– Сектор за правни работи–

Друштво за комуникациски услуги А1 Македонија ДООЕЛ Скопје
Бр. 08-5960/1
29 -08- 2022
Скопје

Архивски број: 03-8938/1
Датум: 24 -08- 2022

ДОГОВОР
за јавна набавка на стоки -
софтвер за антивирусна заштита на корисници / сервер

Склучен помеѓу:

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

и

2. Друштво за комуникациски услуги А1 МАКЕДОНИЈА ДООЕЛ Скопје, со седиште на Плоштад Пресвета Богородица бр.1 во Скопје, претставувано од Стевчо Ристески, директор на бизнис и ИКТ продажба, во понатамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на овој договор е набавка на стоки – софтвер за антивирусна заштита на корисници /сервер - Sophos Central Intercept X Advancet with XDR (for Endpoint and server), по спроведената поедноставена отворена постапка за набавка по оглас бр.10800/2022.

Предметот на договорот опфаќа и инсталација на антивирусниот софтвер со вклучени лиценци за период од 1 (една) година, ремоте обука за користење на системот на вработените во договорниот орган, како и минимум 1 (еден) ден ремоте во месецот за консултации во времетраење на претплатата, во согласност со техничките спецификации (Прилог 1 кон Договорот) и понудата на носителот на набавката, прифатена од договорниот орган.

– Сектор за правни работи–

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната максимална вредност на договорот без пресметан данок на додадена вредност изнесува 870.130,00 денари.

Вкупниот износ на данокот на додадена вредност изнесува 43.506,50 денари.

Вкупната максимална вредност на договорот со пресметан данок на додадена вредност изнесува 913.636,50 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

Цените од член 2 се крајни, фиксни и непроменливи се до целосна реализација на договорот.

Во понудените цени се опфатени патните, дневните или евентуално други трошоци на носителот на набавката.

IV. НАЧИН И РОК НА ИСПОРАКА

Член 4

Носителот на набавката е должен софтверот да го испорача, инсталира и конфигурира во период од 10 (десет) календарски денови по добивање на писмената порачка од договорниот орган.

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

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 договорниот орган.

V. ГАРАНЦИЈА ЗА НАВРЕМЕНО И КВАЛИТЕТНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 5

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

– Сектор за правни работи–

Услов за потпишување на договорот со избраниот најповолен понудувач е обезбедување гаранција од страна на избраниот најповолен понудувач за квалитетно и навремено извршување на договорот во висина од 5% од вкупната максимална вредност на склучениот договор со пресметан ДДВ.

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

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

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

Гаранцијата за квалитетно и навремено извршување на договорот треба да биде издадена од банка.

Гаранцијата за квалитетно и навремено извршување на договорот носителот на набавката ја доставува заедно со потпишаниот договор во рок од 5 (пет) работни дена од денот на добивање на договорот од страна на договорниот орган.

Гаранцијата за квалитетно и навремено извршување на договорот се доставува во определениот рок, и тоа: по пошта или лично на лицето за контакт определено од страна на договорниот орган.

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

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

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

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

Договорниот орган ќе ја наплати гаранцијата за квалитетно и навремено извршување на договорот и доколку дојде до негово едностранo раскинување

поради неизвршување на обврските од договорот од страна на носителот на набавката.

Договорниот орган нема да бара активирање на банкарската гаранција за квалитетно и навремено извршување на договорот од банката која ја има издадено доколку носителот на набавката поради непредвидени околности (виша сила или други оправдани причини) не можел да ја изврши набавката што е предмет на овој договор, во кој случај носителот на набавката треба да достави писмено образложение до договорниот орган во кое ќе ги наведе причините за неизвршување или ненавремено извршување на набавката, а кое треба да биде писмено прифатено од договорниот орган.

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 на ул. „Даме Груев" бр.12 во Скопје.

Кон фактурата носителот на набавката задолжително доставува Работен налог / Записник согласно член 4 од овој договор 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 испорача стручно, навремено и квалитетно, врз основа на барањата на договорниот орган дефинирани во техничките спецификации кои се составен дел од овој договор и понудата прифатена од договорниот орган.

Носителот на набавката е должен да се придржува кон рокот за извршување на предметната набавка на стока, кој е дефиниран во член 4, став 1 од овој договор.

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

Носителот на набавката е должен веднаш по потпишување на договорот да му достави на договорниот орган податоци за лицата кои ќе бидат определени за реализација на предметната набавка.

– Сектор за правни работи–

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 се обврзува дека плаќањето на носителот на набавката ќе го врши во согласност со членот 6 на овој договор.

Договорниот орган се обврзува да му ги даде на располагање на носителот на набавката потребните податоци за непречено извршување на договорот, како и друга документација со која располага вклучувајќи ја комуникацијата и сите други информации и објаснувања кои се потребни на носителот на набавката.

IX. ВАЖНОСТ НА ДОГОВОРОТ

Член 9

Договорот е со важност од 12 (дванаесет) месеци сметано од денот на неговото потпишување од двете договорни страни.

X. ДОВЕРЛИВОСТ НА ИНФОРМАЦИИ И ПОДАТОЦИ

Член 10

Определените лица од Носителот на набавката за реализација на Договорот, задолжително потпишуваат Изјава за доверливост на информации и податоци непосредно пред испораката на стоката - 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.

– Сектор за правни работи–

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. За ваквото барање Носителот на набавката веднаш ќе го извести одговорното лице на Договорниот орган.

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.

– Сектор за правни работи–

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 ПРЕКИНУВАЊЕ ИЛИ РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 18

Овој договор може да се раскине спогодбено со согласност на договорните страни.

Член 19

Кога една од договорните страни нема да ја исполни својата обврска, другата договорна страна може да бара остварување на своите права и исполнување на обврските од другата договорна страна или да го раскине договорот.

– Сектор за правни работи–

Член 20

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 на договорниот орган.

Ако договорната страна која не ја исполнила својата обврска во рокот утврден со овој договор или не ја исполни обврската ни во дополнителниот рок, другата договорна страна може да го раскине договорот.

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

XII. ВИША СИЛА

Член 21

Ниту една од договорните страни нема да биде одговорна кон друга за губитокот, повредата или неизвршувањето на одредбите на овој договор кои се предизвикани од виша сила дефинирана со закон.

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 од поголеми размери 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, а најдоцна во рок од 24 часа, 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.

– Сектор за правни работи–

По отстранувањето на последиците од вишата сила, договорот може да се реализира, доколку неговата реализација не е завршена пред настапувањето на вишата сила.

XIII. ПРИМЕНЛИВ ЗАКОН

Член 22

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

XIV. ЗАВРШНИ ОДРЕДБИ

Член 23

Двете договорни страни се должни со податоците и документите до кои дошле при извршување на предметот на овој договор, да постапуваат согласно со глава „X. Доверливост на информации и податоци" од овој договор.

Член 24

Договорните страни можат да ги дополнат или изменат одредбите од овој договор само спогодбено.

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

Одредбите од овој договор можат да се изменат или дополнат со склучување на анекс на договорот во согласност со Законот за јавните набавки.

Член 25

Сите евентуални спорови кои би произлегле од овој договор, а кои договорните страни не би можеле да ги решат спогодбено, ќе ги решава надлежниот суд во Скопје.

Член 26

При секоја обработка на личните податоци во текот на реализацијата на овој договор договорните страни, соодветно ќе ги применуваат одредбите од Законот за заштита на личните податоци.

– Сектор за правни работи–

Член 27

Овој договор е составен и потпишан во 4 (четири) истоветни и полноважни примероци, по два за секоја страна.

Договорен орган:
Република Северна Македонија
Министерство за финансии
Скопје

Dr. Fatmir Besimi
Министер за финансии

Носител на набавката:
Друштво за комуникациски услуги
А1 МАКЕДОНИЈА ДООЕЛ
Скопје

Стевчо Ристески
Директор

Друштво за комуникациски услуги
А1 Македонија ДООЕЛ Скопје
31

Изработил: Рената Николоска/Марија Анѓелеска
Контролирал: Даниела Јанкова
Одобрил: Татјана Васева
Проверил: Daut Hajrullahi
м-р Маја Стаменковска Угриновска
Согласен: д-р Јелена Таст

– Сектор за правни работи–

Прилог 1 кон Договор:

ТЕХНИЧКИ СПЕЦИФИКАЦИИ:

Набавка и инсталација на антивирусен софтвер со вклучени лиценци за период од 1 (една) година за:

- 630 работни станици (Windows 7, 8, 10 и Mac OC);

- 8 сервери (Windows Server 2008, 2012, 2016, Windows Server 2019 Data Center or Standard).

На 4 од серверите ќе биде поставен Microsoft Exchange Server, па антивирус софтверот и лиценците мора да бидат компатибилни со тие сервери на кој ќе биде поставен Microsoft Exchange Serverot и треба да ја нуди потребната заштита.

Решението треба да ги испони следните карактеристики:

1. Решението треба да има централизирани и интуитивни операции преку една конзола и еден агент. Агентот треба да ја поддржува Next Generation EPP / EDR во еден самостоен агент. Се бара поддршка за оперативните системи Windows, macOS и Linux.

2. Решението треба да биде способно да идентификува софистицирани закани, напади без датотеки и модерен малициозен софтвер без користење на репутација или потписи. Под репутација ги подразбираме сите ставки со репутација: IP, DNS, URL, HASH.
    a. Решението е потребно да се користи Static AI, Dynamic AI за да се идентификуваат новите малициозен софтвер директно на крајната точка и во реално време.

3. Агентот треба да биде целосно автономен што значи: не треба да има никаква зависност од серверот за управување или облакот или НИКОЈ надворешен ресурси од агентот за да открие и соодветно да реагира на софистицирани закани (Zero Day, File-less, Ram-based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) во реално време додека се откриваат заканите.

– Сектор за правни работи–

4. Решението треба да одговори со автоматско ублажување на заканите речиси во реално време и автономно со следните опции за ублажување Alert, Kill, Quarantine, Disconnect from Network, Remediate and Rollback.

5. Решението треба да има целосно автоматизирана опција за обновување. Автономна и санација со 1 клик и патентирано враќање назад.

6. Решението треба да поддржува SaaS режим (Agent-> Cloud SaaS услуга) или On-premises (Virtual Appliance) или Хибриден режим на распоредување.

7. Решението треба да ги поддржува следните механизми за откривање малициозен софтвер:

   a. Предизвршување: Идентификација на малициозен софтвер базирана на датотеки преку услугите за репутација. Решението не бара ажурирања на базата на податоци за потписи или ажурирања на DAT или датотека со потпис. Мора да биде динамичен. Оваа специфична функција е дозволено да зависи од Cloud или од серверот за управување. Затоа, скенирањето на HD малициозен софтвер треба да се случи САМО при првичната инсталација и не треба да ги обезбедува сите безбедносни функции.
   b. Предизвршување: Решението треба да идентификува непознат злонамерен софтвер базиран на датотеки врз основа на анализата на Static Machine Learning. Таквата анализа мора да се случи автономно на крајната точка без надворешни зависности или обработка и без да се земат предвид познатите IOC's (DNS, IP, URL, HASH). (PDF PE OFFICE ELF)
   c. Време на извршување: Агентот треба да идентификува и да реагира на софистицирани злонамерни ситуации (без датотеки, нула-ден, скрипта на школка, странично движење, откупни софтвери, тројанци, уметност итн.) без никакви надворешни зависности или човечка интервенција или анализа на податоци надвор од крајната точка. Мора да се направи речиси во реално време преку имплементација на методологии за вештачка интелигенција.
   Познатиот IOC (DNS, IP, URL, HASH) како средство за идентификација не треба да се смета за усогласеност со оваа ставка.

8. Решението мора да обезбеди силен механизам 'Anti-tamper'. Таквиот механизам треба да биде заштитен со единствена лозинка за секој компјутер

на крајна точка. Состојбата anti-tampering ON OFF против манипулации треба да биде опција во контекст на безбедносната политика

9. Контекстот на политиката треба да обезбеди опција за вклучување или исклучување на уникатни мотори или според by Type of engine (Pre-Execution and Run-Time Engines).

10. Решението треба да содржи ОТВОРЕНО API за интеграција, следење и автоматизација. Алатките за документација за развој на API треба да бидат природно достапни и достапни за администраторските корисници во конзолата за управување.

11. Решението мора да поддржува Multi-Site или Multi-Tenancy за целосно одвојување на објектите и административниот пристап меѓу локациите во архитектурата со multi-Site.

12. Решението мора да поддржува SSO автентикација SAMLv2

13. Решението мора да поддржува 2 факторска автентикација за пристап до администрација со Google Authenticator или Nano.

14. Решението мора да ги поддржува следните формати на системски логови: CEF, CEF2, RFC-5424, STIX и IOC. Треба да поддржува SSL и X.509 сертификати за шифрирање и автентикација за транспорт на системски дневник.

15. Решението мора да обезбеди можност за испраќање текстуални пораки до корисникот од управувачката конзола, дури и кога таквите агенти се во режим на изолација на мрежа / карантин.

16. Решението мора да се интегрира со Active Directory за автоматско пресликување од агенти во групи, заради асоцијација на политиките. Управувачката конзола НЕ треба да се поврзува со Active Directory директно преку ADFS или кој било друг метод за да се изведат атрибути на Уред и кориснички AD. Серверот за управување со решенија не треба да има никакви зависности од состојбата AD.

17. Решението мора да содржи контролна табла што ги прикажува сите компјутери, филтрирање врз основа на карактеристики и атрибути на EP: оперативен систем, тип, верзија на агентот, ако е ранлив или не, атрибути за

AD, телеметриски информации, приватна IP, јавна IP, карактеристики на хардвер, битност, Процесорите, адресите на Mac, интерфејсите, името на домаќинот, работната група, доменот) треба да бидат можни за прегледување, примена на дејство на подмножество на EP или мапирање на EP во групи. Мора да обезбеди опција да се продлабочат деталите на компјутерот, таквите детали треба да прикажуваат телеметриски аспекти, статус, апликации и да обезбедуваат можности за акција: исклучување од мрежа, повторно поврзување на мрежа, рестартирање, исклучување, испраќање порака до корисник, деинсталирање софтвер, преглед закани.

18. Акциите за одговор за заштита на политиката треба да овозможат одговор врз основа на Доверба на настанот (Закана наспроти сомнително) Таквиот одговор треба да овозможи алармирање или заштита на опциите засновани на класификација на доверливост. Одговорот „Заштита" треба да може автономно да дејствува од агентот дури и кога не е поврзан на мрежа.

19. Решението треба да има функционалност на Firewall за крајната точка со политички контекст единствен за секоја група крајни точки. IEEE OSI L4 Firewall и треба да поддржува FQDN, IP, CIDR, опсег. Windows, Linux и MacOS мора да бидат поддржани

20. Решението треба да има функционалност за контрола на уредот за крајните точки со контекст на политика единствен за секоја група крајни точки. Потребна е поддршка за USB и Bluetooth.

21. Решението треба да известува за пропустите на апликациите пронајдени на секој компјутер и да обезбеди специфични информации и детали за CVE.

22. Решението треба да има реконструкција на напад со машинско напојување. Настаните автоматски се реконструираат во лесно Storyline, focused & contextualized предупредувања за аналитичарите значи побрз MTTR.

23. EDR Задржувањето на податоците мора да трае најмалку 14 дена во модел базиран на SaaS Cloud

24. Функционалноста мора да има способност за автоматско и автономно извршување на претходно индексирање и претходно поврзување на настаните како што се случуваат, во реално време, таквото индексирање треба да се случи во крајната точка, а не во облакот, таквите настани се бара да имаат

единствен идентификатор. Барањето на таков идентификатор треба да врати табела со сите настани (IP, DNS, FILES, РЕГИСТРИ, ПРОЦЕС, URL итн.) што ја составува дадената ситуација без разлика дали е поврзана со малициозен софтвер или не. Дополнително, контролната табла на EDR ги враќа податоците за даденото барање за „идентификатор на ситуацијата" треба да содржи истражувач на „Дрвото на процесите" за графичка визуелизација и продлабочување на настаните.

25. Решението мора да се интегрира во еден автономен агент.

26. Решението треба да е во согласност со Општа регулатива за заштита на податоците (GDPR- General Data Protection Regulation, Regulation (EU) 2016/679).

27. Решението мора да биде именуван како лидер во 2021 Gartner Magic Quadrant за EPP.

28. Решението на мора да поддржува лов на закани користејќи тактики и техники на MITTRE.

29. Решението да е од водечките во евалуацијата на MITRE ATTACK последните две години.

30. Мора да поддржува прилагодени правила за откривање. За да му дозволите на аналитичарот, претворете ги (EDR/XDR) барањата во автоматизирани правила за лов што активираат предупредувања и автоматизирани одговори Kill, Quarantine, Remediate, Rollback, Isolate from Network) кога правилата откриваат совпаѓања.

31. EDR мора природно да се интегрира со компонентата EPP во еден автономен агент

32. EDR мора да поддржува оперативни системи Windows, MacOS и Linux.

33. EDR мора да обезбеди прелистувач на дрво за процеси.

34. EDR мора автоматски да индексира и да ги корелира настаните под единствен идентификатор на приказната.

35. Решението треба да обезбеди Secure Remote Shell за да може администраторот да извршува команди на крајната точка дури и кога крајната точка е во состојба на изолација на мрежа / мрежна исклучување. Покрај тоа, решението треба да зачува препис од сесијата. Таквиот препис треба да биде заштитен со лозинка и далечинскиот пристап Secure Remote Shell треба да го принуди со 2 факторска автентикација за администраторот пред да дозволи пристап. Secure Remote Shell треба да се вклучи/исклучи преку контекст на политиката.

Услови:

- Инсталација на антивирусен софтвер на сите клиенти и сервери. На серверите е поставен Active Directory и Фајл сервер, како и апликациски сервери и сервери со бази на податоци кои не смеат да имаат downtime, со што инсталацијата, доколку е потребно, би се имплементирала надвор од работно време. Носителот на набавката треба да ги предвиди сите подесувања (правила и исклучоци) на софтверот за да апликациите и сервисите кои ги користи Министерството за финансии продолжат непречено да функционираат;
- Обука на двајца вработени за користење и понатамошно одржување и поддршка за антивирусниот пакет;
- Во моментов во инфраструктурата на Министерството е инсталиран и поставен антивирусен софтвер - Kaspersky Endpoint Security for Business на 630 работни станици. Носителот на набавка на понуденото софтверско решение во соработка со ИТ лица од Министерството, е должен да го деинсталира тековниот софтвер од сите работни станици и сервери и да го инсталира новиот софтвер на работните станици и сервер. Деинсталацијата на старото антивирусно решение и инсталацијата на новото ќе се врши преку конзолата за централно управување на антивирусните решенија и со физички пристап на самите работни станици лоцирани во објектите на Министерството во Скопје. За останатите работни станици, во подрачните единици надвор од Скопје, инсталацијата ќе се врши далечински. По инсталација на софтверот носителот на набавката доставува детален извештај до Министерството за финансии;
- Бесплатни 'program upgrades' и 'program patches';
- Вклучена основна поддршка од страна на производителот на софтверот (право на надградби, закрпи, нови верзии и основна on-line техничка поддршка) за период од 1 (една) година;
- Носителот на набавката е должен во период од 1 (една) година да дава техничка подршка на on-site локација во случај на настанати проблеми (по

пријава на договорниот орган). Времето на достапност на сервисот за техничка подршка треба да биде секој работен ден од 08-17 часот. Од страна на Министерството ќе биде овозможена и VPN врска за пристап доколку има потреба. Министерството располага со 6 локации во Скопје и 45 во државата. Доколку има потреба од интервенција на лице место на локацијата надвор од Скопје, превозот за максимум 2 технички лица од носителот на набавката го обезбедува Министерството со службено возило;

- По склучување на договорот, Министерството ќе достави барање за инсталирање на антивирусниот софтвер и активација на лиценците по што носителот на набавка ќе биде должен да ја изврши инсталацијата во рок од 10 (десет) календарски денови од денот на добивање на барањето и обезбедување на технички предуслови од страна на Министерството.

Носителот на набавката е должен за решението (софтвер за антивирусна заштита на корисници / сервер) да вклучи и обезбеди: инсталација на истиот во времетраење од 10 (десет) календарски денови, ремоте обука за користење на системот на вработените во договорниот орган, како и минимум 1 (еден) ден ремоте во месецот за консултации во времетраење на претплатата, во согласност со техничките спецификации.