– Сектор за правни работи–

Архивски број: 03-7533/1
Датум: 07-07-2022

Друштво за професионални и консултантски услуги
ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ
Бр. 03-117/1
11.07.2022 год.
СКОПЈЕ

ДОГОВОР
за јавна набавка на стоки - заштитен sид на веб апликација WAF

Склучен помеѓу:

1. МИНИСТЕРСТВО ЗА ФИНАНСИИ, со седиште на ул.„Даме Груев“, бр.12 - Скопје, претставувано од Dr.Fatmir Besimi, министер за финансии, во натамошниот текст: договорен орган и
2. Друштво за професионални и консултантски услуги ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ Скопје, со седиште на ул.„Фјодор Достоевски“, бр.72, вл.1-4/5 во Скопје, претставувано од Боби Цветковски, управител, во понатамошниот текст: носител на набавката.

I. ПРЕДМЕТ НА ДОГОВОРОТ

Член 1

Предмет на договорот е јавна набавка на стоки – заштитен sид на веб апликација WAF, согласно со Техничките спецификации кои се составен дел од овој договор (Прилог 1), а по претходно спроведена поедноставена отворена постапка, по оглас број 07471/2022.

II. ВРЕДНОСТ НА ДОГОВОРОТ

Член 2

Вкупната максимална вредност на договорот без пресметан данок на додадена вредност изнесува 4.290.000,00 денари.

Вкупниот износ на данок на додадена вредност изнесува 772.200,00 денари.

Вкупната максимална вредност на договорот со пресметан данок на додадена вредност изнесува 5.062.200,00 денари.

III. РАЗЛИКА ВО ЦЕНА (КОРЕКЦИЈА НА ЦЕНИ)

Член 3

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

– Сектор за правни работи–

IV. РОК НА ВАЖНОСТ НА ДОГОВОРОТ

Член 4

Овој договор се склучува за период од 3 (три) години од денот на потпишувањето од двете договорни страни.

V. НАЧИН, МЕСТО И РОК НА ИСПОРАКА

Член 5

Носителот на набавката е должен предметот на договорот (заштитен sид на веб апликација WAF) да го изврши во согласност со техничките спецификации, потребите и барањата на договорниот орган и во рок кој ќе го определи договорниот орган во писмена порачка која ќе биде испратена до носителот на набавката.

Носителот на набавката е должен за извршувањето на предметот на договорот (заштитен sид на веб апликација WAF) да вклучи и обезбеди инсталација на истиот во времетраење од минимум 5 (пет) дена, 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.

Носителот на набавката е должен за предметот на договорот (заштитен sид на веб апликација WAF) да обезбеди претплата за период од 3 (три) години.

Носителот на набавката е должен за извршувањето на предметот на договорот (заштитен sид на веб апликација WAF) да издаде Работен налог/ Извештај / Записник, кој мора да ги содржи податоците за извршувањето на предметот на договорот.

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

Испораката на предметот на договорот (заштитен sид на веб апликација WAF) ќе се врши во просториите на договорниот орган во Скопје.

– Сектор за правни работи–

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 (заштитен sид на веб апликација WAF), доставена по пошта или лично во писарницата на Министерството за финансии на ул. „Даме Груев" бр.12 во Скопје.

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

VII. ПРАВА И ОБВРСКИ НА НОСИТЕЛОТ НА НАБАВКАТА

Член 7

Носителот на набавката е должен предметот на договорот (заштитен sид на веб апликација WAF) да го изврши согласно техничките спецификации (Прилог 1 кон Договор), барањата и потребите на договорниот орган наведени во писмената порачка и податоците наведени во него.

Носителот на набавката е должен да го изврши предметот на договорот (заштитен sид на веб апликација WAF) во рокот определен во писмената порачка, доставена од страна на договорниот орган.

Член 8

Носителот на набавката е особено должен:

- да обезбеди ефикасно и навремено извршување на договорот и да ги применува соодветните регулативи за конкретниот вид на стоки/услуги, придржувајќи се кон барањата нагласени од договорниот орган;
- да дава соодветни препораки за решавање на секој проблем кој би се појавил во текот на реализација на предметниот договор;
- да му се укаже на договорниот орган за било која неправилност во врска со непочитувањето на законската регулатива или било кој друг факт кој би можел негативно да влијае на исходот или очекувањата на договорниот орган;
- да пристапи кон извршување на предметот на договорот (заштитен sид на веб апликација WAF) по приемот на писмена порачка од договорниот орган за набавка;

- во рамките на извршувањето на своите обврски блиску да соработува со вработените кај договорниот орган кои ќе бидат задолжени за реализација на предметниот договор.

Носителот на набавката се обврзува и е должен во рамките на извршувањето на своите обврски да ги смета барањата и интересите на договорниот орган кои се предмет на овој договор за приоритетни во секое време и да го информира договорниот орган, веднаш доколку се појават одредени околности кои би влијаеле на извршувањето на активностите кои се предмет на овој договор.

VIII. ПРАВА И ОБВРСКИ НА ДОГОВОРНИОТ ОРГАН

Член 9

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

Договорниот орган е должен да достави писмена порачка со точни спецификации и барања со цел да се изврши реализација на предметот на договорот.

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

IX. ГАРАНЦИЈА ЗА КВАЛИТЕТНО И НАВРЕМЕНО ИЗВРШУВАЊЕ НА ДОГОВОРОТ

Член 10

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

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

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

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

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

– Сектор за правни работи–

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

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

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

Гаранцијата за квалитетно и навремено извршување на договорот договорниот орган му ја враќа на носителот на набавката по пошта, лично во седиштето на 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 едностране раскинување поради неизвршување на обврските од договорот од страна на носителот на набавката.

Договорниот орган нема да бара активирање на банкарската гаранција за квалитетно 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.

X. ДОВЕРЛИВОСТ НА ПОДАТОЦИ И ИНФОРМАЦИИ

Член 11

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

Под поимот информации и податоци се подразбираат сите внатрешни и надворешни документи, спецификации, лични податоци, истражувања на пазарот или податоци за него, финансиски или маркетиншки информации, други

податоци или бизнис, оперативни или технички информации, како и сите останати податоци и информации и независно дали се дадени во писмена, вербална или електронска форма и се во сопственост на договорниот орган.

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

Член 12

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

Член 13

Носителот на набавката под целосна морална, материјална и кривична одговорност, се обврзува за време на важноста на договорот и во период од (5) пет години од датумот на неговото истекување или раскинување да ги чува во тајност сите информации и податоци од било која област на договорниот орган, кои ќе му бидат дадени во процесот на соработката и притоа нема да ги искористи истите за лични цели, во име на друго лице, ниту ќе ги даде на увид на трета страна.

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

Член 14

Носителот на набавката може да ги открие кои било од информациите и податоците наведени во членот 11 став 2 и 3 заради постапување по писмено барање од страна на надлежен орган, со легитимна наредба врз основа на закон. За ваквото барање носителот на набавката веднаш ќе го извести одговорното лице на договорниот орган.

– Сектор за правни работи–

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

Член 15

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

Член 16

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

Член 17

Објавувањето податоци, рекламирањето или публицитетот, како и прес конференциите направени од страна на носителот на набавката во однос на овој договор или вршење на заеднички деловни активности на договорните страни треба да бидат претходно одобрени од договорниот орган пред нивното спроведување.

Член 18

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

– Сектор за правни работи–

XI. УСЛОВИ ЗА ПРЕКИНУВАЊЕ ИЛИ РАСКИНУВАЊЕ НА ДОГОВОРОТ

Член 19

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

Член 20

Овој договор може да се раскине и едностранo, поради непридржување или неисполнување на договорните обврски утврдени со овој договор, како и поради неквалитетно вршење на работите утврдени со договорот.

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

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

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

Член 21

Кога носителот на набавката нема да ја исполни својата обврска во определениот рок, договорниот орган 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 носителот на набавката не ја исполнил својата обврска во рокот утврден во овој договор или не ја исполнил ниту во дополнителниот кој бил даден од договорниот орган, договорниот орган 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 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.).

– Сектор за правни работи–

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. ОПШТИ И ЗАВРШНИ ОДРЕДБИ

Член 23

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

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

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

Дополнувањата и измените на овој договор се важечки ако се направени во писмена форма и ако се потпишани од двете договорни страни.

Член 24

Сите спорови кои ќе настанат во текот на работата, странките ќе се обидат да ги решат спогодбено, во спротивно ќе решава надлежниот суд во Скопје.

Член 25

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

Член 26

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

– Сектор за правни работи–

Член 27

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

Договорен орган:
Република Северна Македонија
Министерство за финансии
Скопје

Dr. Fatmir Besimi
Министер за финансии

Носител на набавката
Друштво за професионални и консултантски услуги ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ Скопје

Боби Цветковски
Управител

Друштво за професионални и консултантски услуги ТЕЛЕЛИНК БИЗНИС СЕРВИСИС ДООЕЛ СКОПЈЕ

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

Прилог 1

ТЕХНИЧКИ СПЕЦИФИКАЦИИ

за јавна набавка на стоки – заштитен ѕид на веб апликација WAF

Опис на WAF решението
Архитектура на WAF решението
Решението треба да биде базирано на уреди и треба да биде достапно со следните формати: • Физички уред • Виртуелен уред • Амазон Веб Сервиси Инстанца на Машина • Мајкрософт Азур Машина
Уредот треба да може да ги поддржува следните режими на мониторирање на веб сообраќајот: • Преку SPAN/TAP мониторинг порт начин на работа • Преку инлине Layer 2 transparent bridge mode мора да биде обезбедено од самиот уред како функционалност , не преку интеграција со т.н. 3rd party интеграции • Reverse Proxy начин на работа • Transparent Layer-2 Reverse Proxy мод (Layer-2 но со терминирање на релевантните TCP сесии)
За Layer 2 Inline Bridge начин на имплементација и за физичките уреди решението треба да има вградено т.н.бајпас поддршка "fail-open" начин на работа. Решението треба да има можност и за поддршка "fail-close" начин на работа. Мора да биде обезбедено од самиот уред како функционалност , не преку интеграција со т.н. 3rd party интеграции
Целото решение мора да биде централно управувано за секојдневните операции. Известувањето, креирањето политики, управувањето со предупредувања, конфигурацијата за заштита на веб-апликацијата итн. мора да се управуваат од серверот за управување. Управувачкиот сервер мора централно да управува со сите различни уреди. Решението мора да му овозможи на корисникот да користи стандарден прелистувач за пристап до интерфејсот за управување.
При скалирање на решението, решението мора да поддржува т.н. "scale-out" пристап за додавање на дополнителни уреди за мониторирање со тоа што ќе треба само да се регистрираат уредите на менаџмент серверот.
Решението мора да поддржува WAN/global дистинуиран начин на имплементација при што може да има повеќе сервери за управување распоредени за различни географски региони. Сите сервери за управување мора да бидат способни да бидат централно

управувани од „ Manager of Managers". „ Manager of Managers" мора да ги обезбеди следните функционалности: • Унифицирано управување и администрирање на федеративни средини низ сите сервери за управување • Креирање, конфигурирање и дистрибуција на политики низ системот низ сите сервери за управување • Единствена точка на пристап до секој сервер за управување • Мониторирање на целокупното решение и неговата состојба • Системски преглед на безбедносните активности
Решението мора да може да поддржи мониторинг и заштита, и во случај каде некои веб-апликации се заштитени во "Transparent Reverse Proxy" режим на, а некои веб-апликации да бидат заштитени во режимот на "Later-2 transparent inline bridge". Мора да биде обезбедено од самиот уред како функционалност, не преку интеграција со т.н. 3rd party интеграции. Да се опише како се постигнува ова !!!
Решението мора да биде едноставно и интуитивно за поставување и конфигурирање. Со сите потребни одобренија за управување со промени и достапни информации за мрежата.
Решението мора да има минимално влијание врз постоечките веб-апликации и мрежната архитектура при поставување или отстранување на решението од мрежата. Да се опише како се постигнува ова !!!
Кога е имплементирано решението на платформата за веб-услуги Amazon Web Service, решението мора да поддржува способност за автоматско скалирање.
Кога е имплементирано решението на платформата за веб-услуги Google Cloud platform, решението мора да поддржува способност за автоматско скалирање.
Кога е имплементирано решението на платформата за веб-услуги Microsoft Azure platform, решението мора да поддржува способност за автоматско скалирање.
Решението мора да дојде со опција за проширување на опсегот на заштита на Cloud со Cloud WAF базиран. Cloud WAF базиран облак, исто така, мора да доаѓа со мрежна заштита на DDoS, заштита на DNIS, безбедност на API, напредна заштита од ботови, Client Side Protection CDN и Layer-7 балансирање. Cloud WAF-от и решението поставено кај крајниот корисник мора да се интегрираат со унифициран модел на контролирање и управување како и за известување и предупредување.

Безбедносни карактеристики на WAF решението
Решението мора да ги поддржува следните механизми за автенкикација при пристап на менаџмент конзолата: • Вградена автентикација на самото решение • LDAPS автентикација и авторизација кога се користат следните Windows платформи: 2008, 2008 R2, 2012, and 2012 R2, Windows 2019. • RADIUS автентикација • Smart card базирана автентикација
Решението мора да биде Common Criteria сертифицирано.
Решението мора да обезбеди Role-Based Access Control или раздвојување на корисничките рољи преку дефинирање на различни нивоа на пристап и привилегии.
Решението мора да поддржува различни можности за менаџирање на лозинките без притоа да се користи и да се потпира на надворешен систем: • Валидност на лозинката одреден временски период во денови • Должина на лозинката и примена на дефиниран број на карактери и бројки во лозинката • Дали новата лозинка да биде значително поразлична од последната користена лозинка • Дали лозинката мора да вклучува големи букви, броеви, мали букви и неалфа-нумерчки карактери или да не вклучува.
Решението мора да може да поддржува конфигирација на механизам за заклучување на интефејсот за пристап на менџмент серверот во случаи кога: • После одреден број неуспешни обиди за најава корисиникот да не може да пристапи одреден број на минути. • После одреден број на неуспешни обиди за најава корисникот да биде заклучен • Времетраење на зклучувањето во минути.
Решението мора да ја поддржува способноста за комуникација базирана на доверба помеѓу различните компоненти во решението. т.е. комуникацијата помеѓу компонентите на решението треба да се врши со помош на сертификати.
Решението мора да поддржува openssl 1.0.2

Карактеристики на WAF решението
Понуденото WAF решение мора да биде во лидер квадрантот на Gartner Magic Quadrant for Web Application Firewalls во последните 7 години.
Решението мора да го поддржува пристапот на позитивниот безбедносен модел. Позитивниот безбедносен модел наведува каков влез и однесување е дозволено и се друго што отстапува од позитивниот безбедносен модел се предупредува и/или блокира.
Решението мора да го поддржува пристапот на негативниот безбедносен модел. Негативниот безбедносен модел експлицитно ги дефинира познатите потписи и вектори за напад.

Решението мора да обезбеди речиси нула стапка на лажно-позитивна стапка со користење на однапред конфигурирани политики OOTB (Out Of The Box) што овозможуваат распоредување на WAF во режим на блокирање без потреба од прилагодување на политиките.
Решението мора да може да блокира трансакции со содржина што одговара на познати потписи за напад, додека дозволува сè друго.
Решението мора да биде способно да поддржува и вградена и нелиниска симулација и активен режим на извршување. Во режимот на симулација, администраторот може да гледа предупредувања, напади, грешки на серверот и други неовластени активности. Во режимот на активно извршување, решението може да изврши сè што е направено во режим на симулација и дополнително да може да блокира напади.
Решението мора да може да ги изврши следните дејства при откривање напад или која било друга неовластена активност: • Можност за отфрлање барања и одговори, • Блокирање на TCP сесијата, • Блокирање на корисникот на апликацијата или • Блокирање на IP адресата
Решението мора да може да го блокира корисникот или IP адресата за одреден временски период што може да се конфигурира.
Решението мора да може да испрати TCP RST пакет на двата краја на веб-врската кога е распоредена во режим на "sniffing" во случај на активен режим на распоредување на примена.
Решението мора да може да ги заштити и HTTP веб-апликациите и SSL (HTTPS) веб-апликациите.
Решението мора да може да ги проверува и заштити протоколите HTTP/1.x и HTTP/2.
Решението мора да може да дешифрира SSL веб сообраќај помеѓу клиентите и веб-серверите.
Решението мора да може да го дешифрира веб-сообраќајот на SSL што користи протоколи за размена на клучеви Diffie-Hellman со уредот кога е имплементиран во режим transparent layer-2 bridge mode (Advanced Bridge Mode).
Решението мора да обезбеди можност за усогласување со сертификатот A+ со кликнување на копче.
Решението мора да обезбеди можност за контрола на поставките за SSL преку интерфејс базиран на GUI.
Решението мора да може да го дешифрира веб-сообраќајот на SSL за проверка без да ја прекине или менува HTTPS врската. (Со исклучок на протоколите за размена на клучеви Diffie-Hellman).

Решението мора да ги обезбеди следните карактеристики и заштита, т.н <u>out of the box</u>: • Потврда на протоколот HTTP (1.x и 2). • Валидација на напад поврзан со сервисот за веб-услуги • Потписи за напад на HTTP протокол • Прилагодена заштита на сервисот за веб-услуги • Потврда за потпишување колачиња • Против отфрлање на локацијата • Заштита на веб-профилот • Заштита од веб-црви • Потписи за напад на веб апликации • Прилагодена заштита на сервисот на веб апликации • OCSP валидација на протоколот • Предизвик CAPTCHA
Решението мора да вклучува однапред конфигурирана листа на сеопфатни и точни потписи за веб-напади.
Решението мора да има база на податоци од минимално 6000+ потписи кои се дизајнирани да откриваат познати проблеми и напади на веб-апликации.
Решението мора да обезбеди заштита на потписот од познати пропусти во софтверот за комерцијална инфраструктура како што се Apache, IIS, Oracle и така натаму. Содржината обезбедена од механизмот за откривање потпис мора да се заснова на истражувањето направено од одделот за разузнавање за закани од продавачот на решенија и комбинација од други ресурси како што се Snort, CVE и така натаму. Овој сет на потписи мора постојано и автоматски да се ажурира.
Решението мора да им дозволи на администраторите да додаваат и менуваат потписи.
Решението мора да ги поддржува следните типови на дефиниција за прилагодени потписи: • Single Part Signatures (например. part="hello world") • Multi Part Signatures (например. part="bash", part="select", part="%27") • Absolute Modifiers кои го ограничуваат делот што треба да се совпадне со одредена област на потокот. • (например. part="cmd.exe", amin="10", amax="20". Овој потпис ја бара низата cmd.exe само од позицијата 10 до позицијата 20 во преносот). • Relative Modifiers кои го ограничуваат делот на одредена област по претходниот дел. (на пример part="cmd", part=".exe", rmax="10". Овој потпис вклучува два дела. Вториот дел се бара во опсег од 10 знаци од првиот дел. Низата cmd12345.exe се совпаѓа со овој потпис. Сепак, низата cmd12345678.exe не се совпаѓа со потписот бидејќи делот „.exe“ завршува 12 знаци по делот „cmd“.)

Решението мора да поддржува регуларни изрази за следните цели: • Дефиниција на потписи • Дефиниција за чувствителни податоци • Дефиниција на тип на параметар • Дефиниција за имиња на домаќини и префикси на URL • Фино подесување на параметрите кои динамички се учат од профилот на веб апликацијата
Решението мора да поддржува автоматско ажурирање на базата на податоци за потпис за да обезбеди целосна заштита од најновите закани за веб-апликации.
Решението мора да може да открие познати напади на повеќе нивоа. Ова вклучува мрежа, оперативен систем, софтвер за веб-сервер и напади на ниво на апликација.
Решението мора да има вграден механизам за корелација за да обезбеди корелација на настани, автоматско поставување на основната линија и да ги намали лажните позитиви
Решението мора да може да открие познати злонамерни корисници кои често се одговорни за автоматизирани напади и напади на ботнет. Изворот на малициозни корисници вклучува злонамерни IP адреси, анонимни адреси на прокси и TOR мрежи.
Изворот на малициозни корисници треба автоматски и периодично да се ажурира (Дневно ажурирање на базата).
Решението мора да ги прегледа и надгледува сите HTTP(S) податоци и нивото на апликацијата, вклучувајќи ги заглавијата на HTTP(S), полињата за формулари и телото HTTP(S).
Решението мора да може да ги проверува барањата и одговорите на HTTP.
Решението мора да може да ги идентификува WebSocket врските.
Решението мора да може да ги потврди кодираните податоци во сообраќајот HTTP.
Решението мора да може да врши валидација на сите типови на внесување, вклучувајќи URL-адреси, формулари, колачиња, низи за прашања, скриени полиња и параметри, HTTP методи, XML елементи и дејства SOAP.
Решението мора да биде способно автоматски да врши динамично профилирање на веб-апликации.
Технологијата за динамичко профилирање на решенијата мора да може да открие и заштити од закани кои се специфични за приспособениот код на веб-апликацијата. По фазата на динамичко профилирање/учење, решението мора да може да ја разбере структурата на секоја заштитена URL адреса.
Решението мора автоматски да ги изгради/учи профилите на веб-апликациите и да ги користи за откривање отстапувања и разни аномалии (или прекршувања) и блокирање напади на приспособениот код на апликацијата.

Решението мора да биде способно автоматски да ја научи употребата на веб и структурата на апликацијата и елементите и очекуваното однесување на корисниците веднаш штом ќе се инсталира системот. Структурата и елементите вклучуваат URL-адреси, директориуми, колачиња, полиња и параметри за формулари и HTTP методи. Корисничките однесувања вклучуваат должина на очекуваната вредност; прифатливи знаци по поле за параметар; дали вредноста на параметарот е само за читање или може да се уредува од корисникот и дали параметарот е задолжителен или опционален.
Решението мора да може автоматски да се префрли на заштитниот режим (режим на блокирање) по соодветен период на учење што може рачно да го дефинира администраторот.
Режимот за учење со динамичко профилирање на решенија мора да може да ги препознае промените на веб-апликацијата и истовремено да ги заштити веб-апликациите во исто време.
Решението мора да може да врши динамично профилирање и истовремено да може да се стави во режим на активно блокирање на извршување.
Решението мора да дозволи динамичните профили да се менуваат рачно и да може да се додаваат и отстрануваат информации за фино прилагодување на профилите.
Решението мора да поддржува динамично профилирање само од збир на доверливи корисници за да го научат нормалното прифатливо однесување и користење на веб-апликацијата.
Решението мора да овозможи повторно учење на профилот на апликацијата на база на URL или на страница. Од администраторот не треба да се бара повторно да ја научи целата апликација кога се сменети само неколку страници.
Решението мора да ја поддржува конфигурацијата за да дозволи некои страници во веб-апликацијата да бидат во заштитен режим, а некои страници да бидат во режим на учење на динамично профилирање.
Решението мора да може да врши динамично профилирање на веб-апликации во средина каде што има мешавина од добар и лош сообраќај. Решението мора да може автоматски да го разликува добриот и лошиот сообраќај при учењето на профилот. Лошиот сообраќај не треба да се учи и додава на профилот.
Решението мора да може автоматски да ги научи сите имиња на домаќини на веб-апликациите што се заштитени.
Решението мора да може да врши динамично профилирање на JSON. Барањата за HTTP во JSON формат мора да ги научи WAF со параметрите и вредностите.
Решението мора да може да ги заштити веб-апликациите што вклучуваат содржина на веб-услуги (XML).
XML заштитата што ја нуди решението мора да биде слична на заштитата на веб-апликацијата обезбедена со автоматско динамичко профилирање/ способност за учење. Нема потреба да се додава WSDL-датотеката.

Решението мора да поддржува сопствени безбедносни правила. Администраторите треба да бидат способни да дефинираат правила за позитивниот и негативниот безбедносен модел и да креираат правила за корелација со повеќе критериуми.
Решението мора да може дигитално да потпишува колачиња, да ги шифрира колачињата и да ги препишува УРЛ-адресите кога е распореден во режим на обратен прокси.
Решението мора да поддржува и препишување URL и препишување содржина за http заглавието и телото кога е во режим на обратен прокси.
Решението мора да биде способно да изврши виртуелно поправање на заштитените веб-апликации за да обезбеди итна санација на ранливоста на апликацијата.
Решението мора да ги поддржува сите следни алатки за проценка на ранливоста на веб-апликации (скенери за веб-апликации) за виртуелно да ги закрпи пропустите на веб-апликациите: • Acunetix • Beyond Security • Cenzic • Denim Group • HP Fortify WebInspect • IBM AppScan • NT OBJECTives • Qualys • Rapid7 • Trend Micro • Veracode • WhiteHat
Решението мора да се однесува на Критериумите за евалуација на заштитниот ѕид на веб-апликации (WAFEC), како што е дефинирано од Конзорциумот за безбедност на веб-апликации (www.webappsec.org).
Решението мора да може да обезбеди довод и услуга за разузнавачки закани врз основа на репутацијата на изворот. Доводот мора да се обезбеди во речиси реално време за следните познати извори на напади: • Malicious IP • Anonymous Proxies • TOR IPs • Comment Spam IPs • Phishing URLs • IP Forensics • Geo Location

Решението мора да биде способно да обезбеди довод и услуга за разузнавачки закани што се засноваат на техники за "crowdsourcing" во заедницата. Оваа услуга мора да може да собира податоци за напади во живо од WAF распоредени низ целиот свет и потоа да ги дистрибуира шемите на нападот и податоците за репутацијата во речиси реално време до решението. Оваа разузнавачка служба за закана мора да ги обезбеди следните податоци за напад: • Remote File Inclusion • SQL Injection IPs • Scanner IPs
Решението мора да може да обезбеди довод и услуга за разузнавачки информации за закани за заштита на ботови. Оваа разузнавачка служба за закани мора да ги обезбеди следните способности и податоци: • Bot Класификација на сообраќај во луѓе, Trusted Bot, Bad Bot, General Bot и Непознат нов бот • Bot тип: Click Bot, Comment Spammer Bot, Crawler, Feed Fetcher, Hacking Tool, Masking Proxy, Search Bot, Spam Bot, Vulnerability Scanner, Worm, Site Helper and DDoS Tool • CAPTCHA услуга • Контролна табла за дистрибуција на посетители и број на посети • Контролна табла за дистрибуција на лоши ботови и број на посети
Решението мора да има способност да обезбеди услуга за итни информации за разузнавачки закани. Оваа услуга ќе го обезбеди најновиот сет на потписи од продавачот на решенија за ублажување на пропустите на нула-ден веднаш штом ќе се идентификуваат.
Решението мора да ја поддржува способноста да се дефинираат безбедносни политики врз основа на доводите за разузнавачки информации за заканите наведени претходно за извршување на следните функции: • Alert • Block IP • Block Session • Block User
Решението мора да обезбеди "anti-automation" заштита која може да ги блокира автоматските напади користејќи алатки за хакерство, скрипти, рамка итн.
Решението мора да поддржува интеграција со производи за откривање на малициозен софтвер како што е системот за заштита на малициозен софтвер FireEye (MPS) кој ги идентификува домаќините заразени со малициозен софтвер на внатрешните IP-адреси. Оваа интеграција мора да му овозможи на администраторот да дефинира одбранбени дејства против веб-активностите генерирани од домаќините заразени со малициозен софтвер (идентификувани од MPS). Врз основа на нивото на закана на домаќините заразени со малициозен софтвер, безбедносните политики дефинирани во

решението мора да бидат способни да активираат одбранбена акција како ревизија, предупредување или блокирање.
Решението мора да може да ги следи и следи корисниците на веб-апликации. Овој механизам за следење на корисници мора да биде автоматизиран, без промени во постоечката апликација или шема за автентикација.
Решението мора да поддржува следење на корисникот со користење на автентикација на корисникот заснована на формулари и на сертификат.

Способности на WAF решението за предупредување и блокирање
Решението мора да обезбеди автоматизиран механизам за предупредување за настани во реално време.
Решението мора да може да ги следи и блокира корисниците кога е потребно.
Решението мора да поддржува маскирање на чувствителни податоци во предупредувањата.
Решението мора да поддржува испраќање предупредувања до алатките на SIEM како што се Qradar, RSA Envision, Splunk и Arcsight.
Решението мора да поддржува испраќање пораки Syslog во JSON формат со интуитивни парови клуч-вредност. Ова е за да се осигура дека е полесно за SIEM-от да врши парсирање и пребарување/индексирање на пораките од дневникот на WAF.
Решението мора да може да поддржува порака со големина од 8.192 бајти
Решението мора да го поддржува создавањето пораки за приспособени пораки и да обезбеди механизам на променливи во системот за да се овозможи овој случај на употреба. На пример, заштитното место за корисничко име изгледа како (${Alert.username}).
Решението мора да поддржува испраќање на логови во CEF стандардот.
Решението мора да поддржува флексибилен сет на последователни активности што треба да се преземат во случај на генерирање предупредувања. На пример, ако се генерира предупредување врз основа на политика, испратете е-пошта до администраторот X и менаџерот Y проследено со испраќање системски логови до Дестинацијата 1 и дневник форматиран CEF до Дестинацијата 2.
Решението мора да биде способно да генерира системски настани/дневници за настани што се случиле во системот, како што се најавување или директен резултат на системски промени како што се ажурирања на потпис, промени во конфигурацијата, активирање на поставките, градење профили, автоматски профил надградби, обнова на индекси на бази на податоци, старт/стоп на серверот, грешки или предупредувања поврзани со системот (на пр., претходно дефинираните дефиниции на прагови се надминуваат) и така натаму.

Решението мора да може автоматски да ги извршува следните дејства за да дејствува на алармирање:

- Send Syslog
- Remedy Create Incident
- SNMP trap
- SMTP email
- Run a OS Shell Command
- Monitor an IP
- Monitor an user
- Block an user
- Block an IP
- Create a review task
- Assign a task

Извештаи

Решението мора да обезбеди однапред спакувани можности за известување "out of the box" без интервенција на корисникот/понатамошна конфигурација:

- Alert analysis (For Application user, Known attack patterns, severity, Source IP with severity & type, URL, User with severity & type, Violation Types)
- Daily & weekly Top 10 WAF violations
- Daily Summary Blocked Connections
- Data Leakage Report
- Directory Browsing Detection Report
- List of Alerts
- PCI - WAF violations
- Sensitive Error Messages Leakage Report
- Slow HTTP/S Alerts
- Threat Intelligence Daily, Quarterly and Monthly Reports for Anonymous Proxies, Comment Spam IPs, Malicious IPs, Phishing URLs, RFI Signatures, SQL Injections IPs, Scanner IPs and TOR IPs.
- Top Bot Violations Daily Report

Решението мора да го поддржува создавањето на следните извештаи за динамичко профилирање:

- Cookies learnt
- Learned Hostnames
- Susceptible Directories Learned
- URL Patterns Learned
- URLs Learned
- Web Application User Tracking

Решението мора да обезбеди функционалност за да помогне во форензиката на безбедносните настани.
Решението треба да има способност да се интегрира со алатката Attack Analytics. Алатката за анализа на напади треба да ги анализира сите безбедносни предупредувања и да им помогне на безбедносните администратори да ги потврдат најрелевантните безбедносни предупредувања.
Алатката Attack Analytics треба да може да ги консолидира безбедносните настани од WAF распоредени во облакот, On-Premise WAF и WAF Cloud Service.
Решението мора да ја има функционалноста во рамките на интерфејсот "out of the box" што му овозможува на администраторот да креира приспособени шаблони за извештаи врз основа на постоечките извештаи надвор од кутијата.
Решението мора да поддржува уредување и креирање безбедносни политики што се водени од кориснички кликање и пушти интерфејс.
Решението мора да поддржува генерирање извештаи и со табеларни прикази и со графички прикази за анализа на податоци.
Решението мора да поддржува автоматско генерирање извештаи врз основа на дефиниран распоред
Решението мора да поддржува закажување на генерирање извештаи за да започне само во однапред дефиниран датум и време

Администрација и менаџмент на WAF решението
Решението мора да има посветен централизиран модул/уред за управување.
Решението мора да обезбеди лесен за употреба веб-инсталатер кој овозможува распоредување WAF користејќи едноставен процес базиран на водечка конзола за инсталација.
Решението мора да обезбеди поддршка за API што овозможува автоматско распоредување на WAF во средини DevOps.
Уредот за управување со решенија мора да може да управува до 200 WAF уреди
Уредот за управување со решенија мора да може да се справи со до 40.000 поставени SSL сертификати (големина на клучот од 1024 бити).
Управувањето со решенијата мора да може да поддржува "muti tenancy" за управување со уреди.
Решението мора да доаѓа со веб-административен интерфејс и GUI.
Решението мора да има две порти за управување за да поддржува управување надвор од опсегот.
Уредот за управување со решенија мора да поддржува централизирано управување и известување за повеќе уреди за следење.
Уредот за управување со решение во просторија мора да може да управува со инстанца на WAF-уредот што е распореден во платформата AWS и истовремено да управува со уред WAF што е распореден кај крајниот корисник.

Уредот за управување кај корсникот мора да може да управува со инстанца на WAF уред што е распореден во платформата Microsoft Azure и истовремено да управува со уред WAF што е распореден во корисникот.
Кога е обезбедено како виртуелен уред, решението мора да доаѓа како генеричка слика на VM (пар .ovf и .vmdk). Односно, единствена слика на VM за инсталирање на сите компоненти (управувачки сервер, уред за портал, итн.)
Хардверското решение мора да доаѓа со LCD дисплеј кој минимално ги прикажува следните функции: • Прикажи информации за име на домаќин, модел на решение и верзија • Прикажи го статусот на решението (конфигуриран, работи, запрен, итн.) • Информации за мрежата: IP адреса, стандардна IP на портата, • Способност за пинг на стандардната порта; Пинг на IP адреса; Поставете менаџмент IP адреса на апаратот; Поставете го стандардниот портал • Рестартирајте го и исклучете го апаратот.
Решението мора да обезбеди централизирано управување со софтверот за да се поедностави распоредувањето на закрпи и надградбите на WAF уредот.
За време на надградбата на решението, решението не треба да бара никаква човечка интервенција за да се рестартира. Сите рестартирања на системот за време на надградбите треба да бидат автоматски и системот мора да се рестартира сам по потреба.
Решението мора да доаѓа со способности за следење на здравјето на системот за да се обезбеди свесност во реално време за здравјето на сите елементи во распоредувањето на решението. Здравствениот мониторинг мора минимално да доаѓа со предупредувања/аларми за следните прашања: • Редундантност и висока достапност • Оптоварување и капацитет • Мрежно поврзување • Хардверски проблеми • Несовпаѓање на конфигурацијата помеѓу различни компоненти

Висока достапност и преформанси на WAF решението
Решението мора да поддржува висока достапност.
Решението мора да има вграден модул за бајпас (fail-open) кога хардверскиот уред е распореден во режим на линија.
Хардверскиот уред мора да има минимум 2 внатрешни бајпас сегменти.
Решението мора да може да поддржува операции и распоредување со повеќе јазли.
Решението мора да поддржува VRRP или механизам за висока достапност.
Хардверскиот уред мора да поддржува додаток на хардверски модул за забрзување SSL.
Решението мора да може да поддржува пропусната брзина на линијата и доцнењето под милисекунди за да не влијае на перформансите на веб-апликацијата.

Носителот на набавката е должен за решението (заштитен ѕид на веб апликација WAF) да вклучи и обезбеди: инсталација на истиот во времетраење од минимум 5 (пет) дена, 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.

Носителот на набавката е должен за решението (заштитен ѕид на веб апликација WAF) да обезбеди претплата за период од 3 (три) години.