Друштво за трговија и услуги
БОСОН СОЛУШНС ДОО експорт-импорт
Бр. 0307/25-1
26.11 2025 год.
СКОПЈЕ

Архивски број: 03-12237/1
Датум: 25-11-2025

ДОГОВОР
за јавна набавка на стоки – Систем за управување со дата-центар мрежна безбедност

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. Друштво за трговија и услуги БОСОН СОЛУШНС ДОО експорт-импорт Скопје со седиште на ул.„Орце Николов" бр.109А во Скопје, претставувано од Мирослав Хаџи-Велков, управител во натамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на стоки – Систем за управување со дата-центар мрежна безбедност, 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, по претходно спроведена отворена постапка, по оглас број 16161/2025.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната вредност на договорот без пресметан данок на додадена вредност изнесува 6.725.000,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 1.210.500,00 денари.

Вкупната вредност на договорот со пресметан данок на додадена вредност изнесува 7.935.500,00 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

При реализација на договорот за јавна набавка не се предвидува корекција на цените, односно цените искажани во понудата на носителот на набавката ќе бидат фиксни за целото времетраење на договорот за јавна набавка.

IV. ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Овој договор започнува да важи од денот на потпишувањето на истиот од двете договорни страни, па се до истекот на важноста на лиценците за Системот за управување со дата-центар мрежна безбедност, која е во времетраење од 12 (дванаесет) месеци.

V. НАЧИН, МЕСТО И РОК НА ИСПОРАКА

Член 5

Предметот на договорот вклучува испорака, инсталација, конфигурација на Систем за управување со дата-центар мрежна безбедност, како и хардверска и софтверска претплата во период од 12 месеци, сметано од денот на целосната инсталација и ставање во употреба на системот, согласно со техничките спецификации (Прилог 2).

Носителот на набавката е должен да го испорача, инсталира и конфигурира предметот на договорот во рок од 45 (четириесет и пет) дена од денот на приемот на писмена порачка од договорниот орган.

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

Работниот налог/Записникот 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 предметот на договорот, носителот на набавката ги вклучува лицата од стручниот кадар за извршување 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 техничката и професионалната способност 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 извршувањето на предметот на договорот 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 испорака, 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 2 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 за ваков предмет на договор.

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 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 предметот на договорот.

Договорниот орган се обврзува дека плаќањето на носителот на набавката ќе го изврши во рокот од член 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 5% 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 орган.

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 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 договорни 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:	Носител на набавката:
Република Северна Македонија	Друштво за трговија и услуги
Министерство за финансии	БОСОН СОЛУШНС ДОО
Скопје	експорт-импорт Скопје
Министер за финансии	Управител
м-р Гордана Димитриеска-Кочоска	Мирослав Хаџи-Велков

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

Прилог 1

Образец на понуда

Врз основа на огласот 16161/2025 објавен од страна на Министерство за Финансии, за Систем за управување со дата-центар мрежна безбедност, со спроведување на набавка од Отворена постапка, и тендерската документација, ја поднесуваме следнава:

П О Н У Д А

Дел I – Информации за понудувачот

I.1. Име на понудувачот: Друштво за трговија и услуги БОСОН СОЛУШНС ДОО експорт-импорт Скопје

I.2. Контакт информации

- Адреса: ОРЦЕ НИКОЛОВ 109А
- Телефон:070222971
- Факс:
- Е-пошта: miroslav.hadzi-velkov@boson-solutions.com
- Лице за контакт: Мирослав Хаџи-Велков

I.3. Одговорно лице: Мирослав Хаџи-Велков

[redacted]Д Скопје

Елементи на понудата

- Потврда дека не е отворена постапка за стечај од надлежен орган
- Потврда дека не е отворена постапка за ликвидација од надлежен орган

- Потврда од Регистарот на казни за сторени кривични дела на правните лица дека не му е изречена споредна казна забрана за учество во постапки за јавен повик, доделување на договори за јавна набавка и договори за јавно-приватно партнерство
- Потврда од Регистарот на казни за сторени кривични дела на правните лица дека не му е изречена споредна казна привремена или трајна забрана за вршење на одделна дејност
- Уверение дека со правосилна пресуда не му е изречена прекршочна санкција - забрана за вршење на професија, дејност или должност, односно привремена забрана за вршење одделна дејност
- Потврда за платени даноци, придонеси и други јавни давачки од надлежен орган од земјата каде економскиот оператор е регистриран
- Изјава дека во последните 5 години не е изречена правосилна судска пресуда за сторено кривично дело од член 88 став 1 од ЗЈН
- Документ за регистрирана дејност
- со листа на главни испораки на стоки или извршени услуги со вредности, датуми, купувачи (договорни органи или економски оператори), со обезбедување потврда за извршени испораки или извршени услуги
- со опис на техничкиот персонал и техничките органи кои ќе учествуваат во извршувањето на јавната набавка, особено на оние кои се одговорни за контролата на квалитетот, а во случај на јавна набавка на работи, оние што ќе бидат вклучени во изведување на работите, без оглед на тоа дали се вработени во економскиот оператор или не
- Стандарди за системи за квалитет
- Изјава за сериозност
- Техничка понуда
- Финансиска понуда

**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.*

ТЕХНИЧКА ПОНУДА

Согласни сме да ви го обезбедиме предметот на набавка - Систем за управување со дата-центар мрежна безбедност во се според барањата дефинирани во техничките спецификации кои се составен дел од тендерската документација.

Понудувачот заедно со понудата задолжително треба да достави Технички опис на понудената опрема со приложен проспектен материјал со референца во проспектниот материјал каде што може да се види бараната техничка карактеристика (Број на страна и маркиран текст во проспектниот материјал каде што може да се види бараната техничка карактеристика), Овластување/ авторизација MAF (Manufacturer Authorisation Form) издадена од производителот на понудената опрема, каде треба да биде назначено името на авторизираниот понудувач (економски оператор) за ставките/стоките кои се бараат согласно техничката спецификација и официјален документ од производителот на понудената опрема дека опремата е неупотребувана и нова, во спротивно понудата ќе биде отфрлена како неприфатлива.

1. Безбедносен уред за заштита на кампус и Дата Центар – кол. 2

Елементи/ функционалност	Минимални технички карактеристики	Понудено: Quantum Force 9200 Base Appliance with SandBlast subscription
Достапност:	Уредите треба да можат да бидат имплементирани во решение со висока достапност (HA)	Уредите можат да бидат имплементирани во решение со висока достапност (HA). Документ: "quantum-force-9200-datasheet.pdf", страница 4 и "Техничка спецификација на понудената опрема.pdf"
Интерфејси:	Минимум 8 x 1GbE RJ-45 мрежни приклучоци.	8 x 1GbE RJ-45 мрежни приклучоци. Документ: "quantum-force-9200-datasheet.pdf", страница 4 и 5
	Минимум 4 x 10GBase-F SFP+ / 25GBase-F SFP28 оптички порти со минимум 2x10GBase-SR SFP+ примопредаватели.	4x 10GBase-F SFP+ / 25GBase-F SFP28 оптички порти и 2x10Gbase-SR SFP+ примопредаватели Документ: "quantum-force-9200-datasheet.pdf", страница 3 и 5 и "Техничка спецификација на понудената опрема.pdf"
Напојување:	Уредот треба да има редундантно AC напојување.	Уредот има редундантно AC напојување. Документ: "quantum-force-9200-datasheet.pdf", страница 4
Складирање на податоци и логови:	Интегриран HDD SSD SATA диск со капацитет од најмалку 384 GB.	Уредот има интегриран HDD SSD SATA диск со капацитет од 480 GB. Документ: "quantum-force-9200-datasheet.pdf", страница 3
Работна меморија:	Минимум 32 GB RAM меморија.	Понудениот уред има 32 GB RAM меморија. Документ: "quantum-force-9200-datasheet.pdf", страница 3 и "Техничка спецификација на понудената опрема.pdf"
Истовремени сесии:	минимум 7 милиони истовремени сесии	7,27 милиони истовремени сесии. Документ: "quantum-force-9200-datasheet.pdf", страница 3
Нови конекции/сесии во секунда:	Минимум 240000 конекции во секунда	250 000 конекции во секунда. Документ: "quantum-force-9200-datasheet.pdf", страница 3
Firewall со IPS комбинирано:	Најмалку 18 Gbps NGFW (Firewall, контрола на апликации и IPS) пропусна моќ	19 Gbps NGFW (Firewall, контрола на апликации и IPS) пропусна моќ. Документ: "quantum-force-9200-datasheet.pdf", страница 3

Firewall со целосна заштита од закани комбинирано:	Најмалку 6,5 Gbps пропусна моќ при целосна заштита од закани	8 Gbps пропусна моќ при целосна заштита од закани. Документ: "quantum-force-9200-datasheet.pdf", страница 3
Вклучени лиценци за:	Лиценци за: Систем за превенција на упади и Контрола на апликации. Овие безбедносни функционалности мора да бидат лиценцирани и активни за имплементација и работа. Времетраење на лиценците: мин. 1 година	Вклучени лиценци за: Систем за превенција на упади и Контрола на апликации. Овие безбедносни функционалности се лиценцирани и активни за имплементација и работа. Времетраење на лиценците: 1 година Документ: "Техничка спецификација на понудената опрема.pdf"
Firewall к-ки:	Перформанси: најмалку 55 Gbps пропусна моќ на огнениот ѕид Режим на работа во Layer 2 (transparent) и Layer 3 (routing). Понуденото решение треба да поддржува: 1. Reverse-proxy функционалност 2. Користење на динамички правила (полиси) базирани на корисници или група на корисници 3. Интеграција со Microsoft Active Directory со цел добивање на кориснички идентитет 4. Можност за добивање кориснички идентитет со автентикација на корисници преку веб прелистувач за недоменски корисници; 5. Можност за креирање на виртуелни инстанци на огнен ѕид	60 Gbps пропусна моќ на огнениот ѕид. Документ: "quantum-force-9200-datasheet.pdf", страница 3 Режим на работа во Layer 2 (transparent) и Layer 3 (routing) Документ: "quantum-force-9200-datasheet.pdf", страница 4 Понуденото решение поддржува: 1. Reverse-proxy функционалност. Документ: "CP_R81.10_MobileAccess_AdminGuide.pdf", страница 235 2. Користење на динамички правила (полиси) базирани на корисници или група на корисници. Документ: "check-point-identity-awareness-datasheet.pdf", страница 2 3. Интеграција со Microsoft Active Directory со цел добивање на кориснички идентитет. Документ: "check-point-identity-awareness-datasheet.pdf", страница 2 4. Можност за добивање кориснички идентитет со автентикација на корисници преку веб прелистувач за недоменски корисници. Документ: "check-point-identity-awareness-datasheet.pdf", страница 3 5. Можност за креирање на виртуелни инстанци на огнен ѕид. Документ: "check-point-appliance-comparison-chart.pdf", страница 7
IPSec VPN:	1. Перформанси на IPSec VPN: мин. 26 Gbps VPN пропусна моќ со AES-GCM шифрирање	1. 28,6 Gbps IPSec VPN пропусна моќ со AES-GCM шифрирање. Документ: "quantum-force-9200-datasheet.pdf", страница 4 2. Поддршка за Site-to-site IPsec VPN. Документ: "CP_R81.20_SitetoSiteVPN_AdminGuide.pdf", страница 21

	2. Поддршка за Site-to-site IPsec VPN 3. Можност за VPN автентикација со сертификати 4. IPSec NAT Traversal 5. Воспоставување на VPN во случај на динамички ИП адреси	3. Можност за VPN автентикација со сертификати. Документ: "CP_R81.20_SitetoSiteVPN_AdminGuide.pdf", страница 38 4. IPSec NAT Traversal Документ: "CP_R81.20_SitetoSiteVPN_AdminGuide.pdf", страница 187 5. Воспоставување на VPN во случај на динамички ИП адреси . Документ: "CP_R81.20_SitetoSiteVPN_AdminGuide.pdf", страница 106
Далечински пристап од надвор:	Мора да обезбеди оддалечен пристап за корисниците до локалната мрежа со користење на client и clientless VPN за најмалку 4 истовремени корисници Моделот на лиценцирање мора да биде по принципот на број на истовремени корисници, а не по број на вкупни корисници	Понудениот уред може да обезбеди оддалечен пристап за корисниците до локалната мрежа со користење на client и clientless VPN за 5 истовремени корисници. Моделот на лиценцирање е по принципот на број на истовремени VPN корисници, а не по број на вкупни корисници. Документ: "Check Point VPN License Guide.pdf" и "Техничка спецификација на понудената опрема.pdf"
Превенција од упад:	1. Минимум поддршка на следниве механизми на детекција: аномалии на протоколи, анализа базирана на однесување, искористување на потписи (signatures exploit) 2. Креирање на правила коишто овозможуваат изземање на мрежи (network exceptions) за IPS анализа на основа на: source и destination IP адреси, сервиси и/или комбинација на претходните три опции 3. Детекција и блокирање на апликации за далечинска контрола	Понудениот уред има: 1. Поддршка на следниве механизми на детекција: аномалии на протоколи, анализа базирана на однесување, искористување на потписи (signatures exploit). Документ: "intrusion-prevention-system-ips-datasheet.pdf", страница 1 2. Можност за креирање на правила кои што овозможуваат изземање на мрежи (network exceptions) за IPS анализа на основа на: source и destination IP адреси, сервиси и/или комбинација на претходните три опции. Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 134 3. Детекција и блокирање на апликации за далечинска контрола. Документ: "ds-anti-bot.pdf"
Контрола на апликации:	1. Препознавање на минимум 9 000 Интернет апликации 2. Инспекција на SSL шифриран сообраќај во дојдовна и појдовна насока	Понудениот уред обезбедува: 1. Препознавање на над 10000 Интернет апликации. Документ: "CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf", страница 288 и "AppWiki _ Check Point Software.pdf" 2. Инспекција на SSL шифриран сообраќај во дојдовна и појдовна насока. Документ:

		"CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf", страница 457
Препознавање и контрола на типот на содржина:	1. Препознавање и контрола на типот на содржината што се испраќа односно презема 2. Решението мора да ги поддржува минимум следниве типови на содржина: a. Архиви (zip, 7z, gzip, RAR/ WinRAR); b. Слики (bmp, gif, png); c. Word (docx, odt, doc, rtf, one); d. Spreadsheet (xlsx, xls, ods); e. Presentation (pptx, ppt, odp, otp)	Понудениот уред има можност за: 1. Препознавање и контрола на типот на содржината што се испраќа односно презема. Документ: "ATRG_ Content Awareness (CTNT).pdf", страница 1 2. Поддршка на следниве типови на содржина: a. Архиви (zip, gzip, tar, java, RAR и WinRAR) b. Слики (bmp, gif, png) c. Word (docx, odt, doc, rtf, one) d. Spreadsheet (xlsx, xls, ods) e. Presentation (pptx, ppt, odp, otp) Документ: "Supported file types in Content Awareness Software Blade.pdf"
URL филтрирање:	Со докупување на соодветна лиценца, решението треба да поддржува on-prem URL филтрирање на самите уреди со: 1. Можност за контрола на пристапот до URL страници и апликации врз база на нивна категоризација. 2. Можност да користи правила за URL филтрирање со цел да му овозможи на администраторот грануларна контрола на HTTPS инспекцијата	Со докупување на соодветна лиценца, понудениот уред има можност за: 1. контрола на пристапот до URL страници и апликации врз база на нивната категоризација. Документ: "ATRG_ URL Filtering.pdf", страница 1 2. користење правила за URL филтрирање со цел да му овозможи на администраторот грануларна контрола на HTTPS инспекцијата. Документ: "ATRG_ URL Filtering.pdf", страница 2
Мрежен Анти-вирус и Anti-bot заштита:	Со докупување на соодветна лиценца, решението треба да	Со докупување на соодветна лиценца, решението поддржува on-prem Anti-Virus и Anti-Bot заштита кое се прави на самите безбедносни уреди и е со следниве карактеристики:

	поддржува on-prem Anti-Virus и Anti-Bot заштита кое се прави на самите безбедносни уреди и е со следниве карактеристики: 1. Anti-bot заштитата мора да има можност за: a. детекција и блокирање на сомнително (малициозно) однесување во мрежата; b. скенирање на интерна мрежа со цел детекција на бот активности; c. детекција и блокирање на пристап до малициозни домени или URL адреси врз база на нивната репутација; 2. Анти-вирус заштитата мора да има можност за: a. скенирање на архиви; b. за блокирање пристап на злонамерни URL страници; c. инспекција на SSL шифриран сообраќај;	: 1. Anti-bot функционалност со можност за: a. детекција и блокирање на сомнително (малициозно) однесување во мрежата. Документ: "ds-anti-bot.pdf", страница 1-2 b. скенирање на интерна мрежа со цел детекција на бот активности. Документ: "ds-anti-bot.pdf", страница 1-2 c. детекција и блокирање на пристап до малициозни домени или URL адреси врз база на нивната репутација. Документ: "ds-anti-bot.pdf", страница 1-2 2. Анти-вирус функционалност со можност за: a. скенирање на архиви. Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 88 b. за блокирање пристап на злонамерни URL страници. Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 28 c. инспекција на SSL шифриран сообраќај. Документ: "CP_R81.20_Quantum_SecurityManagement_AdminGuide.pdf", страница 457
Anti-spam заштита:	Со докупување на соодветна лиценца, решението треба да има можност за on-prem Anti-spam заштитата која се прави на самите уреди и е со можност за детекција на спам e-mail пораки по следните критериуми: 1. Content based Anti-Spam 2. IP Reputation Anti-Spam 3. Block List Anti-Spam 4. Mail Anti-Virus	Со докупување на соодветна лиценца, решението има Anti-spam заштитата со можност за детекција на спам e-mail пораки по следните критериуми: 1. Content based Anti-Spam 2. IP Reputation Anti-Spam 3. Block List Anti-Spam 4. Mail Anti-Virus 5. Zero Hour Malware Protection 6. IPS for mail protection Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 343

	5. Zero Hour Malware Protection 6. IPS for mail protection	
Заштита од непознати злонамерни програми за коишто не постојат анти-вирусни дефиниции врз база на локално Sandbox решение:	Со докупување на соодветна лиценца, решението треба да има можност за zero-day заштита врз база на Cloud Sandbox технологија, обезбедувајќи заштита од закани кои доаѓаат по пат на: HTTP, HTTPS, FTP, SMTP и SMTP TLS сообраќај; Решението мора да има можност за: 1. скенирање на линкови во електронска пошта за zero-day напади т.е. непознати злонамерни програми; 2. емулирање на извршни датотеки, архиви, документи, JAVA и Flash апликации, т.е. најмалку на следниве типови на датотеки: doc, docx, dot, dotm, dotx, exe, jar, pdf, potx, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, gz, cab, csv, cmd, jse, vba, vbe, vbs, wsf, wsh, pif, cpl, од кои cmd, jse, vba, vbe, vbs wsf и wsh кога доаѓаат прикачени како архива во e-mail. 3. отстранување на активни и потенцијално злонамерни делови од документот и безбедниот документ да го достави на крајниот	Со докупување на соодветна лиценца, понудениот уред има можност за zero-day заштита врз база на Cloud Sandbox технологија за заштита од закани кои доаѓаат по пат на: HTTP, HTTPS, FTP, SMTP и SMTP TLS сообраќај. Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 29 и "Техничка спецификација на понудената опрема.pdf" Решението има можност за: 1. скенирање на линкови во електронска пошта за zero-day напади т.е. непознати злонамерни програми; Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 58 2. емулирање на извршни датотеки, архиви, документи, JAVA и Flash апликации, т.е. најмалку на следниве типови на датотеки: doc, docx, dot, dotm, dotx, exe, jar, pdf, potx, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, gz, cab, csv, cmd, jse, vba, vbe, vbs wsf и wsh кога доаѓаат прикачени како архива во e-mail. Документ: "File types supported by Threat Emulation.pdf" 3. отстранување на активни и потенцијално злонамерни делови од документот и безбедниот документ да го достави на крајниот корисник по пат на електронска пошта пред емулацијата, а истовремено да го прати оригиналниот документ/датотека на емулација; Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 30 4. Преземање на оригиналниот документ ако истиот не е злонамерен. Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 30-31, 103 5. Anti-evasion техника за блокирање на активностите на malware-от кој сака да детектира емулација на виртуелна машина и да ги сокрие своите злонамерни активности. CP_R81.20_ThreatPrevention_AdminGuide.pdf.pdf, страница 29 Документ: "Threat Emulation Engine Release Updates.pdf", страница 1-4

	корисник, а истовремено да го прати оригиналниот документ - датотека на емулација; 4. Преземање на оригиналниот документ ако истиот не е злонамерен. 5. Можност за anti-evasion техника односно блокирање на malware-от кој сака да детектира емулација на виртуелна машина и да ги сокрие своите злонамерни активности;	
Zero Phishing:	Со докупување на соодветна лиценца, понуденото решение мора да има можност да обезбеди заштита од познати и непознати phishing напади на Веб страниците во реално време.	Со докупување на соодветна лиценца, понудениот уред има можност да обезбеди заштита од познати и непознати phishing напади на Веб страниците во реално време. Документ: "CP_R81.20_ThreatPrevention_AdminGuide.pdf", страница 31
Димензија и инсталација:	Rack mountable – сите додатоци мора да бидат вклучени. Сите кабли потребни за инсталација мора да бидат обезбедени.	Понудените уреди се вградливи во rack и сите додатоци за тоа се вклучени во понудата. Истот така, сите кабли потребни за инсталација ќе бидат обезбедени. Документ: "CP_9000_Appliances_GettingStartedGuide.pdf", страница 36
Управување:	Управувањето со уредите и полисите кои се аплицирани на нив треба да може да се направи од постоечката Security Management Server апликација за управување или да се понуди решение кое треба да ги има минимум следниве карактеристики: 1. креирање на безбедносни правила, собирање, чување и преглед на записи од сите безбедносни функционалности: FireWall, IPS,	Управувањето со понудедните безбедносни уреди за заштита ќе се направи од постоечката Security Management Server апликација.

	URL филтрирање, контрола на апликации, анти-вирус и anti-bot, zero-day заштита; 2. графички интерфејс за прикажување колку пати безбедносно правило било користено; 3. механизам за верификација на безбедносните полиси пред инсталација на полисата; 4. креирање на ревизии на безбедносните полиси и можност за враќање на таа ревизија; 5. едноставно и брзо креирање на безбедносни правила со користење на повлекување на објектите (drag and drop) во безбедносното правило; 6. групирање на безбедносните правила во нивоа и креирање под правила во одредено ниво; 7. креирање на повеќе администраторски корисници, повеќе администраторски профили со различни привилегии, при што администраторите можат истовремено да работат на исто безбедносно правило без меѓусебно прекинување на работата (промена на правилата и инсталација на правила); 8. креирање на администраторски	

	корисници во зависно од неговата улога; на пример, администратори кои имаат само можност за следење на: записи, URL правила, IPS правила, итн. 9. механизам за креирање на напредни извештаи и статистики, со корелација на настани од складираните лог записи без користење на дополнителни ресурси (имплементација на истиот уред каде што се наоѓа апликацијата за управување).	
Гарантен рок и системски надградби:	Мин. 1 година за хардвер и за системски ажурирања и надградби.	Понудениот уред има гаранција од 1 година за хардверот и за системски ажурирања и надградби. "Техничка спецификација на понудената опрема.pdf"
Поддршка:	Достапност на техничка помош од производителот по принцип најмалку 24 часа x 7 дена со вклучен неограничен број на инциденти, како и бесплатна надградба 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 едногодишно одржување од страна на производителот како и неопходните лиценци за работа и преземање на нови дефиниции.	Во понудата е вклучена техничка помош од производителот по принцип најмалку 24 часа x 7 дена со неограничен број на инциденти, како и бесплатна надградба 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 едногодишно одржување од страна на производителот како и неопходните лиценци за работа и преземање на нови дефиниции. Документ: "checkpoint-support-datasheet.pdf"

2. **Лиценци за собирање и менаџирање на мрежна телеметрија - кол. 1400**

Елементи/ функционалност	**Минимални технички карактеристики**	**Понудено**
Скалабилност:	Понуденото решение, потребно е истото да ги исполнува следните барања за 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	1. Системот е издвоен во три апликациски целини имплементирани на 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 Во вашата инфраструктура е веќе инсталиран системот со 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: "Cisco Secure Network Analytics (formerly Stealthwatch) Data Sheet.pdf" страна 8 "Data Store", страна 9 "Flow Rate License"

	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	1. Поддржува IPFIX, Netflow или еквивалентен протокол, дефиниран како отворен стандард 2. Собира информации од повеќе типови и производители на мрежни уреди 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,	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

	без потреба од негова декрипција	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	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,

	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 геo-локациски информации за сообраќајот кон и од конкретни земји. 11. Системот мора да детектира и алармира врз база на различни атрибути – времетраење на	преку идентификација на уреди/корисници и нивно мрежно деактивирање. 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

	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	(formerly Stealthwatch) Data Sheet.pdf, страна 5, Key Bennefits 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

	и други софистицирани напади преку корелација со реномиран глобален threat-intelligence сервис.	14. Од целосната достапна телеметрија, системот овозможува креирање на "flow search" извештаи за најразлични намени, како на пример мрежна искористеност. 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	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 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

	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.	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
Интеграција во постоечка мрежа	1. Лиценците треба да се активираат на системот за безбедносна анализа на сообраќај Cisco Secure Network Analytics, или да се понуди решение со	1. Лиценците ќе се активираат на системот кој е веќе поставен во постоечката мрежа. 2. Системот има можност за надградба на капацитетот преку зголемување на Flow Rate лиценцата што би овозможило анализирање на дополнителна телеметрија.

	горенаведените карактеристики 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.	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"
Рок на важност на лиценците:	1 година	Лиценците кои се вклучени во понудата се се со рок важност од 1 година Документ: "Техничка спецификација на понудената опрема.pdf"
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 лиценци неопходни за работа на решението.

3. **Агрегациски преклопници – кол. 2**

Елементи/ функционалност	**Минимални технички карактеристики**	**Понудено:** **C9200L-24T-4G-E**
Хардверски карактеристики	Уредот треба да има минимум капацитет на преклопување од 50Gbps во единечен режим и 130Gbps при групирање(stacking)	Уредот има минимум капацитет на преклопување од 56Gbps во единечен режим и 136Gbps при групирање(stacking) Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 15.
	Уредот треба да има минимум брзина на префрлање пакети од 40Mpps во единечен режим и 100Mpps при групирање (stackig)	Уредот има брзина од 41,67Mpps во единечен режим и 101Mpps при групирање(stackig). Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 15.
	Уредот треба да има минимум 4 x 1Gb uplink порти со опција за бакарен или оптички конектор.	Уредот има 4 x 1GB uplink порти со опција за бакарен или оптички конектор. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 7.
	Уредот треба да биде со големина од максимум 1 RU.	Уредот е со големина од 1 RU. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 24.
	Уредот да има минимум 2 GB RAM меморија.	Уредот има 2 GB RAM меморија. Документ:

		Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 14.
	Уредот да има минимум 4 GB Flash меморија.	Уредот има 4 GB Flash меморија. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 14.
Скалабилност	Уредот да има можност да се надогради со функција за групирање (stacking) со минимум 8 уреди во група. Минимален проток помеѓу уредите од 80Gbps.	Уредот има можност да се надогради со функција за групирање (stacking) со минимум 8 уреди во група. Минимален проток помеѓу уредите од 80Gbps. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 12.
Софтверски Карактеристики	Уредот да поддржува минимум 15 000 MAC адреси.	Уредот поддржува 16 000 MAC адреси. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 14.
	Уредот да поддржува минимум 4000 број на VLAN-и	Уредот поддржува 4096 број на VLAN-и. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 14.
	Уредот да поддржува минимум 10 000 број на рути.	Уредот поддржува 11 000 број на рути. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 14.

	Уредот да поддржува Flexible NetFlow.	Уредот поддржува Flexible NetFflow. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 18.
Quality of Service	Уредот да ги поддржува минимум следните типови на QoS:	Уредот ги поддржува минимум следните типови на QoS:
	- 802.1p Class of Service	802.1p Class of Service, Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 18.
	- Differentiated Services Code Point (DSCP)	Differentiated Services Code Point (DSCP), Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 18.
	- Shaped Round Robin (SRR)	Shaped Round Robin (SRR), Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 18.
	- Committed Information Rate (CIR)	Committed Information Rate (CIR). Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 18.
Контрола на инвентар	Уредот да има вграден RFID tag за едноставен asset management со користење на стандарден RFID читач.	Уредот има вграден RFID tag за едноставен asset management со користење на стандарден RFID читач. Документ:

		Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 19.
Безбедност во транспорт	Уредот да подджува MACsec со AES-128 алгоритам.	Уредот поддржува MACsec со AES-128 алгоритам. Документ: Cisco Catalyst 9200 Series Switches Data Sheet.pdf, страна 4.
Гаранција	24 месеци хардверска и софтверска гаранција и поддршка на уредот од производителот на опремата, која опфаќа и бесплатни upgrade-и на околината.	24 месеци хардверска и софтверска гаранција и поддршка на уредот од производителот на опремата, која опфаќа и бесплатни upgrade-и на околината. Документ: Техничка спецификација на понудената опрема.pdf sntc-datasheet.pdf
	24 месеци одржување на уредот од страна на понудувачот со информирање и препорачување за upgrade на верзиите на software/firmware на сите елементи на системот. Проактивно одржување на сите елементи на уредот.	24 месеци одржување на уредот од страна на понудувачот со информирање и препорачување за upgrade на верзиите на software/firmware на сите елементи на системот. Проактивно одржување на сите елементи на уредот. Документ: Техничка спецификација на понудената опрема.pdf sntc-datasheet.pdf
	Бесплатна замена на делови во рамки на гаранцискиот период и бесплатни upgrade-и на софтвер на системот.	Бесплатна замена на делови во рамки на гаранцискиот период и бесплатни upgrade-и

		на софтвер на системот. Документ: Техничка спецификација на понудената опрема.pdf sntc-datasheet.pdf

НАПОМЕНА 1: Задолжително да се пополнат празните полиња во колоната „Понудено“ во табелите во спротивно понудата ќе се отфрли како неприфативa.

НАПОМЕНА 2: Економскиот оператор ја потпишува со валиден дигитален сертификат и прикачува техничката понуда во моментот на поднесување на понудата како дел од целокупната документација.

Недоставувањето на техничка понуда е основ за отфрлање на понудата.

Прилог 2

ТЕХНИЧКИ СПЕЦИФИКАЦИИ
за јавна набавка на стоки –
Систем за управување со дата-центар мрежна безбедност

Предмет на оваа јавна набавка е следното:

- Инсталација на нови безбедносни уреди за заштита на кампусот и Дата Центарот.
- Набавка и инсталација на лиценци за собирање и менаџирање на мрежна телеметрија
- Замена на два агрегациски преклопници

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

- Набавка, инсталација и конфигурација на два безбедносни уреди на влез во примарниот Дата Центар, во режим на висока достапност и согласно најдобрите пракси дефинирани од страна на производителот. Со позиционирањето на ова решение во инфраструктурата на МФ, целта е да се имплементира сегментација и диференцирање на различните безбедносни политики на посебен дедициран безбедносен систем, кој би ги издвоил кампусот и дата центар мрежата и контролата на пристапот до нив од останатиот дел од мрежната инфраструктура.

  Понудените безбедносни уреди треба да можат да се менаџираат со постоечката Check Point апликација за управување или за нив да се обезбеди нов алтернативен начин на управување со соодветни карактеристики за policy management, event management и корелација на безбедносните логови согласно потребите.

  Инсталацијата и конфигурацијата треба да се изврши во претходна координација со договорниот орган за да се запазат безбедносните практики и да се постигне што помал прекин на сервисите на договорниот орган.
- Набавка и инсталација на лиценци за собирање, менаџирање и анализа на мрежна телеметрија. Предмет на оваа набавка е овозможување на системот за безбедносна анализа на сообраќај да може да обработува мрежна телеметрија со капацитет од 1400 мрежни текови во секунда, со цел зголемена прегледност на мрежниот сообраќај како и напредно и автоматско откривање и спречување на закани.
- Набавка, инсталација и конфигурација на два агрегациски преклопници - предмет на оваа набавка, со кои ќе се заменат два постоечки, согласно најдобрите пракси дефинирани од страна на производителите. Замената треба да се изврши во претходна координација со договорниот орган за да се запазат безбедносните практики и да се постигне што помало влијание при замената на уредите.

  Напомена: Во понудената цена треба да се вклучени трошоците за транспорт, инсталација и конфигурација, како и сите други трошоци поврзани со предметот на набавката.

1. **Безбедносен уред за заштита на кампус и Дата Центар – кол. 2**

Елементи/ функционалност	Минимални технички карактеристики
Достапност:	Уредите треба да можат да бидат имплементирани во решение со висока достапност (HA)
Интерфејси:	Минимум 8 x 1GbE RJ-45 мрежни приклучоци.
	Минимум 4 x 10GBase-F SFP+ / 25GBase-F SFP28 оптички порти со минимум 2x10GBase-SR SFP+ примопредаватели.
Напојување:	Уредот треба да има редундантно AC напојување.
Складирање на податоци и логови:	Интегриран HDD SSD SATA диск со капацитет од најмалку 384 GB.
Работна меморија:	Минимум 32 GB RAM меморија.
Истовремени сесии:	минимум 7 милиони истовремени сесии
Нови конекции/сесии во секунда:	Минимум 240000 конекции во секунда
Firewall со IPS комбинирано:	Најмалку 18 Gbps NGFW (Firewall, контрола на апликации и IPS) пропусна моќ
Firewall со целосна заштита од закани комбинирано:	Најмалку 6,5 Gbps пропусна моќ при целосна заштита од закани
Вклучени лиценци за:	Лиценци за: Систем за превенција на упади и Контрола на апликации. Овие безбедносни функционалности мора да бидат лиценцирани и активни за имплементација и работа. Времетраење на лиценците: мин. 1 година
Firewall к-ки:	Перформанси: најмалку 55 Gbps пропусна моќ на огнениот ѕид Режим на работа во Layer 2 (transparent) и Layer 3 (routing). Понуденото решение треба да поддржува: 1. Reverse-proxy функционалност 2. Користење на динамички правила (полиси) базирани на корисници или група на корисници 3. Интеграција со Microsoft Active Directory со цел добивање на кориснички идентитет

	4. Можност за добивање кориснички идентитет со автентикација на корисници преку веб прелистувач за недоменски корисници; 5. Можност за креирање на виртуелни инстанци на огнен ѕид
IPSec VPN:	1. Перформанси на IPSec VPN: мин. 26 Gbps VPN пропусна моќ со AES-GCM шифрирање 2. Поддршка за Site-to-site IPsec VPN 3. Можност за VPN автентикација со сертификати 4. IPSec NAT Traversal 5. Воспоставување на VPN во случај на динамички ИП адреси
Далечински пристап од надвор:	Мора да обезбеди оддалечен пристап за корисниците до локалната мрежа со користење на client и clientless VPN за најмалку 4 истовремени корисници Моделот на лиценцирање мора да биде по принципот на број на истовремени корисници, а не по број на вкупни корисници
Превенција од упад:	1. Минимум поддршка на следниве механизми на детекција: аномалии на протоколи, анализа базирана на однесување, искористување на потписи (signatures exploit) 2. Креирање на правила коишто овозможуваат изземање на мрежи (network exceptions) за IPS анализа на основа на: source и destination IP адреси, сервиси и/или комбинација на претходните три опции 3. Детекција и блокирање на апликации за далечинска контрола
Контрола на апликации:	1. Препознавање на минимум 9 000 Интернет апликации 2. Инспекција на SSL шифриран сообраќај во дојдовна и појдовна насока
Препознавање и контрола на типот на содржина:	1. Препознавање и контрола на типот на содржината што се испраќа односно

	презема 2. Решението мора да ги поддржува минимум следниве типови на содржина: a. Архиви (zip, 7z, gzip, RAR/ WinRAR); b. Слики (bmp, gif, png); c. Word (docx, odt, doc, rtf, one); d. Spreadsheet (xlsx, xls, ods); e. Presentation (pptx, ppt, odp, otp)
URL филтрирање:	Со докупување на соодветна лиценца, решението треба да поддржува on-prem URL филтрирање на самите уреди со: 1. Можност за контрола на пристапот до URL страници и апликации врз база на нивна категоризација. 2. Можност да користи правила за URL филтрирање со цел да му овозможи на администраторот грануларна контрола на HTTPS инспекцијата
Мрежен Анти-вирус и Anti-bot заштита:	*Со докупување на соодветна лиценца*, решението треба да поддржува on-prem Anti-Virus и Anti-Bot заштита кое се прави на самите безбедносни уреди и е со следниве карактеристики: 1. Anti-bot заштитата мора да има можност за: a. детекција и блокирање на сомнително (малициозно) однесување во мрежата; b. скенирање на интерна мрежа со цел детекција на бот активности; c. детекција и блокирање на пристап до малициозни домени или URL адреси врз база на нивната репутација; 2. Анти-вирус заштитата мора да има можност за: a. скенирање на архиви; b. за блокирање пристап на злонамерни URL страници; c. инспекција на SSL шифриран сообраќај;
Anti-spam заштита:	Со докупување на соодветна лиценца, решението треба да има можност за on-prem Anti-spam заштитата која се прави на

	самите уреди и е со можност за детекција на спам e-mail пораки по следните критериуми: 1. Content based Anti-Spam 2. IP Reputation Anti-Spam 3. Block List Anti-Spam 4. Mail Anti-Virus 5. Zero Hour Malware Protection 6. IPS for mail protection
Заштита од непознати злонамерни програми за коишто не постојат анти-вирусни дефиниции врз база на локално Sandbox решение:	Со докупување на соодветна лиценца, решението треба да има можност за zero-day заштита врз база на Cloud Sandbox технологија, обезбедувајќи заштита од закани кои доаѓаат по пат на: HTTP, HTTPS, FTP, SMTP и SMTP TLS сообраќај; Решението мора да има можност за: 1. скенирање на линкови во електронска пошта за zero-day напади т.е. непознати злонамерни програми; 2. емулирање на извршни датотеки, архиви, документи, JAVA и Flash апликации, т.е. најмалку на следниве типови на датотеки: doc, docx, dot, dotm, dotx, exe, jar, pdf, potx, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, gz, cab, csv, cmd, jse, vba, vbe, vbs, wsf, wsh, pif, cpl, од кои cmd, jse, vba, vbe, vbs wsf и wsh кога доаѓаат прикачени како архива во e-mail. 3. отстранување на активни и потенцијално злонамерни делови од документот и безбедниот документ да го достави на крајниот корисник, а истовремено да го прати оригиналниот документ - датотека на емулација; 4. Преземање на оригиналниот документ ако истиот не е злонамерен. 5. Можност за anti-evasion техника односно блокирање на malware-от кој сака да детектира емулација на виртуелна

	машина и да ги сокрие своите злонамерни активности;
Zero Phishing:	Со докупување на соодветна лиценца, понуденото решение мора да има можност да обезбеди заштита од познати и непознати phishing напади на Веб страниците во реално време.
Димензија и инсталација:	Rack mountable – сите додатоци мора да бидат вклучени. Сите кабли потребни за инсталација мора да бидат обезбедени.
Управување:	Управувањето со уредите и полисите кои се аплицирани на нив треба да може да се направи од постоечката Security Management Server апликација за управување или да се понуди решение кое треба да ги има минимум следниве карактеристики: 1. креирање на безбедносни правила, собирање, чување и преглед на записи од сите безбедносни функционалности: FireWall, IPS, URL филтрирање, контрола на апликации, анти-вирус и anti-bot, zero-day заштита; 2. графички интерфејс за прикажување колку пати безбедносно правило било користено; 3. механизам за верификација на безбедносните полиси пред инсталација на полисата; 4. креирање на ревизии на безбедносните полиси и можност за враќање на таа ревизија; 5. едноставно и брзо креирање на безбедносни правила со користење на повлекување на објектите (drag and drop) во безбедносното правило; 6. групирање на безбедносните правила во нивоа и креирање под правила во одредено ниво; 7. креирање на повеќе администраторски корисници, повеќе администраторски

	профили со различни привилегии, при што администраторите можат истовремено да работат на исто безбедносно правило без меѓусебно прекинување на работата (промена на правилата и инсталација на правила); 8. креирање на администраторски корисници во зависно од неговата улога; на пример, администратори кои имаат само можност за следење на: записи, URL правила, IPS правила, итн. 9. механизам за креирање на напредни извештаи и статистики, со корелација на настани од складираните лог записи без користење на дополнителни ресурси (имплементација на истиот уред каде што се наоѓа апликацијата за управување).
Гарантен рок и системски надградби:	Мин. 1 година за хардвер и за системски ажурирања и надградби.
Поддршка:	Достапност на техничка помош од производителот по принцип најмалку 24 часа x 7 дена со вклучен неограничен број на инциденти, како и бесплатна надградба 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 едногодишно одржување од страна на производителот како и неопходните лиценци за работа и преземање на нови дефиниции.

2. **Лиценци за собирање и менаџирање на мрежна телеметрија - кол. 1400**

Елементи/ функционалност	**Минимални технички карактеристики**
Скалабилност:	Понуденото решение, потребно е истото да ги исполнува следните барања за 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
Интеграција во постоечка мрежа	1. Лиценците треба да се активираат на системот за безбедносна анализа на сообраќај Cisco Secure Network Analytics, или да се понуди решение со горенаведените карактеристики 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.
Рок на важност на лиценците:	1 година
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.

3. **Агрегациски преклопници – кол. 2**

Елементи/ функционалност	**Минимални технички карактеристики**
Хардверски карактеристики	Уредот треба да има минимум капацитет на преклопување од 50Gbps во единечен режим и 130Gbps при групирање(stacking)
	Уредот треба да има минимум брзина на префрлање пакети од 40Mpps во единечен режим и 100Mpps при групирање (stackig)
	Уредот треба да има минимум 4 x 1Gb uplink порти со опција за бакарен или оптички конектор.
	Уредот треба да биде со големина од максимум 1 RU.
	Уредот да има минимум 2 GB RAM меморија.
	Уредот да има минимум 4 GB Flash меморија.
Скалабилност	Уредот да има можност да се надогради со функција за групирање (stacking) со минимум 8 уреди во група. Минимален проток помеѓу уредите од 80Gbps.
Софтверски Карактеристики	Уредот да поддржува минимум 15 000 MAC адреси.
	Уредот да поддржува минимум 4000 број на VLAN-и
	Уредот да поддржува минимум 10 000 број на рути.
	Уредот да поддржува Flexible NetFlow.
Quality of Service	Уредот да ги поддржува минимум следните типови на QoS:
	- 802.1p Class of Service
	- Differentiated Services Code Point (DSCP)
	- Shaped Round Robin (SRR)
	- Committed Information Rate (CIR)
Контрола на инвентар	Уредот да има вграден RFID tag за едноставен asset management со користење на стандарден RFID читач.
Безбедност во транспорт	Уредот да подджува MACsec со AES-128 алгоритам.
Гаранција	12 месеци хардверска и софтверска гаранција и поддршка на уредот од производителот на опремата, која опфаќа и бесплатни upgrade-и на околината.

	12 месеци одржување на уредот од страна на понудувачот со информирање и препорачување за upgrade на верзиите на software/firmware на сите елементи на системот. Проактивно одржување на сите елементи на уредот.
	Бесплатна замена на делови во рамки на гаранцискиот период и бесплатни upgrade-и на софтвер на системот.

- <u>Рок на имплементација на решението е 45 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 заедно со понудата задолжително треба да достави Технички опис на понудената опрема со приложен проспектен материјал со референца во проспектниот материјал каде што може да се види бараната техничка карактеристика (Број на страна и маркиран текст во проспектниот материјал каде што може да се види бараната техничка карактеристика), Овластување/ авторизација MAF (Manufacturer Authorisation Form) издадена од производителот на понудената опрема, каде треба да биде назначено името на авторизираниот понудувач (економски оператор) за ставките/стоките кои се бараат согласно техничката спецификација и официјален документ од производителот на понудената опрема дека опремата е неупотребувана и нова, во спротивно понудата 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.