ЗАЯВКА по Договор № 100 от 19.12.2023 г. (вх. № ПО-16-3466/19.12.2023 г. на „Информационно обслужване“ АД)		☒
ЗАЯВКА (актуализирана)		☐ [1]
Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*4.1*
Описание на дейност/проект съгласно ПГ:	***4.1 Осигуряване на управлението на събития и сигурността на информацията и Cloudflare "Pro" за нуждите на МФ - ПРЕХОДЕН ПРОЕКТ***	
CPV код	*72150000-1 Консултантски услуги по компютърен одит и консултантски услуги по хардуер*	
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*	*Общо за изпълнение на проекта: 697 000,00 лв.* *Разпределение по години:* *2024 г. – 221 000,00 лв.* *2025 г. – 232 000,00 лв.* *2026 г. – 244 000,00 лв.*	
Начин на плащане: *(еднократно, на части, периодично, авансово или др.)*	*Периодично, за тримесечни периоди както следва:* *Четири плащания през 2024 г. (по 55 250 лв. без ДДС за всеки тримесечен период), четири плащания за 2025 г. (по 58 000 лв. без ДДС за всеки тримесечен период),четири плащания за 2026 г. (по 61 000 лв. без ДДС за всеки тримесечен период) въз основа на:* • протокол за изпълнение на проект по чл. 9, ал.1 от Договора, към който се прилагат: - финансова справка; - отчет за изпълнени дейности по проект; • фактура	
Плащане с акредитив или авансово ДА/НЕ	*Не е приложимо*	
Документи за плащане с акредитив или авансово	*Не е приложимо*	
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*a) дейности по управление на събития и сигурността на информацията в МФ – от 01.01.2024 до 31.12.2026* *b) осигуряване на Cloudflare „Pro” – от 06.01.2024 до 31.12.2026*	
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Не е приложимо*	
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Периодично, в сроковете и с отчетните документи съгласно ТП.*	
Приложения: (*напр: технически параметри, образци на отчетни документи***)**	*Технически параметри за Осигуряване на управлението на събития и сигурността на информацията и Cloudflare "Pro" за нуждите на МФ - ПРЕХОДЕН ПРОЕКТ*	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		

[1] Отбелязва се в случай че заявката е актуализирана

Ръководители на проект/дейност по заявката (напр: представител на дирекцията – Заявител):	
ЗАЯВКАТА е ОДОБРЕНА ОТ:	
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:	
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:	
Координатор по заявката и Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	
Ръководител на проект/дейност по заявката	

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

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ОСИГУРЯВАНЕ НА УПРАВЛЕНИЕТО НА СЪБИТИЯ И СИГУРНОСТТА НА ИНФОРМАЦИЯТА И CLOUDFLARE "PRO" ЗА НУЖДИТЕ НА МФ - ПРЕХОДЕН ПРОЕКТ

м. януари, 2024 г.

1. Цел

1.1. Настоящият документ формулира изискванията на Възложителя за предоставяне на услуга за осигуряване на управлението на събития и сигурността на информацията и Cloudflare „Pro“ (Услугата) за нуждите на Министерство на финансите (МФ). Услугата следва да осигури автоматично откриване на събития, които могат да повлияят на мрежовата и информационната сигурност на важните за дейността на МФ информационни и комуникационни системи и облачна услуга от типа мрежа за доставка на съдържание Cloudflare „Pro”.

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 МФ.

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

1.3.2. Предприемане на мерки за своевременно актуализиране на специализирания приложен софтуер, използван от МФ, чрез идентифициране на потенциални заплахи.

2. Съществуващо положение

2.1. В резултат на изпълнение на Услуга №7 по договор № ДОГ- 56/01.09.2020 г. между МФ и „Информационно обслужване“ АД (ИО АД) и в съответствие с изискванията на НМИМИС, на МФ са предоставени и конфигурирани съвременни софтуерни средства IBM QRadar SIEM с вградени и настроени автоматични алгоритми за управление на сигурността на информацията и събитията, наричани за краткост „Системата“.

2.2. В инфраструктурата на МФ са създадени виртуални машини (за Log Collector и Flow Collector), с капацитет (1 000 eps (event per second), извършени са необходимите мрежови конфигурации, в инфраструктурата на МФ са инсталирани Event Collector и Flow Collector, които са интегрирани с аналогичните компоненти IBM QRadar SIEM системата в ИО АД с оглед непрекъснат мониторинг на събития и даване на своевременни препоръки за действия на ИТ екипа на МФ в случай на идентифицирани заплахи.

2.3. Към Системата са присъединени източници на журнални (log) записи като: Microsoft Windows (домейн контролери, файлов сървър и др.); защитни стени; антивирусен софтуер и др. Като източници за трафични потоци към Системата са присъединени граничните маршрутизатори на МФ.

3. Изисквания към мрежовата и информационната сигурност

3.1. 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.

3.2. Изпълнителят следва да осигури изпълнението на изискванията съгласно раздел IV от документа „Общи изисквания за изпълнение на проекти / дейности по системна интеграция“, неразделна част от План-графика за 2024 г.

4. Място на изпълнение

Предоставянето на услугата се извършва за управляваните от дирекция „Информационни системи“ (ДИС) на МФ ИТ активи, разположени в локация гр. София, ул. „Г. С. Раковски“ № 102.

5. Изисквания към предоставянето на Услугата

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

5.2. 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:

5.2.1. Осигури наблюдение на крайните точки, присъединени към Системата, както и присъединяване на нови точки до достигане на предоставената от Системата възможност (1 000 eps (event per second), непрекъснат мониторинг и анализ, с оглед предприемане на ответни мерки в случай на инцидент. ИО АД следва да изпраща информация по e-mail за не-критични аларми, по които е нужна допълнителна проверка от системен администратор на МФ до 4 часа след тяхното настъпване. При установяване на неуспешна атака или фалшиво-позитивна аларма, e-mail към МФ не е нужно да се изпраща. МФ носи изцяло отговорност за управлението и диагностиката на аларми и инциденти с вектор на атака: електронна поща и крайни работни станции. При нужда от асистенция, екипът на ИО АД ще съдейства за отстраняването на заплахите и възстановяване на работоспособността на системите и услугите.

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

5.2.3. Извършва анализ на базата на събраната информация и при необходимост предлага решения за извършване на промени в ИТ инфраструктурата в дългосрочен план.

5.2.4. При необходимост да се провеждат срещи със служители на ДИС, на които да 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. Измерването на ефективността на предприетите мерки, чрез повторен анализ и оценка на действията по отстраняване на заплахи се извършва за всеки месец.

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

5.3.1. Мониторинг за наличността на ключови услуги и своевременно информиране на ДИС при наличие на DDoS атаки. В случай на критични инциденти, пълна или частична липса на достъп и работоспособност на публични услуги, комуникацията се извършва по телефон между страните, като първоначалното сигнализиране е до 1 час след настъпване на инцидента.

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

5.3.3. Идентифициране на засегнатите от заплахите услуги/активи и даване на препоръки за действия от страна на ДИС.

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

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

5.3.6. Осигуряване на ползването на Cloudflare „Pro".

6. Отчитане и плащане

6.1. Изпълнението се документира с отчетни документи за тримесечни периоди. Отчетните документи за изпълнение на дейностите по настоящите ТП, са съгласно „Общи изисквания за изпълнение на проекти / дейности по системна интеграция" към План-графика за 2024 г. и са както следва:

а) Образец № 1 - Протокол за изпълнение на проект;

б) Образец № 2 – Финансова справка. Прилага се към Протокола за изпълнение на проект.

в) Образец № 3а – Отчет за изпълнение на дейности по проект. Прилага се към Протокола за изпълнение на проект. В отчета се описват в случай на приложимост, резултатите от наблюденията и оказаната методическа помощ, проведените работни срещи, дадените методическите указания и др. Към отчета се прилагат генерираните от Системата:

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

(2) Приложение № 2 - Доклад за открити уязвимости в публичните мрежи и услуги на МФ;

(3) Приложение № 3 - Детайли за всички генерирани аларми и предприети действия– пълен екстракт от QRadar за всички генерирани аларми. Синтезиран екстракт с важна информация за всички генерирани аларми; Графика за най-честите източници на аларми;

(4) Други доклади или извадки, генерирани от Системата в случай на приложимост, напр. двуседмични доклади и др.

Приложенията, описани по-горе се предават на споделено пространство, до което се осигурява достъп на ръководителя на проект по заявката от страна на Възложителя.

6.2. Плащанията по проекта се извършват периодично, както следва:

а) За 2024 г., както следва:

- за периода 01.01.2024 г. (за Cloudflare „Pro" от 06.01.2024 г.) – 31.03.2024 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.04.2024 г. – 30.06.2024 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.07.2024 г. – 30.09.2024 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;

- за периода 01.10.2024 г. – 31.12.2024 г. на база подписани отчетни документи по т. 6.1 за периода 01.10.2024 г. – 10.12.2024 г. по букви а), б) и в) и издадена фактура за посочената във финансовата справка стойност за предоставянето на услугата до 31.12.2024 г. Дейностите по предоставяне на услугата в периода от 11.12.2024 г. до 31.12.2024 г. се отчитат заедно със следващия отчетен период 01.01.2025 г. - 31.03.2025 г., като за тях не се дължи заплащане.

б) За 2025 г., както следва:

- за периода 01.01.2025 г. – 31.03.2025 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.04.2025 г. – 30.06.2025 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.07.2025 г. – 30.09.2025 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.10.2025 г. – 31.12.2025 г. на база подписани отчетни документи по т. 6.1 за периода 01.10.2025 г. – 10.12.2025 г. по букви а), б) и в) и издадена фактура за посочената във финансовата справка стойност за предоставянето на услугата до 31.12.2025 г. Дейностите по предоставяне на услугата в периода от 11.12.2025 г. до 31.12.2025 г. се отчитат заедно със следващия отчетен период 01.01.2026 г. – 31.03.2026 г., като за тях не се дължи заплащане.

в) За 2026 г., както следва:

- за периода 01.01.2026 г. – 31.03.2026 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.04.2026 г. – 30.06.2026 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.07.2026 г. – 30.09.2026 г. на база подписани отчетни документи по т. 6.1, букви а), б) и в) и издадена фактура;
- за периода 01.10.2026 г. – 31.12.2026 г. на база подписани отчетни документи по т. 6.1 за периода 01.10.2026 г. – 10.12.2026 г. по букви а), б) и в) и издадена фактура за посочената във финансовата справка стойност за предоставянето на услугата до 31.12.2026 г. За периода от 11.12.2026 г. до 31.12.2026 г. се предоставят отчетни документи до 15.01.2027 г. по т.6.1, букви а) и в), които не са основание за плащане.