**Приложение № 2**
**към рамков договор ИС-28/02.10.2023 г.**

| | |
|---|---|
| **ЗАЯВКА по Рамков договор № ИС-28/02.10.2023 г. (ПО-16-2803/02.10.2023 г. на ИО АД)** | ☒ |
| **ЗАЯВКА по Рамков договор № ИС-28/02.10.2023 г. ((ПО-16-2803/02.10.2023 г. на ИО АД) (актуализирана)** | ☐ [1] |

| | | |
|---|---|---|
| **Позиция от ПГ-2026 г.:** | *№ по ред от ПГ* | *11* |
| **Описание на проект съгласно ПГ:** | *Мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи* | |
| **CPV код** | *72222300-0* | |
| **Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта** | *Рег.№ 90-03-406/07.08.2026* | |
| **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* | *До 50 960,00 евро без ДДС* | |
| **Начин за плащане:** *(еднократно, на части, периодично, авансово или др.)* | *На части,*<br>• *За периода от осигуряването г. до 31.10.2026 г., след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура, изчислена пропорционално на календарните дни (на стойност 237.91 евро без ДДС на ден)*<br>• *За периода от 01.11.2026 г. до 15.12.2026 г. след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност 10 705,95 евро без ДДС*<br>• *За периода от 16.12.2026 г до 31.12.2026 г. . след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи и издадена фактура на стойност* | |

[1] Отбелязва се в случай че заявката е актуализирана

| | |
|---|---|
| | *3 806,56 евро без ДДС* |
| **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***)** | *Срок за осигуряване: от осигуряване на услугата. до 31.12.2026 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)* | *На части,*<br>• *За периода от осигуряването г. до 31.10.2026 г., след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи*<br>• *За периода от 01.11.2026 г. до 15.12.2026 г. след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи*<br>• *За периода от 16.12.2026 г до 31.12.2026 г. . след подписването на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ мониторинг по сигурността, наблюдение и докладване на кибер – инциденти в режим 24*7 на информационните системи* |
| **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 ): | |
| **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.*

*Приложение 1*

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

**Гр. София, 2026 г.**

## 1. Описание

1.1. Настоящите технически параметри представят описание на услуга за мониторинг по сигурността, наблюдение и докладване на кибер-инциденти в режим 24*7 за нуждите на Агенция по геодезия, картография и кадастър (АГКК). Услугата следва да осигури автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността на АГКК 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 АГКК.

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 АГКК чрез предоставяното от Услугата интегрирано управление на данните от различни ИТ източници.

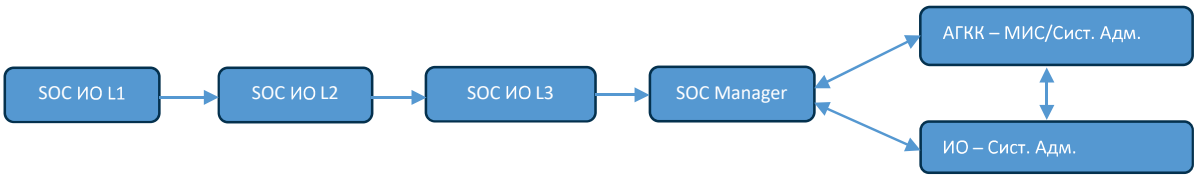
1.3.2. Своевременно идентифициране на подходящи мерки за актуализиране на специализирания приложен софтуер, използван от АГКК, с цел минимизиране на потенциални заплахи.

## 2. 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.

## 3. Място на изпълнение и ескалационна матрица

Предоставянето на услугата се извършва за Административната сграда на Агенция за геодезия, картография и кадастър, с адрес: гр. София 1618, ул. „Мусала“ № 1




Фиг.1 Ескалационна верига при инцидент

## 4. Изисквания към предоставянето на Услугата

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

4.2. 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:

4.2.1. Осигури наблюдение на крайните работни точки, присъединяване на други журнални файлове (log) към Системата, както и присъединяване на нови системи за непрекъснат мониторинг и анализ, с оглед предприемане на ответни мерки в случай на инцидент. ИО АД следва да изпраща информация по e-mail за аларми, по които е нужна допълнителна проверка от системен администратор на АГКК до 4 часа след тяхното настъпване. При установяване на неуспешна атака или фалшиво-позитивна аларма, e-mail към АГКК не е необходимо да се изпраща.

4.2.2. Извърши анализ на наличните уязвимости във вътрешната ИТ инфраструктура и предоставят препоръки и проследяване на изпълнението им, както и оказване на методическа помощ на „Експерт по мрежова и информационна сигурност“ в АГКК при идентифициране на потенциални заплахи и набелязване на мерки в краткосрочен план.

4.2.3. 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.

4.2.4. Провеждат срещи със служители на АГКК, 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 за всеки отчетен период.

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

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

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

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

4.3.3. Идентифициране на засегнатите от заплахите услуги/активи и даване на препоръки за действия от страна на АГКК.

4.3.4. Управление на инциденти свързани със сигурността.

4.3.5. Извършване на последващ контрол, координирано с АГКК за отстранени инциденти.

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

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

4.3.8. Процес по отстраняване и проследяване на уязвимости.

5. Обхват на услугата:

5.1. Incident Triage, Analysis & Response – анализ на аларми и реакция, което обхваща:

a. Real-Time Alert Monitoring and Triage - Извършване на триаж и краткосрочен анализ на потенциални инциденти със сигурността, генерирани почти в реално време и предупредителни емисии за сигурност.

b. Incident Reporting Acceptance - Получаване и обработка на доклади за потенциални инциденти със сигурността от други SOC и трети страни. Тези

доклади могат да идват чрез писмени (напр. електронна поща) или устни средства (voice).

c. Incident Analysis and Investigation - Извършване на задълбочен, подробен анализ на предполагаеми инциденти. Това включва идентифициране на подробности като произхода, степента и последиците от инцидента както и характеризиране на вида атаки.

d. Containment, Eradication, and Recovery - Извършване на дейности, подкрепящи ог-раничаването на инциденти/атакуващи, управлението на последствията, премах-ване на противника и възстановяването на системата, за да се намали текущото въздействие и да се премине към състояние, което ще предотврати бъдещи инци-денти.

e. Incident Coordination - Извършване на събиране на информация, разпространение на информация и уведомяване в подкрепа на текущ инцидент. Насочване и/или ко-ординиране на реакцията в партньорство със заинтересовани страни в отговор на инциденти, други SOC и трети страни.

f. Forensic Artifact Analysis - Изследване на системи и цифрови артефакти (твърди дис-кове, файлове, памет), за да се направят подробни наблюдения и заключения за предполагаема дейност, като анализ на съдържанието и реконструкция на време-вата линия.

g. Malware Analysis - Разглеждане на подозрителни файлове, за да се разбере произ-ходът, родословието, функциите и намерението на предполагаемите проби от зло-намерен софтуер. Това включва използването на различни методологии, включи-телно статичен код обратно инженерство и динамичен анализ по време на изпъл-нение.

5.2. Cyber Threat Intelligense, Threat Hunting – кибер разузнаване, което обхваща:

a. Cyber Threat Intelligence Collection, Processing, and Fusion - Събиране на продукти за разузнаване на киберзаплахи, включително CTI емисии и доклади. Обработка и ин-тегриране на CTI в SOC системи и анализиране и филтриране на информация за по-нататъшно потребление от SOC.

d. Threat Hunting - Извършване на проактивни операции за идентифициране на потен-циално злонамерена дейност, извън обхвата на установените SOC сигнали, въз ос-нова на хипотези, че противникът действа в дадена среда или отрасъл. Това включва разработване и усъвършенстване на персонализирани аналитични въз-можности.

5.4. Vulnerability Management – управление на уязвимости и процес по отстраняването им, което обхваща:

b. Vulnerability Scanning - Сканиране на активите за състоянието на уязвимостта, вклю-чително нивото на patch и инсталирания софтуер, и конфигурацията, свързана със сигурността, за целите на изчисляването на риска за сигурността и състоянието на съответствието.

**6. Отчитане**

Приемането на предоставената услуга се документира с приемо-предавателен протокол по чл. 6 от договора за всеки отчетен период, така както е регламентирано в заявката.

- За периода от осигуряването г. до 31.10.2026 г
- За периода от 01.11.2026 г. до 15.12.2026 г.
- За периода от 16.12.2026 г до 31.12.2026 г.

Към него се предават и генерираните от Системата:

(1) Приложение № 1 - Доклад за открити уязвимости във вътрешната мрежа за управление на АГКК за всеки месец;

(2) Приложение № 2 - Доклад за открити уязвимости в публичните мрежи на АГКК, в който влизат публични услуги на АГКК 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 ръководителя на проект по заявката от страна на Бенефициера.