ЗАЯВКА по Рамков договор № РД-14-40 от 29.05.2023 г. (вх. № ПО-16-2224/29.05.2023 г. на „Информационно обслужване“ АД)	☒
ЗАЯВКА по Рамков договор № РД-14-40 от 29.05.2023 г. (вх. № ПО-16-2224/29.05.2023 г. на „Информационно обслужване“ АД) (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*21*
Описание на проект съгласно ПГ:	*Предоставяне на услуга за мониторинг по сигурността, наблюдение и докладване на кибер-инциденти в режим 24*7*	
CPV код	*32323500-8*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-9230/25.06.2025 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*	*513 000,00 лв., от които:* *За 2025 г. – 171 000,00 лв.* *За 2026 г. – 342 000,00 лв.*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Периодично, както следва:* • *За периодите 01.07.2025 г. - 30.09.2025 г., 01.01.2026 г. - 31.03.2026 г., 01.04.2026 г. - 30.06.2026 г., 01.07.2026 г. - 30.09.2026 г., след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за съответния тримесечен период и фактура на стойност 85 500,00 лв. без ДДС за съответния тримесечен период;* • *За периода 01.10.2025 г. - 31.12.2025 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за периода 01.10.2025 г. - 08.12.2025 г. и фактура на стойност 85 500,00 лв. без ДДС за периода 01.10.2025 г. - 31.12.2025 г.* • *За периода 01.10.2026 г. - 31.12.2026 г. след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга за периода 01.10.2026 г. - 08.12.2026 г. и фактура на стойност 85 500,00 лв. без ДДС за периода 01.10.2026 г. - 31.12.2026 г.*
Плащане с акредитив или авансово ДА/НЕ	*НЕ*
Документи за плащане с акредитив или авансово	*неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*18 месеца, считано от 01.07.2025 г*
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)*	*Периодично, както следва:* - *За 2025 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на*

[1] Отбелязва се в случай че заявката е актуализирана

	предоставената услуга, както следва: • *За периода 01.07.2025 г. - 30.09.2025 г.* • *За периода 01.10.2025 г. - 08.12.2025 г;* • *За периода 09.12.2025 г. - 31.12.2025 г. (без финансов ангажимент)* - *За 2026 г. с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на предоставената услуга, както следва:* • *За периода 01.01.2026 г. - 31.03.2026 г.;* • *За периода 01.04.2026 г. - 30.06.2026 г.;* • *За периода 01.07.2026 г. - 30.09.2026 г.;* • *За периода 01.10.2026 г. - 08.12.2026 г.;* • *За периода 09.12.2026 г. - 31.12.2026 г. (без финансов ангажимент)* *Към приемо-предавателените протоколи, по чл. 6 от договора, удостоверяващи приемане на предоставената услуга, за съответните периоди за 2025г. и 2026г., се предават и генерирани от системата(описана в ТП):* *(1)Приложение № 1 - Доклад за открити уязвимости във вътрешната мрежа за управление на НЗОК за всеки месец;* *(2) Приложение № 2 - Доклад за открити уязвимости в публичните мрежи на НЗОК, в който влизат публични услуги на НЗОК за всеки месец;* *(3) Приложение № 3 - Детайли за всички генерирани аларми и предприети действия за всеки месец;* *(4) Други доклади или извадки, генерирани от Системата в случай на приложимост.* *Приложенията, описани по-горе се предават на споделено пространство, до което се осигурява достъп на ръководител на проекта по заявката от страна на БЕНЕФИЦИЕРА.*	
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:		
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.

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ПРЕДОСТАВЯНЕ НА УСЛУГА ЗА МОНИТОРИНГ ПО СИГУРНОСТТА, НАБЛЮДЕНИЕ И ДОКЛАДВАНЕ НА КИБЕР-ИНЦИДЕНТИ В РЕЖИМ 24*7

София, 2025

1. Цел

1.1. Настоящият документ дефинира изискванията на Бенефициера за предоставяне на услуга за мониторинг по сигурността, наблюдение и докладване на кибер-инциденти в режим 24*7 за нуждите на Национална здравноосигурителна каса (НЗОК). Услугата следва да осигури автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността на НЗОК информационни и комуникационни системи.

1.2. Чрез осигуряването на услугата ще се постигне:

1.2.1. Изпълнение на изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС).

1.2.2. Непрекъснато наблюдение на критичната информационна инфраструктура на НЗОК.

1.3. Предприемане на своевременни мерки за намаляване на риска от заплахи чрез анализ на мрежовия трафик, логовете на критични ИТ активи - мрежови устройства, операционни системи, бази данни, приложен софтуер и др.

1.3.1. Своевременно подобряване на политики и правила, свързани с информационната сигурност в НЗОК чрез предоставяното от Услугата интегрирано управление на данните от различни ИТ източници.

1.3.2. Своевременно идентифициране на подходящи мерки за актуализиране на специализирания приложен софтуер, използван от НЗОК, с цел минимизиране на потенциални заплахи.

Предоставянето на услугата се извършва за управляваните от дирекция ИТСЗОП на НЗОК ИТ активи.

3. Изисквания към предоставянето на Услугата

3.1. В резултат на изпълнение на съответствие с изискванията на НМИМИС, на НЗОК се предоставят и конфигурират съвременни софтуерни средства с вградени и настроени автоматични алгоритми за управление на сигурността на информацията и събитията, наричани за краткост „Системата“.

3.2. Системата отговаря за предоставяне на услуга по системна интеграция за мониторинг по сигурността, наблюдение и докладване на кибер-инциденти в режим 24*7 за нуждите на НЗОК.

3.3. В инфраструктурата на НЗОК се създават виртуални машини (за Log Collector и Flow Collector), извършват се необходимите мрежови конфигурации, инсталират се Event Collector и Flow Collector, които се интегрират с аналогичните компоненти на Системата в инфраструктурата на ИО АД с оглед непрекъснат мониторинг на събития и предприемане на своевременни действия на SOC екипа в случай на идентифицирани заплахи.

3.4. Към Системата се присъединяват източници на журнални (log) записи като: Microsoft Windows (домейн контролери, мейл сървър), защитни стени; антивирусен софтуер и др. Като източници за трафични потоци към Системата се присъединяват и граничните маршрутизатори на НЗОК.

3.5. За изпълнението на Услугата Изпълнителят следва да осигури компетентен и аналитичен екип, като се осигури 24/7 автоматизирано наблюдение.

3.6. Услугата следва да осигури постоянен мониторинг на ИТ дейности, комуникационна и информационна инфраструктура, ИТ услуги и взаимодействия с външни фактори в съответствие с изискванията на НМИМИС като се:

3.6.1. Осигури наблюдение на крайните точки, присъединени към Системата, както и присъединяване на нови точки до достигане на предоставената от Системата възможност (5 000 eps (event per second), непрекъснат мониторинг и анализ, с оглед предприемане на ответни мерки в случай на инцидент.

3.6.2. Извърши анализ на наличните уязвимости във вътрешната ИТ инфраструктура и предоставят препоръки и проследяване на изпълнението им, както и оказване на методическа помощ на ИТСЗОП при идентифициране на потенциални заплахи и набелязване на мерки в краткосрочен план.

3.6.3. Извърши анализ на базата на събраната информация поне за шестмесечен период и се предложат решения за извършване на промени в ИТ инфраструктурата в дългосрочен план.

3.6.4. Провеждат срещи със служители на ИТСЗОП, на които се дискутират, анализират и планират действия и мерки срещу актуалните заплахи към ИТ инфраструктурата, както и се оценява ефективността на предприетите мерки, чрез повторен анализ и оценка на действията по отстраняване на заплахи.

3.6.5. Измерва ефективността на предприетите мерки, чрез повторен анализ и оценка на действията по отстраняване на заплахи се извършва за всеки отчетен период.

3.6.6. При поискване от страна на ИТСЗОП преглеждат, коригират и допълват изискванията за сигурност, включени в технически параметри или технически спецификации в областта на информационните и комуникационните системи.

3.7. Услугата следва да предостави и дейности по непрекъснато подобрение на сигурността чрез:

3.7.1. Мониторинг за наличността на ключови услуги и своевременно информиране на ИТСЗОП при наличие на атаки до 1 час от установяването им;

3.7.2. Съобщаване на установени от Системата инциденти до 1 работен ден с конкретни препоръки за отстраняването им;

3.7.3. Установяване на кореновата причина за наличието на инцидент, извършване на корелационен анализ и препоръки за отстраняване;

3.7.4. Управление на инциденти свързани със сигурността.

3.7.5. Извършване на последващ контрол, координирано с ИТСЗОП за отстранени инциденти.

3.7.6. Идентифициране на засегнатите от заплахите услуги/активи и даване на препоръки за действия от страна на ИТСЗОП.

3.7.7. Даване на препоръки за подходящи съвременни решения на ИТСЗОП за справяне с безфайлови (извършващи се в паметта) атаки - инжектиране на код, например чрез PowerShell и др. при необходимост;

3.7.8. Ежемесечна автоматизирана проверка за наличие на уязвимости в публично видимите услуги на клиента и вътрешна мрежа за управление.

3.7.9. Процес по отстраняване и проследяване на уязвимости.