Д О Г О В О Р

№ ИНФОРМАЦИОННО ОБСЛУЖВАНЕ ПО-16-244/09.01.2025 .....

В гр. София, между:

1. МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО, адрес: гр. София 1000, пл. "Света Неделя" № 5, БУЛСТАТ 000695317, представлявано от д-р Галя Кондева – министър на здравеопазването и , директор на дирекция „БФ", наричано **ВЪЗЛОЖИТЕЛ**, от една страна,

и

1. **„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ" АД**, ЕИК 831641791, със седалище, адрес на управление и адрес за кореспонденция: гр. София 1504, район Оборище, ул. „Панайот Волов" № 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, в качеството му на системен интегратор по смисъла на § 45, ал.1 от ***Преходните и заключителни разпоредби към Закона за изменение и допълнение на закона ЗЕУ*** и публичен възложител на обществени поръчки по смисъла на чл. 5, ал. 2, т. 14 от ***Закона за обществените поръчки*** (ЗОП) във връзка с §2, т. 43 от ***Допълнителните разпоредби на ЗОП***, наричано по-долу за краткост ИЗПЪЛНИТЕЛ, от друга страна, двете наричани по-долу за краткост „страни", като взеха предвид че:

- услугите, както и дейностите, които осигуряват изпълнението на тези услуги, предмет на настоящия Договор, представляват дейности по системна интеграция, по смисъла на чл. 7с от ЗЕУ;
- Съгласно § 45, ал. 1 от ***Преходните и заключителни разпоредби към Закона за изменение и допълнение на ЗЕУ*** (Обн. - ДВ, бр. 94 от 2019 г., изм. - ДВ, бр. 102 от 2019 г., в сила от 29.11.2019 г.) системната интеграция по чл. 7с от ЗЕУ се извършва от „Информационно обслужване" АД, което по закон притежава правото да предоставя услуги по изграждане, поддържане, развитие и наблюдение на работоспособността на информационните и комуникационните системи, използвани от административните органи, както и дейности, които осигуряват изпълнението на тези услуги;
- на основание § 45, ал. 2 от Преходните и Заключителните разпоредби към Закона за изменение и допълнение на ЗЕУ, съгласно т. 21 до т.27 вкл. от Решение № 727 на Министерския съвет от 2019 г., с последващи изменения и

допълнения, Министерството на здравеопазването, Изпълнителната агенция по лекарствата, Изпълнителна агенция „Медицински надзор“, Регионалните здравни инспекции, Националната експертна лекарска комисия, Националния център по трансфузионна хематология и Районните центрове по трансфузионна хематология са определени като административни органи, който при изпълнение на своите функции, свързани с дейности по системна интеграция, възлагат изпълнението на тези дейности на „Информационно обслужване“ АД;

- Предвид това, че услугата е от общ икономически интерес, както и с цел изключване на риск от евентуално нарушаване на конкуренцията, „Информационно обслужване” АД се задължава да предприеме действия за осигуряване на изпълнението на дейностите, включени в Техническата спецификация (Технически параметри) към този договор, чрез възлагането им на трето лице, в качеството си на публичен възложител по ЗОП, съгласно § 45, ал. 1 от Преходните и заключителни разпоредби към ЗИДЗЕУ,
- На основание с чл. 7с от ***Закона за електронното управление*** (ЗЕУ), § 45, ал. 1 от Преходните и заключителни разпоредби към Закона за изменение и допълнение на ЗЕУ и чл. 9 от Закона за задълженията и Договорите (ЗЗД), се сключи настоящият Договор („Договора“) за следното:

I. ПРЕДМЕТ НА ДОГОВОРА И МЯСТО НА ИЗПЪЛНЕНИЕ

Чл. 1. (1) ВЪЗЛОЖИТЕЛЯТ възлага, а **ИЗПЪЛНИТЕЛЯТ** приема да осигури чрез трето лице, избрано след проведена процедура по реда на Закона за обществените поръчки (ЗОП), изпълнението на дейности по системна интеграция, попадащи в обхвата на чл. 7с от ЗЕУ, по проект: „Повишаване на капацитета за реагиране при инциденти, засягащи информационната и комуникационна сигурност в сектор Здравеопазване“, финансиран по Оперативна програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“, по приоритетна ос „Цифрова трансформация на публичния сектор“, съгласно заложеното в Техническа спецификация (Технически параметри) (Приложение № 1), неразделна част от настоящия договор.

(2) В обхвата на договора се включва : доставка и гаранционна поддръжка на информационните ресурси, описани в Приложение 1 - Техническа спецификация (Технически параметри)

(3**)** ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите по ал. 1, ал. 2 в съответствие на изискванията на Техническа спецификация (Технически параметри)на ВЪЗЛОЖИТЕЛЯ, което е неразделна част от настоящия договор.

Чл. 2. Място на изпълнение на дейностите по договора гр. София, Министерство на здравеопазването, пл. “Света Неделя” № 5

II. СРОК НА ДЕЙСТВИЕ И ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ

Чл. 3. Договорът влиза в сила от датата на подписването му от страните с електронен подпис, с начална дата на изпълнение на дейностите, включени в Техническа спецификация (Технически параметри), считано от датата на подписване на договор за обществена поръчка между „Информационно обслужване“ АД и избран изпълнител по ЗОП и срокове, както следва:

1. Срок за изпълнение на доставката на информационни ресурси: до 6 месеца;
2. Срокът за гаранционна поддръжка е 36 (тридесет и шест) месеца след приемане на дейностите по доставка

Чл. 4. (1) Договорът се прекратява:

1. При изтичане на периода на предоставяне на дейностите по чл. 3, от договора;
2. По взаимно съгласие на страните, изразено писмено;
3. При настъпване на обективна невъзможност за изпълнение на договора, вкл. отмяна на изключителните права за системния интегратор за изпълнение на съответните дейности, посредством промяна в нормативната уредба.

(2) В случай, че ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, същият следва да го отстрани в срок от 30 (тридесет) дни от писмено уведомление за извършеното нарушение. При настъпването на всяко „нарушаване на съществено условие по Договора“ от страна на ИЗПЪЛНИТЕЛЯ, се съставя протокол, подписан от лицата по чл. 16 и чл. 17, определени от страните по

Договора, отговарящи за изпълнението му. За „съществено условие" по смисъла на изречение първо се счита такова условие, което е свързано с основните права и задължения на страните по Договора, и чието неизпълнение води до неизпълнение на целия предмет на Договора или част от него.

(3) ВЪЗЛОЖИТЕЛЯТ може по своя преценка да удължи 30-дневния период по ал. 2 за такъв период, за който ИЗПЪЛНИТЕЛЯТ продължава нормалните усилия за отстраняване на неизпълнението.

(4) ВЪЗЛОЖИТЕЛЯТ има право едностранно да прекрати договора:

1. при започване на процедура по ликвидация на ИЗПЪЛНИТЕЛЯ;

2. при откриване на производство за обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ, както и при обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ;

(5) При прекратяване на Договора, ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ всички суми за дейностите, изпълнени съгласно този Договор, които са били дължими към момента на прекратяването му.

(6) При непредвидени обстоятелства вкл. обжалване на решения на ВЪЗЛОЖИТЕЛЯ или на ИЗПЪЛНИТЕЛЯ, посоченият в ал. 1 срок за предоставяне на услугите се счита за автоматично продължен със срока на действие на съответните непредвидени обстоятелства, за което се изготвя констативен протокол.

(7) По искане на ВЪЗЛОЖИТЕЛЯ и при съгласие на ИЗПЪЛНИТЕЛЯ, срокът на договора може да бъде удължен с подписване на допълнително споразумение между страните.

III. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 5. (1) Максимално допустимата стойност за изпълнение на услугата, съгласно предмета на договора по чл. 1, е в размер на 1 039 370,00 лв. (един милион тридесет и девет хиляди триста и седемдесет) без ДДС, съответно 1 247 244 лв. (един милион двеста четиридесет и седем хиляди двеста четиридесет и четири) с включен ДДС, при действаща 20% ставка на ДДС. При законодателна промяна в размера на приложимата ставка, възнаграждението се актуализира в съответствие с настъпилото изменение, без необходимост от подписване на допълнително споразумение.

(2) ВЪЗЛОЖИТЕЛЯТ заплаща на ИЗПЪЛНИТЕЛЯ обща стойност за изпълнение на услугата по чл. 1 от договора в размер, съгласно ценовото

предложение на избрания изпълнител, определен от „Информационно обслужване“ АД след провеждане на процедура за възлагане на обществена поръчка по реда на Закона за обществените поръчки.

(3) В Цената по ал. 1 са включени всички разходи на **ИЗПЪЛНИТЕЛЯ** за изпълнение на Услугите, като **ВЪЗЛОЖИТЕЛЯТ** не дължи заплащането на каквито и да е други разноски, направени от **ИЗПЪЛНИТЕЛЯ**.

(4) Цената по ал. 1 включва изпълнението на дейностите по чл.1, ал.2.

(5) ВЪЗЛОЖИТЕЛЯТ заплаща на **ИЗПЪЛНИТЕЛЯ** цената за услугата, предмет на този договор *еднократно*, в срок до 20 дни от получаване на издадена от **ИЗПЪЛНИТЕЛЯ** оригинална фактура и подписани двустранни приемо-предавателни протоколи (за приемането на извършената доставка по чл.1, ал.2) от координаторите по договора за двете страни, при спазване на условията по ал. 6.

(6) Плащането по този Договор се извършва въз основа на следните документи:

1. приемо-предавателни протоколи (за приемането на извършената доставка по чл.1, ал.2 от договора), подписани от координаторите по договора за **ВЪЗЛОЖИТЕЛЯ** и **ИЗПЪЛНИТЕЛЯ,** в съответствие на изискванията на Техническа спецификация (Технически параметри)на ВЪЗЛОЖИТЕЛЯ, която е неразделна част от настоящия договор и при съответно спазване на разпоредбите на Раздел VI (Отговорности) от Договора; и

2. фактура, издадена от **ИЗПЪЛНИТЕЛЯ**, съдържаща отделни стойности на информационните ресурси по чл.1, ал.2, представена на **ВЪЗЛОЖИТЕЛЯ** и подписана от координатора по договора за **ВЪЗЛОЖИТЕЛЯ.**

(7) Плащанията се извършват съобразно правилата за извършване на плащания по договори на стойност равна или надвишаваща 10 000 лв. от разпоредители с бюджет, съгласно чл. 182а и чл. 182б от Данъчно–осигурителния процесуален кодекс (ДОПК).

Чл. 6. **(1)** Изплащането на договореното възнаграждение по чл. 5, ал. 1 ще бъде извършвано по следната, посочена от ИЗПЪЛНИТЕЛЯ банкова сметка в

Заличаването на IBAN на Изпълнителя е на основание чл. 72 и чл. 73 от ДОПК.

(2) При промяна на банковата сметка, посочена от ИЗПЪЛНИТЕЛЯ, преди

извършване на дължимото плащане, същият уведомява ВЪЗЛОЖИТЕЛЯ писмено в 3-дневен срок от настъпване на промяната. В случай, че не уведоми ВЪЗЛОЖИТЕЛЯ в този срок, плащането по посочената в Договора сметка се счита за валидно извършено.

Чл. 7. Страните се съгласяват, че в случай, че съответната коректно издадена фактура не е получена от ВЪЗЛОЖИТЕЛЯ в срок от 10 (десет) дни от датата на издаването ѝ, няма да е налице забава от страна на ВЪЗЛОЖИТЕЛЯ за плащане на дължимите суми и не се дължи лихва за забава за периода, с който е забавено представянето на фактурата.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 8. (1) ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите, предмет на договора, съгласно чл. 1 от същия, при спазване на изискванията на ВЪЗЛОЖИТЕЛЯ, дадени в Техническа спецификация (Технически параметри)– Приложение № 1 към същия.

(2) ИЗПЪЛНИТЕЛЯТ се задължава при подготовка на образеца на ценово предложение към документацията за провеждане на процедурата за възлагане на обществена поръчка по реда на ЗОП да заложи остойностяване на информационните ресурси по чл.1, ал.2 от договора,.

(3) ИЗПЪЛНИТЕЛЯТ се задължава да избере трето лице – изпълнител на доставката и гаранционната поддръжка по чл.1, ал.2, посредством прилагане на критерий за възлагане „най-ниска цена“.

Чл. 9. (1) ИЗПЪЛНИТЕЛЯТ се задължава да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 17 от Договора. Да опазва и да не разгласява пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена по закон или по силата на Договора информация, която е станала известна при изпълнението на дейностите по чл.1, като представи декларация по образец – Приложение №2 за това.

(2) При изпълнение на предмета на Договора, посочен в чл. 1, ИЗПЪЛНИТЕЛЯТ се задължава да прилага някои или всички изброени по-долу изисквания, съобразно обхвата на възложената дейност:

а) да спазва изискванията на действащата нормативна уредба в областта на

мрежовата и информационната сигурност;

б) да прилага адекватни мерки за мрежова и информационна сигурност, включително да доказва прилагането им чрез документи и/или провеждане на одити при необходимост;

в) да прилага система за прозрачност на веригата на доставките, като при поискване, трябва да може да докаже произхода на предлагания ресурс/ услуга и неговата сигурност;

(3) При възлагане изпълнението на дейностите на трети лица, , ИЗПЪЛНИТЕЛЯТ следва да изисква от същите да прилагат някои или всички, изброени в ал. 2, изисквания, съобразно обхвата на възложената дейност.

Чл. 10 (1) При изпълнение на дейностите по договора ИЗПЪЛНИТЕЛЯТ, неговите подизпълнители и служители се задължават:

1. да спазват политиката, правилата и процедурите по информационна сигурност на ВЪЗЛОЖИТЕЛЯ;

2. да опазват и да не разгласяват пред трети лица съдържанието на документацията, която е станала известна при изпълнението на договора, без писменото съгласие на ВЪЗЛОЖИТЕЛЯ, с изключение на случаите, когато са задължени по закон за това;

3. да опазват и да не разгласяват пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор;

4. да обработва законосъобразно и добросъвестно лични данни, доколкото тези данни са изрично необходими за целите на изпълнение на поетия ангажимент;

5. да предоставя лични данни на публични органи (държавни и общински), когато такива данни са изискани въз основа на валидно законово основание и по законоустановен за целта ред, като своевременно уведоми за това ВЪЗЛОЖИТЕЛЯ;

6. да предприеме всички необходими организационни и технически мерки за осигуряване на целостта и поверителността на данните в случай, че ВЪЗЛОЖИТЕЛЯТ предостави на ИЗПЪЛНИТЕЛЯ достъп до собствени IT активи, документи и данни;

7. да опазват и да не разгласяват пред трети лица информация, която е станала известна при изпълнението на договора относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ, изготвени в хода на изпълнението

документи и/или всякакви други резултати от изпълнението, както и да не разгласяват, използват или предоставят на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на договора, с изключение на случаите, когато са задължени по закон за това;

8. да спазват вътрешните правила за достъп и режим на работа в сградата на ВЪЗЛОЖИТЕЛЯ;

9. да спазват всички процедури и изисквания на ВЪЗЛОЖИТЕЛЯ за работа в информационната инфраструктура на ВЪЗЛОЖИТЕЛЯ;

10. да не осъществяват достъп до компютърни данни в компютърна система без разрешение, да не добавят, променят, изтриват или унищожават компютърна програма или компютърни данни, да не въвеждат компютърен вирус в компютърните системи или мрежи на ВЪЗЛОЖИТЕЛЯ, да не разпространяват пароли или кодове за достъп до компютърна система или до компютърни данни на ВЪЗЛОЖИТЕЛЯ, от което би могло да последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна;

11. да спазват изискванията за популяризиране на проекта, в т.ч. всяка комуникационна дейност, свързана с проекта (включително на конференции, семинари, информационни материали като брошури, листовки, плакати, презентации и т.н., в електронна форма, чрез социални медии и т.н.),всяка инфраструктура, оборудване или основен резултат, финансиран от безвъзмездната помощ, както и всеки отчетен документ (приемо-предавателен протокол, доклад, фактура и т.н.), трябва да показват емблемата на ЕС и да включват следния текст: „Този [въведете подходящо описание, напр. доклад, публикация, конференция, инфраструктура, оборудване, вмъкване на типа резултат и т.н.] е финансиран по Оперативна програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“, по приоритетна ос „Цифрова трансформация на публичния сектор“.

12. да предоставят - по време на изпълнение на дейностите по договора или след това - всякаква информация, която се изисква при извършване на одити и проверки на място от европейски институции /Европейска Комисия, Европейска сметна палата, Главна дирекция “Европейска служба за борба с измамите“-OLAF, с цел да се провери допустимостта на разходите и правилното изпълнение на дейностите по настоящия договор, съгласно сключеното между ВЪЗЛОЖИТЕЛЯ и ЕК грантово споразумение.

(2) С оглед изпълнението на задълженията по ал. 1, ИЗПЪЛНИТЕЛЯТ (представляващите го лица), както и лицата, ангажирани с изпълнението на дейностите (екипа на ИЗПЪЛНИТЕЛЯ), представят декларация за опазване на информацията.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ

Чл. 11. (1) ВЪЗЛОЖИТЕЛЯТ следва да предостави на ИЗПЪЛНИТЕЛЯ необходимото съдействие за изпълнение на договора, както и да приеме и заплати извършеното от ИЗПЪЛНИТЕЛЯ в съответствие с договора.

(2) При необходимост, ВЪЗЛОЖИТЕЛЯТ ще осигури условия за провеждане на работни срещи за изпълнението на договора. Местата ще бъдат осигурени на ангажираните от изпълнителя по ЗОП лица, при съблюдаване на изискванията на здравословни и безопасни условия на труд (ЗБУТ).

(3) ВЪЗЛОЖИТЕЛЯТ се задължава да осигури на ИЗПЪЛНИТЕЛЯ и избрания изпълнител, определен от „Информационно обслужване“ АД след провеждане на процедура за възлагане на обществена поръчка по реда на ЗОП, достъп до сградата на ВЪЗЛОЖИТЕЛЯ, съгласно вътрешните процедури на ВЪЗЛОЖИТЕЛЯ за осигуряване на достъп, за целите на изпълнение на дейностите по договора.

(4) ВЪЗЛОЖИТЕЛЯТ се задължава да предостави достъп до необходимите за изпълнение на дейностите по договора ИТ активи, документация и данни, при получаване на обосновано искане от изпълнителя по ЗОП.

VI. ОБЩИ И СПЕЦИАЛНИ УСЛОВИЯ ПО ЗАКОНА ЗА ЗДРАВОСЛОВНИ И БЕЗОПАСНИ УСЛОВИЯ НА ТРУД (ЗЗБУТ)

Чл. 12 (1) В случаите на осигуряване на работни места, ВЪЗЛОЖИТЕЛЯТ и ИЗПЪЛНИТЕЛЯТ се задължават да осигурят прилагането на правила за съвместно осигуряване на здравословни и безопасни условия на труд за административните сгради, с адрес: гр. София, пл. “Света Неделя” № 5, в изпълнение на разпоредбата на чл. 18 от Закона за здравословни и безопасни условия на труд (ЗЗБУТ), както следва:

1. определят задълженията и отговорностите си за осигуряване на здравословни и безопасни условия на труд (ЗБУТ) при работа на работниците и служителите, както и здравословни и безопасни условия за други лица, които се намират в района на мястото на извършване на дейностите по Техническа спецификация (Технически параметри);

2. информират своевременно за възможните опасности и рисковете при работа съгласно ЗЗБУТ и действащите вътрешни правила;

3. координират дейностите си за предпазване на работниците и служителите от тези рискове;

4. прилагат всички нормативни документи, отнасящи се до спазване на изискванията за ЗБУТ.

(2) С възлагане на дейността, ВЪЗЛОЖИТЕЛЯ и избрания от „Информационно обслужване“ АД изпълнител по ЗОП, следва да поемат следните конкретни задължения за осигуряване на ЗБУТ:

1. На служителите на изпълнителя по ЗОП се провежда начален и периодични инструктажи от длъжностните лица, определени за това, съгласно изискванията на Наредба № РД-07-2/2009 г.;

2. ВЪЗЛОЖИТЕЛЯТ следва да запознае служителите на изпълнителя по ЗОП с разработения, съгласно Наредба № 8121з-647/2014 г. план за пожарна и аварийна безопасност, план за евакуация, схеми за евакуация с обозначение на евакуационните изходи и средствата за пожарогасене и да извърши обучение за евакуация и работа с пожарогасителна техника;

3. ВЪЗЛОЖИТЕЛЯТ предоставя на служителите на изпълнителя по ЗОП информация за рисковете за здравето и безопасността на неговите служители, както и за мерките, които се предприемат за отстраняването, намаляването или контролирането им, при необходимост.

4. Всички останали изисквания по време на изпълнение на дейностите, извън посочените в настоящия документ ангажименти на ВЪЗЛОЖИТЕЛЯ по отношение на работна среда и условията за работа, ще бъдат допълнително уточнени с ВЪЗЛОЖИТЕЛЯ, след получаване на заявка от страна на изпълнителя по ЗОП, ведно с обосновка на необходимостта за тяхното предоставяне и съгласно възможността от страна на ВЪЗЛОЖИТЕЛЯ за това.

(3) При необходимост, ВЪЗЛОЖИТЕЛЯТ се задължава да осигури:

1. ползване на стационарни телефони с вътрешна и външна линия, като разговорите се заплащат от изпълнителя по ЗОП въз основа на издадена фактура от ВЪЗЛОЖИТЕЛЯ;

2. условия за провеждане на работни срещи.

VII. ОТГОВОРНОСТИ

Чл. 13. (1) При пълно виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи неустойка в размер на 10 % от максимално допустимата стойност на договора без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 20-дневен срок от уведомяването. За пълно неизпълнение се приема неизвършването на нито една от дейностите, включени в обхвата на договора по чл. 1, ал. 2.

(2) При частично виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи неустойка в размер на 5 % от максимално допустимата стойност на договора без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 20-дневен срок от уведомяването. За частично неизпълнение се приема неизвършването на дейност, включена в обхвата на договора по чл. 1, ал. 2.

(3) В случай че ИЗПЪЛНИТЕЛЯТ е в забава по негова вина, ВЪЗЛОЖИТЕЛЯТ има право да получи неустойка за забавено изпълнение в размер на 0,01% на ден върху максимално допустимата стойност на договора без ДДС, считано от деня, следващ деня, в който ИЗПЪЛНИТЕЛЯТ е следвало да извърши съответната дейност, но не повече от 1% от максимално допустимата стойност на договора без ДДС.

(4) В случай че е налице забава по вина на ВЪЗЛОЖИТЕЛЯ, ИЗПЪЛНИТЕЛЯТ не дължи неустойка за забавено изпълнение.

(5) При констатирано лошо или друго неточно или частично изпълнение или при отклонение от изискванията на ВЪЗЛОЖИТЕЛЯ, същият има право да поиска от ИЗПЪЛНИТЕЛЯ да изпълни изцяло и качествено, без да дължи допълнително възнаграждение за това. В случай, че и повторното изпълнение на дейността е некачествено, ВЪЗЛОЖИТЕЛЯТ има право да изиска неустойка в размер на 2 % от максимално допустимата стойност на договора без ДДС.

(6) Всяка забава се удостоверява с констативен протокол, подписан от страните, чрез координаторите по чл. 16 и чл. 17.

(7) ВЪЗЛОЖИТЕЛЯТ може да претендира обезщетение за нанесени вреди и/или пропуснати ползи по общия ред, независимо от начислените неустойки, включително при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност.

(8) В случай на извършване на финансови корекции за изпълнението на настоящия договор ВЪЗЛОЖИТЕЛЯТ може да упражни правото си на регресен иск и да предяви претенции за заплащане на неустойка от ИЗПЪЛНИТЕЛЯ в размера на извършената корекция.

Чл. 14. Страните запазват правото си да търсят обезщетение за вреди, ако тяхната стойност е по-голяма от изплатените неустойки по реда на този раздел.

VII. ДРУГИ УСЛОВИЯ

Чл. 15. Всички съобщения и уведомления на страните по настоящия договор ще се извършват само в писмена форма, като условие за действителност. Кореспонденция, свързана непосредствено с извършване на дейностите по договора, може да бъде извършвана и чрез електронна поща на електронните адреси посочени в чл. 17 и чл. 18 от договора или чрез Среда за електронен обмен на съобщения (СЕОС).

Чл. 16. Спорни въпроси, възникнали при действието на този договор се решават по пътя на споразумения, а нерешените се отнасят за решаване от компетентния съд.

Чл. 17. Отговарящ за изпълнението на договора от страна на **ВЪЗЛОЖИТЕЛЯ** и координатор за времето на неговото действие е……(име и фамилия, длъжност)……; тел:……; имейл:……., а в негово отсъствие: ……(име и фамилия, длъжност)……; тел:……; имейл:…….,.

Чл. 18. Отговарящ за изпълнението на договора от страна на **ИЗПЪЛНИТЕЛЯ** за времето на неговото действие е: – Старши експерт, сигурност на ИКТ - администратор по сигурността - Отдел Оперативен център за киберсигурност; тел: ; имейл:

Чл. 19. (1) Всяка от Страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала ѝ известна при или по повод изпълнението на Договора („Конфиденциална информация“). Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство, свързани с изпълнението на Договора

(2) Конфиденциална информация за целите на настоящия договор включва и:

1. съдържанието на документацията, която е станала известна при изпълнението на договора;

2. съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на договора;

3. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, разработена в полза на ВЪЗЛОЖИТЕЛЯ или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящата поръчка.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на Договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) С изключение на случаите, посочени в ал. 5 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата Страна, като това съгласие не може да бъде отказано безпричинно.

(5) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другата Страна по Договора.

(6) Задълженията по този член се отнасят до ИЗПЪЛНИТЕЛЯ, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, като ИЗПЪЛНИТЕЛЯТ отговаря за изпълнението на тези задължения от страна на такива лица.

(7) Задълженията, свързани с неразкриване на Конфиденциалната информация остават в сила и след прекратяване на Договора на каквото и да е основание.

(8) ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на дейностите, предмет на този договор, независимо дали е въз основа на данни и материали на ВЪЗЛОЖИТЕЛЯ или на резултати от работата на ИЗПЪЛНИТЕЛЯ, без предварителното писмено съгласие на ВЪЗЛОЖИТЕЛЯ, което съгласие няма да бъде безпричинно отказано или забавено.

VIII. НЕПРЕОДОЛИМА СИЛА

Чл. 20. (1) Страните не отговарят за неизпълнение на задължение по този Договор, когато невъзможността за изпълнение се дължи на непреодолима сила. За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата Страна в срок до 3 *(три)* дни от настъпване на непреодолимата сила. Към уведомлението се прилагат всички релевантни и/или нормативно установени доказателства за настъпването и естеството на непреодолимата сила, причинната връзка между това обстоятелство и невъзможността за изпълнение, и очакваното времетраене на неизпълнението.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира, като страните подписват протокол, в който удостоверяват началната дата на спиране. Засегнатата Страна е длъжна, след съгласуване с насрещната Страна, да продължи да изпълнява тази част от задълженията си, които не са възпрепятствани от непреодолимата сила.

(4) След отпадане на непреодолимата сила, засегнатата страна в срок до 3 *(три)* дни уведомява писмено другата Страна, като прилага всички релевантни и/или нормативно установени доказателства за отпадането й. Страните подписват протокол, с който удостоверяват датата, от която се възобновява изпълнението на задълженията.

(5) Не може да се позовава на непреодолима сила Страна:

1. която е била в забава или друго неизпълнение преди настъпването на непреодолима сила;

2. която не е информирала другата Страна за настъпването на непреодолима сила; или

3. чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на Договора.

(7) Липсата на парични средства не представлява непреодолима сила.

IX. АВТОРСКИ ПРАВА И ИЗХОДЕН КОД

Чл. 21 (1) Всички авторски и сродни права върху произведения, обект на закрила на Закона за авторското право и сродните му права, включително, но не само, компютърните програми, техният изходен програмен код, структурата и дизайнът на интерфейсите и базите данни, чието разработване е включено в обхвата на Техническа спецификация (Технически параметри), възникват за ВЪЗЛОЖИТЕЛЯ в пълен обем без ограничения в използването, изменението и

разпространението им и представляват произведения, създадени по поръчка на ВЪЗЛОЖИТЕЛЯ, съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права (ЗАПСП).

(2) Авторските и всички сродни права и собствеността върху изработените функционалности/софтуерни продукти, техният изходен програмен код, дизайнът на интерфейсите и базите данни, чиято разработка е предмет на Техническа спецификация (Технически параметри)и всички съпътстващи изработката им проучвания, разработки, скици, чертежи, планове, модели, документи, софтуер, дизайни, описания, документи, данни, файлове, матрици или каквито и да било средства и носители и свързаната с тях документация и други продукти, възникват директно за ВЪЗЛОЖИТЕЛЯ, в пълния им обем, съгласно действащото законодателство, а в случай че това не е възможно ще се считат за прехвърлени на ВЪЗЛОЖИТЕЛЯ в пълния им обем, без никакви ограничения в използването, изменението и разпространението им без ВЪЗЛОЖИТЕЛЯТ да дължи каквито и да било допълнителни плащания и суми освен договорената цена за изпълнение на дейностите от Техническа спецификация (Технически параметри).

(3) Техническа спецификация (Технически параметри) на ВЪЗЛОЖИТЕЛЯ и цялата информация предоставена на ИЗПЪЛНИТЕЛЯ от ВЪЗЛОЖИТЕЛЯ за изпълнение на дейностите по договора, са изключителна собственост на ВЪЗЛОЖИТЕЛЯ и същият притежава авторските права върху тях, като всички резултати в изпълнение на дейностите от Техническата спецификация (Техническите параметри), както и авторските права върху тях остават изключителна собственост на ВЪЗЛОЖИТЕЛЯ и могат да бъдат използвани по негово собствено усмотрение свободно в други проекти, развивани, или осъществявани от него.

(4) Правата на ВЪЗЛОЖИТЕЛЯ върху Софтуерните продукти и обектите, обхващат всички видове използване, както е предвидено в ЗАПСП, без никакви ограничения по отношение на срокове и територия, включително но не само: право на ползване, промяна, изменение, възпроизвеждане, публикуване, разпространение, продажба, адаптиране, прехвърляне, представяне, маркетинг, разпореждане по какъвто и да било начин и с каквито и да било средства в най-широк възможен смисъл и по най-широк възможен начин за целия срок на действие и закрила на авторското право, за всички държави, където това право може да бъде признато.

Това право на ВЪЗЛОЖИТЕЛЯ е без ограничение по отношение на броя на възпроизвеждането, разпространението или представянето и е валидно за всички държави, езици и начин на оперирane.

(5) „Информационно обслужване АД“ и третото лице – изпълнител на услугата по ЗОП нямат право да прехвърлят на трети лица каквито и да било права свързани със софтуерните продукти, включително, но не само правото на ползване и/или на промяна, както и няма право да използват и/или прехвърлят, разкрива или предоставя по какъвто и да било начин на трети лица изработените функционалности/софтуерни продукти, техният изходен програмен код, дизайнът на интерфейсите и базите данни, чиято разработка е предмет на Техническа спецификация (Технически параметри)и всички съпътстващи изработката им проучвания, разработки, скици, чертежи, планове, модели, документи, софтуер, дизайни, описания, документи, данни, файлове, матрици или каквито и да било средства и носители и свързаната с тях документация и други продукти.

Настоящият договор е изготвен като електронен документ и влиза в сила след подписването му с квалифициран електронен подпис от представителите на двете страни, като приложенията са негова неразделна част.

Приложения:

1. Приложение № 1 – Техническа спецификация (Технически параметри);
2. Приложение № 2 – Образец на декларация за опазване на информацията.

Д-Р ГАЛЯ КОНДЕВА
МИНИСТЪР НА ЗДРАВЕОПАЗВАНЕТО

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР

ДИРЕКТОР НА ДИРЕКЦИЯ „БФ“

ГЛАВЕН СЧЕТОВОДИТЕЛ

ПРИЛОЖЕНИЕ 1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ (ТЕХНИЧЕСКИ ПАРАМЕТРИ) ЗА ДОСТАВКА НА ИНФОРМАЦИОННИ РЕСУРСИ ЗА ПОВИШАВАНЕ НА КАПАЦИТЕТА ЗА РЕАГИРАНЕ ПРИ ИНЦИДЕНТИ, ЗАСЯГАЩИ ИНФОРМАЦИОННАТА И КОМУНИКАЦИОННА СИГУРНОСТ В СЕКТОР ЗДРАВЕОПАЗВАНЕ

1. Решение за разширена защита и разследване на заплахи на ниво крайна точка

Минимални технически изисквания	
REQ.1.	Предложеното решение трябва да включва лицензи за 2500 крайни точки.
REQ.2.	Предложеното решение трябва да включва достъп до онлайн платформа на производителя за персонализирано обучение на служители на организацията за работата им с компонентите на решението.
REQ.3.	Решението трябва да се предоставя под формата на облачна SaaS услуга, без наличието на каквито и да е локално разположени компоненти, освен за целите на интеграция с конкретни решения – например SIEM технология.
REQ.4.	Решението трябва да се управлява от единна конзола за управление за всичките му компоненти.
REQ.5.	Централната конзола за управление на решението трябва да е уеб базирана и да може да се достъпва през уеб-браузър, като комуникацията трябва да е защитена от тип HTTPS (минимално използвайки TLS 1.2).
REQ.6.	Решението трябва да разполага с API интерфейс за интеграции с други решения.
REQ.7.	Централната конзола за управление на решението трябва да е облачно разположена и да е с минимален процент на време за достъпност от поне 99.9%, като решението да може да използва агенти за защита на локалните работни станции и сървъри.
REQ.8.	Всички компоненти на решението трябва да са предоставени от един производител.
REQ.9.	Решението трябва да поддържа използването на списъци със забранени публични IP адреси, които да не могат да достъпват конзолата за управление.
REQ.10.	Решението трябва да поддържа OAuth2 базиран API достъп до платформата.
REQ.11.	Решението трябва да поддържа SAML 2.0 интеграция с външни потребителски директории за единен достъп до платформата, като да се поддържат минимално поне следните доставчици на услуги за идентичности: Active Directory Federation Services (ADFS); Azure AD; OKTA; PingOne; PingFederate.
REQ.12.	Решението трябва да може автоматично да предоставя временен достъп (just-in-time) на нови потребители чрез AML списъци, минимално със следните функции: * JIT създаване на акаунт * JIT управление на роли * JIT управление на групи от потребители
REQ.13.	Решението трябва да разполага с вградена потребителска директория и да поддържа двуфакторна автентикация чрез токени за временна еднократна парола (Time-Based One-Time Password).
REQ.14.	Решението трябва да поддържа използването на правила за комплексни пароли за администраторите: минимална дължина от 12 символа, наличие на малки и главни символи, наличие на цифри, наличие на специални символи.
REQ.15.	Решението трябва да поддържа използването на отделни конзоли за отделни звена на организацията или за подорганизации (multi-tenancy), като броят на конзолите да е неограничен.
REQ.16.	Решението трябва да може да се поставя на крайни точки, които разполагат с конкурентни антивирусни/EDR решения, важащо за фазата на инсталиране на агентите (да не се изисква първо да трябва да се премахнат конкурентните агенти, за да се извърши процесът по инсталация).
REQ.17.	Решението трябва да може да съхранява и обработва събраните данни в Европейската икономическа зона (European Economic Area).

REQ.18.	Решението трябва да отговаря на изискванията на GDPR (General Data Protection Regulation) регулациите, да притежава ISO/IEC 27001:2022 сертификати и да е съвместимо с изискванията на SOC 2 Type 2.
REQ.19.	Решението не трябва да е забранено, независимо дали за постоянно или временно, за използване от административните структури на НАТО.
REQ.20.	Решението трябва да е с минимална ефективност от поне 93% от тестовете на 2023 MITRE Engenuity Enterprise Evaluations в минимално следните категории: засичане на използвани техники от атаки (процент на засечени техники и предоставяне на тяхното описание), защитни мерки (процент на блокирани под-процеси на атака).
REQ.21.	Решението трябва да е позиционирано като "Strong Performer" или "Leader" в тестовете от доклада Forrester Wave For Extended Detection and Response Platforms Q2 2024.
REQ.22.	Решението трябва да е позиционирано в лидерския квадрант на Gartner за 2024-та година в категория Endpoint Protection Platforms.
REQ.23.	Решението трябва да може да съхранява събраната информация за аларми и инциденти за време от поне 90 дни назад от постъпването им в системата.
REQ.24.	Решението трябва да позволява съхранение и историческо търсене за поне 365 дни назад, директно от конзолата за управление или чрез API, за минимално следните типове индикатори за компрометиране: SHA256 и MD5 хеш суми, IPv4 и IPv6 адреси, имена на домейни.
REQ.25.	Решението трябва да може да съхранява логове за одит за период от поне 365 дни, като да се записват поне следните събития: вписване на потребители, промени по системната конфигурация, извършване на отдалечени сесии.
REQ.26.	Агентите на решението трябва да могат да се поставят на минимално следните операционни системи: Microsoft (Windows 7 SP1, Windows 10 (x86-64 и arm64), Server 2008 R2 SP1, Server 2012 и 2012 R2, Server 2016 и Server Core 2016, Server 2019 и Server Core 2019, Server 2022 и Server Core 2022. Linux: CentOS 6, 7 и 8; Debian 9,10, 11 и 12; Oracle Linux 6, 7, 8 и 9; Red Hat Enterprise Linux 6, 7, 8 и 9; Red Hat Enterprise CoreOS 4; Rocky Linux 8 и 9; SUSE 11, 12 и 15; Ubuntu 14, 16, 18, 20 и 22. Apple macOS: macOS Monterey 12; macOS Ventura 13; macOS Sonoma 14. Apple iOS 15.x, 16.x и 17.x; Android 12.x, 13.x и 14.x.
REQ.27.	Решението трябва да позволява поставянето на агенти на остарели системи като Windows 7 SP1, които вече не се покриват от активната поддръжка на производителя.
REQ.28.	Решението трябва да позволява поставянето на агенти на Virtual Desktop Infrastructure (VDI) системи.
REQ.29.	Агентите и компонентите на решението трябва да могат да се поставят под формата на генерирани инсталационни пакети, минимално в следните формати: MSI или EXE за Microsoft системи (Windows), RPM и DEB пакети за Linux системи, PKG пакети за macOS системи.
REQ.30.	Решението трябва да позволява поставянето на агенти на мобилни устройства, като: iOS устройства, през Mobile Device Management (MDM) система или през Apple App Store; Android устройства, през MDM система или през Google Play Store.
REQ.31.	Решението трябва да е оценено минимално с "A+" рейтинг за всичките му функции и услуги от публично достъпния инструмент https://www.ssllabs.com.
REQ.32.	Комуникацията между агентите на решението и конзолата за централизирано управление трябва да се извършва чрез криптиран HTTPS протокол за поне версия TLS 1.2, като да може да се извършва по следните начини: директно; индиректно чрез системно прокси; индиректно чрез зададено прокси по време на инсталацията.
REQ.33.	Документацията на решението трябва да описва IP адресите и URL адресите, с които агентите комуникират, когато се свързват с конзолата за управление на решението.
REQ.34.	Решението трябва да позволява да се забранява достъп до конзолата за управление от IP адреси извън зададен списък с позволени такива.
REQ.35.	Решението трябва да използва ролево-базиран достъп, като да могат да се задават различни роли на различни потребители или групи от потребители, за целите на по-фин достъп до системни ресурси. Ролите трябва да описват поне следните параметри: 1. Достъп до конкретни раздели от административните зони на конзолата за управление 2. Тип на достъпа (само за четене на информация или пълен достъп) 3. Обхват на достъпа (видимост до всички защитени хостове или само на група от селектирани хостове)
REQ.36.	Решението трябва да може автоматично да групира елементи по следните параметри (или каквито и да е комбинации от тях):

	* тагове за групиране (поставени по време или след инсталацията) * тип операционна система (работни станции или сървъри) * вид операционна система (Windows, Linux, MacOS) * конкретна версия и подверсия на операционна система * домейн от AD * организационна група от AD * Kernel версия * локални IP/CIDR адреси * имена на хостове, включително използване на regex език за филтриране на prefix/sufix * версия на сензор
REQ.37.	Решението трябва да предоставя алармиране за събития, като алармите да се поддържат с различни степени според важността им, минимално: информационни, с нисък риск, със среден риск, с висок риск, от критична важност.
REQ.38.	Решението трябва да може да групира сходни или свързани аларми, с цел по-бърз анализ на инциденти.
REQ.39.	Решението трябва да може автоматично да изгражда вериги от тип причинител-следствие за групираните аларми за даден инцидент, които да представят графично връзките между използваните процеси по време на атака и съответните телеметрични данни, за да се позволи: 1. Анализ на използваните техники 2. Определяне на обхвата на дадена атака 3. Идентифициране на целите на дадена атака 4. Потвърждение, дали целите на дадена атака са реално постигнати и какви са последствията от тях.
REQ.40.	Решението трябва да позволява управление на възникналите инциденти, минимално: 1. Добавяне на даден инцидент на конкретен анализатор 2. Промяна на статуса на даден инцидент: * В момента разследван * Грешно показание * Вярно показание * Дублиран инцидент * За целите на тестване 3. Да могат да се добавят бележки към инциденти
REQ.41.	Решението трябва да може да обвързва възникналите аларми с MITRE ATT&CK рамката за инциденти.
REQ.42.	Решението трябва да може да предоставя отчет от sandbox модул за файлове, които са свързани с даден инцидент, като да може отчетите да се извличат извън системата в различни формати.
REQ.43.	Решението трябва да може да управлява преносими USB-свързани устройства, минимално за Windows и macOS системи, със следните поддържани функции: 1. Да може да се определя кои USB устройства могат да се свързват 2. Да може да се определя обхвата на достъп на USB устройства за съхранение на данни: * забранен достъп * достъп само за четене на информация * достъп за четене и записване на информация * достъп за четене, записване и изпълнение
REQ.44.	Решението трябва да предоставя следните функции за управление на преносими USB устройства: 1. Предоставяне на детайлна информация за файловата активност (записани файлове на USB устройства), с контекстни метаданни, които да позволяват разследване на потенциални инциденти за непозволено изтичане на данни. 2. Да се поддържат следните файлови категории: архивирани файлове, документи, файлове за дизайн (dwg, dxf, idw), мултимедия, програмен код (скриптове), изпълними файлове, виртуални машини (VDI, VMDK), файлове за електронна поща (Email, Emailarc, elm, msg, out, pst), файлове за логиране и данни (blf, dmp, ese) и други (dmglnk). 3. Информацията за записани файлове да се съхранява от решението за поне 30 дни назад.
REQ.45.	Решението трябва да позволява да се управлява защитната стена на хостовете за поне Windows и MacOS системи.
REQ.46.	Решението трябва да позволява използването на политики за ръчно или автоматично обновяване на агентите на решението на конкретни групи от крайни точки. Автоматичната конфигурация на агентите трябва да позволява следното: 1. Определяне на дни от седмицата и зададени времеви обхвати, когато обновяването да не се

	извършва 2. Определяне на броя крайни точки, които да се обновят 3. Определяне на използваната версия: последната налична версия, последната предходна версия, конкретно зададена версия.
REQ.47.	Решението трябва да събира одитна информация за промени по политиките за сигурност.
REQ.48.	Решението трябва да позволява поставянето на правила за изключения от сканиране за алгоритмите за машинно самообучение.
REQ.49.	Решението трябва да позволява поставянето на правила за изключения от сканиране за алгоритмите за анализ на поведение.
REQ.50.	Решението трябва да предоставя опция за отдалечено свързване до крайни точки, защитени с агент на решението, с минимално следните функции: 1. Преглед на активни процеси 2. Преглед на файловите системи 3. Преглед на статуса на мрежовите сокети 4. Терминиране на конкретен процес 5. Изпълнение на скрипт от библиотека 6. Извличане на файл от крайната точка 7. Поставяне на файл на крайната точка 8. Извличане на списък с процесите 9. Извличане на паметта на операционната система 10. Спиране или рестартиране на крайната точка 11. Показване на списък с мрежовите свързвания от крайната точка 12. Премахване на файл на крайната точка 13. Извличане на файл от крайната точка с опция за криптиране и поставяне от администратора на парола за декриптиране 14. Стартиране на изпълним файл 15. Добавяне/премахване на скачени мрежови файлови дялове 16. Описание на локалните потребителски акаунти
REQ.51.	Решението трябва да поддържа създаването на библиотека от скриптове, които да могат да се изпълняват дистанционно на конкретна крайна точка или група от крайни точки. Да се поддържат минимално следните езици: * Windows: PowerShell * Linux: Bash скриптове * MacOS: Zsh скриптове
REQ.52.	Решението трябва да предоставя функция от графичния интерфейс или чрез API за поставяне на крайна точка под карантирана, в изолиран от Интернет контейнер. По време на изолацията да се блокира целият мрежови трафик с изключение на оставяне на дистанционен достъп от решението и свързване чрез DHCP протокол.
REQ.53.	Решението трябва да позволява задаване на списъци с изключение от поставяне на крайни точки в изолация според техните IP адреси.
REQ.54.	Решението трябва да позволява извършване на цялостно сканиране на дадена крайна точка в отговор на възникнала аларма.
REQ.55.	Решението трябва да поддържа директна интеграция с услугите на VirusTotal.
REQ.56.	Решението трябва да позволява глобално блокиране или блокиране за група от крайни точки на изпълними файлове чрез описване на техните SHA256 хешове.
REQ.57.	Решението трябва да позволява изграждането на собствени правила за засичане и защита на процеси, на базата на дефинирани причинители или на конкретни изпълнени параметри от команден интерфейс.
REQ.58.	Решението трябва да позволява изграждането на собствен списък с индикатори за компрометиране под формата на имена на домейни, IPv4 и IPv6 ареси и SHA256 и MD5 хешове, като да може минимално: * Да се вмъкват индикатори от зададен файл * Ръчно да се добавят индикатори * Програмно да се добавят индикатори чрез API
REQ.59.	Решението трябва да позволява изграждането на собствени изгледи в конзолата за управление с избрани от потребителите елементи и контроли.
REQ.60.	Решението трябва да позволява търсенето в цялата събрана база от телеметрични данни, чрез подсказки или с директно писане на заявки. Заявките трябва да позволяват комбинирането на телеметрични данни от различни източници, с опции за филтриране и трансформиране на

	резултатите. Правилата за създаване на заявки трябва да са добре описани в документацията на решението.
REQ.61.	Решението трябва да позволява да се запазват заявки или телеметрични данни в глобална база, която да е достъпна за всички потребители.
REQ.62.	Решението трябва да позволява изпълнението на заявки за телеметрични данни и получаване на резултатите за преглед чрез API.
REQ.63.	Решението трябва да позволява извличането на резултатите от заявки за телеметрични данни под формата на текстови файл.
REQ.64.	Решението трябва да позволява да могат циклично да се изпълняват заявки по зададен график или еднократно в зададено време, като резултатите да могат автоматично да се изпращат до зададени email адреси под формата на прикачени текстови файлове.
REQ.65.	Решението трябва да позволява да се преобразуват заявки за телеметрични данни в правила за корелации, които да се изпълняват по зададен график, като да могат да вдигат аларми, ако в резултата им присъства повече от един върнат запис.
REQ.66.	Решението трябва да може да обработва логове от трети страни, с минимално следните параметри: * Поне 10GB от логове на ден * Съхранение на логове за поне 7 дни * Поддържане на следните интеграции за получаване на логове: 1. Palo Alto Networks защитни стени 2. Fortinet защитни стени 3. Proofpoint защита за електронна поща 4. Cisco Secure Email Gateway 5. VMware ESXi 6. Microsoft Azure хъбове за събития 7. Microsoft Exchange Online 8. Microsoft Graph API 9. Vectra AI 10. ZScaler 11. Универсален колектор на Http събития
REQ.67.	Инсталирането на агентите на решението не трябва да изисква рестартиране на операционните системи на крайните точки.
REQ.68.	Агентите на решението трябва да могат да извършват проверка на зададените сертификати за мрежови свързвания, с цел предпазване от man-in-the-middle атаки.
REQ.69.	Агентите на решението трябва да имат функции за самозащита от спиране на функциите му или затруднение в изпълнението на процесите му, независимо дали действията са продиктувани от потребители с висок достъп (anti-tampering).
REQ.70.	Агентите на решението трябва да могат да са защитени от премахване чрез използване на уникална поставена парола за всяка крайна точка.
REQ.71.	Агентите на решението трябва да могат да се поставят или премахват чрез инструменти като SCCM, Ansible, Jamf.
REQ.72.	Агентите на решението трябва да поддържат използването на токени за инсталиране.
REQ.73.	Агентите на решението трябва да поддържат използването на токени за премахване, които да са обвързани с конкретен хост.
REQ.74.	Агентите за Windows, MacOS, и Linux системи трябва да могат да събират и изпращат следните телеметрични данни: * Създаване на нов процес или спиране на процес * Мрежови операции със сокети за TCP и UDP * Файлови операции * Логирани опити за автентикиране * Операции с регистри (само за Windows системи)
REQ.75.	При поставяне на агентите на решението, трябва да има опция за поставяне на тагове на агентите, които да не могат да се премахват от конзолата за управление и които да могат да се използват за групиране на крайни точки.
REQ.76.	При поставяне на агентите на решението, трябва да има опция за определяне на прокси сървър, чрез който агентите да се свързват с конзолата за управление.
REQ.77.	Агентите на решението трябва да могат да засичат и блокират опити за спиране на Volume Shadow Copy Service (VSS) услугата, както и други опити за повреждане на генерирани VSS snapshot копия.

REQ.78.	Агентите на решението трябва да могат да предпазват от Bring Your Own Vulnerable Driver (BYOVD) атаки чрез засичане и блокиране на опити за зареждане на уязвими драйвери.
REQ.79.	Агентите на решението трябва да могат да предпазват от познати и непознати зловредни бинарни файлове, директно на защитената крайна точка, минимално по следните начини: 1. Да могат да верифицират репутацията на файловете в база от данни за репутации на производителя на решението 2. Да могат да извършват локален статичен анализ на базата на машинно самообучение (Machine Learning)
REQ.80.	Агентите на решението трябва да могат да предпазват от познати и непознати зловредни макроси в Microsoft Word и Microsoft Excel файлове, минимално по следните начини: 1. Да могат да верифицират репутацията на макросите в база от данни за репутации на производителя на решението 2. Да могат да извършват локален статичен анализ на базата на машинно самообучение (Machine Learning)
REQ.81.	Агентите на решението трябва да могат да премахват засечени зловредни макроси в Microsoft Word и Microsoft Excel файлове.
REQ.82.	Агентите на решението трябва да могат да засичат зловредни процеси, използвайки както дефиниции, така и на база поведение на процесите, за разпознаване на познати и непознати заплахи. Дефинициите и моделите на поведение трябва да могат да се обновяват често.
REQ.83.	Агентите на решението трябва да могат да предоставят защита от криптиране на дискове или файлове от зловредни процеси (anti-ransomware).
REQ.84.	Агентите на решението трябва да могат да извършват анализ на бинарни файлове, след като те са били записани на файловите системи.
REQ.85.	Агентите на решението трябва да могат да предпазват от използването на познати и непознати уязвимости от зловредни процеси.
REQ.86.	Агентите на решението трябва да могат да поставят под карантина зловредни файлове.
REQ.87.	Агентите на решението трябва да могат автоматично да сканират преносими устройства в момента на свързването им към USB портовете на крайните точки.
REQ.88.	Агентите на решението, чрез използване на комплексни анализи на техники и технологии, трябва да могат да предпазват от използването на Living Off The Land (LOTL) легитимни инструменти за целите на атаки.
REQ.89.	Агентите на решението трябва да могат да предпазват от атаки, целящи извличане на данните за вписване на потребителски акаунти.
REQ.90.	Агентите на решението трябва да могат автоматично да се справят с комплексни атаки, минимално чрез: блокиране на зловредни процеси, поставяне на файлове под карантина, премахване на задачи по график, изтриване на записи в регистри.
REQ.91.	Агентите на решението трябва да могат да се интегрират с Windows Security Center.
REQ.92.	Агентите на решението трябва да могат да работят: * В kernel режим (чрез използване на драйвер) на Windows системи * В kernel пространството или извън него за Linux системи * Извън kernel пространството на MacOS системи
REQ.93.	Агентите на решението на Linux системите трябва да могат автоматично да превключват в режим на работа без използване на драйвери, ако те не се зареждат правилно.
REQ.94.	Агентите на решението трябва да могат, в случай на загуба на мрежова свързаност с конзолата за управление, локално да съхраняват събраните телеметрични данни и да могат да ги изпращат при възобновяване на мрежовата свързаност.
REQ.95.	Решението трябва да позволява използването на многофакторна автентикация при извършване на отдалечени сесии към защитени крайни точки. Решението трябва да изисква администраторите да въведат повторно своите пароли от многофакторната автентикация преди извършване на дистанционно свързване с конзолата за управление с цел защита при кражба на данни за вписване в системата.
REQ.96.	Решението трябва да разполага с вградена система за оркестриране и автоматизиране на процеси, която да разполага минимално със следните функции: 1. Изпращане на email известие или Microsoft Teams известие при спиране на функциите на агентите за засичане и предпазване от атаки. 2. Стартиране на сканиране на крайна точка в отговор на възникнала аларма с определена тежест. 3. Изпращане на email известие до определени получатели в отговор на възникнала аларма с определена тежест, за потвърждение на изпълнение на процеса за изолиране на крайната точка от

	мрежовата среда. 4. Създаване на ticket в Jira система, в отговор на възникнала аларма с определена тежест. Алтернативно, изпълнение на настроен webhook процес при възникване на аларма с определена тежест. 5. Изпращане на всекидневно email известие за налични сървъри, където агентът на решението е с offline статус. 6. Автоматично изолиране на крайна точка на базата на конкретни техники и тактики от MITRE модела 7. Поставяне под карантина на файл и убиване на процес на базата на засечен SHA256 хеш 8. Автоматично прекратяване на функциите за засичане при настъпване на определено действие (например при убиването на даден процес) 9. Автоматично извличане на допълнителни данни в реално време от крайните точки за активни мрежови свързвания и вписани потребители 10. Вмъкване/извличане на workflows процеси в и от графичния интерфейс на решението 11. Добавяне на функция за изискване на човешко одобрение за действия от чувствителен характер от автоматизираните процеси на решението.
REQ.97.	Решението трябва да може да извършва корелация на засечените индикатори за компрометиране, тактики, техники и процедури и да ги обвързва с информация за групировки от организираната киберпрестъпност или Advanced Persistent Threat (APT) групи, ако има признаци за тях.
REQ.98.	Решението трябва да може да се интегрира директно с Microsoft Teams, като минимално: 1. Да могат да се изпращат известия за аларми, инциденти и логирани събития 2. Да се позволява двустранна комуникация с анализатор за потвърждение на извършване на действие по изолиране на крайна точка от мрежата при възникнал инцидент.
REQ.99.	Агентите на решението, поне за Windows системи, трябва да поддържа хардуерно-ускорено сканиране на паметта, за да не се влияе негативно на производителността на системите.
REQ.100.	Решението трябва да може да се интегрира с решения от трети страни като SIEM системи (например Splunk), SOAR системи и защитни стени за изпълнението на автоматизирани действия в отговор на възникнали заплахи. Интеграцията трябва да включва обмен на известия между системите за настъпили събития.
Гаранция и поддръжка:	
REQ.101.	Включена поддръжка от производителя на решението за период от минимум 36 месеца
REQ.102.	Гаранционната поддръжка трябва да е от тип: 24x7x365
REQ.103.	Възможност за обновление на софтуера в периода на поддръжката
REQ.104.	Възможност за обновления на информацията за заплахите от базата данни на производителя

2. Решение за сканиране и управление на уязвимости:

Минимални технически изисквания	
REQ.1.	Брой лицензи, отговарящи на активите, които ще бъдат сканирани – 1000 броя
REQ.2.	Вид решение - софтуерно - изцяло разположено локално (on-premise) или с възможност за облачна конзола за управление
REQ.3.	Решението трябва да може да достъпва и сканира конфигурации за сигурност, политики за сигурност и ниво и състояние на киберсигурността.
REQ.4.	Решението трябва да може да създава и да слага етикет на всеки актив и уязвимост
REQ.5.	Решението трябва да разполага с отчети, които да предоставят препоръчително стъпки за предприемане като ответни мерки за отстраняването на всяка уязвимост
REQ.6.	Решението трябва да може да задава за определена уязвимост, че е "преценен риск", когато въпросната уязвимост ще внесе излишен "шум" в определен контекст
REQ.7.	Решението трябва да може да сканира контейнеризирани елементи, за да може по този начин да засича уязвимости на пакетите на операционните системи, използвани в организацията
REQ.8.	Решението трябва да поддържа използване на CIS уязвимости, за да извършва базови проверки на активната директория

Минимални технически изисквания	
REQ.9.	Решението трябва да разполага с OpenAPI интерфейс за интеграции, който да позволява всички операции да могат да се извършват в уеб интерфейса за централизирано управление на решението
REQ.10.	Решението трябва да е ASV сертифицирано и да предоставя официални и неофициални PCI отчети
REQ.11.	Решението трябва да позволява да може да сравнява нивото и текущото състояние на киберсигурността на организацията (security posture) с тези на други подобни организации от същият бизнес отрасъл
REQ.12.	Решението трябва да разполага с предефинирани отчети за съответствие със стандарти като CIS и FISMA
REQ.13.	Решението трябва да разполага с възможности за изготвяне на отчети, които да могат да се персонализират
REQ.14.	Решението трябва да разполага с отчети за всякакъв тип потребители като например отчети, свързани с кръпки на уязвимости за Microsoft среди, пригодени отчети за мениджмънт отдела на организацията, както и отчети, свързани с пълни детайли по уязвимостите
REQ.15.	Решението трябва да е в съответствие със SOC2
REQ.16.	Решението трябва да може да създава статични или динамични групи от активи
REQ.17.	Решението трябва да поддържа агент за сканиране за Windows, Linux и MacOS среди
REQ.18.	Решението трябва да позволява да се инсталират неограничен брой скенери за уязвимости
REQ.19.	Решението трябва да има възможност да покаже мрежова карта, която ще покаже връзките между активите, индикаторите за заплахи и потенциалния вектор на атака
REQ.20.	Решението трябва да поддържа точкова система за уязвимости, базирана на CVSS точки
REQ.21.	Решението трябва да може да помага да се приоритизират уязвимостите и начина им на отстраняване в зависимост от вероятността им те да бъдат експлоатирани
REQ.22.	Скенерите на решението трябва да имат предефинирани политики за сканиране, както и възможност за създаване на персонализирани политики
REQ.23.	Решението трябва да има възможност от същата конзола за управление да сканира и уеб апликации чрез закупуване на допълнителен лиценз. Сканирането на уеб апликации трябва да е базирано на OWASP top10 категории
REQ.24.	Решението трябва да поддържа сканиране за откриване на зловреден софтуер чрез закупуване на допълнителен лиценз
REQ.25.	Решението трябва да поддържа сканиране на мрежово ниво за откриване на нови активи без това да консумира автоматично от лицензите
REQ.26.	Решението трябва да поддържа обновяване на скенерите поне на всеки две седмици за новооткрити уязвимости за подобряване на сканиранията и колкото е възможно по-скоро за критични уязвимости
REQ.27.	Решението трябва да поддържа сканиране чрез автентикация за поне Windows, Linux, PostgreSQL и VMware ESX
REQ.28.	Решението трябва да поддържа дефиниране на отклонения относно риска, както и профилиране на риска
REQ.29.	Решението трябва да поддържа изгледи с данни за стъпките по отстраняването на уязвимостите чрез графики и таблици
REQ.30.	Решението трябва да поддържа данните в покой и в движение да са криптирани чрез AES256
REQ.31.	Решението трябва да поддържа сканирания по определен зададен график
Гаранция и поддръжка:	
REQ.32.	Включена поддръжка от производителя на решението за период от минимум 36 месеца
REQ.33.	Гаранционната поддръжка трябва да е от тип: 24x7x365
REQ.34.	Възможност за обновление на софтуера в периода на поддръжката
REQ.35.	Възможност за обновления на информацията за заплахите от базата данни на производителя

3. 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 1000 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 асоциран 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.

Минимални технически изисквания	
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

Минимални технически изисквания	
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 минимум 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

Минимални технически изисквания	
	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

Приложение №2

(Образец)

Д Е К Л А Р А Ц И Я
ЗА ОПАЗВАНЕ НА ИНФОРМАЦИЯ

Долуподписаният/ та ……..,
ЕГН: .....,[1] в качеството ми на ……., декларирам, че ще пазя в тайна, станалата ми известна във връзка с изпълнението на Договор № ……/…..... г.[2] информация, съдържаща данни, представляващи данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация. За неизпълнение на тези задължения ми е известно, че нося предвидената в съответните нормативни актове отговорност.

Запознат/а съм с разпоредбата на чл. 270 от ***Данъчно-осигурителния процесуален кодекс***, съгласно която, ако разглася, предоставя, публикувам, използвам или разпространя по друг начин факти и обстоятелства, представляващи данъчна и осигурителна информация, ако не подлежа на по-тежко наказание, ще бъда наказан/а с глоба от 1000 лв. до 5000 лв., а в особено тежки случаи - от 5000 лв. до 10 000 лв.

Декларирам, че ще пазя в тайна, станалата ми известна информация, относно съдържанието на документация, вътрешни правила, процедури, организация, структура, начин на функциониране, комуникации, мрежи и информационни системи на ……..(ВЪЗЛОЖИТЕЛЯ), изготвени в хода на изпълнението документи и/или всякакви други постигнати резултати от изпълнението, както и че няма да разгласявам, използвам или предоставям на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ документация или програмен код в явен и изпълним вид във връзка с изпълнението на този договор, с изключение на случаите, когато съм задължен по закон за това.

При обработването на данните се задължавам да спазвам разпоредбите на

---

1 *В случай, че лицето е чужденец, се вписват съответните идентификационни данни.*

2 *Вписва се референтен номер на Договора, в договорния регистър на ВЪЗЛОЖИТЕЛЯ.*

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО и ***Закона за защита на личните данни***.

Известна ми е отговорността по чл. 284 от ***Наказателния кодекс***, а именно: налагане на наказание лишаване от свобода до две години или пробация, ако във вреда на държавата, на предприятие, организация или на частно лице съобщя другиму или обнародвам информация, която ми е поверена или достъпна по служба и за която зная, че представлява служебна тайна.

Ще спазвам изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност.

Известна ми е отговорността по Глава 9а от Особената част на ***Наказателния кодекс***, относно достъп до компютърни данни в компютърна система без разрешение, добавяне, промяна, изтриване или унищожаване на компютърна програма или компютърни данни, въвеждане на компютърен вирус в компютърните системи или мрежи на ВЪЗЛОЖИТЕЛЯ, разпространение на пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна.

Подпис:

(подписване с електронен подпис)