Приложение № 2

към рамков договор № 93-00-97/03.07.2020 г.

Заявка

по рамков договор № 93-00-97 от 03.07.2020 г.

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*22*
Описание на дейност/проект съгласно ПГ:	*Закупуване на софтуер за сканиране за уязвимости и киберзащита*	
CPV код	*48000000-8*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**		*Обща сума в размер на 92 470,00 лв. без ДДС*[1]
Срок за плащане: *(еднократно, на части, периодично или др.)*		*Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставкаи фактура.*
Плащане с акредитив / Авансово плащане (условия) ДА/НЕ		*НЕ*
Документи за плащане с акредитив		*неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*Съгласно чл.1 ал. 2 от Договора, заявката следва да бъде изпълнена след осигурено финансиране от страна на Възложителя.* *Срок за осигуряване – до 4 месеца от подписване на заявката.* *Срок за доставка – до 60 дни след получаване на уведомление за осигурено финансиране от страна на Възложителя.*
Гаранционен срок:		*Съгласно условията на ТС*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*		*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка.*
Приложения: (*напр: технически параметри, образци на отчетни документи*)		*Техническа спецификация*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		
Ръководител на проект/дейност по заявката (напр.: представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“		

[1] Заявката се подписва под условие и ще бъде изпълнена при осигурено финансиране от страна на Възложителя.

АД по заявката		
Ръководител на проект/дейност по заявката		
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

За закупуване на софтуер за сканиране за уязвимости и киберзащита

1. Обект на заявката

Обекта на заявката съгласно Общия терминологичен речник – CPV е с код, както следва:

CPV код	Описание
48000000-8	Софтуерни пакети и информационни системи

2. Обща информация

Агенция по вписванията поддържа и развива информационни системи от национално значение. За поддържане на високите нива за мрежова и информационна сигурност е необходимо закупуване на софтуер за сканиране за уязвимости и киберзащита.

Тези сканирания дават на организацията представа за това пред какви заплахи за сигурността може да са изправи, като дават представа за потенциални слабости в сигурността, присъстващи в тяхната публична среда и какво виждат злонамерените групи за организацията. Повишаване на киберзащитата в АВ, чрез централизиране на управлението при кибер атаки и потенциални заплахи посредством услуги и инструменти за автоматизация. Тази автоматизация се извършва чрез обединяване на всички интеграции, определяне как трябва да се изпълняват задачите и разработване на план за реакция при инциденти, който отговаря на нуждите на АВ. Осигуряването на софтуер за сканиране за уязвимости и киберзащита трябва да покрива минимум 1500 броя активни устройства за периода на техническа поддръжка.

3. Предмет

Необходимо е да бъде осигурен софтуер за сканиране за уязвимости и киберзащита при следните минимални технически изисквания:

Спецификация – минимални изисквания	
REQ. 1	Да се достави софтуер за сканиране на уязвимости в инфраструктурата на Възложителя. Решението трябва да осигури всички необходими лицензи с права за ползване на всички изисквани функционалности за минимум 1500 броя активи (асети);
REQ. 2	Предложеното решение да включва функционалност за централизирано управление на откритите след сканиране уязвимости в мрежата и критичните системи и да предоставя подробен отчет от направените тестове на уязвимостите;

REQ. 3	Предложеното решение за сканиране и управление на уязвимости трябва да бъде изпълняван от програмен код инсталиран на място (във вътрешната мрежа на Възложителя, на съществуваща Линукс базирана виртуална среда.)
REQ. 4	Предложеното решение да може да сканира системи и устройства с IP адреси за актуални уязвимости в информационната сигурност;
REQ. 5	Предложеното решение да включва функционалност за сканиране, чрез инсталиран агент върху крайното устройство, който да предоставя подробна информация за използването на крайното устройство. В случай, че крайното устройство не е налично, агента да извърши сканирането веднага след стартирането му;
REQ. 6	Предложеното решение да включва функционалност получените данни от сканирането да могат да се сортират в различни полета, които се създават от администратора. Сортирането да включва като минимум: • Агенти; • Типове крайни устройства; • Открити заплахи и уязвимости; • Сайтове и локации; • Операционни системи; • Инсталирани програми; • Отворени портове; • Проследяване на отстраняването на уязвимостите; • Автоматично отстраняване на уязвимост;
REQ. 7	Предложеното решение да бъде с 64 битова архитектура и да може да се инсталира на минимум следните платформи: • Ubuntu Linux; • Microsoft Windows Server 2016, 2019, 2022; • Red Hat Enterprise Linux Server 7, 8, 9;
REQ. 8	Предложеното решение да включва централна конзола за управление на всички инсталирани скенери, като предоставя обобщени данни за сканирането и потребителският достъп, без да се изискват допълнителни модули или софтуер;
REQ. 9	Предложеното решение да включва функционалност за ролеви достъп с предварително зададени и персонализирани роли;
REQ. 10	Предложеното решение да включва интеграция с Active Directory, Kerberos или която и да е LDAP съвместима директория;
REQ. 11	Предложеното решение да включва интеграция със ServiceNow, Jira или друга Ticketing система, която да предоставя възможност за автоматично отваряне на заявки за поддръжка при откриване на нови уязвимости и затварянето им, когато уязвимостите са фиксирани;
REQ. 12	Предложеното решение автоматично да актуализира базата си данни за уязвимости, без да се налага рестартиране, което да позволява на потребителите да изпълняват сканиране за най-новите уязвимости веднага, без прекъсване на работата; в предварително дефиниран часови диапазон;

REQ. 13	Предложеното решение да включва интеграция с виртуални платформи на VMware, която да осигурява автоматично и динамично проследяване на виртуални активи и оценка на риска им;
REQ. 14	Предложеното решение да включва функционалност за планирани сканирания, които да са повторяеми през определени времеви прозорци и интервали;
REQ. 15	Предложеното решение да включва функционалност за използване на двупосочен API за интеграция с други софтуерни решения;
REQ. 16	Предложеното решение да включва функционалност за запазване на потребителските имена и паролите, които използва по време на сканирането в дигитален защитен и криптиран сейф;
REQ. 17	Предложеното решение да включва вграден механизъм за откриване и локализиране на работещи хостове чрез ICMP и TCP/UDP механизми и да може да открива: • затворени портове; • операционна система; • системни функции; • отворени портове; • работещи услуги; • приложения; • потребители; • групи;
REQ. 18	Предложеното решение да включва предварително дефинирани шаблони за сканиране с различни цели (откриване, оценка на уязвимости, съответствие с конфигурацията, съответствие с нормативните изисквания, най-добри практики и т.н.);
REQ. 19	Предложеното решение да включва функционалност за редактиране/конфигуриране на предварително дефинираните шаблони за сканиране с цел избор/смяна на портове, които да бъдат сканирани и избор и смяна на метод за определяне на типове хостове;
REQ. 20	Предефинираните шаблони за сканиране да могат да бъдат модифицирани за извършване на специфични проверки като например SCADA audit, PCI Internal and External audit, Microsoft hotfix, Web audit, Internal DMZ audit, CIS, DISA, Full audit, Denial of service audit;
REQ. 21	Предложеното решение да включва функционалност за дефиниране на хостовете и при адреси тип IPv6;
REQ. 22	Предложеното решение да проверява за дефиниран от потребителя подпис за уязвимост и проверка на създаването;
REQ. 23	Предложеното решение да включва функционалност автоматично да категоризира потребители въз основа на множество атрибути (например инсталирана операционна система, тип устройство и др.);
REQ. 24	Предложеното решение да включва функционалност автоматично да открива и маркира нови потребители, веднага щом се появят в мрежата;
REQ. 25	Предложеното решение да включва функционалност автоматично да открива и оценява нови устройства и нови уязвимости в момента, в който те получат достъп до мрежата;

REQ. 26	Предложеното решение да включва функционалност за инвентаризация на всички външни устройства, свързани с даден домейн;
REQ. 27	Предложеното решение да идентифицира известни заплахи и набори от зловреден софтуер, свързани с вече открити уязвимости;
REQ. 28	Предложеното решение да има възможност за бъдещо надграждане на функционалностите, чрез закупуване на допълнителен лиценз от същия производител за проверка на уязвимости, базирани на категориите на „OWASP Top Ten“ и сканиране на WEB 2.0 технологии, включително AJAX, ASP .NET 2.0 и Flash базирани сайтове;
REQ. 29	Решението да включва функционалност за анализиране на данните на уеб сайтове и да открива доказателства за пропуски в сигурността, като например SQL инжектиране, cross-site scripting (CSS/XSS), backup script files и други проблеми, произтичащи от софтуерни дефекти или грешки в конфигурацията;
REQ. 30	Предложеното решение да включва функционалност за сканиране в облачна инфраструктура, включително AWS и Azure;
REQ. 31	Предложеното решение да предоставя примери за най-добри практики и вградени шаблони за сканиране на различни корпоративни и/или регулаторни мрежи, включително PCI, HIPAA, SOX и SCADA;
REQ. 32	Предложеното решение да включва функционалност при сканиране на уязвимости в него да бъде включена оценка на конфигурацията и съответствието;
REQ. 33	Предложеното решение да включва функционалност за персонализиране на политиките в потребителския интерфейс;
REQ. 34	Предложеното решение да включва функционалност за приемане на допустими уязвимости на индивидуална конфигурация на ниво индивидуален актив;
REQ. 35	Предложеното решение да включва функционалност за приоритизиране на уязвимостите и показване на насоки за отстраняване на уязвимостта;
REQ. 36	Предложеното решение да включва функционалност за централизирано управление и промяна на политиките и да открива неправилни конфигурации в работната среда. Да открива и показва хостовете, които не отговарят на настройките на конфигурационната политика по зададен елемент;
REQ. 37	Предложеното решение да осигурява една точка на управление за всички отчети, независимо от това къде се извършва сканирането в мрежата, без това да налага закупуването на допълнителни модули или софтуер;
REQ. 38	Предложеното решение да включва функционалност за разпространение на отчетите от интерфейса по имейл.
REQ. 39	Предложеното решение да включва функционалност за генериране на отчети в следните формати: HTML, PDF, CSV и XML.
REQ. 40	Предложеното решение да включва функционалност за генериране на следните типове отчети: • Управленски отчет; • Отчет за тенденции; • Отчет за уязвимости;

	• Отчет за открити устройства/асети; • Отчет за отстранени уязвимости;
REQ. 41	Предложеното решение да включва функционалност за представяне на количествени показатели (например от 1 до 1000) за риска от уязвимостта и качествени показатели за критичност (например висока, средна, ниска);
REQ. 42	Предложеното решение да включва функционалност за предоставяне на доклади и инструкции за свързване към външни бази данни за пачове, изтегляния и препратки.
REQ. 43	Предложеното решение да включва функционалност за създаване на задачи и делегирането им към отделни служители или екип, включващи конкретни цели и SLA с показатели за ефективност при отстраняването на уязвимости. Всички показатели да бъдат динамични и да позволяват генериране на управленски доклад с обобщена информация за статуса и прогреса на изпълнението на поставените задачи;
REQ. 44	Предложеното решение да включва интеграция с Governance, Risk & Compliance (GRC) решения;
REQ. 45	Предложеното решение да включва интеграция с решение за тестване на сигурността на информационни системи с цел симулиране на действителни атаки и тестване на защитата, с утвърждаване на резултатите от скенера за уязвимост, като използва автоматизиран процес със затворен цикъл;
REQ. 46	Предложеното решение да включва интеграция със SIEM решения като: IBM, Rapid7, RSA, McAfee, Micro Focus, RSA, Splunk и други;
REQ. 47	Участникът трябва да осигури техническа поддръжка от производителя за целия срок на предоставеното право на ползване;
REQ. 48	Техническа поддръжка трябва да бъде достъпна по телефона, чрез електронна поща и/или уеб интерфейс;
REQ. 49	Поддръжката трябва да включва права за ползване на софтуерни обновления, софтуер за корекции на грешки и помощ при отстраняване на несъвместимости с документираното поведение на софтуера;
REQ. 50	Поддръжка от производителя за период от минимум 36 (тридесет и шест) месеца
REQ. 51	Поддръжка от производителя за получаване на нови версии на софтуера за срок от минимум 36 (тридесет и шест) месеца

***4. Допълнителни изисквания**:*

4.1. Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или негово официално представителство за правото на разпространение/доставка и предоставяне на гаранционна поддръжка на предлаганите софтуерни продукти на територията на Република България.

4.2. Актуализации на програмите, фиксове (поправки) и предизвестия за информационна сигурност;

4.3. Програмни кодове за обновяване;

4.4. Основни продуктови и технологични версии, което включва версии, свързани с общата поддръжка, подбрани версии, свързани с поддържане на функционалността и актуализации на документи;

4.5. Съдействие при подаване на заявки за техническа помощ;

4.6. Достъп до web базирана система, включително и възможност за подаване на заявки за техническа помощ чрез Интернет;

4.7. Право на ъпгрейд на продуктите, което включва получаването на нови версии на софтуера, релийзи за поддръжка и софтуерни пачове, с цел да се осигури стабилност, предсказуемост и подобряване на сигурността, чрез елиминирането на известните проблеми;

4.8. Осигуряване на възможност за изтегляне от производителя на бюлетини, техническа документация, версии на продуктите и др.

4.9. Всички софтуери трябва да бъдат доставени на името на Агенция по вписванията.

5. *Други условия:*

В рамките на една седмица да се осигурят до 2 онлайн семинара до 2 часа всеки, с цел базово запознаване на експерти (екип до петима служители) от Агенция по вписванията от дирекция „ИОТ“ с основни функционалности на продукта.

6. *Място на изпълнение*

Място на изпълнение: гр. София, ул. „Елисавета Багряна“ № 20.