Приложение № 2

към рамков договор № РД02-29-240 от 31.12.2020 г.

ЗАЯВКА по Рамков договор № РД02-29-240 от 31.12.2020 г.	☒
ЗАЯВКА по Рамков договор № РД02-29-240 от 31.12.2020 г. (актуализирана)	☐ [1]

Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*18*
Описание на проект съгласно ПГ:	*Осигуряване на специализиран софтуер за антивирусна защита (EDR) на крайни потребителски станции и сървъри*	
CPV код	*72260000*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МЕУ-11898/14.08.2025*	
Изискване за достъп до класифицирана информация ДА/НЕ	*Не*	

Стойност: (*стойността следва да съответства на заложената в Планграфика***) без ДДС***, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*	*143 600, 00 лв.*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно. След подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ осигуряване на специализиран софтуер за антивирусна защита (EDR) на крайни потребителски станции и сървъри и издадена фактура*
Плащане с акредитив или авансово ДА/НЕ	*Не*
Документи за плащане с акредитив или авансово	*Неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Срок за осигуряване: до 4 месеца след подписване на заявката.* *Срок на валидност: 36 месеца, считано от датата на осигуряване*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*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 осигуряването на специализиран софтуер за антивирусна защита (EDR) на крайни потребителски станции и сървъри за 36 месеца*
Приложения: (*напр: технически параметри, образци на отчетни документи***)**	*Технически параметри*

[1] Отбелязва се в случай че заявката е актуализирана

Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:		
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		

Ръководител на договора от страна на БЕНЕФИЦИЕРА:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата*

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

от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

ОСИГУРЯВАНЕ НА СПЕЦИАЛИЗИРАН СОФТУЕР ЗА АНТИВИРУСНА ЗАЩИТА (EDR) НА КРАЙНИ ПОТРЕБИТЕЛСКИ СТАНЦИИ И СЪРВЪРИ

София, 2025 г.

1. ЦЕЛ

Цел на проектът е осигуряването на специализиран софтуер за антивирусна защита (EDR) на крайни потребителски станции и сървъри за нуждите на ГД ГРАО.

2. ОБХВАТ

Обхватът на поръчката е да се осигури на ГД ГРАО специализиран софтуер за антивирусна защита (EDR) на крайни потребителски станции и сървъри- решение за защита и разследване на заплахи на ниво крайна точка, отговарящо на следните минимални изисквания:

REQ.1.	Предложеното решение трябва да включва лицензи за 280 крайни точки, от които 250 работни станции и 30 сървъра. Предложените лицензи трябва да с валидност и включена поддръжка за период от 36 месеца.
REQ.2.	Всички модули на решението трябва да са предоставени от един производител.
REQ.3.	Решението трябва да може да засича и блокира атаки, които не използват файлове, а работят предимно в паметта на крайните точки.
REQ.4.	Решението трябва да може да засича в Windows системи зловредно изпълнение на код директно в паметта на системите, като при наличие на политика за блокиране, да може да прекъсне зловредните процеси. Функцията трябва да може да защитава от семейства зловреден код като Cobal Strike, Emotet, Beacon, Lockbit 3.0, Black Basta, Dridex, BazarLoader, Conti, Reflective DLL Shellcodes, IceID. Ако има наличие на криптирани файлове от зловредните процеси, решението трябва да може да възстанови засегнатите файлове от snapshot.
REQ.5.	Решението трябва да може да защитава от атаки базирани на MS Office и RTF файлове, които често се използват за фишинг. Използвайки алгоритми за машинно самообучение, решението трябва да може да засича зловреден код, който е вграден в документи, преди даденият файл да бъде изпълнен.
REQ.6.	Решението трябва да може да сканира скрипт файлове на Windows\Linux\Mac операционни системи.
REQ.7.	Решението трябва да може да засича атаки базирани на .NET framework, както и съдържание, което е свалено чрез скриптове от зловредна активност. Решението трябва да може да блокира тези действия.
REQ.8.	Решението трябва да може да засича и блокира познати атаки.
REQ.9.	Решението трябва да може да засича и блокира непознати атаки на база на алгоритми за машинно самообучение и изкуствен интелект, както и на анализ на поведението на засечените атаки.
REQ.10.	Решението трябва да има ниско ниво на грешни показания – ниско или много ниско ниво според тестовете на AV Comparatives.
REQ.11.	Решението трябва да разполага с блокиращи механизми за зловреден код преди да бъде изпълнен (pre-execution), както и да може да прекъсне зловредното поведение по време на изпълнението му (on-execution).
REQ.12.	Решението трябва да може периодично да сканира файлове „в покой“, независимо дали в режим на бързо или на цялостно сканиране.
REQ.13.	Решението трябва да може да сканира неизпълними файлове (документи, общи файлови формати) на Windows\Linux\Mac операционни системи.
REQ.14.	Решението трябва да предпазва от уязвимости в паметта на Windows крайни точки (например 0-day злоупотреби), включително Mandatory ASLR, Bottom-Up ASLR, SEHOP, EAF, DEP.

REQ.15.	Решението трябва да може да предоставя защита според поведението на процесите от събраните телеметрични данни от защитените крайни точки.
REQ.16.	Решението трябва да може да поставя оценка на индивидуалното поведение на процеси, както и да извършва корелации и сравнения измежду отделните крайни точки.
REQ.17.	Решението трябва да може да корелира еднакви опасни поведения, които са засечени на различни крайни точки и да ги поставя в общ изглед в конзолата за управление на решението.
REQ.18.	Решението трябва да предпазва от зловредни файлове сваляни от Интернет.
REQ.19.	Решението трябва да може да засича опити за движение настрани (Lateral Movement) от зловредните процеси на атаките (например Pass-the-hash атаки, отдалечено създаване на задачи по график и други).
REQ.20.	Решението трябва да позволява използването на добавените външни индикатори за компроментиране за всички защитени крайни точки или за избрана група от тях.
REQ.21.	Решението трябва да може да засича изпълнявани в паметта техники за избягване на засичане, използвани от зловреден код (например плаващ код, представяне за друг процес, използване на DGA алгоритъм).
REQ.22.	Решението трябва да може да сканира файлове и бързо да разпознава непознати заплахи, чрез използване на fuzzy hashing алгоритми, който откриват прилики в поведението на познати атаки с поведението на нови версии на такива.
REQ.23.	Решението трябва да може да анализа събраните телемтрични данни без те да се филтират предварително на крайните точки, като да не се използват лимити за даден тип данни (например лимит на броя DNS заявки за даден период от време).
REQ.24.	Решението трябва да може да блокира опитите за копиране или изпълнение на криптовируси.
REQ.25.	Решението трябва да може да предпазва от криптовируси на база поведение за непознати криптовирусни процеси.
REQ.26.	Решението трябва да може да мониторира операции с файлове свързани с атаки и да може да прави сравнение дали дадени файлове често се модифицират или реално се криптират.
REQ.27.	Решението трябва да може да засича операции, целящи спиране на Volume Shadow Copy Service (VSS) услугата и изтриване на съхранени VSS архиви на Windows операционни системи.
REQ.28.	Решението трябва да може да засича криптовируси, които правят опити за повреда на Master Boot Record (MBR) на крайните точки (bootkit атаки).
REQ.29.	Решението трябва да поддържа функция за Windows системи, която да позволява възстановяване на файлове в оригиналния им вид ако са били успешно криптирани. Решението трябва да позволява определяне на процента от дисковото пространство на системите, което да е заделено за snapshot копия на файловете.
REQ.30.	Защитата от криптовируси на решението трябва да може да предоставя списък с файлове, които са били успешно криптирани.
REQ.31.	Решението трябва да разполага с напреднала защита от криптовируси в "Kernel" режим, за по-бързо засичане на поведението на типични криптовирусни атаки.
REQ.32.	Защитата от криптовируси не трябва да разчита на възстановяване на целите системи от архивирани копия, когато бъде засечено действие със зловредно криптиране, а защитата трябва да е проактивна.

REQ.33.	Решението трябва да може да предоставя детайлна информация за инциденти с криптовируси, като: - отговорните процеси за криптовирусната атака и коренният файл, от която тя е изпълнена - мрежови свързвания и DNS заявки, които са генерирани от криптовирусните процеси - името или имената на крайните точки, на които са засечени криптовирусни операции, както и имената на обвързаните потребителски акаунти с изпълнението на зловредните процеси
REQ.34.	Защитата от криптовируси трябва да обхваща и скачените мрежови и облачни дялове към крайните точки.
REQ.35.	Решението трябва да може да извършва действия с цел премахване на последици от зловредни действия на крайните точки (за работни станции и сървъри).
REQ.36.	Решението трябва да може да изолира дадена крайна точка от мрежата, като се подсигурява, че ще бъде оставен начин за отдалечен достъп от решението за извършване на допълнителен анализ.
REQ.37.	Изолирането на крайните точки от решението трябва да позволява дефинирането на допълнителни IP адреси и портове, с който изолираната крайна точка да може да комуникира. Трябва да могат да се добавят изключения на глобално ниво (за всички крайни точки) или за избрани подгрупи от крайни точки.
REQ.38.	Решението трябва да предоставя начин за извършване на отдалечена Remote Shell сесия към конкретни крайни точки, предоставяйки на администраторите на решението PowerShell интерфейс до таргетираните крайни точки под Windows или конзолен достъп до таргетирани Linux и MacOS системи.
REQ.39.	Решението трябва да може да групира наличните операции за ответни мерки при засичане на заплахи, които могат да се изпълнят на дадена крайна точка/групи от крайни точки, за съответна заплаха/група от заплахи.
REQ.40.	Решението трябва да позволява лимитиране на правата за Remote Shell достъп на базата на ролеви-базирани правила.
REQ.41.	Решението трябва да може да съхранява цялостен лог запис с всички действия при използване на Remote Shell фунцкията, като да се съхраняват всички изпълнени команди по време на дадена сесия с дадена крайна точка.
REQ.42.	Решението трябва да разполага с функция за автоматично поставяне на опасни файлове под карантина.
REQ.43.	Освен автоматично изтриване на опасни файлове, решението трябва да позволява ръчното маркиране на файлове като такива.
REQ.44.	Решението трябва да позволява добавянето на хеш сумата на даден изпълним файл под Windows системи в списъци за блокиране, предотвратяващи изпълнението му на защитените крайни точки.
REQ.45.	Решението трябва автоматично да предоставя набор от ответни мерки според типа на засечената заплаха.
REQ.46.	Решението трябва да може автоматично да събира всички телеметрични данни в почти реално време (да не се изисква потребителско действие, важащо за всички типове данни).
REQ.47.	Решението трябва да може да съхранява централизирано всички събрани телеметрични данни, за да може да корелира събитията от различни крайни точки. Агентите на крайните точки трябва да разполагат с механизъм за буфериране на събраните данни при временно неналичие на мрежова

	комуникация с централизираното хранилище на решението, за целите на по-късно изпращане при възстановяване на мрежовата комуникация.
REQ.48.	Решението трябва да може да корелира всякакъв тип активи с даден потребителски акаунт и активността му на различни устройства.
REQ.49.	Решението трябва да може да предоставя списъци с всички процеси, услуги, драйвери и автоматични стартирания на процеси за всички защитени крайни точки.
REQ.50.	Решението трябва да може да дава информация за използваната команда в CLI за изпълнението на даден процес.
REQ.51.	Решението трябва да може да дава информация за всички мрежови свързвания и DNS заявки, които са създадени от даден процес.
REQ.52.	Решението трябва да позволява търсене на изпълними файлове по име или по хеш сума.
REQ.53.	Решението трябва да позволява свалянето на конкретни файлове от крайните точки.
REQ.54.	Решението трябва да предоставя информация за всички DNS заявки, разделени по типа на заявките и по получените отговори на тях.
REQ.55.	Решението трябва да позволява събирането на информация за всички събития от даден тип от крайните точки – не трябва да има лимити за броя събития събрани по този начин от даден тип.
REQ.56.	Събраните телеметрични данни от решението трябва да включват минимално следните елементи:
REQ.57.	а) мрежови свързвания от/към крайната точка, с детайли за: адреси, портове, статус на свързванията, количество получени/изпратени данни, дата и време на създаване на свързването, използвани мрежови протоколи, прокси сървъри (ако са налични), URL домейни
REQ.58.	в) данни за всички драйвери, инсталирани на дадена крайна точка
REQ.59.	г) метаданни за файлове (име, път, размер, тип, разширение), хеш сума (минимално MD5, SHA-1 и SHA-256), дигитална сигнатура ако има налична (MD5 и SHA1), време и дата на създаване, време и дата на последна модификация, информация дали файла е свален от Интернет – URL адрес, от който е свален файла
REQ.60.	д) операции с файлове – операции по създаване, преименуване и изтриване на файлове, както и информация за изпълнените процеси, които са изпълнили даденото действие, също и информация за вписаният потребител в крайната точка при изпълнението им
REQ.61.	з) мрежови сесии , които са отворени на крайните точки – включително информация за локален адрес, порт, протокол
REQ.62.	и) Windows сесии по вписване – включително IP на сесията, IP на източника на сесията, тип приложение, време и дата на създаване, отдалечени машини, участващи в сесията, отворени процеси в дадената сесия, потребител, който е отворил дадената сесия
REQ.63.	й) данни за крайните точки, като: име, FQDN, тип на крайната точка, операционна система, статистика за използване на процесор, свободна памет, окупирано дисково пространство, MBR хеш сума, активни процеси на крайната точка, вписани потребители, активни услуги на крайната точка, масово свързани устройства с памет към крайната точка
REQ.64.	к) активни модули на крайните точки: име, размер, хеш сума, адрес, обособен размер на хедъра, асоциирани файлове с модула, защита на хедъра
REQ.65.	л) налични мрежови интерфейси

REQ.66.	о) Регистрите на крайните точки свързани с Autorun, включително ключове и техните стойности
REQ.67.	п) операции в регистрите, с възможност за посочване на допълнителни секции, които се покриват от функциите за мониториране на решението
REQ.68.	р) данни за отдалечени сесии с вписване в крайните точки, включително: използван протокол за автентикация, устройството и потребителя, извършили дистанционното вписване, изпълнени процеси по време на отдалечената сесия
REQ.69.	с) RPC заявки, включително: ниво и тип на услугата по автентикация, използвана от RPC, теаргетирани RPC адрес и порт, RPC източник, RPC UUID, RPC протокол, създадени процеси от RPC
REQ.70.	т) задачи по график, включително: кой е добавил дадена задача в график и времето и датата на последното обновяване, статус на задачата, информация за последното извикване на задачата, използвани аргументи при създаването на задачата, път към действието на задачата, асоциирани файлове със задачата
REQ.71.	у) услуги в операционната система, включително: статус на услугата и под-статус, тип на услугата, използвани данни за вписване от услугата при стартиране, асоциирани бинарни файлове с услугата, изпълнени команди в команден интерфейс от стартиращата програма на услугата, път към използваните файлове от услугата, процесите, които са създали услугата, асоциираните драйвери с услугата
REQ.72.	ф) данни за всички потребители, включително: име, организация, домейн, ниво на достъп, SID, последно вписване, изминало време от последна промяна на парола, имена на крайни точки, в които потребителя се е вписвал, изпълнени процеси от даден потребител
REQ.73.	х) WMI активност – локална и отдалечена, включително: операции, които са генерирали WMI активност, източник на WMI активност, време и дата на създаване, изпълнени процеси в контекста на WMI, постоянни обекти, генерирани от WMI активност, WMI заявки
REQ.74.	Решението трябва да позволява търсенето на който и да е файл с конкретно име (или на част от името му), който се намира на защитена крайна точка, дори да няма взаимодействие с даденият файл от зловреден процес.
REQ.75.	Опцията на решението за търсене на информация от крайни точки под Windows, Linux и MacOS платформи трябва да позволява интерактивно търсене на твърдите дискови ресурси на крайните точки и възможност за преглеждане на съдържанието на файловите директории на тях.
REQ.76.	Модула за решението за търсене на информация от крайни точки под Windows, Linux и MacOS платформи трябва да позволява търсенето на който и да е файл на базата на съответни условия, които са част от създадено YARA правило.
REQ.77.	Решението трябва да позволява поставянето на каквито и да са инструменти за отговор на инциденти под Windows и Linux платформи (скриптове, програми и т.н.) на избрани защитени крайни точки, като решението след това да може да извиква тези инструменти със зададени параметри за целите на събиране на следствени данни.
REQ.78.	Функцията за търсене на файлове на решението трябва да може да се лимитира за конкретни потребителски роли.
REQ.79.	Решението трябва да може да разрешава или изключва управлението на I/O портове на крайни точки.
REQ.80.	Решението трябва да разрешава управлението на устройства чрез определяне на:

	а) какви USB устройства могат да се свързват с дадена крайна точка б) какви действия са позволени по подразбиране след свързване на USB устройства с крайна точка (само четене, пълен достъп, блокиране)
REQ.81.	Решението трябва да позволява контрол над локалните мрежови портове на крайните точки, с възможност за поставяне на правила за входящ и изходящ мрежови трафик.
REQ.82.	Решението трябва да може да контролира и да се възползва от BitLocker механизмите на крайните точки за криптиране на данни
REQ.83.	Като част от генерираните инциденти, решението трябва да може автоматично да предоставя информация за устройства и потребителски акаунти, които са засегнати или участват в дадена атака.
REQ.84.	Решението трябва да може да консолидира данните за първоначални причинители (root cause анализ – да може да показва съмнения и доказателства, дървото с процесите, включително родителски и дъщерни процеси и т.н.).
REQ.85.	Решението трябва да подсигури дългосрочен архив на данните от консолидирани инциденти за период от минимум 12 месеца.
REQ.86.	Генерираните и консолидирани инциденти от решението трябва да предоставят графична времедиаграма с всички обвързани настъпили ключови събития и подозрения, изпълнени процеси, както и разпространението на дадената атака на множество крайни точки, като да има възможност за интерактивно проследяване на детайлите от тези събития.
REQ.87.	Решението трябва да може да изгражда изгледи в потребителският интерфейс за управление на решението за всеки инцидент, като да са включени ключови данни за коренния причинител, обхвата на атаката (списък с обвързани крайни точки и потребителски акаунти), индивидуалните фази на атаките във времедиаграма, времето и датата на началото и края на инцидента, мрежовите комуникации, установени по време на дадената атака.
REQ.88.	Решението трябва да може да предоставя цялостен дървовиден изглед за дадена атака с изобразени всички зловредни и безвредни процеси.
REQ.89.	Платформата на решението трябва да може да генерира хронологичен списък от събития, които са се случили на дадена крайна точка, свързани с избран процес от списък, за конкретна времева рамка (например до + или – 30 минути от стартовата точка на изпълнение на процеса. Списъка със събития трябва да включва минимално следните елементи: - мрежови свързвания - използвани драйвери - използвани файлове - събития с достъп до файлове - сесии за вписване - Msrpc - използвани процеси - събития с регистри - Scheduled Tasks събития
REQ.90.	Решението трябва да позволява на анализаторите да маркират конкретни събития за визуализиране само на тях от хронологичният списък със събития на крайните точки.
REQ.91.	Решението трябва да разполага с dashboard, който да предоставя статистики, обобщаващи инцидентите в единен изглед, предоставяйки минимално следната информация:

	- всички инциденти с дадена система за избран период от време (минимално разделение за последните 24 часа/последната седмица/последният месец/ последните 3 месеца/последната година/всички събития) - брой на блокираните инциденти - активни/ескалирани инциденти - MTTR време (Mean Time to Repair/Resolution) – средното време от откриването на инцидент до справянето с него
REQ.92.	Решението трябва да може да класифицира суровите данни на базата на съвпадащи модели на поведение, атаки, използвани техники и тактики (TTP), Threat Intelligence данни, доказателства, съмнения и други.
REQ.93.	Решението трябва да позволява добавянето на коментари към инциденти от администраторите на решението, за улесненото им обработване и улеснена съвместна работа на анализаторите.
REQ.94.	Решението трябва да може да блокира изпълнението на конкретни изпълними файлове (.exe и .dll) в Windows-базирани крайни точки. Списъка с файлове за блокиране трябва да може да се създава динамично по време на настъпил анализ на инцидент (да може да се добавя ответна мярка за блокиране към даден инцидент), както и чрез добавяне на статичен списък.
REQ.95.	Блокирането на автоматично стартирани файлове от Startup процеси трябва да е възможно на базата на SHA-1 и SHA-256 хеш суми.
REQ.96.	Решението трябва да може да предотвратява изпълнението на изпълними файлове, при добавянето им като нов запис в списъка за блокиране на процеси на решението.
REQ.97.	Опитите за стартиране на файл от списъка с блокирани такива трябва автоматично да създава инцидент в решението.
REQ.98.	Решението трябва да използва заделена облачна среда и ресурси само за една организация, да не се съхранява и споделя информация с други клиентски организации на вендора.
REQ.99.	Решението трябва да позволява поставянето на роля анализатор и администратор само за конкретни инсталирани агенти на решението, като те да имат достъп само до събраната информация от конкретните агенти.
REQ.100.	Агентите на решението трябва да могат да се регистрират в Windows Security Center като пълноправни антивирусни решения на крайните точки.
REQ.101.	Решението трябва да разполага с функция за засичане на регистрирани устройства с Активна Директория, които не са защитени от решението (нямат инсталиран агент).
REQ.102.	Решението трябва да позволява поставянето на различни политики за сигурност на различни групи от агенти, като динамично да може да се променя асоциирането им при необходимост.
REQ.103.	Решението трябва да разполага с механизъм за засичане на агенти, на които активната политика за сигурност не отговаря на зададената политика на групата от агенти, към която те принадлежат (агента използва различни настройки от зададените на ниво група, към която принадлежи).
REQ.104.	Решението трябва да позволява пренаписването на индивидуални настройки на конкретни агенти, независимо от зададените настройки на групово ниво.
REQ.105.	Облачната конзола за управление на решението трябва да позволява да се лимитира обмена и обработването на данни само за територията на Европейският съюз.
REQ.106.	Решението трябва да позволява инсталирането на локални EDR сензори на работните станции и сървърите, без да е необходимо тяхното рестартиране (с изключение на функциите за антивирусни сигнатури).

REQ.107.	Решението трябва да позволява на сензорите му да работят в прозрачен режим за крайните потребители, без визуални следи по крайните точки и с възможност за изключване на известия към тях.
REQ.108.	Решението трябва да разполага с механизъм за самозащита от злоупотреба със сензорите му, които работят под Windows среда, чрез защита на процесите, файловете, услугите и регистрите на сензорите от неоторизирани или зловредни модификации или опити за спирането им. В допълнение, самозащитата трябва да предпазва сензорите от неволни потребителски действия, който могат да доведат до компроментиране на сигурността на сензорите, като например спирането на сензорен процес.
REQ.109.	При изпращането на телеметрични данни от потребителските крайни точки към решението, EDR сензорите трябва предварително да могат да компресират изпращаните данни, без да има загуба на детайли, като да се генерират средно не повече от 15MB от данни от Windows-базирани работни станции на ден (предполагайки средно 10 работни часове активност на работните станции).
REQ.110.	Решението трябва да разполага с централизирана конзола за управление за всички компоненти и настройване на политики за сигурност, както и за необходимата работа на анализаторите на инциденти.
REQ.111.	Решението трябва да може да работи с ролево-базиран достъп, като да може да се разделят различните нива анализатори (например L1, L2, L3), както и да има разделение на потребителите с роля за отговор при инциденти.
REQ.112.	Решението не трябва да изисква рестарт на дадена крайна точка или сървър при първоначалната инсталация на компонентите на решението за защита или при обновяването им.
REQ.113.	Решението трябва да поддържа многостъпков процес за обновяване на сензорите му, с възможност всеки сензор да може да си свали обновленията, но без да ги инсталира веднага. Обновлението да може да се извърши само след като администратор ръчно е задал команда от интерфейса за централизирано управление на решението.
REQ.114.	Решението трябва да предоставя функция за премахване на сензорите му директно от интерфейса за централизирано управление, както и чрез създаване на двоичен файл, който да може да се изпълни директно на дадена крайна точка.
REQ.115.	Решението трябва да позволява задаването на изключения от сканиране за неговите компоненти, ръчно от интерфейса за централизирано управление, както и чрез вмъкването на CSV файлове за масови изключения.
REQ.116.	Решението трябва да позволява конфигурирането на изключения за функциите за контрол над крайните точки в политиките за сигурност и на групово ниво.
REQ.117.	Решението трябва да поддържа използването на агенти за Windows 7/8/8.1/10/11 системи.
REQ.118.	Решението трябва да поддържа използването на агенти за Linux крайни точки, включително: - CentOS - Red Hat - Oracle Linux - Ubuntu (14 LTS, 16 LTS, 18.04 LTS, 20.04 LTS, 20.10, 22.04 LTS, 22.10, 23.04) - SLES 15 - Debian - Amazon Linux (AMI 2017.03/Linux 2/Linux 2023) - Rocky Linux 8.5 до 9.2

	- CloudLinux 7 - AlmaLinux
REQ.119.	Решението трябва да може да се интегрира с SIEM системи, поне доколкото се отнася за изпращане на информация до тях за засечени инциденти под syslog в CEF формат.
REQ.120.	Решението трябва да може да изпраща syslog данни по криптиран канал за комуникация.
REQ.121.	Решението трябва да разполага с отворен API интерфейс за интеграции.
REQ.122.	API интерфейса на решението трябва да разполага с минимално следните функции:
REQ.123.	а) стартиране на процес по следствено търсене, включително: търсене за конкретен файл, мрежово свързване, процес
REQ.124.	б) управление на агенти, включително: проверка на версия, събиране на списък за online/offline агенти в даден момент, търсене за агенти, принадлежащи към конкретни групи, сваляне на логове от агенти, сваляне на настройките на агенти
REQ.125.	в) стартиране на процес по взимане на ответни мерки на възникнал инцидент, включително: стопиране на процес, поставяне на файл под карантина, изтриване на запис от регистрите на крайната точка, блокиране на изпълнение на файл
REQ.126.	г) добавяне на нови ръчно създадени правила за засичане на заплахи
REQ.127.	д) обновяване на списъците с данни за репутации на решението
REQ.128.	е) изолиране от мрежова свързаност на крайни точки
REQ.129.	Решението трябва да позволява автоматизация на управлението на инциденти чрез интеграции с решения като тикетинг системи и други.

Навсякъде в техническите параметри, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ“.

3. Изисквания към изпълнението

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

3.2 Всички лицензи трябва да бъдат доставени на името на „Гражданска регистрация и административно обслужване“ (ГД ГРАО)

3.3 Комуникацията за поставяне и решаване на възникналите проблеми ще се осъществява през сайта на производителя.

3.4 Всички осигурени лицензи трябва да предоставят възможност за актуализация до последна поддържана версия за съответния продукт;

3.5 Изпълнителят следва да осигури техническа поддръжка и получаване на нови версии на лиценза за срока на валидност.

4. МЯСТО НА ИЗПЪЛНЕНИЕ

Дейностите, по осигуряване на специализиран софтуер за антивирусна защита (EDR) на крайни потребителски станции и сървъри се осъществяват отдалечено, при необходимост от съдействие на място – сградата на главна дирекция „Гражданска регистрация и административно обслужване“ (ГД ГРАО) в гр. София, ул. „Алабин“ № 16-20.

5. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ

5.1 Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност, и подзаконовите нормативни актове към тях.

5.2 Във връзка с мрежовата и информационната сигурност на Бенефициера и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата и които ще имат достъп до информация и активи, при взаимодействието им със служители на Бенефициера ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурността на информацията на Бенефициера и на МЕУ. За целта ангажираните от Изпълнителя за предоставяне на Услугата лица, в т.ч. и на трети страни, с които Изпълнителят има сключен договор за изпълнение, които ще имат достъп до информация и активи на МРРБ, подписват Декларации за опазване на информацията [Приложение №3 към Рамков Договор № РД 02-29-240/31.12.2020 г. (вх. № ПО-16-1962/31.12.2020 г. на „Информационно обслужване“ АД), Образец], които се предават по електронна поща на Бенефициера. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават своевременно по същия ред.

(в) осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

(г) се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Бенефициера.

5.3 Служителите по чл. 20 от договора, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване:

(а) при изпълнението на задълженията си, осъществяват комуникация с ръководителите на проекта и с ръководителите на договора от страна на Бенефициера и Изпълнителя, а при необходимост ескалират възникнал проблем до прекия си ръководител;

б) служителят от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя в т.ч. и на трети страни, с които Изпълнителят има сключен договор за осигуряване изпълнението на услуги по предмета на Договора;

(в) При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за проекта, служителите по чл. 20 от договора от страна на Бенефициера и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок. Резултатите от анализа, както и конкретни решения за осигуряване на сигурността се предоставят на ръководителите на договора и на проекта.