението трябва да позволява преобразуване на заявка към телеметрични данни от крайни точки в правило за корелация, което да може да се изпълнява по зададен график, генерирайки предупреждения, ако заявката върне повече от един запис.
REQ. 57.	Решението трябва да предоставя вграден модул, който автоматично открива управлявани, неуправлявани и неподдържани списъци с устройства, налични в инфраструктурата, за да се гарантира достатъчна видимост във вътрешната мрежа и какво трябва да бъде защитено.
REQ. 58.	Решението трябва да предоставя вграден модул, който автоматично проверява активността по акаунтите в защитените крайни точки, използвайки информация, събрана от агента на решението. Трябва да може да се проследява историята на вписванията и да може да се следи за събития извън нормалните операции с възможност за допълнително разследване в платформата на решението.
REQ. 59.	Решението трябва да предоставя вграден модул, който да може да следи приложенията по защитените крайни точки, включително разширенията на уеб-браузърите на крайните точки.
REQ. 60.	Решението трябва да може да контролира устройства, свързани към USB портове, минимално на Windows и macOS системи, в следния обхват: -Определяне кои USB устройства могат да бъдат свързани -Определяне на обхвата на достъп до USB устройства за съхранение: забранен достъп, достъп само за четене, достъп само за четене и писане, достъп за четене, писане и изпълнение
REQ. 61.	Решението трябва да може да предоставя подробна информация за активността на файлове, записани на USB устройствата, с контекстуални метаданни, които да позволяват да се разследват потенциални събития за изтичане на данни.
REQ. 62.	Решението трябва да поддържа минимално следните категории файлове, записани на USB устройствата, за предоставяне на подробна информация за активността им: архивни файлове, документи, файлове за дизайн (dwg, dxf, idw), мултимедия, изходен код (скрипт), изпълними файлове, файлове за виртуална машина (VDI, VMDK), имейли файлове (Emailarc,

	elm, msg, out, pst), регистрационни файлове (blf, dmp, ese) и други (dmglnk).
REQ. 63.	Решението трябва да позволява информацията за файлове, записани на USB устройствата да може да се съхранява за минимално 30 дни в платформата.
REQ. 64.	Решението трябва да позволява управлението на минимално следните преносими устройства за Windows системи: -USB устройства -Четци за SD карти
REQ. 65.	Решението трябва да позволява управлението на минимално следните преносими устройства за MacOS системи: -USB устройства -Четци за SD карти -Bluetooth устройства -Устройства за масово съхранение от тип Thunderbolt
REQ. 66.	Обучение на администратори на МЕ за работа със софтуера.
Гаранция и поддръжка:	
REQ. 67.	Период на поддръжка: минимум 12 (дванадесет) месеца
REQ. 68.	Възможност за актуализиране на софтуера в периода на поддръжката до последна актуална версия на производителя.

III. СРОК НА ИЗПЪЛНЕНИЕ.

1. Срокът за осигуряване на решението за защита на крайни устройства е до 4 месеца след подписване на заявката.

2. Периодът на изпълнение на услугите е 12 месеца, считано от датата на осигуряване на решението.

IV. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Услугите по осигуряване на решение за защита на крайни устройства се предоставят отдалечено, при необходимост от оказване на съдействие на място е 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 (МИДТ/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

[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 (МИДТ/МЕ), които са предмет на защита съгласно приложимото законодателство в областта.

информация и активи, при взаимодействието им със служители на Възложителя/Бенефициера (МИДТ/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 (МИДТ/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 (МИДТ/МЕ), подписват декларации по образец на Изпълнителя за опазване на информацията, които се предават на Възложителя/Бенефициера (МИДТ/МЕ). При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до два работни дни от промяната.

(в) определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Възложителя/Бенефициера (МИДТ/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 (МИДТ/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 (МИДТ/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 (МИДТ/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 (МИДТ/МЕ) и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.