**ОДОБРЯВАМ:**

**ЦВЕТАН НАНОВ**

**ГЛАВЕН СЕКРЕТАР НА НСИ**

**ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ**

**за**

**доставка и гаранционно обслужване на място на софтуер за събиране и анализ на журнални записи, свързани с информационната сигурност и защита, наблюдение и управление на базите от данни и хардуер**

**1. Предмет:**

Предмет на настоящата техническа спецификация е доставка и гаранционно обслужване на място на софтуер за събиране и анализ на журнални записи, свързани с информационната сигурност и защита, наблюдение и управление на базите от данни, и хардуер

**2. Минималните технически изисквания:**

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

| **№** | **Минимално изискване** |
| --- | --- |
|  | Софтуерът да позволява централизирано управление посредством web базиран интерфейс. |
|  | Административните правомощия трябва да позволяват дефиниране на достъп според устройства, група от устройства или мрежови диапазон. |
|  | 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. |
|  | Софтуерът трябва да позволява автоматично откриване на активи, които са обект на защита и наблюдение. |
|  | Софтуерът трябва да позволява автоматична класификация на активите, които са обект на защита. |
|  | Софтуерът трябва да предоставя възможност за модификация на комуникационните портове между компонентите си. |
|  | Софтуерът трябва да позволява отворено API за достъп до информацията в базите от данни. |
|  | Софтуерът трябва да предоставя възможност за криптиране на комуникацията между компонентите си. |
|  | Софтуерът трябва да позволява интеграция с външни системи за автентикация. |
|  | 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 трябва да има възможност за автоматична класификация (tagging) на отчетените събития. |
|  | Софтуерът трябва да позволява от една централна конзола прозрачно извличане, агрегация, филтрация и анализ на данни от компонентите за събиране на журнални записи с цел централна обработка на всички данни. |
|  | Софтуерът трябва да предоставя web-базиран графичен интерфейс за управление, анализ и извличане на рапорти. |
|  | Софтуерът трябва да позволява създаване на различни работни плотове според специфичните изисквания на всеки отделен потребител. |
|  | Софтуерът трябва да разполага с набор от преконфигурирани шаблони на работни плотове, които да могат да се използват без допълнителни промени. |
|  | 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. |
|  | Архитектурата трябва да предоставя възможност за внедряване както софтуерно решение върху виртуална платформа и/или цялостно хардуерно решение. |
|  | Софтуерът трябва да гарантира интегритет на събраните данни (журнални записи). |
|  | 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. |
|  | Софтуерът трябва да позволява компонентите му да не спират своята работа при срив в друг компонент или нарушена свързаност помежду им. Пример: При срив в управленската конзола, компонентите, които събират журнални записи продължават своята работа. |
|  | Софтуерът трябва да предоставя автоматизиран процес за архивни копия (конфигурации и събрани журнални записи) и тяхното възстановяване. |
|  | Софтуерът трябва да предоставя автоматизирани проверки на работоспособност и при възникване на проблем да изпраща нотификация. |
|  | Софтуерът трябва да позволява съхранение на събраните журнални записи върху външни системи (независимо от производителя) за съхранение. |
|  | Софтуерът трябва да предоставя възможност за компресия на събраните журнални записи. |
|  | 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 трябва да позволява нормализация на базовите събитийни полета. В това число: потребителски имена, IP адреси, имена на хостове, източници на журнални записи. |
|  | Софтуерът трябва да позволява анализ на събитията в близко до реалното време. |
|  | Софтуерът трябва да позволява анализ за събитията в дълъг период от време, показване на базова линия (baseline) и прогноза (trend) върху тези събития. |
|  | Софтуерът трябва да създава аларми базирани на наблюдавани аномалии и поведенчески промени в събитията свързани със сигурността. |
|  | Софтуерът трябва да предоставя възможност за рапорт на всички компоненти, подлежащи на управление през графичният потребителски интерфейс. |
|  | Софтуерът трябва да притежава конфигурируеми модули за създаване на рапорти, позволяваща гъвкавост и промени на генерираните рапорти. |
|  | Софтуерът трябва да позволява създаване на рапорти за определен интервал от време: час, ден, седмица месец или на специфично зададен период. |
|  | 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 трябва да предоставя възможност за алармиране, базирано на засечени заплахи за сигурността въз основа на наблюдаваните устройства. |
|  | Софтуерът трябва да предоставя възможност да корелира информация събрана от различни дистрибутирани компоненти. |
|  | Софтуерът трябва да предоставя възможност за алармиране, базирано на установени политики. |
|  | 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 трябва да позволява изпращане на аларми към външни системи посредством e-mail, SNMP и Syslog. |
|  | 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 трябва да позволява корелация на свързани помежду си събития и представянето им като един инцидент. |
|  | 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. |
|  | Софтуерът трябва да алармира когато има прекъсване в събирането на журнални записи от устройствата 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 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 ползвате и географската му локация. |
|  | Софтуерът трябва да може при интеграция с Vulnerability Management решение да инкорпорира и информация за уязвимостите на даден актив. |
|  | Софтуерът трябва да може да определя ниво на риска от даден инцидент по сигурността на база теглови коефициент и уязвимости за дадения актив. Респективно това ниво на риска трябва да може да се използва за определяне на приоритети на инцидентите по сигурността. |
|  | 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 трябва да предоставя вградени работни процеси, които улесняват и насочват действията на оперативните служители по сигурността. |
|  | Софтуерът трябва да има вграден модул, който да позволява назначаване на даден инцидент по сигурността на определен потребител. |
|  | Всеки един потребител трябва да има възможност да види всички свой (назначени на него) инциденти по сигурността, подредени по определен приоритет за обработка. |
|  | 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. |
|  | 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 трябва да предоставя механизъм за прихващане на всички релевантни аспекти свързани с инцидент в сигурността в обединена логическа визуализация. |
|  | Софтуерът трябва да предоставя механизъм за добавяне на коментари в събраната и обособена логически информация за текущ инцидент в сигурността. |
|  | 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 трябва да позволява събиране на журнални записи от Microsoft базирани сървърни крайни устройства. |
|  | Софтуерът трябва да позволява събиране на журнални записи от Linux/Unix базирани сървърни крайни устройства. |
|  | Софтуерът трябва да позволява събиране на журнални записи от бази от данни като:   * MSSQL Server; * Oracle; * IBM DB2; * Sybase; * MySQL; * IBM Informix |
|  | Софтуерът трябва да позволява събиране на журнални записи от системи за активно наблюдение на бази от данни. |
|  | Софтуерът трябва да позволява събиране на журнални записи от системи за управление на идентичности и достъп (Identity and access Management). |
|  | Софтуерът трябва да позволява събиране на журнални записи от директориини продукти (AD, LDAP и др.). |
|  | 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 трябва да позволява събиране на журнални записи от водещи в индустрията скенери за уязвимости като:   * Nessus; * Nmap; * Qualys; * Rapid7 Nexpose. |
|  | 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 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 трябва бъде скалируем и да предоставя възможности за разрастване без да е необходима пренастройка на инсталираната среда. |
|  | 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 трябва да може да работи в режим High Availability при бъдещо добавяне на идентични компоненти. |
|  | 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 трябва да предоставя възможност за управление на уязвимости чрез вградена функционалност. |
|  | Софтуерът трябва да бъде с централизирано управление на всички компоненти. |
|  | Софтуерът трябва да се достави с минимум един централен компонент за управление на останалите компоненти и агрегиране на данните от тях. |
|  | Софтуерът трябва да се достави с минимум един компонент за наблюдение, събиране и обработка на журнални записи. |
|  | Софтуерът трябва да се достави с лицензи за наблюдение и обработка на минимум 2500 EPS (events per seconds). |
|  | Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5 |

**2.2. Софтуер за защита, наблюдение и управление на бази от данни – 1 брой**

| **№** | **Минимално изискване** |
| --- | --- |
|  | Софтуерът трябва да предоставя централизирано управление на всички свои компоненти и административни функционалности посредством web базиран интерфейс. |
|  | Административните правомощия трябва да позволяват дефиниране на ролево-базиран достъп до различни функционални области на системата. Това включва ограничаване на достъпа до специфична функционалност извън обхвата на потребителската роля. |
|  | Административният достъп трябва да може да бъде одитиран и да се пазят записи за осъществените потребителски сесии както и за извършените промени от администратора и потребителите. |
|  | Софтуерът трябва да позволява създаване на различни работни плотове според специфичните изисквания на всеки отделен потребител. |
|  | Софтуерът трябва да е снабден с набор от готови шаблони на работни плотове. |
|  | Софтуерът трябва да позволява създаване на персонализирани доклади. |
|  | Софтуерът трябва да предоставя възможност за експорт на доклади в различни формати като: PDF, CSV, CEF. |
|  | Софтуерът трябва да предоставя възможност за изпращане в реално време на съобщения за настъпили събития и тревоги чрез:   * Mail; * SNMP; * SYSLOG. |
|  | Софтуерът трябва да предоставя възможност за наблюдение на всички операции за достъп до информация в бази от данни от релационен тип. Като минимум трябва да поддържа следните видове бази данни:   * MS SQL Server; * IBM DB2 (Linux, UNIX); * Oracle (including ASO and SSL); * IBM Informix; * Oracle MySQL and MySQL Cluster; * MariaDB; * PostgreSQL; * SAP Sybase. |
|  | Софтуерът трябва да включва възможности за откриване и класифициране на информация в база данни по зададени критерии. |
|  | Софтуерът трябва да поддържа функционалност за динамично скриване на информация (data masking) в реално време посредством:   * Маскиране на информацията при нейното презентиране на искащото приложение (без да се налага промяна на SQL заявката); * Пренаписване на SQL заявките преди изпращането им към базата от данни. |
|  | Софтуерът трябва да предоставя възможност за блокиране на достъп до информация включително и временно прекратяване на потребителска сесия към база данни при опит за нерегламентиран достъп като: изпълняване на заявки използващи таблици с чувствителна информация, опит за промяна на чувствителна информация, създаване на нови или промяна на правата на съществуващи потребителски акаунти за база данни. |
|  | Софтуерът трябва да може да следи и анализира действията и на привилегированите потребители и администратори на бази данни. |
|  | Софтуерът трябва да предоставя възможност за откриване на системи с база данни в различни мрежови сегменти. |
|  | Софтуерът трябва да може да анализира действията и достъпа на потребители до база данни и да посочва аномалии в тях по признаци като: използван различен мрежови адрес, достъп до ресурси в извън работно време, засечена много висока активност и др. |
|  | Софтуерът трябва да не нарушава работоспособността на наблюдаваните системи. |
|  | Софтуерът трябва да бъде скалируем, да може да се разширява обхвата и броя на наблюдаваните от него бази от данни. |
|  | Софтуерът трябва да може да открива уязвимости в бази данни и конфигурациите им. |
|  | На база на направените открития за уязвимости и проблеми със сигурността, да предлага стъпки и решения за тяхното отстраняване. |
|  | Софтуерът трябва да поддържа динамични доклади и анализи за откритите слабости и уязвимости. |
|  | Софтуерът трябва да може да акумулира събраната информация и да я съхранява на отделно място от наблюдаваните системи. |
|  | Събраната информация трябва да се обработва и анализира на отделни от платформите за бази данни системи, за да не се нарушава производителността им. |
|  | Събраната информация трябва да може да се експортира за дългосрочно архивиране на външни носители или споделени ресурси. |
|  | Софтуерът трябва да включва предварително дефинирани политики за сигурност, доклади и съобщения за тревоги. |
|  | Софтуерът трябва да предоставя възможност за надграждане и добавяне на наблюдение на достъп до файлове, откриване на уязвимости в средата на база данни и изготвяне на доклади за тях. |
|  | Софтуерът трябва да може да бъде инсталиран в High Availability режим. |
|  | Софтуерът трябва да поддържа криптиращите алгоритми – AES 256, RSA 2048. |
|  | Софтуерът трябва да поддържа криптиране на следните операционни системи: Windows, Redhat, CentOS, AIX и Solaris. |
|  | Софтуерът трябва да предоставя достъп до криптирано съдържание, базирайки се на политиките които позволяват идентификация на потребителя и процеса. |
|  | Софтуерът да поддържа идентификация на потребители от AD и LDAP. |
|  | Идентификацията трябва да има възможност да се прави и за потребители от външни източници. |
|  | Софтуерът трябва да предоставя функционалност за първоначално криптиране във фонов режим минимум за Windows системи. |
|  | Софтуерът да предоставя възможност за бъдещо разширение за използване и сигурност на ниво файлове с минимум функции за:   * Откриване и класифициране; * Активно следене за аномалии; * Блокиране на достъп. |
|  | Софтуерът да предоставя възможност за бъдещо разширение за използване и сигурност на ниво системи за съхранение на Big Data с поддръжка на минимум Cassandra, Hortonworks, MongoDB. |
|  | Софтуерът да предоставя възможност за интегриране с външни приложения за управление на инциденти свързани със сигурността (SIEM). Трябва да има възможност за препращане на информация за настъпили събития в реално време към външни SIEM системи чрез:   * SYSLOG; * Export to CSV. |
|  | Архитектурата трябва да предоставя възможност за внедряване както софтуерно решение върху виртуална платформа и/или цялостно хардуерно решение. |
|  | Архитектурата трябва да позволява скалируемост при необходимост от допълнителен капацитет. |
|  | Да има възможност за дистрибутирана архитектура за по-високо скалируемост. |
|  | Софтуерът трябва да позволява компонентите му да не спират своята работа при срив в друг компонент или нарушена свързаност помежду им. |
|  | Архитектурата трябва да предоставя централизирана конзола за управление и наблюдение. |
|  | Софтуерът трябва да разполага с приложен програмен интерфейс с възможност за изпълнение на потребителски дефинирани операции |
|  | Софтуерът трябва да се достави с минимум един компонент за осигуряване на контрол върху бази от данни. |
|  | Софтуерът трябва да се достави с минимум един централен компонент за управление на останалите компоненти и агрегиране на данните от тях. |
|  | Софтуерът трябва да се достави с цялото необходимо лицензно обезпечаване за наблюдението на минимум 8 DB сървъра и работещите на тях бази данни. |
|  | Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5 |

**2.3. Сървър тип 1 – 1 брой**

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

**2.4. Сървър тип 2 – 1 брой**

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

**2.5. Сървър тип 3 – 1 брой**

| **№** | **Минимално изискване** |
| --- | --- |
|  | CPU: 2 броя, Xeon 2.4 GHz, 10 ядрени |
|  | RAM: 128 GB |
|  | HDD: 10K rpm, 4 броя по 1.2 TB, защитени чрез RAID 5 |
|  | Networking:   * + - 2 броя 10/100/1000 Base-T     - 2 броя 10 Gbps SFP + ports |
|  | Захранване: резервирани захранващи блокове |
|  | Конструкция: за инсталиране в 19“ сървърен шкаф |
|  | Да се достави със всички кабели за свързването му към инфраструктурата |
|  | Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5 |

**2.6. Сървър тип 4 – 1 брой**

| **№** | **Минимално изискване** |
| --- | --- |
|  | CPU: 2 броя, Xeon 2.4 GHz, 10 ядрени |
|  | RAM: 128 GB |
|  | HDD: 10K rpm, 8 броя по 1.8 TB, защитени чрез RAID 5 |
|  | Networking:   * + - 2 броя 10/100/1000 Base-T     - 2 броя 10 Gbps SFP + ports |
|  | Захранване: резервирани захранващи блокове |
|  | Конструкция: за инсталиране в 19“ сървърен шкаф |
|  | Да се достави със всички кабели за свързването му към инфраструктурата |
|  | Гаранция и поддръжка Срок: 3 (три) години от производителя на цялата конфигурация, Режим: 8x5 |

**3. Изисквания към изпълнението.**

**3.1.** Доставката да се извърши в НСИ – Централно управление, гр. София, ул. „Панайот Волов“ № 2, до посочено от заявителя помещение.

**3.2.** 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.

**3.3.** 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.*

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

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

**3.6.** Участникът да изготви детайлно техническо описание/дизайн.

**3.7.** Участникът да извърши физически монтаж на оборудването, съгласно утвърдените практики на Национален статистически институт.

**3.8.** Участникът да инсталира доставения софтуер върху доставения хардуер.

**3.9.** Участникът да извърши свързване, конфигуриране и тестване на работоспособността на връзката между оборудването и мрежата/оборудването на Национален статистически институт.

**3.10.** Участникът да конфигурира системите съгласно одобрения детайлен дизайн на предложените решения.

**3.11.** Участникът да изготви процедури за функционални тестове.

**3.12.** Участникът да интегрира системите към съществуващата мрежа на Национален статистически институт, без функционални прекъсвания на работата.

**3.13.** Участникът да извърши функционални тестове на системите съгласно приетите процедури.

**3.14.** Участникът да обнови цялата техническа документация на решенията след тяхното приемане.

**3.15.** Участникът следва да проведе обучение на посочени от Възложителя – 5 (петима) служители в рамките на 3 (три) работни дни за работа с функционалните възможности на Софтуер за събиране и анализ на журнални записи свързани с информационната сигурност и Софтуер за защита, наблюдение и управление на бази от данни.

**3.16.** 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.

**3.17.** 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.

**3.18.** 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“.