Друштво за производство на компјутери и деловно информатички услуги КИНГ ИЦТ ДООЕЛ
Бр. 56-2025
13.03 2025 год.
СКОПЈЕ

Архивски број: 03-3150/1
Датум: 13-03-2025

ДОГОВОР
за јавна набавка на стоки – Систем за безбедносна анализа на мрежен сообраќај

Склучен помеѓу:

1. МИНИСТЕРСТВОТО ЗА ФИНАНСИИ НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА, со седиште на ул.„Даме Груев", бр.12 - Скопје, претставувано од м-р Гордана Димитриеска-Кочоска, министер за финансии во натамошниот текст: договорен орган и
2. Група на носители на набавка: Друштво за производство на компјутери и деловно информатички услуги КИНГ ИЦТ ДООЕЛ Скопје (носител на група) и Друштво за трговија и услуги БОСОН СОЛУШНС ДОО експорт-импорт Скопје (член на група), претставувана од Друштво за производство на компјутери и деловно информатички услуги КИНГ ИЦТ ДООЕЛ Скопје со седиште на ул.„Владимир Комаров" бр.11а кат ПР/Синерџи-Б Центар во Скопје, претставувано од Влатко Петревски, управител во натамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на стоки – Систем за безбедносна анализа на мрежен сообраќај, согласно со понудата на носителот на набавката прифатена од страна на договорниот орган (Прилог 1) и техничките спецификации (Прилог 2), кои се составен дел од овој договор, а по претходно спроведена поедноставена отворена постапка, по оглас број 22497/2024.

Комерцијално име на системот за безбедносна анализа на мрежен сообраќај е Cisco Secure Network Analytics, Cisco Secure Network Analytics Management Console, UCS C225 M8.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 1.485.500,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 267.390,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 1.752.890,00 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. ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Договорот важи од денот на потпишувањето од двете договорни страни па до истекот на 12 (дванаесет) месеци сметано од денот на целосната инсталација и ставање во употреба на системот за безбедносна анализа на мрежен сообраќај.

V. НАЧИН, МЕСТО И РОК НА ИСПОРАКА

Член 5

Носителот на набавката е должен системот да го испорача, инсталира и конфигурира во период од 15 (петнаесет) работни денови по добивање на писмена порачка од договорниот орган, а по склучување на договорот.

За извршената испорака, инсталација и конфигурација договорните страни потпишуваат документ - работен налог или записник.

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 задолженото 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 предметот 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 за извршената набавка, во писарницата на Министерството за финансии.

Кон фактурата носителот на набавката задолжително доставува Работен налог/Записник кој мора да содржи податоци за извршувањето, потпишан од двете договорни страни и соодветен доказ/лог за извршената инсталација и конфигурација на системот, 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 (Прилог 2) и понудата прифатена од договорниот орган (Прилог 1).

Носителот на набавката е должен да се придржува кон рокот за извршување на предметниот договор, кој е дефиниран во член 5 став 1 од овој договор.

Носителот на набавката се обврзува предметниот договор да го извршува со разумно знаење и внимание во согласност со професионалните стандарди и тековната легислатива која влијае на ваков предмет на набавка.

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 одговорни за реализација на предметната набавка.

VIII. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 8

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

Договорниот орган е должен да достави писмено барање (порачка) со точни спецификации и барања со цел да се изврши реализација на договорот.

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 9

Носителот на набавката е должен заедно со потпишаниот договор да достави банкарска гаранција за квалитетно и навремено извршување на договорот во висина од 10% од вкупната вредност на договорот со пресметан ДДВ.

Со банкарската гаранција за квалитетно и навремено извршување на договорот носителот на набавката безусловно гарантира за целосно, квалитетно и навремено извршување на обврските по овој договор.

Банкарската гаранција за квалитетно и навремено извршување на договорот треба да биде безусловна, неотповиклива и на прв повик наплатлива од страна на договорниот орган, треба да биде издадена од банка со седиште во Република Северна Македонија или од странска банка.

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

Недоставување на банкарската гаранција претставува основ за раскинување на овој договор.

Договорниот орган се обврзува на носителот на набавката да му ја врати банкарската гаранција за квалитетно и навремено извршување на договорот во рок од 14 (четиринаесет) дена од денот на целосното реализирање на договорот.

Договорниот орган нема да ја врати банкарската гаранција за квалитетно и навремено извршување на договорот и ќе бара нејзино активирање од банката која ја има издадено, доколку предметната набавка не е реализирана според одредбите од договорот.

Во случај носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) да не можел да ја изврши услугата, договорниот орган нема да бара активирање на банкарската гаранција, доколку носителот на набавката достави писмено образложение до договорниот орган во

кое ќе ги наведе причините за неизвршената или ненавремено извршената услуга, а образложението биде писмено прифатено од страна на договорниот орган.

X. ДОВЕРЛИВОСТ НА ПОДАТОЦИ И ИНФОРМАЦИИ

Член 10

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 11

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 12

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 13

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 10 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 14

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 15

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 16

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 17

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 РАСКИНУВАЊЕ И ПРЕКИНУВАЊЕ НА ДОГОВОРОТ

Член 18

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

Член 19

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 наплата 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 20

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 21

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 22

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. ЗАВРШНИ ОДРЕДБИ

Член 23

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 24

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 25

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 26

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

Член 27

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	Носител на набавката: Друштво за производство на компјутери и деловно информатички услуги КИНГ ИЦТ ДООЕЛ Скопје
м-р Гордана Димитриеска-Кочоска Министер за финансии	Влатко Петревски Управител

Изработил: Мариа Анѓелеска
Контролирал: Рената Николоска
Даниела Јанкова
Одобрил: Татјана Васева
Проверил: м-р Маја Стаменковска Угриновска
Михајло Михајловски
Проверил: Андреј Ангеловски
Владимир Стојанов
Согласен: д-р Андриана Матлиоска

Прилог 1 – Групна понуда на Друштво за производство на компјутери и деловно информатички услуги КИНГ ИЦТ ДООЕЛ Скопје (носител на група) и Друштво за трговија и услуги БОСОН СОЛУШНС ДОО експорт-импорт Скопје (член на група)

KING ICT
КИНГ ИЦТ ДООЕЛ Скопје, Бизнис Центар Синерџи, 1000 Скопје, ул. Владимир Комаров бр.11а, кат -ПР, Македонија
Тел: ++389 (0)2 3202 970, Факс: ++389 (0)2 3202 980, www.king-ict.mk , e-mail: king@king-ict.mk

Прилог 1

ОБРАЗЕЦ НА ПОНУДА

Врз основа на оглас **22497/2024** објавен од страна на Министерството за финансии, за доделување на договор за јавна набавка на стоки – Систем за безбедносна анализа на мрежен сообраќај, 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: Група на економски оператори КИНГ БОСОН КОНЗОРЦИУМ
Друштво за производство на компјутери и деловно информатички услуги КИНГ ИЦТ ДООЕЛ Скопје-Носител на група
Друштво за трговија и услуги БОСОН СОЛУШНС ДОО експорт-импорт Скопје-Член на група
I.2. Контакт информации:
-Адреса:ул.Владимир Комаров бр.11а кат ПР/Синерџи-Б.Центар Скопје
-Телефон: +389(0)2 3202 970
-Факс: +389(0)2 3202 970
-Е-пошта: sales@king-ict.mk
-Лице за контакт: Бојан Славковиќ
I.3. Одговорно лице: Влатко Петревски
I.4. Даночен број: 4030008020265
I.5. Матичен број на понудувачот:6325270
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 – Систем за безбедносна анализа на мрежен сообраќај **Cisco Secure Network Analytics, Cisco Secure Network Analytics Management Console и сервер UCS C225 M8** (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:

Елементи/ функционалност	**Минимални технички карактеристики**	**Понудено** **Cisco Secure Network Analytics, Cisco Secure Network Analytics Management Console, UCS C225 M8**
Скалабилност:	1. Системот треба да е издвоен во најмалку три апликациски целини	1. Системот е издвоен во три апликациски целини имплементирани на еден дедициран серверски систем:

	имплементирани на најмалку еден дедициран серверски систем : a. за собирање на телеметриски податоци од мрежните уреди b. за анализа и генерирање телеметриски податоци во сегменти каде што мрежните уреди немаат таква функција c. за мониторинг, организација и презентација на мрежните анализи 2. Можност за проширување на системот со дополнителни уреди за зголемување на перформанси на системот	a. за собирање на телеметриски податоци од мрежните уреди b. за анализа и генерирање телеметриски податоци во сегменти каде што мрежните уреди немаат таква функција c. за мониторинг, организација и презентација на мрежните анализи Во понудата се вклучени следниве елементи од Cisco Secure Network Analytics решението: - Secure Network Analytics Management Console - за мониторинг, организација и презентација на мрежните анализи - Secure Network Analytics Flow Sensor - за анализа и генерирање телеметриски податоци во сегменти каде што мрежните уреди немаат таква функција - Secure Network Analytics Flow Collector - за собирање на телеметриски податоци од мрежните уреди преку Netflow или превземање на готови анализи од Flow Sensor 2. Системот има можност за проширување со дополнителни уреди за зголемување на перформанси на системот. Системот може да се надгради со дополнителни Data Store кластери, Flow Collectors или надградба со дополнителна Flow Rate лиценца. Документ: "Boson_MoF_Stealthwatch_RFP_1y.xsls", "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.pdf" страна 8, "Data Store", страна 9, "Flow Rate License"
Собирање на мрежни податоци:	1. Поддршка за IPFIX, Netflow или еквивалентен протокол, дефиниран како отворен стандард 2. Можност за собирање на информации од повеќе	1. Поддржува IPFIX, Netflow или еквивалентен протокол, дефиниран како отворен стандард 2. Собира информации од повеќе типови и производители на мрежни уреди

	типови и производители на мрежни уреди 3. Вклучена поддршка за собирање на информации од мрежни уреди кои не поддржуваат IPFIX/Netflow или еквивалентен протокол	3. Вклучува поддршка за собирање на информации од мрежни уреди кои не поддржуваат IPFIX/Netflow или еквивалентен протокол Flow Collector користи меѓу другото Netflow и IPFIX како извор на телеметрија за сообраќајот кој го испраќаат самите мрежни уреди. Тоа се стандардизирани протоколи па според тоа секој уред од било кој производител кој ги поддржува овие протоколи може да испраќа телеметриски податоци до Stealthwatch. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.pdf", *страна 7, "Flow Collector"* За оние уреди кои самите не можат да генерираат телеметриски податоци за сообраќајот преку гореспоменатите протоколи, користиме Flow Sensor – кој преку SPAN порта го анализира сообраќајот и генерира телеметрија која потоа се испраќа до Flow Collector-от. Документ: *"Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet", страна 9, "Flow Sensor"*
Анализа на податоците:	1. Анализа на податоците во скоро реално време со метод на машинско учење 2. Детекција на аномалии во однос на "нормално" однесување на ендпоинтите 3. Вклучена поддршка за анализа на криптиран сообраќај, без потреба од негова декрипција	1. Анализира податоци во скоро реално време со метод на машинско учење 2. Детекција на аномалии во однос на "нормално" однесување на ендпоинтите 3. Вклучува поддршка за анализа на криптиран сообраќај, без потреба од негова декрипција Encrypted Traffic Analysis (ETA) е уникатна функција на Cisco Systems која служи за безбедносна анализа на криптиран сообраќај без негово декриптирање. Достапен е во голем број на мрежни уреди на Cisco и доколку имате во вашата мрежа такви уреди тие може да генерираат ETA телеметрија и да ја испратат до Stealtwatch. За сите сегменти каде што тоа не е возможно, го користиме Flow Sensor-от кој е исто така способен за т.н. Encrypted Traffic Analyses (ETA) без да се извршува декрипција.

		Понатаму се применува повеќеслојно машинско учење со цел детектирање на напредни безбедносни закани во скоро реално време. Документ: *"ETA-at-a-glance-c45-740079.pdf" ;* "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf":* - *страна 3, "Solution Overview"* - *страна 4, "Primary use cases"* *страна 9, "Flow Sensor"*
Функции:	1. Чување на податоците за период од најмалку 1 година 2. Системот треба да може да изврши автоматска идентификација на податоците од една иста конекција кои поминале низ повеќе уреди, со цел да се земат во предвид само еднаш при анализата. 3. Вклучена можност за правење на заштитни копии на базата и конфигурацијата на системските елементи на надворешен CIFS file систем 4. Можност во системот да се имплементира додатен елемент кој ќе ги агрегира мрежните информации за анализа од разни формати (NetFlow, sFlow, syslog, SNMP) и потоа ќе ги препрати кон една или повеќе дестинации 5. Можност за интеграција со други системи кои овозможуваат контрола на мрежа, преку идентификација на уреди/корисници и нивно мрежно деактивирање	1. Чува податоци за период од најмалку 1 година Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf", страна 8, "Data Store"* 2. Системот врши автоматска идентификација на податоците од една иста конекција кои поминале низ повеќе уреди, со цел да се земат во предвид само еднаш при анализата. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf, страна 7, "Table 2" – "Deduplication and stitching"* 3. Вклучена можност за правење на заштитни копии на базата и конфигурацијата на системските елементи на надворешен CIFS file систем. Документ:*SW_7_0_x_to_7_0_3_Stealthwatch_System_Update_Guide_DV_1_0" страна 28, "Back up the Databases"* 4. Можност во системот да се имплементира додатен елемент кој ќе ги агрегира мрежните информации за анализа од разни формати (NetFlow, sFlow, syslog, SNMP) и потоа ќе ги препрати кон една или повеќе дестинации. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf, страна 10, "Cisco Telemetry Broker"* 5. Можност за интеграција со други системи кои овозможуваат контрола на мрежа, преку идентификација на уреди/корисници и нивно мрежно деактивирање.

	6. Системот мора да детектира закани и напади преку идентификација на сомнителен сообраќај и однесување преку разни аларми како што се: Anomaly, C&C (Command & Control), Data Exfiltration, Data Hoarding, Exploitation, Recon. 7. Системот мора да користи нелинеарни алгоритми за проценка и класификација на разновидни настани и напади. 8. Системот мора да детектира и алармира за таргетирани и дистрибуирани DDoS напади. 9. Системот мора да детектира за нови уреди, неавторизирани апликации и активности 10. Системот мора да поддржува гео-локациски информации за сообраќајот кон и од конкретни земји. 11. Системот мора да детектира и алармира врз база на различни атрибути – времетраење на сесија, име на корисник, време. 12. Системот треба да може да детектира малициозни активности дури и во енкриптиран сообраќај, преку анализа на метадата содржината на мрежните пакети. 13. Системот мора да поддржува интеграција со глобален репутациски безбедносен cloud систем од истиот или различни производители за да идентификува скриени	StealthWatch како дел од Cisco Security портфолиото припаѓа на еден екосистем во кој мултивендорската интеграција и интероперабилност се клучни за креирање на еден ефикасен безбедносен систем. Преку интеграцијата со Cisco ISE се добива увид во идентитетот на ендпоинтите и корисниците во мрежата. Документ: *"at-a-glance-c45-738248"* *"Cisco Secure Network Analytics - ISE Configuration Guide 7.5.1.pdf"* 6. Системот детектира закани и напади преку идентификација на сомнителен сообраќај и однесување преку разни аларми како што се: Anomaly, C&C (Command & Control), Data Exfiltration, Data Hoarding, Exploitation, Recon. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf, страна 3, "Solution Overview", страна 4, "Primary Use Cases", страна 5, "Key benefits"* 7. Системот користи т.н. "multilayered machine learning". Делот за проценка и класификација на настани користи е второ ниво ("Layer 2") и во тој дел се користи магнитуда на различни модели како на пр. multiple-instance learning, neural networks, random forests и други. Документ: "white-paper-c11-740605*", What is multilayered machine learning and how effective is it? , Figure 3. ,* 8. Системот детектира и алармира за таргетирани и дистрибуирани DDoS напади. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf, страна 3, "Solution Overview", "Security_Events_and_Alarm_Categories_DV_2_1. pdf" страна 295 - 296, "DDoS Source" "DDoS Target"* 9. Системот детектира и класифицира нови уреди Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf, страна 5, Key Bennefits*

	C&C комуникации, неавторизирано користење на DNS протокол од страна на DGA-базиран малвер, напредни P2P протокол аналитики, и пасивен мониторинг на криптиран сообраќај 14. Системот мора обезбеди информации за активни и неактивни хостови, статистика за топ најактивни хостови и сервиси на линк, искористеност на линкови, информација дали одреден хост користи специфичен сервис и клиентска апликација, искористеност на TCP/UPD порти, трендови на мрежен сообраќај. 15. Дополнителни безбедносни анализи за детекција на botnet и други софистицирани напади преку корелација со реномиран глобален threat-intelligence сервис.	неавторизирани апликации и активности *Документ: "Identifying_Applications_on_the_Network_Use_Case_doc.pdf"* 10. Системот поддржува гео-локациски информации за сообраќајот кон и од конкретни земји. При тоа овозможува дефинирање на земји со висок ризик со што ќе влијае во ризик анализата на сообраќајот. *Документ: "Reporting_Traffic_from_Specific_Geographies.pdf"* 11. Системот детектира и алармира врз база на различни атрибути – времетраење на сесија, име на корисник, време, апликација итн. Врз база на сите достапни телеметриски податоци се прават моќни репорти за разни намени. За референца е еден таков пример: *Документ: "Using_Secure_Network_Analytics_for_Network_Usage_Accounting"* 12. Системот детектира малициозни активности дури и во енкриптиран сообраќај, преку анализа на метадата содржината на мрежните пакети. Документ: "at-a-glance-c45-740079.*pdf", страна 2, "Encrypted traffic analytics"* 13. Системот поддржува интеграција Cisco Talos како глобален безбедносен cloud систем со цел да понуди дополнително ниво на заштита од софистицирани напади. За оваа функционалност е потребна дополнителна лиценца *Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.pdf, Cisco Secure Network Analytics Threat Feed,страна 11*

		14. Од целосната достапна телеметрија, системот овозможува креирање на "flow search" извештаи за најразлични намени, како на пример мрежна искористенот. За референца се посочени неколку документи кои обработуваат такви примери: *Документ: "Determining_Why_an_Interface_is_Over_Capacity.pdf"* *Документ: "Investigating_Hosts_Using_the_Most_Bandwidth.pdf"* 15. Системот овозможува дополнителни безбедносни анализи за детекција на botnet и други софистицирани напади преку корелација со реномиран глобален threat-intelligence сервис. Документ: "white-paper-c11-740605", *страна 5, "Global threat intelligence"*
Мониторинг и Менаџмент:	1. Мониторинг на протокот се извршува речиси во реално време 2. Можност за брза откривање на безбедносни пропусти, со детекција на несоодветно однесување преку прегледност во искористување на мрежните ресурси (Policy Violation, Data Hoarding) 3. Детектираните инциденти да бидат мапирани во согласност со MITRE ATT&CK дефинираните тактики и техники. 4. Преземање на соодветни акции за сите детектирани инциденти од една централна точка	1. Мониторинг на протокот се извршува речиси во реално време 2. Можност за брзо откривање на безбедносни пропусти, со детекција на несоодветно однесување преку прегледност во искористување на мрежните ресурси (Policy Violation, Data Hoarding) 3. Детектираните инциденти се мапирани во согласност со MITRE ATT&CK дефинираните тактики и техники. 4. Преземање на соодветни акции за сите детектирани инциденти од една централна точка 5. Вклучена поддршка за графички приказ и креирање на соодветни мапи на мрежната инфраструктура 6. Вклучена е поддршка за преглед на целиот сообраќај помеѓу било кои два мрежни елементи

	5. Вклучена поддршка за графички приказ и креирање на соодветни мапи на мрежната инфраструктура 6. Вклучена поддршка за преглед на целиот сообраќај помеѓу било кои два мрежни елементи 7. Вклучена поддршка за форензички анализи врз база на ревизорски траги од сите мрежни трансакции 8. Дефинирање на безбедносни настани согласно сопствени потреби врз основа на аномалии во сообраќајот 9. Креирање и испраќање на автоматски известувања и извештаи по случување на одредени аларми или безбедносни настани.	7. Вклучена е поддршка за форензички анализи врз база на ревизорски траги од сите мрежни трансакции 8. Дефинирање на безбедносни настани согласно сопствени потреби врз основа на аномалии во сообраќајот 9. Креирање и испраќање на автоматски известувања и извештаи по случување на одредени аларми или безбедносни настани. Понуденото решение Cisco Secure Network Analytics Management Console ги поддржува сите точки од барањето. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.*pdf, страна 6 "Table 1"*, "Secure Network Analytics and the MITRE ATT&CK Enterprise matrix" страна 2.
Програмабилност:	Можност за конфигурирање и мониторинг на системот преку т.н. API интерфејс	Системот има можност за конфигурирање и мониторинг на системот преку т.н. API интерфејс Cisco Stealthwatch Enterprise има отворен и документиран API интерфејс за програмабилност. Документ: "Stealthwatch Enterprise REST API - Cisco DevNet.*pdf" страна 1*
Серверски систем:	Понудувачот да понуди и препорачан Хардвер за инсталација на решението.	Во понудата е вклучен и соодветен хардвер за инсталација на решението. Документ: "Boson_MoF_Stealthwatch_RFP_1y.xsls"
Интеграција во постоечка мрежа	1. Системот треба да се постави во постоечката мрежа така што ќе анализира сообраќај од Core свичевите и периметарскиот firewall. 2. Можност за надградба на капацитетот преку	1. Системот ќе се постави во постоечката мрежа и ќе анализира сообраќај од Core свичевите и периметарскиот firewall. 2. Системот има можност за надградба на капацитетот преку зголемување на Flow Rate лиценцата што би овозможило анализирање на дополнителна телеметрија.

	дополнителна лиценца или претплата со што би се овозможило дополнително анализирање на локалниот сообраќај од 18 трезорски канцеларии пред тој да пристигне на централната локација.	Технички може да се изведе на два начина: преку собирање на NETFLOW телеметрија од самите трезорски рутери или со SPAN (порт мироринг) на вкупниот агрегиран сообраќај кој доаѓа на централната локација. Документ: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.pdf" страна 8, "Data Store", страна 9, "Flow Rate License"
Гарантен рок:	1 годин за хардвер и за системски ажурирања и надградби	Во понудата е вклучен гарантен рок за 1 година за хардвер и за системски ажурирања и надградби. Документ: "Boson_MoF_Stealthwatch_RFP_1y.xsls"
Поддршка:	Достапност на техничка помош од производителот мин. 8 часа x 5 дена со вклучен неограничен број на инциденти, како и бесплатна достава на надградби на потврдени грешки во оперативниот систем (функционални и сигурносни) кои се издаваат од страна на производителот на редовна временска основа, во времетраење на гарантниот период. Сите компоненти на решението мора да имаат 1 година одржување од страна на производителот како и неопходните лиценци за работа на решението.	Достапност на техничка помош од производителот мин. 8 часа x 5 дена со вклучен неограничен број на инциденти, како и бесплатна достава на надградби на потврдени грешки во оперативниот систем (функционални и сигурносни) кои се издаваат од страна на производителот на редовна временска основа, во времетраење на гарантниот период. Сите компоненти на решението имаат 1 година одржување од страна на производителот како и неопходните лиценци за работа на решението.. Документ: "Boson_MoF_Stealthwatch_RFP_1y.xsls"
Транспорт, инсталација и конфигурација:	Вклучени во цената	Вклучени во цената

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

Дел III - ФИНАНСИСКА ПОНУДА

III.1. Вкупната цена на нашата понуда, вклучувајќи ги сите трошоци и попусти, без ДДВ, изнесува: 1.485.500,00 (еден милион четиристотини осумдесет и пет илјади и петстотини) денари.

КИНГ ИЦТ ДООЕЛ Скопје, Бизнис Центар Синерџи, 1000 Скопје, ул. Владимир Комаров бр.11а, кат -ПР, Македонија
Тел: ++389 (0)2 3302 970, Факс: ++389 (0)2 3302 980, www.king-ict.mk , e-mail: king@king-ict.mk

Вкупниот износ на ДДВ изнесува 267.390,00 (двеста шеесет и седум илјади триста деведесет) 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 и
- Овластување/авторизација MAF (Manufacturer Authorisation Form).

Место и датум

Скопје, 17.01.2025

Одговорно лице

Влатко Петревски
(потпис*)

Vlatko Petrevski
Digitally signed by Vlatko Petrevski
Date: 2025.01.19 21:20:45 +01'00'

**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.*

Прилог 2

Технички спецификации
за
за јавна набавка на стоки – Систем за безбедносна анализа на мрежен сообраќај

Предмет на оваа набавка е комплетна инсталација и конфигурација на систем за безбедносна анализа на мрежен сообраќај.

Во опфатот на работи во оваа набавка потребно е да се изврши:

Набавка, инсталација и конфигурација на информатичко-безбедносносен систем кој е предмет на оваа набавка согласно најдобрите пракси дефинирани од страна на производителите, со цел максимална можна прегледност на мрежниот сообраќај, преку логичка класификација на информатичката опрема, апликации и сервиси по функција, што треба да овозможи брза безбедносна анализа и напредно и автоматско откривање и спречување на закани, односно ефикасна и ефективна заштита.

1.Систем за безбедносна анализа на мрежен сообраќај – кол. 1

Елементи/ функционалност	**Минимални технички карактеристики**
Скалабилност:	1. Системот треба да е издвоен во најмалку три апликациски целини имплементирани на најмалку еден дедициран серверски систем : a. за собирање на телеметриски податоци од мрежните уреди b. за анализа и генерирање телеметриски податоци во сегменти каде што мрежните уреди немаат таква функција c. за мониторинг, организација и презентација на мрежните анализи 2. Можност за проширување на системот со дополнителни уреди за зголемување на перформанси на системот
Собирање на мрежни податоци:	1. Поддршка за IPFIX, Netflow или еквивалентен протокол, дефиниран како отворен стандард 2. Можност за собирање на информации од повеќе типови и производители на мрежни уреди 3. Вклучена поддршка за собирање на информации од мрежни уреди кои не поддржуваат IPFIX/Netflow или еквивалентен протокол
Анализа на податоците:	1. Анализа на податоците во скоро реално време со метод на машинско учење 2. Детекција на аномалии во однос на “нормално”

	однесување на ендпоинтите 3. Вклучена поддршка за анализа на криптиран сообраќај, без потреба од негова декрипција
Функции:	1. Чување на податоците за период од најмалку 1 година 2. Системот треба да може да изврши автоматска идентификација на податоците од една иста конекција кои поминале низ повеќе уреди, со цел да се земат во предвид само еднаш при анализата. 3. Вклучена можност за правење на заштитни копии на базата и конфигурацијата на системските елементи на надворешен CIFS file систем 4. Можност во системот да се имплементира додатен елемент кој ќе ги агрегира мрежните информации за анализа од разни формати (NetFlow, sFlow, syslog, SNMP) и потоа ќе ги препрати кон една или повеќе дестинации 5. Можност за интеграција со други системи кои овозможуваат контрола на мрежа, преку идентификација на уреди/корисници и нивно мрежно деактивирање 6. Системот мора да детектира закани и напади преку идентификација на сомнителен сообраќај и однесување преку разни аларми како што се: Anomaly, C&C (Command & Control), Data Exfiltration, Data Hoarding, Exploitation, Recon. 7. Системот мора да користи нелинеарни алгоритми за проценка и класификација на разновидни настани и напади. 8. Системот мора да детектира и алармира за таргетирани и дистрибуирани DDoS напади. 9. Системот мора да детектира за нови уреди, неавторизирани апликации и активности 10. Системот мора да поддржува гео-локациски информации за сообраќајот кон и од конкретни земји. 11. Системот мора да детектира и алармира врз база на различни атрибути – времетраење на сесија, име на корисник, време. 12. Системот треба да може да детектира малициозни активности дури и во енкриптиран сообраќај, преку анализа на метадата содржината на мрежните пакети. 13. Системот мора да поддржува интеграција со глобален репутациски безбедносен cloud систем од истиот или различни производители за да идентификува скриени

	C&C комуникации, неавторизирано користење на DNS протокол од страна на DGA-базиран малвер, напредни P2P протокол аналитики, и пасивен мониторинг на криптиран сообраќај 14. Системот мора обезбеди информации за активни и неактивни хостови, статистика за топ најактивни хостови и сервиси на линк, искористеност на линкови, информација дали одреден хост користи специфичен сервис и клиентска апликација, искористеност на TCP/UPD порти, трендови на мрежен сообраќај. 15. Дополнителни безбедносни анализи за детекција на botnet и други софистицирани напади преку корелација со реномиран глобален threat-intelligence сервис.
Мониторинг и Менаџмент:	1. Мониторинг на протокот се извршува речиси во реално време 2. Можност за брза откривање на безбедносни пропусти, со детекција на несоодветно однесување преку прегледност во искористување на мрежните ресурси (Policy Violation, Data Hoarding) 3. Детектираните инциденти да бидат мапирани во согласност со MITRE ATT&CK дефинираните тактики и техники. 4. Преземање на соодветни акции за сите детектирани инциденти од една централна точка 5. Вклучена поддршка за графички приказ и креирање на соодветни мапи на мрежната инфраструктура 6. Вклучена поддршка за преглед на целиот сообраќај помеѓу било кои два мрежни елементи 7. Вклучена поддршка за форензички анализи врз база на ревизорски траги од сите мрежни трансакции 8. Дефинирање на безбедносни настани согласно сопствени потреби врз основа на аномалии во сообраќајот 9. Креирање и испраќање на автоматски известувања и извештаи по случување на одредени аларми или безбедносни настани.
Програмабилност:	Можност за конфигурирање и мониторинг на системот преку т.н. API интерфејс
Серверски систем:	Понудувачот да понуди и препорачан Хардвер за инсталација на решението.

Интеграција во постоечка мрежа	1. Системот треба да се постави во постоечката мрежа така што ќе анализира сообраќај од Core свичевите и периметарскиот firewall. 2. Можност за надградба на капацитетот преку дополнителна лиценца или претплата со што би се овозможило дополнително анализирање на локалниот сообраќај од 18 трезорски канцеларии пред тој да пристигне на централната локација.
Гарантен рок:	1 годин за хардвер и за системски ажурирања и надградби
Поддршка:	Достапност на техничка помош од производителот мин. 8 часа x 5 дена со вклучен неограничен број на инциденти, како и бесплатна достава на надградби на потврдени грешки во оперативниот систем (функционални и сигурносни) кои се издаваат од страна на производителот на редовна временска основа, во времетраење на гарантниот период. Сите компоненти на решението мора да имаат 1 година одржување од страна на производителот како и неопходните лиценци за работа на решението.
Транспорт, инсталација и конфигурација:	Вклучени во цената

- <u>Рок на имплементација на решението е 15 работни денови по добивање на писмена порачка од договорниот орган.</u>

Напомена: Понудената опрема треба да е неупотребувана и нова, што се потврдува со официјален документ од производителот на понудената опрема. Секоја понуда на обновена (Refurbished) опрема се отфрла. Сериските броеви на испорачаната опрема ќе се проверуваат на веб страните на производителот на опремата за да се утврди дека станува збор за нова и претходно неупотребувана опрема.

Понудувачот задолжително со понудата треба да достави Овластување/авторизација MAF (Manufacturer Authorisation Form) издадена од производителот на понудената опрема за продажба и одржување на предметот на набавката на територијата на Република Северна Македонија, во спротивно пондата ќе биде отфрлена како неприфатлива.

При потреба од интервенција за предметната набавка, задолжително е физичко присуство во седиштето на Министерството за финансии на стручното лице/ата кое ги исполнува/ат критериумите од техничката и професионална способност. Он лајн и виртуелно поврзување не е дозволено.