Образец № 2

ДО НАЦИОНАЛЕН СТАТИСТИЧЕСКИ ИНСТИТУТ
гр. София, ул. Панайот Волов № 2

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

ЗА УЧАСТИЕ В ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ: „Доставка и гаранционно обслужване на Система за събиране и анализ на журнални записи, свързани с информационната сигурност и защита, с локация в резервния изчислителен център на НСИ“,

от „Телелинк Бизнес Сървисис“ ЕАД, ЕИК: 130545438,
със седалище и адрес на управление: гр. София 1766, район Витоша, в.з. Малинова долина, ул. „Панорама София” № 6, Бизнес Център Ричхил, блок Б, ет. 2
(пълно наименование, ЕИК/БУЛСТАТ, седалище и адрес на управление)

Чл. 36а, ал. 3 от ЗОП

УВАЖАЕМИ ДАМИ И ГОСПОДА,

С настоящото представяме нашето техническо предложение за изпълнение на поръчка по публикуваната от Вас процедура за възлагане на обществена поръчка с предмет: „Доставка и гаранционно обслужване на Система за събиране и анализ на журнални записи, свързани с информационната сигурност и защита, с локация в резервния изчислителен център на НСИ“, като заявяваме, че:

1. Декларираме, че ще изпълним поръчката, съобразявайки се с условията за изпълнение на поръчката, посочени от Възложителя в документацията за участие.
2. Гарантираме, че сме в състояние да изпълним качествено поръчката, в срок и в пълно съответствие с техническите изисквания.
3. При изготвяне на офертата на представлявания от мен участник са спазени задълженията, свързани с данъци и осигуровки, опазване на околната среда, закрила на заетостта и условията на труд.
4. Доставката ще извършим в НСИ – Централно управление, гр. София, ул. „Панайот Волов“ № 2. Изпълнението ще бъде в резервния изчислителен център на НСИ в село Сливек.
5. Декларираме, че ще изпълним настоящата поръчка в срок до 5 (пет) месеца (не по-дълго от 5 (пет) месеца), считано от датата на сключване на договор.
6. Декларираме, че разполагаме със система за приемане и обслужване на сервизни заявки, която включва организация на гаранционния сервиз, който ще гарантира на възложителя, че оборудването ще бъде обслужвано в параметрите, предписани от производителя и в сроковете изисквани от Възложителя.
7. Притежавам и прилагам документ/и, удостоверяващ/и правата ни за оторизация от производител/и ~~и/или от официален негов/и представител/и~~ (излишното се зачертава) за извършване на доставка, внедряване и поддръжка на предложения софтуер и оборудване.
8. Притежавам и прилагам валиден и действащ сертификат за внедрен стандарт EN ISO/IEC 27001:2013 или еквивалент за въведена системи за управление сигурността на информацията с обхват, сходен с предмета на поръчката.

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

9. Притежавам и прилагам валиден и действащ сертификат за внедрен стандарт EN ISO/IEC 20000-1:2011 или еквивалент за въведена системи за управление на ИТ услуги или обхват, сходен с предмета на поръчката.
10. Декларираим, че ще изготвим детайлно техническо описание/дизайн.
11. Декларирам, че ще извършим физически монтаж на оборудването, съгласно утвърдените практики на Национален статистически институт.
12. Декларирам, че ще инсталираме доставения софтуер върху доставения хардуер.
13. Декларирам, че ще извършим свързване, конфигуриране и тестване на работоспособността на връзката между оборудването и мрежата/оборудването на Национален статистически институт.
14. Декларирам, че ще конфигурираме системите съгласно одобрения детайлен дизайн на предложените решения.
15. Декларирам, че ще изготвим процедури за функционални тестове.
16. Декларирам, че ще интегрираме системите към съществуващата мрежа на Национален статистически институт, без функционални прекъсвания на работата.
17. Декларирам, че ще извърши функционални тестове на системите съгласно приетите процедури.
18. Декларирам, че ще обновим цялата техническа документация на решенията след тяхното приемане.
19. Декларирам, че ще проведем обучение на посочени от Възложителя – до 5 (петима) служители в рамките на 1 (един) работен ден за работа с функционалните възможности на Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност.
20. Декларирам, че при изпълнение на дейностите се задължаваме да пазим в поверителност и да не разкриваме или разпространяваме информация, станала ни известна при или по повод изпълнението на дейностите, предмет на поръчката. Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата страна, от каквото и да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство.
21. Декларирам, че при необходимост от ремонт или подмяна на оборудване се връщат само компоненти, които не съдържат постоянна или временна памет, която може да съдържа чувствителна информация. При фабрично заложена възможност за демонтиране на такава памет без допълнителни инструменти (FLASH памет, EEPROM, твърд диск, RAM памет) същите се демонтират от компонента преди да бъде предаден на Изпълнителя за ремонт или подмяна. Компоненти, при които не съществува такава възможност, не се връщат на доставчика за ремонт или подмяна, а се унищожават. Унищожаването се извършва от Възложителя, в присъствие на представител на Изпълнителя, за което се изготвя двустранен протокол, а Изпълнителя заменя унищожения компонент с нов.

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

4

22. Предлагаме да изпълним поръчката съгласно т. 2 „Минималните технически изисквания“ от Техническата Спецификаци при следните технически параметри:

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
1.	Системата трябва да предоставя web-базиран графичен интерфейс за управление, анализ и извличане на рапорти.		Системата предоставя web-базиран графичен интерфейс за управление на всичките си компоненти, анализ и извличане на рапорти. От графичният интерфейс на системата може да се наблюдават и конфигурират компонентите на системата, както и да се изготвят и задават рапорти.
2.	Софтуерът трябва да позволява от една централна конзола извличане, агрегация, филтрация и анализ на данни от компонентите за събиране на журнални записи с цел централна обработка на всички данни.		Софтуерът предоставя възможност за извличане, агрегация, филтрация и анализ на данни от компонентите за събиране на журнални записи от централна конзола, с цел централна обработка на всички данни. Ако системата се разшири с няколко сървъра, информацията агрегирана и обработвана от всички тях, може да се анализира, извлича, филтрира и др. от една централна конзола.
3.	Софтуерът трябва да позволява интеграция с външни системи за автентикация.		Софтуерът позволява интеграция с външни системи за автентикация като MS активна директория, RADIUS, TACACS, LDAP.
4.	Административните правомощия трябва да позволяват дефиниране на достъп според устройства, група от устройства или мрежови диапазон.		Административните правомощия позволяват дефиниране на достъп според устройства, група от устройства, мрежови диапазон, домейн. Административните правомощия могат да бъдат дефинирани и като достъп до агрегираната информацията според дадено устройство, група от устройства, домейн, мрежови диапазон.
5.	Административните правомощия трябва да позволяват дефиниране на ролево-базиран достъп до различни функционални области на софтуера. Това включва ограничаване на достъпа до специфична функционалност извън обхвата на потребителската роля. Тази		Административните правомощия позволяват дефиниране на ролево-базиран достъп до различни функционални области на софтуера. Това може да включва ограничаване на достъпа до специфична функционалност извън обхвата на

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

5

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА	
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**		
	функционалност може да бъде административна, отчетна, филтрираща събития, корелация на събития, достъп до работен плот и др.		потребителската роля. Тази функционалност може да бъде административна, отчетна, филтрираща събития, корелация на събития, достъп до работен плот и др.	Чл. 36а, ал. 3 от ЗОП
6.	Системата трябва автоматично да открива активи (сървъри, мрежови устройства и др.), които са обект на защита и наблюдение.		Системата може автоматично да открива активи на организацията, в това число сървъри, мрежови устройства и др., които са обект на наблюдение и защита. Информацията за откритите активи се акумулира в отделна база и служи за обогатяване на данните за устройствата.	
7.	Софтуерът трябва да предоставя web-базиран графичен интерфейс за управление, анализ и извличане на рапорти.		Системата предоставя web-базиран графичен интерфейс за управление на всичките си компоненти, анализ и извличане на рапорти. От графичният интерфейс на системата може да се наблюдават и конфигурират компонентите на системата, както и да се изготвят и задават репорти.	
8.	Архитектурата на системата трябва да предостави всички изискани функции в едно устройство.		Архитектурата на системата предоставя всички изискани функции в едно устройство. Функциите за събиране на журнални записи от устройства, прихващане на мрежови потоци, корелиране на информацията, управление на системата и др. могат да се предоставят от едно устройство.	
9.	Софтуерът трябва да разполага с възможност за разширяване на функционалността, чрез добавяне на готови приложения и функции, в потребителския интерфейс, представени и налични за изтегляне в специализиран портал на производителя.		Софтуерът разполага с възможност за разширяване на функционалността, чрез добавяне на готови приложения и функции, в потребителския интерфейс, представени и налични за изтегляне в специализиран портал на производителя. IBM-X Force предоставя за изтегляне множество допълнителни приложения с различни функционалности.	Чл. 36а, ал. 3 от ЗОП
10.	Софтуерът трябва да предоставя възможност за модификация на комуникационните портове между компонентите си.		Софтуерът предоставя възможност за модификация на комуникационните портове между компонентите си.	

Чл. 36а, ал. 3 от ЗОП

6

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
11.	Системата трябва да позволява отворено API за достъп до данните съхраняващи се в базите от данни в системата.		Системата позволява отворено API за достъп до данните съхраняващи се в базите от данни в системата. Към базите може да се изпълнят различни заявки за търсене и филтриране на информация използвайки наличното в системата API.
12.	Софтуерът трябва да позволява разширена таксонометрия на отчетените събития и описващите ги полета. Потребителите трябва да имат възможност да добавят свои уникални имена на събития, за целите на бъдеща филтрация, доклад или корелация.		Софтуерът позволява разширена таксонометрия на отчетените събития и описващите ги полета. Потребителите имат възможност да добавят свои уникални имена на събития, за целите на бъдеща филтрация, доклад или корелация.
13.	Софтуерът трябва да има възможност за автоматична класификация (tagging) на отчетените събития.		Софтуерът предоставя възможност за автоматична класификация (tagging) на отчетените събития. За тази функционалност се използва калкулация на база четири параметъра: relevance, severity, credibility, magnitude.
14.	Софтуерът трябва да позволява създаване на различни работни плотове според специфичните изисквания на всеки отделен потребител.		Софтуерът позволява създаване на различни работни плотове според специфичните изисквания на всеки отделен потребител. Работните плотове, които са променени или създадени от отделен потребител, са налични и се визуализират за този потребителски акаунт без да променят работните плотове по подразбиране за останалите потребители.
15.	Софтуерът трябва да разполага с набор от преконфигурирани шаблони на работни плотове, които да могат да се използват без допълнителни промени.		Софтуерът разполага с набор от преконфигурирани шаблони на работни плотове, които могат да се използват без допълнителни промени. Наличните преконфигурирани шаблони на работни плотове са с различна насоченост – например: шаблон за преглед на състоянието на системата, шаблон за преглед на засечени опасности и детайли за тях.
16.	Софтуерът трябва да поддържа база от данни за всички активи, открити в информационната инфраструктура. Данните за активите трябва да предоставят важна информация събрана		Софтуерът поддържа база от данни за всички активи, открити в информационната инфраструктура. Данните за активите предоставят важна информация събрана за тях, която

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

7

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
	за тях, която включва минимум: системни атрибути, мрежови атрибути и ниво на уязвимост. Софтуерът трябва да позволява корекция на тези атрибути, ако те не могат да бъдат придобити.		включва: системни атрибути, мрежови атрибути и ниво на уязвимост. Софтуерът позволява корекция на тези атрибути, ако те не могат да бъдат придобити. Към базата за активите могат да се импортират и данни за устройства и системи от .CSV файл.
17.	Архитектурата трябва да предоставя възможност за внедряване както софтуерно решение върху виртуална платформа и/или цялостно хардуерно решение.		Архитектурата предоставя възможност за внедряване както като софтуерно решение върху виртуална платформа, така и/или като цялостно хардуерно решение. Поддържа се и комбинация от виртуални и хардуерни компоненти имплементирани в инфраструктурата на организацията.
18.	Софтуерът трябва да гарантира интегритет на събраните данни (журнални записи). -- Архитектурата на системата трябва да гарантира интегритет на събраните журнални записи.		Софтуерът на системата гарантира интегритет на събраните данни (журнални записи). -- Архитектурата на системата гарантира интегритет на събраните журнални записи.
19.	Софтуерът трябва да предоставя дистрибутивен модел на корелация на активности събрани от различните и компоненти. Пример: покажи 8 грешни опити за въвеждане на парола за даден потребител, като данните за тези опити са събрани от всички компоненти. -- Архитектурата на системата трябва да може да предоставя разпределен модел на корелация на активности събрани от различните ѝ източници. Пример: покажи 8 грешни опити за въвеждане на парола за даден потребител, като данните за тези опити трябва да се видят от различни компоненти, обръщения на ниво сървър, мрежови сесии и др.		Софтуерът на системата предоставя дистрибутивен модел на корелация на активности събрани от различните и компоненти. Пример: покажи 8 грешни опити за въвеждане на парола за даден потребител, като данните за тези опити са събрани от всички компоненти. -- Архитектурата на системата може да предоставя разпределен модел на корелация на активности събрани от различните ѝ източници. Пример: покажи 8 грешни опити за въвеждане на парола за даден потребител, като данните за тези опити трябва да се видят от различни компоненти, обръщения на ниво сървър, мрежови сесии и др.
20.	Софтуерът трябва да предоставя автоматизиран процес за архивни копия (конфигурации и събрани журнални записи) и тяхното възстановяване.		Софтуерът предоставя автоматизиран процес за архивни копия (конфигурации и събрани журнални записи) и тяхното възстановяване. Позволява се задаване на график за създаване на архивни

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

8

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
			копия от едно или повече устройства на системата.
21.	Софтуерът трябва да предоставя автоматизирани проверки на работоспособност и при възникване на проблем да изпраща нотификация.		Софтуерът включва автоматизирани проверки на работоспособност и при възникване на проблем може да изпраща нотификация. Следят се редица параметри като може да се модифицират минимални/максимални стойности и др.
22.	Софтуерът трябва да позволява съхранение на събраните журнални записи върху външни системи (независимо от производителя) за съхранение.		Софтуерът позволява съхранение на събраните журнални записи върху външни системи (независимо от производителя) за съхранение. Журналните записи могат да бъдат препращани или копирани към външни системи в обработен (нормализиран) или необработен (raw) вид.
23.	Софтуерът трябва да предоставя възможност за компресия на събраните журнални записи.		Софтуерът предоставя възможност за компресия на събраните журнални записи. Така се намалява необходимото дисково пространство за съхранение на събраните журнални записи, но същевременно се използват и допълнителни механизми за намаляване на времето при търсене сред компресираните данни в системата.
24.	Софтуерът трябва да позволява стандартизирани методи за събиране на журнални записи като минимум: Syslog (TCP/UDP), SNMP, JDBC, OPSEC LEA, SDEE, WMI, FTP/SFTP/SCP като място за съхранение на журнални записи.		Софтуерът предоставя стандартизирани методи за събиране на журнални записи: Syslog (TCP/UDP), SNMP, JDBC, OPSEC LEA, SDEE, WMI, MSRPC и др., FTP/SFTP/SCP като място за съхранение на журнални записи.
25.	Софтуерът трябва да позволява нормализация на базовите събитийни полета. В това число: потребителски имена, IP адреси, имена на хостове, източници на журнални записи.		Софтуерът позволява нормализация на базовите събитийни полета. В това число: потребителски имена, IP адреси, имена на хостове, източници на журнални записи и др. Нормализирането на полета от журнален запис се осъществява с помощта на DSM парсери. Такива парсери са налични за много широка гама от устройства, операционни системи и приложения. Могат да се променят или създават нови парсери за нуждите на организацията.

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

9

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
26.	Софтуерът трябва да позволява анализ на събитията в близко до реалното време.		Софтуерът позволява анализ на събитията в близко до реалното време.
27.	Софтуерът трябва да позволява анализ за събитията в дълъг период от време, показване на базова линия (baseline) и прогноза (trend) върху тези събития.		Софтуерът позволява анализ за събитията в дълъг период от време, показване на базова линия (baseline) и прогноза (trend) върху тези събития. Софтуерът разполага с правила за наблюдение на база анализ на събития и откриване на аномалии (anomaly detection).
28.	Софтуерът трябва да създава аларми базирани на наблюдавани аномалии и поведенчески промени в събитията свързани със сигурността.		Софтуерът може да създава аларми базирани на наблюдавани аномалии и поведенчески промени в събитията свързани със сигурността. Създаването на аларми може да се дефинира в правилата за наблюдение от различен тип, както и при конфигурирането на допълнителни модули за следене на аномалии и др.
29.	Софтуерът трябва да предоставя възможност за рапорт на всички компоненти, подлежащи на управление през графичният потребителски интерфейс.		Софтуерът предоставя възможност за рапорт на всички компоненти, подлежащи на управление през графичният потребителски интерфейс.
30.	Системата трябва да притежава конфигурируема подсистема за създаване на рапорти, позволяваща гъвкавост и промени на генерираните рапорти.		Системата притежава конфигурируема подсистема за създаване на рапорти, позволяваща гъвкавост и промени на генерираните рапорти. Могат да се редактират или създават нови задачи за изготвяне на рапорти. При създаването на нов рапорт може да се дефинира, както информацията, която да включва, така и цялостния изглед на рапорта, включително брандиране с лого на организацията.
31.	Софтуерът трябва да позволява създаване на рапорти за определен интервал от време: час, ден, седмица месец или на специфично зададен период.		Софтуерът позволява създаване на рапорти за определен интервал от време: час, ден, седмица месец или на специфично зададен период.
32.	Софтуерът трябва да позволява направа на шаблони за изготвяне и предоставяне на рапорти за нуждите на широка гама от нива както на оперативната работа, така и на за нуждите на висшето ръководство.		Софтуерът позволява направа на шаблони за изготвяне и предоставяне на рапорти за нуждите на широка гама от нива както на оперативната работа, така и на за нуждите на висшето ръководство. Подсистемата за създаване

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

10

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
			на рапорти позовлява дефинирането на елементите, които да включва даден рапорт и оформяне на изгледа на рапорта.
33.	Софтуерът трябва да предоставя възможност за алармиране, базирано на засечени заплахи за сигурността въз основа на наблюдаваните устройства.		Софтуерът предоставя възможност за алармиране, базирано на засечени заплахи за сигурността въз основа на наблюдаваните устройства.
34.	Софтуерът трябва да предоставя възможност да корелира информация събрана от различни дистрибутирани компоненти.		Софтуерът предоставя възможност да корелира информация събрана от различни дистрибутирани компоненти.
35.	Софтуерът трябва да предоставя възможност за алармиране, базирано на установени политики.		Софтуерът предоставя възможност за алармиране, базирано на установени политики.
36.	Софтуерът трябва да предоставя възможност за алармиране, базирано на претегляне, което ще позволи залагане на приоритизация. Теглата трябва да може да бъдат зачислени на база тип на актива, протокол, и приложение.		Софтуерът предоставя възможност за алармиране, базирано на претегляне, което позволява залагане на приоритизация. Теглата може да бъдат зачислени на база тип на актива, протокол, и приложение.
37.	Софтуерът трябва да позволява изпращане на аларми към външни системи посредством e-mail, SNMP и Syslog.		Софтуерът позволява изпращане на аларми към външни системи посредством e-mail, SNMP и Syslog.
38.	Софтуерът трябва да има вграден инструмент, през който потребителите да могат да описват защо дадена аларма е false positive и респективно тези данни да се използват за намаляване на нивото на фалшивите аларми.		Софтуерът разполага с вграден инструмент, през който потребителите да могат да описват защо дадена аларма е false positive и респективно тези данни се използват за намаляване на нивото на фалшивите аларми. Софтуерът позволява да се дефинират и потребителски причини за описание при затваряне на един инцидент.
39.	Софтуерът трябва да позволява корелация на свързани помежду си събития и представянето им като един инцидент.		Софтуерът позволява корелация на свързани помежду си събития и представянето им като един инцидент. Множество идентични или разнородни събития може да бъдат представени като един инцидент спрямо зададените в правилата за наблюдение настройки.
40.	Софтуерът трябва да има възможност за интеграция с външни източници на информация от трети страни свързана със заплахи (примерно – географско		Софтуерът предоставя възможност за интеграция с външни източници на информация от трети страни свързана със заплахи (примерно – географско

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
	позициониране, ботнет канали, враждебни мрежи). Получената информация трябва да може да се използва по автоматизиран начин.		позициониране, ботнет канали, враждебни мрежи). Съществува вградена функционалност за изтегляне на подобна информация от производителя. Отделно от това могат да се дефинират неограничен брой други източници. Получената информация може да се използва по автоматизиран начин.
41.	Софтуерът трябва да алармира когато има прекъсване в събирането на журнални записи от устройство под наблюдение. Потребителите трябва да имат възможност да дефинират времевият интервал, през който не се наблюдава активност от наблюдаваните устройства. Пример: ако журналните записи не са изпратени от дадено устройство в рамките на X минути трябва да се създаде аларма.		Софтуерът може да алармира, когато има прекъсване в събирането на журнални записи от устройство под наблюдение. Потребителите имат възможност да дефинират времевият интервал, през който не се наблюдава активност от наблюдаваните устройства. Пример: ако журналните записи не са изпратени от дадено устройство в рамките на X минути, да се създаде аларма.
42.	Софтуерът трябва да поддържа създаване и поддържане на списък с всички активи на организацията. За всеки един актив трябва да може да се определя теглови коефициент и да бъде асоцииран с ползвател и географската му локация.		Софтуерът на системата поддържа създаване и поддържане на списък с всички активи на организацията. За всеки един актив може да се определя теглови коефициент и да бъде асоцииран с ползвател, отговорник, географската му локация, както и потребителски дефиниран признак.
43.	Софтуерът трябва да може при интеграция с Vulnerability Management решение да инкорпорира и информация за уязвимостите на даден актив.		Софтуерът позволява, при интеграция с Vulnerability Management решение, да инкорпорира и информация за уязвимостите на даден актив. Може да се създаде график за изтегляне на нова или обновяване на съществуващата информация получена от Vulnerability Management решение. Към системата може да се интегрират подобни решения разработени от водещите производители в областта.
44.	Софтуерът трябва да позволява определяне на ниво на достоверност на всеки един източник на журнални записи, което да може да се взима в предвид при финалното определяне на приоритета на даден инцидент по сигурността.		Софтуерът позволява определяне на ниво на достоверност на всеки един източник на журнални записи, което да може да се взима в предвид при финалното определяне на приоритета на даден инцидент по сигурността.

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

12

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
			Определянето може да се заложи още в процеса на добавяне на източника или да се редактира в последствие.
45.	Софтуерът трябва да предоставя вградени работни процеси, които улесняват и насочват действията на оперативните служители по сигурността.		Софтуерът предоставя вградени работни процеси, които улесняват и насочват действията на оперативните служители по сигурността.
46.	Софтуерът трябва да има вграден модул, който да позволява назначаване на даден инцидент по сигурността на определен потребител на системата.		Софтуерът разполага с вграден модул, който позволява назначаване на даден инцидент по сигурността на определен потребител на системата. Потребителят, на който е назначен даден инцидент, получава необходимите права да разглежда, затваря или защитава от промени дадения инцидент.
47.	Всеки един потребител трябва да има възможност да види всички свои (назначени на него) инциденти по сигурността, подредени по определен приоритет за обработка.		Всеки един потребител има възможност да види всички свои (назначени на него) инциденти по сигурността, подредени по определен приоритет за обработка. Софтуерът разполага с опция за бързо извеждане на списък с всички инциденти назначени на дадения потребител и предоставя възможност за прилагане на филтри с времеви период и подреждане по различни критерии.
48.	Всеки един потребител трябва да има възможност да обработва назначените по инциденти по сигурността и съответно миниум да може да ги затваря (dismiss), наблюдава, конфигурира нотификации и коментира.		Всеки един потребител на системата има възможност да обработва назначените му инциденти по сигурността и съответно може да ги затваря (dismiss), наблюдава, конфигурира нотификации и коментира.
49.	Софтуерът трябва да предоставя API calls с възможност за оторизация, които да могат да бъдат ползвани от външни ТТ системи за управление на инцидентите.		Софтуерът предоставя API calls с възможност за оторизация, които да могат да бъдат ползвани от външни ТТ системи за управление на инцидентите.
50.	Софтуерът трябва да предоставя механизъм за прихващане на всички релевантни аспекти свързани с инцидент в сигурността в обединена логическа визуализация.		Софтуерът предоставя механизъм за прихващане на всички релевантни аспекти свързани с инцидент в сигурността в обединена логическа визуализация.
51.	Софтуерът трябва да предоставя механизъм за добавяне на коментари в събраната и обособена логически информация за текущ инцидент в сигурността.		Софтуерът предоставя механизъм за добавяне на коментари в събраната и обособена логически информация за текущ инцидент в сигурността.

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

13

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
52.	Софтуерът трябва да предоставя механизъм за откриване на инциденти в сигурността на база широк спектър от атрибути свързани с него като: IP адрес, потребителско име, MAC адрес, източник на журнален запис, правило за корелация и др.		Софтуерът предоставя механизъм за откриване на инциденти в сигурността на база широк спектър от атрибути свързани с него като: IP адрес, потребителско име, MAC адрес, източник на журнален запис, правило за корелация и др.
53.	Софтуерът трябва да позволява събиране на журнални записи от Microsoft базирани сървърни крайни устройства.		Софтуерът позволява събиране на журнални записи от Microsoft базирани сървърни крайни устройства. Предоставените варианти за събиране на журнални записи от Microsoft базирани сървъри и станции са няколко. Възможно е да се изтеглят посредством протоколи, които не изискват инсталиране на допълнителни агенти, да бъдат препращани към системата или да се изтеглят с помощта на агент.
54.	Софтуерът трябва да позволява събиране на журнални записи от Linux/Unix базирани сървърни крайни устройства.		Софтуерът позволява събиране на журнални записи от Linux/Unix базирани сървърни крайни устройства. При събирането на журнални записи от системи с такава операционна система е достатъчна конфигурационна настройка, от страна на операционната им система, която указва към кой компонент на QRadar да бъдат препращани журналните записи.
55.	Софтуерът трябва да позволява събиране на журнални записи от бази от данни като: • MSSQL Server; • Oracle; • IBM DB2; • Sybase; • MySQL; • IBM Informix		Софтуерът позволява събиране на журнални записи от бази от данни като: • MSSQL Server; • Oracle; • IBM DB2; • Sybase; • MySQL; • IBM Informix и др.
56.	Софтуерът трябва да позволява събиране на журнални записи от системи за активно наблюдение на бази от данни.		Софтуерът позволява събиране на журнални записи от системи за активно наблюдение на бази от данни.
57.	Софтуерът трябва да позволява събиране на журнални записи от системи за управление на идентичности и достъп (Identity and access Management).		Софтуерът позволява събиране на журнални записи от системи за управление на идентичности и достъп (Identity and access Management).

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

14

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
58.	Софтуерът трябва да позволява събиране на журнални записи от директориини продукти (AD, LDAP и др.).		Софтуерът позволява събиране на журнални записи от директорийни продукти (AD, LDAP и др.).
59.	Софтуерът трябва да позволява събиране на журнални записи от минимум следните устройства/приложения: • Cisco Switches; • Cisco Routers; • Cisco ASA; • Cisco Nexus; • Cisco ACS; • Cisco Wireless LAN Controllers; • Apache HTTP Server; • Check Point Firewalls; • Citrix NetScaler; • Enterasys Matrix Router; • Extreme ExtremeWare; • F5 ASM; • F5 BIG IP; • HP ProCurve; • HP-UX; • Juniper Router; • Juniper Firewalls; • Microsoft Exchange; • Microsoft IIS; • Microsoft Hyper-V; • Microsoft Endpoint Protection; • Microsoft SCOM; • Microsoft DHCP Server; • Microsoft TMG; • Microsoft SharePoint; • IBM WebSphere; • Oracle BEA WebLogic; • Palo Alto Networks; • Radware DefensePro; • Arbor Networks; • RSA Authentication Manager; • VMWare ESX и ESXi; • VMWare vCenter.		Софтуерът позволява събиране на журнални записи от следните устройства/приложения: • Cisco Switches; • Cisco Routers; • Cisco ASA; • Cisco Nexus; • Cisco ACS; • Cisco Wireless LAN Controllers; • Apache HTTP Server; • Check Point Firewalls; • Citrix NetScaler; • Enterasys Matrix Router; • Extreme ExtremeWare; • F5 ASM; • F5 BIG IP; • HP ProCurve; • HP-UX; • Juniper Router; • Juniper Firewalls; • Microsoft Exchange; • Microsoft IIS; • Microsoft Hyper-V; • Microsoft Endpoint Protection; • Microsoft SCOM; • Microsoft DHCP Server; • Microsoft TMG; • Microsoft SharePoint; • IBM WebSphere; • Oracle BEA WebLogic; • Palo Alto Networks; • Radware DefensePro; • Arbor Networks; • RSA Authentication Manager; • VMWare ESX и ESXi; • VMWare vCenter.
60.	Софтуерът трябва да позволява събиране на журнални записи от водещи в индустрията скенери за уязвимости като: • Nessus;		Софтуерът позволява събиране на журнални записи от водещи в индустрията скенери за уязвимости като:

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

15

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА	
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**		
	• Nmap; • Qualys; • Rapid7 Nexpose.		• Nessus; • Nmap; • Qualys; • Rapid7 Nexpose.	
61.	Софтуерът трябва да има възможност за сканиране, откриване и управление на уязвимостите чрез собствена вградена функционалност.		Софтуерът има възможност за сканиране, откриване и управление на уязвимостите чрез собствена вградена функционалност.	Чл. 36а, ал. 3 от ЗОП
62.	Софтуерът трябва да разполага с възможност за извършване на поведенчески анализ на потребителите, с цел своевременно откриване на вътрешни заплахи за сигурността и компрометирани данни за автентикация.		Софтуерът разполага с възможност за извършване на поведенчески анализ на потребителите, с цел своевременно откриване на вътрешни заплахи за сигурността и компрометирани данни за автентикация. След инсталиране на допълнително приложение тези и други опции за анализ на действията с потребителски акаунти са налични от web-базирания графичен интерфейс за администриране на системата.	
63.	Софтуерът да разполага с възможност за разширяване на функционалността, чрез добавяне на готови приложения и функции, в потребителския интерфейс, представени и налични за сваляне в специализиран портал на производителя. Софтуерът трябва да предоставя възможност за разработване на такива допълнителни функции и приложения.		Софтуерът разполага с възможност за разширяване на функционалността, чрез добавяне на готови приложения и функции, в потребителския интерфейс, представени и налични за сваляне в специализиран портал на производителя. Софтуерът предоставя възможност за разработване на такива допълнителни функции и приложения. На страница на производителя е наличен списък с приблизително 200 допълнителни приложения, които могат да бъдат изтеглени и добавени към системата напълно безплатно. Те биват с различна функционалност – от добавяне на нови правила за наблюдение и рапорти до приложения за тунинговане на правилата за наблюдение и визуализиране на инциденти.	Чл. 36а, ал. 3 от ЗОП
64.	Системата трябва бъде скалируема и да предоставя възможности за разрастване без да е необходима пренастройка на инсталираната среда.		Системата е скалируема и предоставя възможности за разрастване без да е необходима пренастройка на инсталираната среда. Към системата може да се добавят допълнителни сървъри с определена функционалност	

Чл. 36а, ал. 3 от ЗОП

16

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой		**Производител: IBM QRadar Описание: Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност**	
			за постигане на резервираност или по-голяма производителност. Към системата може да се добавят допълнителни лицензи за разширяване на наличния капацитет и за нови функционалности.
65.	Софтуерът да разполага с възможност за бъдеща интеграция с външно решение, използващо евристични алгоритми за анализ и обработка на неструктурирана информация, с цел намаляване времето за откриване на признаци за пробив в сигурността.		Софтуерът разполага с възможност за бъдеща интеграция с външно решение, използващо евристични алгоритми за анализ и обработка на неструктурирана информация, с цел намаляване времето за откриване на признаци за пробив в сигурността.
66.	Системата трябва да може да работи в режим High Availability при бъдещо добавяне на идентичен компонент от архитектурата и прехвърляне на работата върху него в случай на нужда.		Системата поддържа работа в режим High Availability чрез добавяне на идентичен компонент от архитектурата и прехвърляне на работата върху него в случай на нужда. Спрямо архитектурата на решението и броя на изграждащите я сървъри, са налични възможности за работа в High Availability при бъдещо разширение с добавяне на идентични компоненти.
67.	Софтуерът трябва да притежава вградена възможност за създаване на резервно копие на конфигурацията върху външни носители през графичния административен интерфейс, както и иницииране на възстановяване от резервно копие през същия интерфейс.		Софтуерът притежава вградена възможност за създаване на резервно копие на конфигурацията върху външни носители, през графичния административен интерфейс, както и иницииране на възстановяване от резервно копие през същия интерфейс.
68.	Софтуерът трябва да бъде с централизирано управление на всички компоненти.		Софтуерът е с централизирано управление на всички компоненти. При бъдещо разширение на архитектурата, с добавяне на допълнителни компоненти и новодобавените устройства ще попадат под централизираното управление.
69.	Софтуерът трябва да се достави с лицензи за наблюдение и обработка на минимум 800 EPS (events per seconds).		Софтуерът се доставя с лицензи за наблюдение и обработка на 800 EPS (events per seconds). Софтуерът се добавя с лиценз за 15000 FPM (flows per minute)
70.	Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5		Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, режим 8x5

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

17

№	МИНИМАЛНО ИЗИСКВАНЕ	№	ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА
Сървър тип 1 – 1 брой		**Производител: Dell** **Описание: PowerEdge R740**	
1.	CPU: 2 броя, Xeon 2.4 GHz, 10 ядрени		CPU: два броя Intel Xeon Gold 5115, 10 ядрени, 2.4G, 10C/20T, 10.4GT/s, 14M Cache, Turbo, HT (85W) DDR4-2400
2.	RAM: 128 GB		RAM: 128 GB RDIMM
3.	HDD: 7,2K rpm, 8 броя по 8 TB, защитени чрез RAID 6		HDD: 8 броя по 8TB, 7.2K RPM, защитени чрез RAID 6
4.	Networking: ○ Минимум 2 броя 100/1000 Base-T ○ Минимум 2 броя 10 Gbps SFP + ports		Networking: ○ 2 броя 100/1000 Base-T; ○ 2 броя 10 Gbps SFP+ порта; ○ 1 брой 100/1000 Mbps Base-T за отдалечено управление на сървърното шаси.
5.	Захранване: резервирани захранващи блокове		Захранване: два броя резервирани захранващи блока, (1+1), 750W.
6.	Конструкция: за инсталиране в 19“ сървърен шкаф		Сървърът разполага с необходимите шини за монтаж в 19” сървърен шкаф (rack).
7.	Да се достави със всички кабели за свързването му към инфраструктурата		Ще се достави с всички необходими кабели за свързването му към инфраструктурата.
8.	Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5		Гаранционната поддръжка е със срок 3 (три) години от производителя на цялата конфигурация, режим 8x5

Чл. 36а, ал. 3 от ЗОП

ПРИЛОЖЕНИЯ:

1. Копие/я от документ/и, удостоверяващ/и правата ни за оторизация от производителя/ите ~~(или от официален/ни негов/и представител/и)~~ за предложените софтуер и оборудване, съгласно т. 2 от Техническата спецификация;

2. Заверено копие на Сертификат EN ISO 27001:2013 или еквивалентен *с обхват, сходен с предмета на поръчката за система за управление на сигурността на информацията;*

3. Заверено копие на Сертификат EN ISO/IEC 20000-1:2011 или еквивалентен *с обхват, сходен с предмета на поръчката за въведена системи за управление на ИТ услуги;*

4. Копия от техническите каталози/брошури на производителя на български и/или английски език, от които се виждат основните технически

~~5. Декларация по чл.102, ал.1 от ЗОП (ако е приложимо, в свобо~~

Чл. 36а, ал. 3 от ЗОП

Чл. 36а, ал. 3 от ЗОП

Дата: **24.06.2019 г.**

Иван Житиянов
Изпълнителен ди
на „Телелинк Би
/име, фамилия, по

Чл. 36а, ал. 3 от ЗОП

18