Чл. 36а, ал. 3 от ЗОП

УТВЪР
СЕРГЕ
ПРЕДС

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за

„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“

1. Предмет:

Предмет на настоящата техническа спецификация е доставка и гаранционно обслужване на софтуер за събиране и анализ на журнални записи, хардуер и съпътстващи услуги свързани с информационната сигурност и защита, който да бъде реализиран в резервният изчислителен център на НСИ.

2. Минималните технически изисквания:

2.1. Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност – 1 брой

№	Минимално изискване
1.	Системата трябва да предоставя web-базиран графичен интерфейс за управление, анализ и извличане на 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.
3.	Софтуерът трябва да позволява интеграция с външни системи за автентикация.
4.	Административните правомощия трябва да позволяват дефиниране на достъп според устройства, група от устройства или 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 функционалност може да бъде административна, отчетна, филтрираща събития, корелация на събития, достъп до работен плот и др.
6.	Системата трябва автоматично да открива активи (сървъри, мрежови устройства и др.), които са обект на защита и наблюдение.
7.	Софтуерът трябва да предоставя web-базиран графичен интерфейс за управление, анализ и извличане на рапорти.
8.	Архитектурата на системата трябва да предостави всички изискани функции в едно устройство.
9.	Софтуерът трябва да разполага с възможност за разширяване на функционалността, чрез добавяне на готови приложения и функции, в

№	Минимално изискване
	потребителския интерфейс, представени и налични за изтегляне в специализиран портал на производителя.
10.	Софтуерът трябва да предоставя възможност за модификация на комуникационните портове между компонентите си.
11.	Системата трябва да позволява отворено API за достъп до данните съхраняващи се в базите от данни в системата.
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.
13.	Софтуерът трябва да има възможност за автоматична класификация (tagging) на отчетените събития.
14.	Софтуерът трябва да позволява създаване на различни работни плотове според специфичните изисквания на всеки отделен потребител.
15.	Софтуерът трябва да разполага с набор от преконфигурирани шаблони на работни плотове, които да могат да се използват без допълнителни промени.
16.	Софтуерът трябва да поддържа база от данни за всички активи, открити в информационната инфраструктура. Данните за активите трябва да предоставят важна информация събрана 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.
17.	Архитектурата трябва да предоставя възможност за внедряване както софтуерно решение върху виртуална платформа и/или цялостно хардуерно решение.
18.	Софтуерът трябва да гарантира интегритет на събраните данни (журнални записи). -- Архитектурата на системата трябва да 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.
20.	Софтуерът трябва да предоставя автоматизиран процес за архивни копия (конфигурации и събрани журнални записи) и тяхното възстановяване.

№	Минимално изискване
21.	Софтуерът трябва да предоставя автоматизирани проверки на работоспособност и при възникване на проблем да изпраща нотификация.
22.	Софтуерът трябва да позволява съхранение на събраните журнални записи върху външни системи (независимо от производителя) за съхранение.
23.	Софтуерът трябва да предоставя възможност за компресия на събраните журнални записи.
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.
25.	Софтуерът трябва да позволява нормализация на базовите събитийни полета. В това число: потребителски имена, IP адреси, имена на хостове, източници на журнални записи.
26.	Софтуерът трябва да 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.
28.	Софтуерът трябва да създава аларми базирани на наблюдавани аномалии и поведенчески промени в събитията свързани със сигурността.
29.	Софтуерът трябва да 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.
31.	Софтуерът трябва да 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.
33.	Софтуерът трябва да 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.
35.	Софтуерът трябва да 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.
37.	Софтуерът трябва да позволява изпращане на аларми към външни системи посредством e-mail, SNMP и Syslog.

№	Минимално изискване
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 .
39.	Софтуерът трябва да позволява корелация на свързани помежду си събития и представянето им като един инцидент.
40.	Софтуерът трябва да има възможност за интеграция с външни източници на информация от трети страни свързана със заплахи (примерно – географско позициониране, ботнет канали, враждебни мрежи). Получената информация трябва да 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.
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.
43.	Софтуерът трябва да може при интеграция с Vulnerability Management решение да инкорпорира и информация за уязвимостите на даден актив.
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.
45.	Софтуерът трябва да 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.
47.	Всеки един потребител трябва да има възможност да види всички свои (назначени на него) инциденти по сигурността, подредени по определен приоритет за обработка.
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.
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.
50.	Софтуерът трябва да предоставя механизъм за прихващане на всички релевантни аспекти свързани с инцидент в сигурността в обединена логическа визуализация.

№	Минимално изискване
51.	Софтуерът трябва да предоставя механизъм за добавяне на коментари в събраната и обособена логически информация за текущ инцидент в сигурността.
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.
53.	Софтуерът трябва да позволява събиране на журнални записи от Microsoft базирани сървърни крайни устройства.
54.	Софтуерът трябва да позволява събиране на журнални записи от Linux/Unix базирани сървърни крайни устройства.
55.	Софтуерът трябва да позволява събиране на журнални записи от бази от данни като: • MSSQL Server; • Oracle; • IBM DB2; • Sybase; • MySQL; • IBM Informix
56.	Софтуерът трябва да 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).
58.	Софтуерът трябва да позволява събиране на журнални записи от директориини 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;

№	Минимално изискване
	• 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; • Nmap; • Qualys; • Rapid7 Nexpose.
61.	Софтуерът трябва да има възможност за сканиране, откриване и управление на уязвимостите чрез собствена вградена функционалност.
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.
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.
64.	Системата трябва бъде скалируема и да предоставя възможности за разрастване без да е необходима пренастройка на инсталираната среда.
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.
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.
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.

№	Минимално изискване
68.	Софтуерът трябва да бъде с централизирано управление на всички компоненти.
69.	Софтуерът трябва да се достави с лицензи за наблюдение и обработка на минимум 800 EPS (events per seconds).
70.	Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5

2.2. Сървър тип 1 – 1 брой

№	Минимално изискване
1.	CPU: 2 броя, Xeon 2.4 GHz, 10 ядрени
2.	RAM: 128 GB
3.	HDD: 7,2K rpm, 8 броя по 8 TB, защитени чрез RAID 6
4.	Networking: o Минимум 2 броя 100/1000 Base-T o Минимум 2 броя 10 Gbps SFP + ports
5.	Захранване: резервирани захранващи блокове
6.	Конструкция: за инсталиране в 19`` сървърен шкаф
7.	Да се достави със всички кабели за свързването му към инфраструктурата
8.	Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5

3. Изисквания към изпълнението.

3.1 Доставката да ще се извърши в НСИ – Централно управление, гр. София, ул. „Панайот Волов“ № 2. Изпълнението на поръчката ще е в резервния изчислителен център на НСИ в село Сливек.3.2. Срокът за изпълнение на настоящата поръчка е до 5 (пет) месеца от датата на подписване на договор между Възложителя и Изпълнителя.

3.3. Участникът трябва да има системата за приемане и обслужване на сервизни заявки, която да включва организация на гаранционния сервиз, който да гарантира на Възложителя, че оборудването ще бъде обслужвано в параметрите, предписани от производителя и в сроковете изисквани от възложителя.

3.4. Участникът (ако не е производител), трябва да е оторизиран от производителя/ите (или от официален негов представител) с права да извършва доставка, внедряване и поддръжка на предложеното решение.

Към техническото си предложение Участникът трябва да представи копие на оторизационно/и писмо/а, договор/и или всякакъв друг документ като доказателство за извършване на доставка, внедряване и поддръжка на предложените софтуер и оборудване.

3.5. Участникът трябва да прилага сертифицирана система за управление на сигурността на информацията, съответстваща на стандарт EN ISO/IEC 27001:2013 или еквивалент, с обхват сходен с предмета на поръчката.

За доказване на посоченото изискване участникът трябва да представи към техническото предложение копие на валиден сертификат за въведена система за

управление на сигурността на информацията съгласно стандарта EN ISO/IEC 27001:2013 или еквивалентен, с обхват сходен с предмета на поръчката.

3.6. Участникът трябва да прилага сертифицирана система за управление на ИТ услуги, съответстваща на стандарт EN ISO/IEC 20000-1:2011 или еквивалентен с обхват, сходен с предмета на поръчката.

За доказване на посоченото изискване участникът трябва да представи към техническото предложение копие на валиден сертификат за въведена система за управление на услугите съгласно стандарта EN ISO/IEC 20000-1:2011 или еквивалентен с обхват, сходен с предмета на поръчката или еквивалентен.

3.7. Изпълнителят да изготви детайлно техническо описание/дизайн.

3.8. Изпълнителят да извърши физически монтаж на оборудването, съгласно утвърдените практики на Национален статистически институт.

3.9. Изпълнителят да инсталира доставения софтуер върху доставения хардуер.

3.10. Изпълнителят да извърши свързване, конфигуриране и тестване на работоспособността на връзката между оборудването и мрежата/оборудването на Национален статистически институт.

3.11. Изпълнителят да конфигурира системите съгласно одобрения детайлен дизайн на предложените решения.

3.12. Изпълнителят да изготви процедури за функционални тестове.

3.13. Изпълнителят да интегрира системите към съществуващата мрежа на Национален статистически институт, без функционални прекъсвания на работата.

3.14. Изпълнителят да извърши функционални тестове на системите съгласно приетите процедури.

3.15. Изпълнителят да обнови цялата техническа документация на решенията след тяхното приемане.

3.16. Изпълнителят следва да проведе 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.

3.17. При изпълнение на дейностите изпълнителят се задължава да пази в поверителност и да не разкрива или разпространява информация, станала му 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.

3.18. 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.

3.19. Към предложението на участника да са представени оригинали/копия от техническите каталози/брошури на производителя на български и/или английски език. От тези материали трябва да се виждат основните технически параметри, по които даденото устройство съответства на заложените технически спецификации.

Забележка:

1. Навсякъде в настоящата техническа спецификация всяко посочване на стандарт, следва да се чете допълнено с думите „или еквивалент".