Заявка

по рамков договор № РД-14-40 от 29.05.2023 г.
(вх. № ПО-16-2224/29.05.2023 г. на „Информационно обслужване“ АД)

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*24*
Описание на дейност/проект съгласно ПГ:	*Осигуряване на софтуер за защита, видимост и одит на потребители, сървъри и конфигурации*	
CPV код	*48200000-0*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика*) **без ДДС**	*930 000,00 лв.*	
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Периодично, както следва:* *През 2024 г. - след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по осигуряване на лицензи за софтуер за защита, видимост и одит на потребители, сървъри и конфигурации и класифициране на данните в ИКТ средите за целия период и издадена фактура за първия 12 месечен период на стойност 310 000,00 лв. без ДДС.* *През 2025 г. – срещу фактура за втория 12 месечен период на стойност 310 000,00 лв. без ДДС, издадена в началото на периода.* *През 2026 г. – срещу фактура за третия 12 месечен период на стойност 310 000,00 лв. без ДДС, издадена в началото на периода.*	
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата*)	*Срок за осигуряване до 28.06.2024 г.* *Срок на валидност: минимум 36 месеца, считано от датата на осигуряване на лицензите*	
Гаранционен срок:	*неприложимо*	
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 извършените дейности по осигуряване на лицензи за софтуер за защита, видимост и одит на потребители, сървъри и конфигурации и класифициране на данните в ИКТ средите*	
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*	
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“ АД по заявката	
Ръководител на проект/дейност по заявката	
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД	

ТЕХНИЧЕСКИ ПАРАМЕТРИ

за

осигуряване на софтуер за защита, видимост и одит на потребители, сървъри и конфигурации и класифициране на данните в ИКТ средите на НЗОК

1. ЦЕЛ

Целта е осигуряване на лицензи за софтуер за защита, видимост и одит на потребители, сървъри и конфигурации и класифициране на данните в ИКТ средите на НЗОК.

Минималните изискванията са, както следва:

1.1. Общи изисквания относно системата

REQ.1.	Тип решение: софтуер
REQ.2.	Брой лицензи: за минимум 2750 потребителски акаунти/пощенски кутии/сървъра
REQ.3.	Брой лицензи: за минимум 150 мрежови устройства

1.2. Изисквания относно събирането и съхранението на данни

REQ.4.	Да работи без да използва агенти, така че да не влияе негативно на производителността на системите и да не спира работния процес.
REQ.5.	Да не се използват никакви не документирани методи за събиране на данни от системите на организацията, тъй като подобни методи могат да доведат до отказване на поддръжка от Microsoft или от други ключови производители.
REQ.6.	Да събира сурови машинни данни и да ги преобразува в опростена, ясна информация за всяко потребителско действие, за да се улесни вземането на правилни решения от организацията.
REQ.7.	Да обединява данни от множество източници (логове за събития, извадки от настройките на средите, записи на действията, свързани с промени и т.н.), за да се извлече възможно най-пълната и надеждна одитна информация, без пропуски.
REQ.8.	Да събира и предоставя пълни детайли за всяка промяна и опит за достъп, включително кога и къде промяната или опитът за достъп са направени, кой ги е направил и какво точно е променено или достъпено.
REQ.9.	Да извършва цялостно сравнение и да събира стойностите преди и след промяната за всички променени обекти.
REQ.10.	Да ползва система за съхранение на данни на две нива (SQL база от данни за отчитане и файлово-базирана система за архивиране на данни в компресиран формат за дълготрайно съхранение). Този архив трябва да съдържа цялостна одитна информация за до повече от 10 години, без да намалява производителността на системата, като трябва да осигурява лесен достъп до данните за целият период.
REQ.11.	Да събира одитна информация от локални и от облачни приложения и да ги съхранява в защитен, централизиран архив, което да позволява използването на общи аларми, търсене, отчитане и анализ на рисковете по сигурността.

1.3. Изисквания относно поддържаните системи и обхвата на одитирането

REQ.12.	За активната директория (Active Directory) и груповите политики: • Да докладва за промени в активната директория и в груповите политики;

	• Да събира информация за промените във времето на активната директория и на груповите политики, включително за участниците в групи с множество домейни и различни права на достъп; • Да одитира вписванията; • Да поддържа доверени и недоверени домейни; • Да докладва за промени в Azure AD групи, потребители, пароли, роли, приложения, сервизни принципи, устройства и контакти.
REQ.13.	За MS Exchange: • Да събира информация за промените на конфигурациите в Exchange Server, Exchange бази от данни, пощенски кутии, делегиранията на пощенски кутии и правата за достъп; • Одитиране на достъпа до пощенски кутии от различен от собственика им потребител; • Да се поддържа Exchange Server 2016 и Exchange Server 2019; • Да докладва за административни промени по Exchange Online, както и промени по пощенски кутии, потребители, групи, права за достъп, политики и роли; • Да докладва за права на достъп до делегирани пощенски кутии, както и дали правата са получени директно или по групова политика.
REQ.14.	За Windows File Servers • Да докладва за промени по файлове, папки, споделени пространства и права за достъп; • Да докладва за преместени, преименувани или копирани файлове; • Да дава информация за успешни и неуспешни опити за прочитане на данни; • Да дава информация за промените във времето на ефективните права за достъп, включително и кои потребители имат превишени права за достъп; • Да създава отчети за собствеността на данните, използването на данните и обема на данните, отдавна неизползвани файлове и дублирани файлове; • Да докладва за чувствителни данни, включително къде са разположени, кой има активни права да ги достъпва и кой е собственик на данните, както и за успешни и неуспешни опити за достъп до данните и опити за промяна на правата за достъп до тях; • Да поддържа множество файлови сървъри и файлови устройства, разположени в няколко физически обекта, домейна и организации; • Да се поддържа Windows Server 2016 и Windows Server 2019
REQ.15.	За мрежови устройства • Да докладва за промени по конфигурациите на мрежовите устройства на организацията; • Да докладва за успешни и неуспешни опити за вписване в мрежовите устройства, директно или чрез VPN свързване; • Да докладва за сканирани заплахи от мрежовите устройства; • Да докладва за хардуерни неизправности на мрежовите устройства; • Да се поддържат като минимум следните видове мрежови устройства: Fortinet FortiGate, Cisco ASA, Cisco IOS, Palo Alto, SonicWall, Juniper, Pulse Secure, Aruba

REQ.16.	За NetApp • Да докладва за промени по файлове, папки, споделени пространства и права за достъп; • Да докладва за преместени, преименувани или копирани файлове; • Да дава информация за успешни и неуспешни опити за прочитане на данни; • Да дава информация за промените във времето на ефективните права за достъп, включително и кои потребители имат превишени права за достъп; • Да създава отчети за собствеността на данните, използването на данните и обема на данните, отдавна неизползвани файлове и дублирани файлове; • Да докладва за чувствителни данни, включително къде са разположени, кой има активни права да ги достъпва и кой е собственик на данните, както и за успешни и неуспешни опити за достъп до данните и опити за промяна на правата за достъп до тях; • Да се поддържат следните версии на NetApp: NetApp ONTAP 9.0 – 9.9; NetApp Clustered Data ONTAP 8.3, 8.3.1, 8.3.2
REQ.17.	За SQL Server • Да докладва за промени по правата за достъп до SQL Server, по сървърните инстанции, по потребителските роли в тях, по базите от данни, по конкретни таблици, колони, съхранени процедури и т.н.; • Да докладва за промени по съдържанието на базите от данни; • Да докладва за вписванията в базите от данни (успешни и неуспешни); • Да се поддържа SQL Server 2016 и SQL Server 2019.
REQ.18.	За VMware • Да докладва за промени по vCenter и неговите сървъри, клъстери, групи от ресурси, хардуерни настройки и настройки на виртуални машини, правата за достъп до тях и техният статус (дали са включени или изключени); • Да поддържа следните версии на VMware: VMware ESX/ESXi: 7.0; VMware vCenter Server: 7.0
REQ.19.	За Windows Server • Да докладва за промени по настройките на сървъра — хардуер и софтуер, услуги, приложения, мрежови настройки, настройки на регистри, DNS, файлови дялове и други; • Да предоставя информация за промените по локалните политики за одитиране, неизправностите в Windows услугите, принудителните спирания на системите и промените по настройките за време; • Да предоставя информация за промените във времето на настройките на Windows сървърите, включително име и версия на операционната система, статус на антивирусната система, файловите дялове, локалните потребители и групи, услугите и инсталираните програми • Да се поддържа Windows Server 2016 и Windows Server 2019

1.4. Изисквания относно одити и аларми

REQ.20.	Да включва предварително зададени одитни отчети и dashboard-ове, които предоставят детайлна информация за промени, опити за достъп и настройки, представени в четим вид, позволявайки на потребителите да филтрират, сортират и извличат одитните данни.

REQ.21.	Да позволява на потребителите лесно да изградят собствен отчет, базиран на конкретни изисквания, включително отчети, които да обхващат множество, разнообразни системи.
REQ.22.	Автоматично да изпраща отчети до зададени получатели по e-mail или да ги запазва в споделен файлов дял по зададен график (веднъж дневно, седмично, т.н.).
REQ.23.	Да поддържа извличането на отчети в няколко различни формата, включително PDF, XLS(X), DOC(X) и CSV.
REQ.24.	Да позволява на потребителите лесно да сортират и филтрират одитната информация чрез Google-подобна интерактивна търсачка, така че те лесно да открият точните данни, които са им необходими.
REQ.25.	Да показва настоящите настройки на одитираните среди или как са изглеждали настройките в даден отрязък от миналото, включително активните права за достъп на даден потребител или обект, настройките на груповите политики и детайлите за настройките на Windows сървърите.
REQ.26.	Да включва готови за ползване отчети, които са пригодени за проверяване на съвместимост със стандарти като ISO/IEC 27001, GDPR, PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST800-53, CJIS, FERPA, NERC CIP.
REQ.27.	Да известява чрез e-mail или чрез SMS съобщение отговорните екипи за подозрително поведение или събития, които могат да прераснат в инциденти по сигурността, включително активност, която надвишава изчислените норми (аларми на базата на повторяемост на едно и също събитие).
REQ.28.	Да може да докладва чрез SQL SRS, да може да използва отчетните услуги на SQL сървъра по индустриален стандарт (да поддържа и безплатната версия SQL Express), за да се предоставя широка гама от одитни отчети.

1.5. Изисквания относно сигурността на информацията

REQ.29.	Да притежава Dashboard-ове за оценяване на ИТ рисковете, които да позволяват на потребителите да идентифицират и оценят рисковете по три ключови показателя: управление на акаунти, права за достъп до системите за сигурност и управление на данни.
REQ.30.	Да притежава Dashboard за откриване на аномално поведение, чрез който да се подобрява засичането на зловредни акаунти в ИТ средата, като предоставя агрегирани данни за аномалното потребителско поведение и да поставя съответна оценка на риска.
REQ.31.	Да предоставя отчети за потребителско поведение и за анализиране на пропуските в системите за наблюдение. Да предоставя информация за потенциални инциденти, свързани със сигурността, като например действия извън нормалните бизнес часове на деня, необичайни вписвания в системите, голям брой неуспешни опити за действия, достъпване на архивирани данни, действия от досега неактивни потребителски акаунти и наличие на потенциално опасни файлове на файловите сървъри.

1.6. Изисквания относно функции от общ характер

REQ.32.	Да има управление на Event logs: Автоматично да се събират, обединяват и архивират данните за настъпили събития, така че администраторите да могат да одитират събития от общ характер, събития, свързани с услуги, вписвания на потребители и състояли се сесии с отдалечен достъп.
REQ.33.	Да има Dashboard за състоянието на системите и за издаване на ежедневен обобщаващ отчет, който да позволява на потребителите да открият проблеми, които влияят на целостта на събраните одитни данни, като лесно да може да

	се достигне до конкретната детайлна информация, която е необходима, за да се отстранят проблемите. Потребителите да могат да получават email отчет веднъж дневно, който да обобщава извършените действия през последните 24 часа.

1.7. Изисквания към интерфейса за управление на системата

REQ.34.	Да има централизирана конзола за управление, която да поддържа множество сървъри, като всеки да може да има собствени, различни настройки.
REQ.35.	Да позволява интегрирането с други решения, да поддържа одитирането на множество от системи и приложения, включително системи, които са интегрирани чрез RESTful API, като всичко трябва да бъде обединено, позволявайки използването на dashboard-ове и отчети за комплексни среди от разнообразни системи.
REQ.36.	Решението да дава цялостен изглед над средата, като всички функционалности да са част от единна платформа, премахвайки необходимостта от използването на множество отделни решения.
REQ.37.	Правата за достъп да са ролево базирани. Платформата трябва да позволява фино разделяне на задълженията по наблюдението на системите от различните потребители, така че всеки от тях да има достъп само до необходимите му системи и настройки.

1.8. Изисквания за възможностите за интегриране с други решения

REQ.38.	Да има напълно документиран RESTful API интерфейс за интеграция с други решения, да може да се интегрира с решения за сигурност, за съответствие с различни сертификати и за автоматизиране на ИТ процесите и на работата на бизнес приложенията, така че да се предостави централизирано одитиране и отчетност или да се улесни управлението на промените и на действията по поддръжката на системите.
REQ.39.	Да може да се интегрира със SIEM решения, за да се защитят инвестициите на организацията в SIEM платформи, като се предостави интегриране с определени SIEM решения, обогатявайки събраните от тях данни, предоставяйки контекста на събитията.
REQ.40.	Да позволява безплатно да се добавят add-on добавки за интегриране с други решения, да има възможност за добавяне на безплатни, предварително създадени add-on добавки, които да улесняват интегрирането с решения, като например SIEM, ServiceNow ITSM и Linux системи.

1.9. Изисквания относно откриването и класифицирането на данни

REQ.41.	Да предоставя предварително зададени отчети, които предоставят детайлна информация за това къде се намират чувствителните данни, какво е съдържанието им, кой може да ги достъпи и кой реално ги използва, както и до кои чувствителни файлове има излишни права за достъп от потребители. Възможност за абонамент към автоматични отчети, които периодично да се изпращат към посочени email адреси или споделени директории.
REQ.42.	Да подпомага отговорните лица за риска и сигурността на данните и съответствието със стандарти и регламенти на организацията да приоритизират техните усилия и да защитят данните в съответствие с тяхната степен на важност. Решението да позволява на експертите да предотвратят лични данни, медицинска информация, банкова информация и данни съдържащи интелектуална собственост да се съхраняват извън отредените за

	това места, както и да могат да се наложат политики, които да гарантират, че организацията е защитила данните си и е в съответствие с наложените изисквания.
REQ.43.	Да предоставя предварително зададени правила за идентифициране на кои данни попадат под регламентите на GDPR, PCI DSS, HIPAA и GLBA, както и на PII, PHI, запис на данни, които са забранени по GDPR и запис на общи финансови данни.
REQ.44.	Да идентифицира дисковите дялове с най-висока концентрация на чувствителни данни и да открива всички данни тип лични идентифициращи данни, медицинска информация, банкова информация и данни съдържащи интелектуална собственост, които се намират извън защитените локации, така че да предоставя възможност да се реагира подобаващо.
REQ.45.	Да позволява на потребителите да модифицират предварително зададените правила за класифициране и да създават свои собствени такива.
REQ.46.	Да позволява на потребителите бързо да открият всички индексирани файлове, които съдържат зададени от потребителите ключови думи.
REQ.47.	Да се използва статистически анализ от концепции с множество думи, за да се изградят сложни правила за класификация на данните, както предварително зададени, така и с възможност за изграждане на собствени такива правила.
REQ.48.	Да се събират и да се натрупват сложни метаданни, които не са базирани на фрази, приблизителност, ключови думи или предварително зададена таксономия, като по този начин се елиминира необходимостта да се ре-индексира цялото хранилище на данни, когато някое правило за класифициране е добавено или променено.
REQ.49.	Автоматично да се засичат, класифицират и индексират нови файлове и промени по настоящи файлове, без необходимост да трябва да се събират наново всички данни от хранилището.
REQ.50.	Да може да проверява дали правата за достъп до чувствителни данни са в съответствие с корпоративните политики и наложените регулации и да могат да се включват притежателите на данните при определяне кой ще може да ги достъпи.
REQ.51.	Да предоставя целия контекст покрай действията, свързани със защитената информация, и да подсигурява, че потребителските действия, които застрашават целостта на тези данни, като например непозволени промени в правата за достъп, са засечени и докладвани.
REQ.52.	Да може да анализира какво количество данни са били достъпени от зловредно лице и кои точно части от тези данни са били реално видяни, модифицирани или изтрити, така че да могат да се известят всички засегнати страни.
REQ.53.	Да показва точното местонахождение на защитените данни и да предоставя доказателства, че само оторизирани служители могат да четат, модифицират, споделят и изтриват файлове от критична важност.
REQ.54.	Да поддържа интеграция с Microsoft Exchange сървър и Outlook Web Access.
REQ.55.	Да се управлява централизирано и да позволява централизирано създаване и управление на категории от данни и правила.
REQ.56.	Да поддържа разпознаване и класификация на данни в графични файлови формати като .pdf документи и изображения.
REQ.57.	Да поддържа класификация на мета данни.
REQ.58.	Да поддържа класификация на данни на Windows файлов сървър.

REQ.59.	Да поддържа класификация на данни на бази от данни, минимално SQL Server 2016 и SQL Server 2019.
REQ.60.	Да поддържа класификация на данни на пощенски сървър, минимално Exchange Server 2016, Exchange Server 2019 и Exchange Online.
REQ.61.	Да предоставя функция за поставяне на маркировка (тагове) на откритите файлове с класифицирани данни (директно в метаданните на файловете), така че да се улесни интеграцията с други решения, като например с решения за защита от изтичане на данни, които могат да използват таговете за създаване на политики за сигурност с по-голяма точност.

1.10. Поддръжка

REQ.62.	Срок на техническа поддържка директно от производителя - минимум 36 месеца.
REQ.63.	Получаване на нови версии на софтуера - минимум 36 месеца.
REQ.64.	Срок за правото на използване на софтуера, обновяване на сигнатури и дефиниции - минимум 36 месеца.

2. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя на софтуера или от официален негов представител с права за извършване на разпространение и предоставяне на поддръжка на предлаганите софтуерни продукти на територията на Република България.

3. МЯСТО НА ИЗПЪЛНЕНИЕ

Място за изпълнение на заявката е ЦУ на НЗОК с адрес: гр. София, ул. „Кричим“ № 1.