Архивски број: 03-138471
Датум:
15-12-2023

Друштво за инфраструктура и решенија за информатичка технологија
ИНФОСОФТ СИСТЕМС ДОО
Бр. 0307-265/1
15.12 2023 год.
СКОПЈЕ

ДОГОВОР
за јавна набавка на стоки–софтвери за мрежна детекција, рано откривање и одговор на малициозни активности

Склучен помеѓу:

1.МИНИСТЕРСТВО ЗА ФИНАНСИИ, со седиште на ул. "Даме Груев", бр.12 - Скопје, претставувано од Dr.Fatmir Besimi, министер за финансии, во натамошниот текст: договорен орган; и

2. ДРУШТВО ЗА ИНФРАСТРУКТУРА И РЕШЕНИЈА ЗА ИНФОРМАТИЧКА ТЕХНОЛОГИЈА ИНФОСОФТ СИСТЕМС ДОО, со седиште на ул. „Наум Наумовски Борче“ бр.40-1/1, Скопје, претставувано од Душко Темков, во својство на управител, во натамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на стоки – софтвери за мрежна детекција, рано откривање и одговор на малициозни активности со назив Gatewatcher, согласно со техничките спецификации (Прилог 1 кон договорот) и понудата на носителот на набавката прифатена од страна на договорниот орган (Прилог 2 кон договорот), кои се составен дел од овој договор, а по претходно спроведена поедноставена отворена постапка, по оглас број бр.20152/2023.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 4.150.000,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 207.500,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 4.357.500,00 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

Цената од член 2 на овој договор е крајна, фиксна и непроменлива за цело времетраење на договорот.

IV. РОК НА ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Овој договор се склучува за период од 12 (дванаесет) месеци, а ќе започне да важи од денот на потпишувањето од двете договорни страни.

V. НАЧИН, МЕСТО И РОК НА ИСПОРАКА

Член 5

Носителот на набавката е должен софтверот да го испорача на начин определен во техничките спецификации кои се составен дел на тендерската документација и според потребите на договорниот орган.

Носителот на набавката е должен софтверот да го испорача, инсталира и конфигурира во период од 5 (пет) работни денови по добивање на писмената порачка од договорниот орган.

За извршената испорака, инсталација и конфигурација договорните страни потпишуваат документ - Работен налог/Записник, кој мора да ги содржи податоците за извршувањето.

Работниот налог/Записник за извршената испорака со полно име и презиме ги потпишуваат определените лица од двете договорните страни, при што по еден примерок се предава на определеното лице кај договорниот орган, еден примерок задржува носителот на набавката за сопствени потреби и еден примерок заедно со фактурата се доставува до Министерството за финансии - Скопје.

Местото на извршување на предметот на договорот е во Скопје на локацијата на Министерството за финансии на ул. „Даме Груев" бр.12.

За извршување на набавката – предмет на договорот, носителот на набавката ги вклучува лицата од стручниот кадар за извршување на набавката - предмет на договорот, согласно со прифатената понуда на носителот на набавката од страна на договорниот орган.

Во исклучителни ситуации носителот на набавката може да изврши замена на лице од техничкиот персонал кој ќе учествува во извршувањето на договорот, со доставување на детално образложение и по добивање на одобрение од договорниот орган, под услов лицето да ги исполнува условите предвидени во потточка 5.3.2 од тендерската документација.

VI. НАЧИН И РОК НА ПЛАЌАЊЕ

Член 6

Договорниот орган плаќањето ќе го изврши во рок до 30 (триесет) дена од денот на доставувањето на фактурата, во писарницата на Министерството за финансии на ул. „Даме Груев" бр.12 во Скопје.

Кон фактурата носителот на набавката задолжително доставува Работен налог / Записник кој мора да ги содржи податоци за извршувањето, во спротивно фактурата нема да биде платена и ќе биде вратена на докомплетирање кај носителот на набавката.

Фактурата се доставува по пошта или лично во писарницата на Министерството за финансии на ул. Даме Груев бр.12 во Скопје.

VII. ПРАВА И ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 7

Носителот на набавката е должен своите обврски да ги извршува стручно, навремено и квалитетно, врз основа на барањата на договорниот орган дефинирани во техничките спецификации кои се составен дел од овој договор и понудата прифатена од договорниот орган.

Носителот на набавката е должен да се придржува кон рокот за извршување на предметната набавка на стока, кој е дефиниран во член 5 од овој договор.

Носителот на набавката се обврзува предметот на договорот да го извршува со разумно знаење и внимание во согласност со професионалните стандарди и тековната легислатива која влијае на друштвата за компјутерски инжинеринг и трговија.

Носителот на набавката е должен веднаш по потпишување на договорот да му достави на договорниот орган податоци (име и презиме, матичен број и број на лична карта) за лицата кои ќе бидат определени за реализација на предметот на договорот.

VIII. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 9

Договорниот орган е должен да определи лица задолжени за реализација на договорот и за истото да го извести носителот на набавката.

Договорниот орган се обврзува дека плаќањето на носителот на набавката ќе го изврши во рокот од членот 6 на овој договор.

IX. ГАРАНЦИЈА ЗА КВАЛИТЕТНО И НАВРЕМЕНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 10

Носителот на набавката е должен заедно со потпишаниот договор да достави банкарска гаранција за квалитетно и навремено извршување на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде во висина од 10% од вкупната вредност на договорот со пресметан данок на додадена вредност.

Гаранцијата се доставува во вид на банкарска гаранција во писмена форма или во електронска форма доколку е издадена како таква од банката во изворно оригинална форма. Гаранцијата треба да биде поднесена во оригинална форма. Копии не се прифаќаат.

Гаранцијата за квалитетно и навремено извршување на договорот треба да биде со важност до целосното реализирање на договорот.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде во валутата на која гласи договорот.

Со гаранцијата носителот на набавката гарантира дека предметот на договорот ќе го изврши на начинот и според динамиката предвидени во тендерската документација, односно техничката спецификација, доставената понуда и склучениот договор со договорниот орган.

Гаранцијата за квалитетно и навремено извршување на договорот ќе биде наплатена доколку носителот на набавката не исполни некоја од обврските од договорот за јавна набавка во рокот на стасаноста, за што писмено ќе го извести носителот на набавката.

Доколку договорот за јавна набавка е целосно реализиран согласно договореното, банкарската гаранција за квалитетно извршување на договорот договорниот орган му ја враќа на носителот на набавката во рок од 14 дена од целосното реализирање на договорот.

Гаранцијата за квалитетно и навремено извршување на договорот договорниот орган му ја враќа на носителот на набавката по пошта, лично во седиштето на носителот на набавката или лично во седиштето на договорниот орган.

Договорниот орган ќе ја наплати гаранцијата за квалитетно и навремено извршување на договорот и доколку дојде до негово едностране раскинување поради неизвршување на обврските од договорот од страна на носителот на набавката.

Договорниот орган нема да бара активирање на банкарската гаранција за квалитетно извршување на договорот од банката која ја има издадено доколку

носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) не можел да ја изврши набавката што е предмет на овој договор, во кој случај носителот на набавката треба да достави писмено образложение до договорниот орган во кое ќе ги наведе причините за неизвршување или ненавремено извршување на обврските од договорот, а кое треба да биде писмено прифатено од договорниот орган.

X. ДОВЕРЛИВОСТ НА ПОДАТОЦИ И ИНФОРМАЦИИ

Член 11

Определените лица од носителот на набавката наведени во понудата за реализација на договорот, задолжително потпишуваат изјава за доверливост на информации и податоци непосредно пред извршувањето на услугата - предмет на договорот.

Под поимот информации и податоци се подразбираат сите внатрешни и надворешни документи, спецификации, лични податоци, истражувања на пазарот или податоци за него, финансиски или маркетиншки информации, други податоци или бизнис, оперативни или технички информации, како и сите останати податоци и информации и независно дали се дадени во писмена, вербална или електронска форма и се во сопственост на договорниот орган.

Исто така, поимот информации и податоци, ги опфаќа и сите други податоци кои не се сопственост на договорниот орган, а се користат за одредени цели во работните задачи и обврски. Тука спаѓаат податоци на сите партнери, клиенти, добавувачи или било кое правно или физичко лице кое со Договорниот орган има засновано деловен или било каков друг однос. Договорниот орган ги става податоците на располагање на носителот на набавката во врска со погоре наведената цел, а за непречено одвивање на работните задачи и обврски.

Член 12

Не се предмет на овој договор информации кои биле или станале јавно достапни, но не како резултат на откривање од страна на носителот на набавката и на договорниот орган и без да бидат прекршени одредбите на овој договор од страна на носителот на набавката што може да се докаже со писмена документација или за кои договорниот орган писмено потврдил дека се ослободени од обврска за неоткривање.

Член 13

Носителот на набавката под целосна морална, материјална и кривична одговорност, се обврзува за време на важноста на договорот и во период од (5) пет години од датумот на неговото истекување или раскинување да ги чува во тајност

сите информации и податоци од било која област на договорниот орган, кои ќе му бидат дадени во процесот на соработката и притоа нема да ги искористи истите за лични цели во име на друго лице, ниту ќе ги даде на увид на трета страна.

Носителот на набавката се обврзува да ги чува во тајност сите документи и податоци кои содржат информации за договорниот орган или неговите активности, како и неговите односи со клиенти или трети лица, а кои биле подготвени или изнесени во врска со работата за која Носителот на набавката е ангажиран од страна на договорниот орган.

Член 14

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 11 став 2 и 3 заради постапување по писмено барање од страна на надлежен орган, со легитимна наредба врз основа на закон.

Носителот на набавката, пред да ги даде бараните податоци ќе се увери дека барањето е валидно и е во согласност со важечки закон и ќе ги открие ваквите податоци само до степен до кој тоа е барано од надлежниот орган кој има овластување да бара такво соопштување.

Член 15

За секој настан или сомневање во однос на закана за нарушување на доверливоста, интегритетот и расположливоста на податоците и информациите, носителот на набавката се обврзува веднаш писмено да го извести определеното лице кај договорниот органот.

Член 16

Носителот на набавката по писмено барање на договорниот орган веднаш ќе ги врати или уништи сите документи кои содржат податоци и информации за договорниот орган, а кои се добиени во врска со работата за која носителот на набавката е ангажиран од страна на договорниот орган, без задржување на било какви фотокопии, изводи или друг вид на копии од нив или дел од нив. И покрај уништувањето на било кој податок и материјали носителот на набавката ќе продолжи да се придржува кон неговата обврска од овој договор и други обврски кои произлегуваат од него за чување во тајност на сите податоци и информации кои ги сознал на било кој начин, при исполнување на неговите обврски кои произлегуваат од овој договор.

Член 17

Објавувањето податоци, рекламирањето или публицитетот, како и прес конференциите направени од страна на Носителот на набавката во однос на овој договор или вршење на заеднички деловни активности на договорните страни

треба да бидат претходно одобрени од договорниот орган пред нивното спроведување.

Член 18

Одредбите од глава X од овој договор се правно валидни и обврзувачки и кај сите вработени кај носителот на набавката кои имаат добиено овластување за користење на информациите и податоците кои се уредени со овој договор.

XI. УСЛОВИ ЗА ПРЕКИНУВАЊЕ ИЛИ РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 19

Овој договор може да се раскине спогодбено во согласност на двете договорни страни.

Член 20

Овој договор може да се раскине и едностранo поради непридржување или неисполнување на договорните обврски утврдени со овој договор.

Договорната страна која поради непридржување или неисполнување на договорните обврски го раскинува договорот, должна е тоа да и го соопшти на другата договорна страна без одлагање во писмена форма.

Договорот се смета за раскинат со денот на приемот на известувањето за раскинување на договорот.

Доколку дојде до раскинување на договорот поради неисполнување или ненавремено исполнување на обврските на договорот од страна на носителот на набавката, покрај наплатата на банкарската гаранција носителот на набавката ќе биде одговорен за евентуалната штета што би ја предизвикал на договорниот орган како директна или индиректна последица на неговото работење.

Член 21

Кога една од договорните страни нема да ја исполни својата обврска, договорната страна може да бара исполнување на обврската од другата договорна страна или да го раскине договорот, а во секој случај има право на надомест на штетата.

Член 22

Кога договорната страна нема да ја исполни својата обврска во определениот рок, другата договорна страна може да и остави примерен дополнителен рок за исполнување на обврската.

Рокот од став 1 на овој член може да биде продолжен само по писмено барање на носителот на набавката и писмена согласност од договорниот орган.

Ако договорната страна која не ја исполнила својата обврска во определениот рок, не ја исполни обврската ни во дополнителниот рок, другата договорна страна може да го раскине договорот.

XII. ВИША СИЛА

Член 23

Ниту една од договорните страни нема да биде одговорна за неисполнување на обврските од овој договор до кое би дошло заради виша сила.

Под виша сила се подразбираат настани или околности на кои договорните страни не можат да влијаат и се надвор од нивната контрола, а го попречуваат нормалното извршување на договорот (елементарни непогоди, воени дејства, граѓански немири, штрајкови и сл.).

Вишата сила не вклучува настан што е предизвикан од небрежност или намерна активност што би предизвикала застој во извршувањето на обврските од договорот.

Ако една од договорните страни е спречена да ги исполнува своите обврски заради виша сила, должна е веднаш писмено да ја извести другата страна, со наведување на причините за вишата сила и по можност обезбедување на соодветен доказ.

За времетраењето на вишата сила сите права и обврски од овој договор мируваат.

Договорните страни се обврзуваат на ист начин да ја известат договорната страна за повторното воспоставување на нормални услови за извршување на договорот, односно за престанокот на дејството на вишата сила.

По отстранувањето на вишата сила договорот продолжува да се реализира.

XIII. ПРЕОДНИ И ЗАВРШНИ ОДРЕДБИ

Член 24

Изменувања и дополнувања на договорот можат да се вршат со заедничка согласност на договорните страни по писмен пат.

Договорната страна која бара измена и/или дополнување на договорот е должна своето барање до другата страна да го достави во писмена форма.

Договорот може да се изменува и дополнува со анекс на договорот потпишан од двете договорените страни во согласност со Законот за јавните набавки.

Член 25

За сé што не е предвидено со овој договор, се применуваат одредбите од Законот за облигационите односи, Законот за јавните набавки и од другите позитивни прописи во Република Северна Македонија.

Член 26

Во случај на спор, договорните страни се согласни спорот да го решат спогодбено, а доколку во тоа не успеат, согласни се спорот да го решава предметно надлежниот суд во Скопје.

Член 27

Обработката на личните податоци при реализацијата на овој договор ќе биде во согласност со Законот за заштита на личните податоци.

Член 28

Овој договор е составен во 4 (четири) еднообразни примероци од кои 2 (два) примероци за договорниот орган и 2 (два) за носителот на набавката.

ДОГОВОРЕН ОРГАН:

РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
МИНИСТЕРСТВО ЗА ФИНАНСИИ
СКОПЈЕ

МИНИСТЕР ЗА ФИНАНСИИ
Dr. Fatmir Besimi

НОСИТЕЛ НА НАБАВКАТА:

ДРУШТВО ЗА ИНФРАСТРУКТУРА
И РЕШЕНИЈА ЗА ИНФОРМАТИЧКА
ТЕХНОЛОГИЈА ИНФОСОФТ СИСТЕМС ДОО
СКОПЈЕ

УПРАВИТЕЛ
Душко Темков

Изработил: Петрина Мале
Контролирал: Даниела Јанкова
Елизабета Калачоска
Одобрил: Татјана Васева
Проверил: Daut Hajrullahi
м-р Маја Стаменковска Угриновска
Љубомир Јорданов
Согласен: д-р Јелена Таст

ПРИЛОГ 1 КОН ДОГОВОРОТ-ТЕХНИЧКИ СПЕЦИФИКАЦИИ

Софтверот за мрежна детекција и рано откривање на малициозни активности, shell кодови, малициозни движења во интерна мрежа, комуникација со злонамерни командни центри и одговор за блокирање и елиминација потребно е да обезбеди целосна видливост и детекција на целокупниот мрежен сообраќај на информатичката инфраструктура преку кој ќе обезбеди идентификување на малициозни активности и сомнителни однесувања преку автомтизирано мапирање на сите ИТ средства во информатичката инфраструктура. Софтверот треба да има способност преку анализа на целокупниот мрежен сообраќај да направи 360 степени моделирање на нивото на ризик поврзано со секоја конекција помеѓу корисниците и ИТ средствата со цел извршување на целокупна напредна анализа на детекција и прегледност. Софтверот треба да има можност за идентификување на мрежни аномалии во проток на енкриптиран сообраќај, да ги мапира сите ИТ средства од информатичка инфраструктура за да се обезбеди детекција на напредни напади на проток Исток-Запад и за јавна мрежа од Север-Југ, односно на хоризонтално ниво, доставување на единствени мета податоци со цел оптимизирање на времето потребно за потенцијална форензичка анализа и моделирање на нивото на компромитација по средство или корисници со преглед на аларми категоризирани по ниво на ризик согласно MITRE ATT&CK framework. Софтверот треба да има можност за пасивно собирање на целокупниот мрежен сообраќај со преземање на копија од истиот за анализа на сите активности во мрежните пакети.

Техничките спецификации кои се потребни да ги има софтверот за мрежна детекција и рано откривање на малициозни активности, shell кодови, малициозни движења во интерна мрежа, комуникација со злонамерни командни центри и одговор за блокирање и елиминација се специфицирани во следната табела:

Мониторирање во реално време	Решението треба да обезбеди мониторинг во реално време на мрежниот сообраќај во однос на детекција и одговор на закани кои можат да се случат
Сепарација на податоци	Решението треба да биде multi-tenant
Својства	Решението треба да има интегриран систем за централирано собирање и следење на логови и настани со цел навремено детектирање на потенцијални закани како и ловење на нови закани
	Решението треба да има можност за детекција на 0-day напади со shell вгнезден код во реално време, без користење на sandbox
	Решението треба да има инкорпорирано malware engines во самата структура за анализа на малициозни кодови

	Решението треба да има можност за графички прикази за движењето на мрежниот сообраќај и можните сомнителни активности од корисниците
Одвојување на функциите	Решението треба да поддржува можност за дефинирање на различни улоги и привилегии (оператори и администратори)
Поддршка на пропусниот опсег	Способност за анализа на протоци до 40Gbit/s
Број на поддржани сесии	Способност за анализа на протоци повеќе од 200000 симултани сесии
Анализа на PCAP фајлови	Решението треба да може да анализира PCAP мрежни пакети и истата да се испрати за анализа преку API
Pcap анализа	Решението треба да има можност да изврши детекција на pcap
Централизирана корисничка автентикација	Решението треба да има можност за поврзување со централен систем за автентикација како LDAP
MFA	Решението треба да поддржува мултифакторски автентикација
UEBA	Решението треба да има способност за извршување на автоматизирано профилирање на однесувањето, конструирање основна линија и напредна анализа за анализа на податоците за пристап и автентикација, воспоставување на кориснички контекст и известување за сомнително однесување
Built-in каталог на правила	Решението треба да има предефинирани (Built-in) правила за детекција и модели
Комплексни услови	Решението треба да има можност за креирање на комплексни правила за детекција базирани на повеќе оператори: - и / или Imbricated And / OR - еднакво, содржи или идентично оператори - негација - regular expressions
Yara правила	Решението треба да има можност за импортирање на Yara правила.
Детекција на прилагодени потписи	Решението треба да има можност за детекција врз основа на прилагодени потписи (suricata, snort, zeek...)
Анализа на фајлови	Решението треба да има можност за анализа на фајлови во sandbox, да детектира малициозни фајлови базирано на хеуристична и статичка анализа. Решението треба да да може да детектира фајлови врз основа на Yara правила.
Правила од други извори	Решението треба да има можност за додавање IOC-и од надворешни CTI извори

Sandbox анализа	Решението треба да има можност да праќа фајлови до third party sandbox решенија и да ги репплицира резултатите од проверките
Поддржани протоколи	Решението треба да може да анализира сообраќај по следните протоколи: DHCP, DNS, HTTP, SMTP, SNMP, ICAP, ARP
Анализа на енкриптиран проток	Решението треба да може да анализира енкриптирани протоци (metadata анализа)
Таргетирана анализа	Решението треба да може да прави категоризација на изворите и дестинациите на протоците (internet, admin мрежа, продукциска мрежа,работна станица, сервер...) во однос на опсегот на ИП адресите и/или FQDN за да може да аплицира правилни правила за детекција на конкретни протоци
Север-југ анализа	Решението треба да има можност за аплицирање на специфична политика за детекција на север-југ протоци (внатрешна мрежа - интернет)
Исток-запад анализа	Решението треба да има можност за аплицирање на специфична политика за детекција на исток-запад протоци (работна станица - сервери)
Прегледност	Решението е треба да има комплетна видливост на целиот мрежен сообраќај и истиот да може да подржува анализа на сите познати мрежни протоколи
Машинско учење	Решението треба да има во својата структура алгоритам за машинско учење за детекција на аномалии и за идентификување на сомнителни активности
Автоматизирано учење со закана од интерна мрежа	Ако веќе има малвер во системот, решението треба да може да ги адаптира и отстрани сите модели кои се однесуваат на таа закана, или пак да продолжи да учи од активностите
Автоматизирано учење од мала количина на податоци	Решението треба да може да учи од мала количина на податоци
Интеграција	Решението треба да може да се интегрира со останати SIEM решенија и да има можност за интеграција преку SYSLOG и да се праќаат настани до SIEM решение
Логирање	Решението треба да има можност за ревизија на дејствата на операторите и администраторите и безбедносните настани.

Формат на логовите	Безбедносните записи (логови) треба да ги вклучуваат следниве информации: - Време - Корисник. - Акција. - Извршена командата - Резултат на акцијата. - Вид на акција. - Изворна IP адреса.
Ротација на логови	Решението треба да има функционалност на ротација на логови пред да се искористи целиот простор наменет за чување на логовите
Разузнавање на закани	Решението треба да поседува инкорпорирани фидови за разузнавање на потенцијални закани со цел да биде организацијата навремено ажурирана со најнови индикатори за закани и идентификување на закани кои се појавуваат
Детекција на база на потписи	Решението треба да може да изврши длабока инспекција и детекција на мрежни пакети
Детекција на база на Вештачка интелигенција	Решението треба да може да врши детекција на сомнителни активности употребувајќи модел на вештачка интелигенција
Детекција на сомнителни и абнормални активности	Решението треба да има детекција на абнормални и сомнителни активности како, bruteforce, сомнителни конекции, сомнителен upload, сомнителен download, детекција на скенирања, каталог од пре-дефинирани сомнителни активности
Скалабилност	Решението треба да може да се проширува со потребите на мрежата во однос на големината и крајните уреди
Алармирање	Решението треба да обезбеди навремено и активно алармирање на тимовите за ИТ безбедност кога ќе се детектираат потенцијални закани
Алармирање по корисник и средство	Решението треба да има можност за алармирање по корисник или сретство со цел да може да се детектира лесно и брзо
Емаил Аларми	Решението треба да има можност за праќање на критични аларми на email
Ниво на аларми	Нивоата на алармите треба да можат да бидат конфигурирани на тој начин што ќе ја покажуваат важноста на алармите

Дополнителни информации во автоматските аларми	Алармите автоматски треба да се дополнат со следните информации : - Време на детекција - Име на изворот (Source Hostname) - Име на дестинацијата (Destination hostname) - Изворна IP адреса - Дестинациска IP адреса - Корисничко име - ID на сесија/проток
Променилва содржина на алармите	Форматот на алармите треба да може да биде променлив и прилагодлив
Агрегација на аларми	Треба да постои можност за агрегација на аларми врз основа на заеднички критериуми (IP, domain, hostname...)
Калсификација на закани	Секој аларм треба да се однесува на TTP (MITRE Att&ck рамка)
Whitelist-инг	Решението треба да поддржува детекција врз основа на whitelist-инг на следните полиња: - IP / IP опсег - Domain - hostname - hash на фајловите Whitelist-те треба да имаат можност за сетирање на време на истекување.
Форензички способности	Решението треба да обезбеди детални форензички способности за истражување на инциденти и разбирање на опсег и влијание на потенцијални прекршувања
Одговор по детектирана закана	Решението треба да има отворено API со цел да може да прати информација до друго имплементирано решение што има можност да ја блокира заканата
Блокирање на сообраќај	Решението треба да има можност за автоматска блокада на протоците од компримитираните средства или од изворот на нападот, без користење на други алатки. Блокирање на протоците треба да можат да направат преку конзола и аналитичарите рачно.
Интеграција со EDR	Решението потребно е да има можност за интеграција со Endpoint protection and response решение
Предлози за отстранување и истражување	Решението треба да има можност да дава предлози за отстранување и и истраги за аналитичарите
SOC автоматизација (SOAR)	Решението треба да има можност за интеграција со други безбедносни решенија со користење на API-ја, и можност за дефинирање на

	автоматизирани акции и работни текови кои терба да извршат како одговоро на специфични инциденти.
Временски тек на истрагите	Решението треба да овозможи симплифициран временски тек за истрагите (кратко резиме за секој лог вовременска рамка)
Извештаи	Решението треба да има можност за експортирање на централниот екран во ПДФ
Групирања	Решението треба да има можност за групирања по хостови, дестинации и функции
Известувања за телеметрија на мрежен сообраќај	Решението треба да има можност за известувања за волументрија, преглед на хостови, покриеност
Вклучени лиценци и подршка од производителот	Мин. 12 месеци за системски ажурирања и надградби
Стандарди и акредитација	Сертифицирано според ANSSI за користење во организации со високи безбедносни стандарди

- **Рок на имплементација на решението е 5 работни денови по добивање на писмена порачка од договорниот орган.**

Прилог 1

ОБРАЗЕЦ НА ПОНУДА

Врз основа на оглас 20152/2023 објавен од страна на Министерството за финансии, за доделување на договор за јавна набавка на стоки – софтвери за мрежна детекција, рано откривање и одговор на малициозни активности, со спроведување на поедноставена отворена постапка преку Електронскиот систем за јавни набавки (https://www.e-nabavki.gov.mk) и на тендерската документација ја поднесуваме следнава:

П О Н У Д А

Дел I – Информации за понудувачот

I.1. Име на понудувачот: ИНФОСОФТ СИСТЕМС ДОО Скопје

I.2. Контакт информации

- Адреса: Наум Наумовски Борче бр.40-1/1
- Телефон: 02 3227055
- Факс: /
- Е-пошта: amazni@infosoftsystems.mk
- Лице за контакт: Александар Мазни

I.3. Одговорно лице: Душко Темков

I.4. Даночен број: МК4038016510973

I.5. Матичен број: 7123990

I.6. Согласни сме да ја дадеме оваа понуда за предметот на договорот за јавна набавка согласно со техничките спецификации.

Дел II – ТЕХНИЧКА ПОНУДА

II.1. Согласни сме да ви го обезбедиме предметот на набавка – софтвери за мрежна детекција, рано откривање и одговор на малициозни активности_____(Комерцијалното име на предметот на набавката да се наведе задолжително) за период од 12 (дванаесет) месеци сметано од денот на целосната инсталација и ставање во употреба на истиот во се според барањата

дефинирани во техничките спецификации кои се составен дел од тендерската документација.

II.2. Во прилог на техничката понуда се доставува технички опис како ќе се постигнат следните карактеристики барани од решението:

Карактеристики што се бараат да ги обезбеди системот		**Опис како се постигнува**
Мониторирање во реално време	Решението треба да обезбеди мониторинг во реално време на мрежниот сообраќај во однос на детекција и одговор на закани кои можат да се случат	Решението обезбедува мониторинг во реално време на мрежниот сообраќај во однос на детекција и одговор на закани кои можат да се случат Референца: GW_Boiler_MémoireTechnique_v EN 2023.pdf точка 3.3.1 на страна 15
Сепарација на податоци	Решението треба да биде multi-tenant	Решението е multi-tenant. Референца: GCENTER_v102-EN-DRAFT страна 28-29
Својства	Решението треба да има интегриран систем за централирано собирање и следење на логови и настани со цел навремено детектирање на потенцијални закани како и ловење на нови закани	Решението има интегриран систем за централирано собирање и следење на логови и настани со цел навремено детектирање на потенцијални закани како и ловење на нови закани Референца : GCENTER_v102-EN-DRAFT страна 3
	Решението треба да има можност за детекција на 0-day напади со shell вгнезден код во реално време, без користење на sandbox	Решението има можност за детекција на 0-day напади со shell вгнезден код во реално време, без користење на sandbox.

ИНФОСОФТ СИСТЕМС ДОО Скопје
Ул. Наум Наумовски Борче бр.40/1-1
Скопје 1000, Македонија
Тел: +389 2 322 7055
Email: contact@infosoftsystems.mk
Web: www.infosoftgroup.com.al

		Референца : GCENTER_v102-EN-DRAFT страна 10, 245, 246, 247
	Решението треба да има инкорпорирано malware engines во самата структура за анализа на малициозни кодови	Решението има инкорпорирано malware engines во самата структура за анализа на малициозни кодови. Референца : GCENTER_v102-EN-DRAFT страна 246 GW_Boiler_MémoireTechnique_vEN%202023.pdf – точка 4.2.1 страна 28
	Решението треба да има можност за графички прикази за движењето на мрежниот сообраќај и можните сомнителни активности од корисниците	Решението има можност за графички прикази за движењето на мрежниот сообраќај и можните сомнителни активности од корисниците Референца : GCENTER_v102-EN-DRAFT страна 97
Одвојување на функциите	Решението треба да поддржува можност за дефинирање на различни улоги и привилегии (оператори и администратори)	Решението обезбедува RBAC контрола на пристап. Во основа, постојат следните ролји: Оператор и Администратор. Операторот може да пристапи до податоците, да изврши истрага и е главно фокусиран на детекција. Администраторот е фокусиран на одржување на платформата, управување со ажурирања и надградби, кориснички сметки, backup и сл. Тој е задолжен за администрација на решението. Референца: GCENTER_v102-EN-DRAFT – страна 69, 162
Поддршка на пропусниот опсег	Способност за анализа на протоци до 40Gbit/s	Решението поддржува анализа на протоци до 40 Gbit/s.

		Референца : GATEWATCHER Grille Comparative des spécifications
Број на поддржани сесии	Способност за анализа на протоци повеќе од 200000 симултани сесии	Решението поддржува анализа на протоци повеќе од 200000 симултани сесии. Референца : GATEWATCHER Grille Comparative des spécifications
Анализа на PCAP фајлови	Решението треба да може да анализира PCAP мрежни пакети и истата да се испрати за анализа преку API	Решението може да анализира pcap мрежни пакети со користење на API. Референца: DocumentationGCap – страна 33, 42, 178
Pcap анализа	Решението треба да има можност да изврши детекција на pcap	Решение овозможува pcap на барање и ги има сите модули за анализа достапни за детекција. Референца: DocumentationGCap – страна 33, 42, 178
Централизирана корисничка автентикација	Решението треба да има можност за поврзување со централен систем за автентикација како LDAP	Решението има можност за поврзување со Active Directory (LDAP) и OpenLDAP. Референца: GCENTER_v102-EN-DRAFT – страна 73
MFA	Решението треба да поддржува мултифакторски автентикација.	Решението поддржува MFA со користење на сертификати интегрирани во веб пребарувач. Референца: Copie de Hermes_NDR_Requirements_v1.3 ach.xlsx
UEBA	Решението треба да има способност за извршување на автоматизирано профилирање на однесувањето, конструирање основна линија и напредна анализа за анализа на податоците за пристап и автентикација,	Решението користи комбинација од набљудуван, ненабљудуван и полунабљудуван ML за детекција на малициозни активности.

	воспоставување на кориснички контекст и известување за сомнително однесување	Референца: Copie de Hermes_NDR_Requirements_v1.3 ach.xlsx
Built-in каталог на правила	Решението треба да има предефинирани (Built-in) правила за детекција и модели	Како дополнение на случаите кои се детектирани од ML, решението поддржува каталог на правила за детекција на сомнителни и малициозни одннесувања. Референца : GCENTER_v102-EN-DRAFT страна 210-217
Комплексни услови	Решението треба да има можност за креирање на комплексни правила за детекција базирани на повеќе оператори: -и/или Imbricated And/OR - еднакво, содржи или идентично оператори -негација - regular expressions	Со suricata, решението може да креиира напредни правила со оператор OR/AND/NOT, и сл. Референца : GCENTER_v102-EN-DRAFT страна 33-44
Yara правила	Решението треба да има можност за импортирање на Yara правила	Решението овозможува употреба на API интерфејсите за поставување на сопствени YARA правила. Референца: GCENTER_v102-EN-DRAFT страна 33-44 (2.5.3)
Детекција на прилагодени потписи	Решението треба да има можност за детекција врз основа на прилагодени потписи (suricata, snort, zeek...)	Решението може да изврши длабока инспекција и детекција на мрежни пакети Референца: GCENTER_v102-EN-DRAFT страна 33-44
Анализа на фајлови	Решението треба да има можност за анализа на фајлови во sandbox, да детектира малициозни фајлови базирано на хеуристична и статичка анализа. Решението треба да да може да	Решението има можност за анализа на фајлови базиран на хеуристичка анализа

	детектира фајлови врз основа на Yara правила	Референца : GCENTER_v102-EN-DRAFT страна 10
Правила од други извори	Решението треба да има можност за додавање IOC-и од надворешни CTI извори	Бараното решение има интегрирана алатка за проактивно пронаоѓање и отстранување на сајбер напади (Threat Hunting) врз основа на индикатори за компромис (IoC). Индикаторите за компромис може да се добијат од надворешни или внатрешни извори. Референца: GCENTER_v102-EN-DRAFT страна 50-53
Sandbox анализа	Решението треба да има можност да праќа фајлови до third party sandbox решенија и да ги репплицира резултатите од проверките	Поддршка за SandBox тип од надворешни мотори за скенирање GCENTER_v102-EN-DRAFT страна 10
Поддржани протоколи	Решението треба да може да анализира сообраќај по следните протоколи: DHCP, DNS, HTTP, SMTP, SNMP, ICAP, ARP	Решението може да анализира размена на DHCP, DNS, HTTP, SMTP, SNMP, ICAP, ARP протоколите. Со анализирање, парсирање и логирање. Референца: DocumentationGCap – EN страна 26, 27
Анализа на енкриптиран проток	Решението треба да може да анализира енкриптирани протоци (metadata анализа)	Решението поддржува разчни начини за детекција на малициозни активности во мрежата. Овозможува fingerprinting со коритење на JA3/JA3S технологии. Најсовремениот метод на AioniQ's (со комбинација на статички правила, AI и анализа на фајлови) овозможува zero-day детекција и напредни тактики за

		напад без декрипција на рамката. Референца: GCENTER_v102-EN-DRAFT страна 17
Таргетирана анализа	Решението треба да може да прави категоризација на изворите и дестинациите на протоците (internet, admin мрежа, продукциска мрежа,работна станица, сервер...) во однос на опсегот на ИП адресите и/или FQDN за да може да аплицира правилни правила за детекција на конкретни протоци	Собирање и зачувување на податоци за проверката на инцидентот, категоризација, приоритизација, ублажување и известување. Можни извори за собирање податоци: периметарот, внатрешната мрежа и крајните точки (сервер и крајни уреди), системи за заштита на крајните уреди, ревизорски записи (audit logs), перформанси на системот и записи од кориснички активности. Референца: GCENTER_v102-EN-DRAFT страна 23,24, 134, 135
Север-југ анализа	Решението треба да има можност за аплицирање на специфична политика за детекција на север-југ протоци (внатрешна мрежа - интернет)	Решението овозможува креирање на полисии за специфичните потреби. Референца: GW_Boiler_MémoireTechnique_v EN 2023 – страна 33
Исток-запад анализа	Решението треба да има можност за аплицирање на специфична политика за детекција на исток-запад протоци (работна станица - сервери)	Решението овозможува креирање на полисии за специфичните потреби. Референца: GW_Boiler_MémoireTechnique_v EN 2023 – страна 33
Прегледност	Решението треба да има комплетна видливост на целиот мрежен сообраќај	Решението има комплетна видливост на целиот мрежен сообраќај и истиот да може да

	и истиот да може да подржува анализа на сите познати мрежни протоколи	подржува анализа на сите познати мрежни протоколи Референца: GCENTER_v102-EN-DRAFT – точка 2.1 страна 25 и 26
Машинско учење	Решението треба да има во својата структура алгоритам за машинско учење за детекција на аномалии и за идентификување на сомнителни активности	Решението има во својата структура алгоритам за машинско учење за детекција на аномалии и за идентификување на сомнителни активности Референца : GCENTER_v102-EN-DRAFT страна 44
Автоматизирано учење со закана од интерна мрежа	Ако веќе има малвер во системот, решението треба да може да ги адаптира и отстрани сите модели кои се однесуваат на таа закана, или пак да продолжи да учи од активностите	Решението употребува различни модули базирани на потпис за идентификување на малициозни активности со отстранување на моделот изучен во периодот на активноста на малверот. Референца: Gatewatcher – страна 5 GCENTER_v102-EN-DRAFT страна 44
Автоматизирано учење од мала количина на податоци	Решението треба да може да учи од мала количина на податоци.	Решението поддржува учење со маа количина на податоци за специфична детекција: алармирање, ексфилтрација на податоци, латерализација. Референца: Gatewatcher – страна 5 GCENTER_v102-EN-DRAFT страна 44
Интеграција	Решението треба да може да се интегрира со останати SIEM решенија и да има можност за интеграција преку SYSLOG и да се праќаат настани до SIEM решение	Решението може да се интегрира со останати SIEM решенија и да има можност за интеграција преку SYSLOG и да

ИНФОСОФТ СИСТЕМС ДОО Скопје
Ул. Наум Наумовски Борче бр.40/1-1
Скопје 1000, Македонија
Тел: +389 2 322 7055
Email: contact@infosoftsystems.mk
Web: www.infosoftgroup.com.al

		се праќаат настани до SIEM решение Референца : GCENTER_v102-EN-DRAFT страна 270
Логирање	Решението треба да има можност за ревизија на дејствата на операторите и администраторите и безбедносните настани	Решението подржува логирање на различни нивоа за акците кои се преземаат. Се следат промени на привилегиите и ролјите, конекциите, акциите, и сл. Референца : GCENTER_v102-EN-DRAFT страна 73
Формат на логовите	Безбедносните записи (логови) треба да ги вклучуваат следниве информации: - Време - Корисник. - Акција. - Извршена командата - Резултат на акцијата. - Вид на акција. - Изворна IP адреса.	Решението поддржува различни логови на различни нивоа.постојат логови на пробите и на менаџерот. Референца : GCENTER_v102-EN-DRAFT страна 162
Ротација на логови	Решението треба да има функционалност на ротација на логови пред да се искористи целиот простор наменет за чување на логовите.	Во случај на искористување на меморискиот простор, постои "emergency mode" што ги брише најстарите податоци додека не се постигне 30% слободен простор во решението.на тој начин, не доаѓа до сатурација на самото решение. Референца : GCENTER_v102-EN-DRAFT страна 63
Разузнавање на закани	Решението треба да поседува инкорпорирани фидови за разузнавање на потенцијални закани со цел да биде организацијата навремено ажурирана со најнови индикатори за закани и	Решението поседува инкорпорирани фидови за разузнавање на потенцијални закани со цел да биде организацијата навремено ажурирана со најнови

	идентификување на закани кои се појавуваат.	индикатори за закани и идентификување на закани кои се појавуваат Референца: GCENTER_v102-EN-DRAFT – страна 98, страна 105, страна 244
Детекција на база на потписи	Решението треба да може да изврши длабока инспекција и детекција на мрежни пакети	Решението може да изврши длабока инспекција и детекција на мрежни пакети Референца: GCENTER_v102-EN-DRAFT – страна 3, страна 23, страна 265
Детекција на база на Вештачка интелигенција	Решението треба да може да врши детекција на сомнителни активности употребувајќи модел на вештачка интелигенција	Решението може да врши детекција на сомнителни активности употребувајќи модел на вештачка интелигенција Референца: Datasheet_Aionbytes_2022.pdf GW_Boiler_MémoireTechnique_v EN 2023 страна 30
Детекција на сомнителни и абнормални активности	Решението треба да има детекција на абнормални и сомнителни активности како, bruteforce, сомнителни конекции, сомнителен upload, сомнителен download, детекција на скенирања, каталог од пре-дефинирани сомнителни активности	Решението има детекција на абнормални и сомнителни активности како, bruteforce, сомнителни конекции, сомнителен upload, сомнителен download, детекција на скенирања, каталог од пре-дефинирани сомнителни активности Референца: GCENTER_v102-EN-DRAFT – страна 95, 96, 97, 98
Скалабилност	Решението треба да може да се проширува со потребите на мрежата во однос на големината и крајните уреди	Решението може да се проширува со потребите на мрежата во однос на големината и крајните уреди

		Референца: GCENTER_v102-EN-DRAFT – страна 112 и 113 Решението има можност да се проширува со дополнителни крајни точки доколку системот детектира дополнителни ИП адреси во мрежниот сообраќај.
Алармирање	Решението треба да обезбеди навремено и активно алармирање на тимовите за ИТ безбедност кога ќе се детектираат потенцијални закани	Решението обезбедува детални форензички способности за истражување на инциденти и разбирање на опсег и влијание на потенцијални прекршувања Референца: GCENTER_v102-EN-DRAFT – страна 103 и 104 и 105
Алармирање по корисник и средство	Решението треба да има можност за алармирање по корисник или средство со цел да може да се детектира лесно и брзо	Решението има можност за алармирање по корисник или сретство со цел да може да се детектира лесно и брзо Референца: GW_Boiler_MémoireTechnique_v EN 2023 страна 33, 34
Емаил Аларми	Решението треба да има можност за праќање на критични аларми на email	Со користење на API интерфејс, решението овозможува скритирање и нотификација по е-маил, на Teams, на Slack, Mattermost, и сл. Референца: DocumentationGCap - EN – страна 27 GCENTER_v102-EN-DRAFT – страна 173
Ниво на аларми	Нивоата на алармите треба да можат да бидат конфигурирани на тој начин што ќе ја покажуваат важноста на алармите	Решението го исполнува ова барање со употреба на бодовна табела на ризици (важност) која се пресметува со истото. Референца: GCENTER_v102-EN-DRAFT – страна 105

ИНФОСОФТ СИСТЕМС ДОО Скопје
Ул. Наум Наумовски Борче бр.40/1-1
Скопје 1000, Македонија
Тел: +389 2 322 7055
Email: contact@infosoftsystems.mk
Web: www.infosoftgroup.com.al

Дополнителни информации во автоматските аларми	Алармите автоматски треба да се дополнат со следните информации : - Време на детекција - Име на изворот (Source Hostname) - Име на дестинацијата (Destination hostname) - Изворна IP адреса - Дестинациска IP адреса - Корисничко име - ID на сесија/проток	Сите овие полиња се достапни за секоја детекција на решението. Референца: GCENTER_v102-EN-DRAFT – страна 103-106
Променилва содржина на алармите	Форматот на алармите треба да може да биде променилив и прилагодлив	Овие полиња се овозможени во основна конфигурација. Референца: GCENTER_v102-EN-DRAFT – страна 103-106
Агрегација на аларми	Треба да постои можност за агрегација на аларми врз основа на заеднички критериуми (IP, domain, hostname...)	Решението агрегира аларми по корисници односно основни средства (основно средство = крајна точка, сервери, и сл. = не е корисник). Референца: GCENTER_v102-EN-DRAFT – страна 103, 104
Калсификација на закани	Секој аларм треба да се однесува на TTP (MITRE Att&ck рамка)	За секој аларм, постои име на тактиката и име на техниката за соодветното поле. Референца: GW_Boiler_MémoireTechnique_v EN 2023 страна 32-34
Whitelist-инг	Решението треба да поддржува детекција врз основа на whitelist-инг на следните полиња: - IP / IP опсег - Domain - hostname - hash на фајловите Whitelist-те треба да имаат можност за сетирање на време на истекување.	Решението овозможува детекција на whitelist по IP, опсег на IP, домеин, hostname, и file-hash. Референца: GCENTER_v102-EN-DRAFT – страна 299
Форензички способности	Решението треба да обезбеди детални форензички способности за	Решението обезбедува детални форензички способности за

ИНФОСОФТ СИСТЕМС ДОО Скопје
Ул. Наум Наумовски Борче бр.40/1-1
Скопје 1000, Македонија
Тел: +389 2 322 7055
Email: contact@infosoftsystems.mk
Web: www.infosoftgroup.com.al

	истражување на инциденти и разбирање на опсег и влијание на потенцијални прекршувања	истражување на инциденти и разбирање на опсег и влијание на потенцијални прекршувања. Референца: GCENTER_v102-EN-DRAFT – страна 245, 246, 247
Одговор по детектирана закана	Решението треба да има отворено API со цел да може да прати информација до друго имплементирано решение што има можност да ја блокира заканата	Решението има отворено API со цел да може да прати информација до друго имплементирано решение што има можност да ја блокира заканата Референца : GCENTER_v102-EN-DRAFT страна 167
Блокирање на сообраќај	Решението треба да има можност за автоматска блокада на протоците од компримитираните средства или од изворот на нападот, без користење на други алатки. Блокирање на протоците треба да можат да направат преку конзола и аналитичарите рачно.	Решението овозможува блокирање на сообраќај со употреба на API интерфејс и да испрати информатија до друго решение за блокирање на заканите.. Референца : GCENTER_v102-EN-DRAFT страна 306-308
Интеграција со EDR	Решението потребно е да има можност за интеграција со Endpoint protection and response решение	Решението овозможува употреба на API интерфејсот и испраќање на информација Tanium ако другото решение има отворен API интерфејс. Референца : GW_Boiler_MémoireTechnique_v EN 2023 – страна 34, 35, 36, 37
Предлози за отстранување и истражување	Решението треба да има можност да дава предлози за отстранување и и истраги за аналитичарите.	Сите продукти се управуваат преку API интерфејс, incident responses included. Референца: GW_Boiler_MémoireTechnique_v EN 2023 – страна 34, 35, 36, 37

SOC автоматизација (SOAR)	Решението треба да има можност за интеграција со други безбедносни решенија со користење на API-ја, и можност за дефинирање на автоматизирани акции и работни текови кои терба да извршат како одговоро на специфични инциденти.	Решението со употреба на отворениот API интерфејс овозможува компатибилност со други решенија кои имаа API. Референца: GW_Boiler_MémoireTechnique_v EN 2023 – страна 36, 37
Временски тек на истрагите	Решението треба да овозможи симплифициран временски тек за истрагите (кратко резиме за секој лог вовременска рамка)	Решението овозможува временски тек на истрагите со различни прикази. Референца: : GW_Boiler_MémoireTechnique_v EN 2023 – страна 35, 36
Извештаи	Решението треба да има можност за експортирање на централниот екран во ПДФ	Решението содржи интегрирана можност за експспортирање во ПДФ. Референца: GCENTER_v102-EN-DRAFT – страна 173-189
Групирања	Решението треба да има можност за групирања по хостови, дестинации и функции	Решението овозможува сорттирање на тагиран сообраќај од хостовите. Референца: DocumentationGCap – EN – страна 19
Известувања за телеметрија на мрежен сообраќај	Решението треба да има можност за известувања за волументрија, преглед на хостови, покриеност	Решението поддржува телеметрија, волументрија, преглед на хостови, покриеност. Референца: : GW_Boiler_MémoireTechnique_v EN 2023 – страна 17
Вклучени лиценци и подршка од производителот	Мин. 12 месеци за системски ажурирања и надградби	Секоја од верзиите на решението се поддржани 1 година (12 месеци). Согласно финансиската понуда.

Стандарди и акредитација	Сертифицирано според ANSSI за користење во организации со високи безбедносни стандарди	Сертифицирано според ANSSI.

НАПОМЕНА: Задолжително да се пополнат празните колони во спротивно понудата ќе се отфрли

Дел III - ФИНАНСИСКА ПОНУДА

III.1. Вкупната цена на нашата понуда, вклучувајќи ги сите трошоци и попусти, без ДДВ, изнесува: **4.150.000,00** *[со бројки]* (**четири милиони сто педесет илјади**) *[со букви]* денари.

Вкупниот износ на ДДВ изнесува **207.500,00** [*со бројки*] **(двеста и седум илјади и петстотини**) [*со букви*] денари.

III.2. Нашата понуда важи за периодот утврден во тендерската документација.
III.3. Се согласуваме со начинот и рокот на плаќање утврден во тендерската документација.
III.4. Ги прифаќаме начинот, местото и рокот за испорака на предметната стока, наведени во тендерската документација.
III.5. Со поднесување на оваа понуда, во целост ги прифаќаме условите предвидени во тендерската документација и не го оспоруваме Вашето право да ја поништите постапката за доделување на договор за јавна набавка согласно со член 114 од Законот за јавните набавки.

Дел IV - СОСТАВНИ ДЕЛОВИ НА ПОНУДАТА:

IV.1. Нашата понуда е составена од следниве делови:
1. ОПШТ ДЕЛ,
2. ТЕХНИЧКА ПОНУДА,
3. ФИНАНСИСКА ПОНУДА,
4. ПРИЛОЗИ:
   - Пополнет образец на понуда (Прилог 1),
   - Изјава за сериозност (Прилог 3),
   - Изјава за докажување способност (Прилог 4) или Документи од точка 5.2 и Документи за докажување на способност од точка 5.3,

Место и датум	Одговорно лице
Скопје, 24.11.2023	Душко Темков Dushko Temkov Digitally signed by Dushko Temkov DN: cn=Dushko Temkov gn=Dushko c=MK o=Infosoft Sistems DOO Skopje ou=VAT - 4038016510973 Reason: I am approving this document Location: Date: 2023-11-27 09:19+01:00 (потпис*)

**Овој образец не се потпишува своерачно, туку исклучиво електронски со прикачување на валиден дигитален сертификат чиј носител е одговорното лице или лице овластено од него.*

***НАПОМЕНА: Доколку понудувачот понудата ја поднесува како група понудувачи, со подизведувач, користи способност од друг субјект или има доверливи информации, понудувачот во прилог на понудата ги доставува и другите барани прилози кон тендерската документација.*