**Приложение № 3**

Образец

**ДО**

**„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД**

**УЛ. „ПАНАЙОТ ВОЛОВ“ № 2**

**ГР. СОФИЯ**

[наименование на участника],

представлявано от [трите имена] в качеството на [длъжност, или друго качество]

с ЕИК […], със седалище […] и адрес на управление […],

адрес за кореспонденция: […],

банкови сметки: […]

**ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ**

**за участие в процедура за избор на доставчик с предмет:**

**„Осигуряване на правото на ползване на централизирана платформа за мониторинг и управление на ИТ активи за нуждите на киберсигурността на „Информационно обслужване“ АД“.**

След запознаване с документацията за участие в процедура за избор на доставчик с предмет: „Осигуряване на правото на ползване на централизирана платформа за мониторинг и управление на ИТ активи за нуждите на киберсигурността на „Информационно обслужване“ АД“, с настоящото Техническо предложение правим следните обвързващи предложения:

1. Срок за изпълнение:
	1. Декларираме, че ще осигурим лицензите в срок до …………..…./……………./ работни дни (*не повече от 10 /десет/ работни дни*), считано от датата на сключване на договор.
	2. Срокът на валидност на лицензите е 36 (тридесет и шест) месеца, считано от датата на осигуряване на лицензите.
2. Приемаме да изпълним предмета на процедурата, съгласно всички условия и изисквания, посочени от Възложителя в поканата за участие в настоящата процедура и Техническото задание - Приложение № 1.
3. Приемаме да осигурим възможност за обновяване по всяко време на софтуерното решение до последна версия за целия период на валидност на лицензите.
4. Предложението е със срок на валидност ………….. / …………………………/ календарни дни *(не по-малко от 60 /шестдесет/ календарни дни)*, считано от датата на представяне на предложението.
5. Приемаме да осигурим правото на ползване на централизирана платформа за мониторинг и управление на ИТ активи за нуждите на киберсигурността, със следната количествена и техническа спецификация:

**Вид продукт и количество**

|  |  |  |
| --- | --- | --- |
| **Вид/ продукт** | **Тип** | **Брой****/количество** |
| Централизирана платформа за мониторинг и управление на ИТ активи за 800 работни станции, 700 сървъра, 250 мрежови устройства (общо 1750 крайни точки) | Software/licence | 1750 |

**Технически и функционални изисквания**

|  |
| --- |
| **Централизирана платформа за мониторинг и управление на ИТ активи** |
|  | Решението трябва да представлява централизирана платформа за мониторинг и управление на ИТ активи, с детайлни изгледи, възможност за автоматизация и отдалечено изпълнение на команди. |
|  | Решението трябва да поддържа следните версии на Windows ОС:- Windows 7 SP1 Professional / Enterprise ;- Windows 8 Professional / Enterprise;- Windows 8.1 Professional / Enterprise;- Windows 10 Pro / Education / Enterprise / Education;- Windows 11 Pro / Education / Enterprise / Education; - Windows HPC Server 2008;- Windows Server 2012 Standard / Datacenter / Foundation / Essentials;- Microsoft Hyper-V Server 2012;- Windows Server 2012 R2 Standard / Datacenter / Foundation / Essentials;- Microsoft Hyper-V Server 2012 R2;- Storage Server 2012 Standard / Datacenter / Foundation / Essentials;- Windows Server 2016 Standard / Datacenter / Essentials;- Windows Storage Server 2016;- Windows Server 2016 Multipoint Premium Server;- Microsoft Hyper-V Sevrer 2016;- Windows Server 2019 Standard / Datacenter;- Windows Server 2022 Standard / Datacenter / Azure; |
|  | Решението трябва да поддържа следните версии на MAC OС:- macOS 10.12 Sierra;- macOS 10.13 High Sierra;- macOS 10.14 Mojave;- macOS 10.15 Catalina;- macOS 11.0 Big Sur;- macOS 12.0 Monterey |
|  | Решението трябва да предоставя различни/независими агенти за сигурност за 32bit и 64bit Linux операционни системи. Решението трябва да поддържа следните версии на Linux OС:- Debian 8.7/Ubuntu 14.04 "Trusty Tahr" (x86\_64 and i686)- Ubuntu 16.04 "Xenial Xerus" (x86\_64 and i686)- Ubuntu 18.04 "Bionic Beaver" (x86\_64)- Ubuntu 20.04 LTS (64-bit)- Red Hat Enterprise Linux/CentOS 6 (x86\_64 and i686)- Red Hat Enterprise Linux/CentOS 7 (x86\_64 and i686)- Red Hat Enterprise Linux/CentOS 8 (64-bit) |
|  | Решението трябва да има възможност за управление на външни крайни устройства (през интернет) без лимитиране на функционалностите  |
|  | Решението трябва да има възможност за управление и актуализация (patch management) на крайни устройства в защитени мрежи |
|  | Решението трябва да събира следната обща информация за крайните устройства:- Производител, модел, сериен номер на устройството- Мрежови hostname на устойството- Информация за домейна- Мрежова конфигурация (IP/MAC адрес, мрежова маска, gateway)- Информация за потребителя (login)- Операционна система- Информация за локални потребители и групи- Дата на последно засичане на устройството в мрежата. |
|  |  Решението трябва да събира следната хардуерна информация за крайните устройства:- Производител, модел, сериен номер, BIOS версия на дънната платка;- Производител, модел и сериен номер на процесор;- Размер на RAM;-Производител, вид, модел, характеристика и сериен номер на дисковете;-Производител, вид, модел, характеристика и сериен номер на видеоадаптера (видеокартата);- Производител, вид, модел, характеристика и сериен номер на мрежови адаптер. |
|  | Решението трябва да събира следната информация за инсталирания софтуер и пачове:- Име;- Версия;- Производител;- Дата на инсталиране. |
|  | Решението трябва да има възможност за извънредно актуализаране (out-of-band patch management) на Windows устройствата, при публикуване на извънрeдни актуализации.  |
|  | Решението трябва да има възможност за актуализиране (patch management) на приложения от трети страни (напр. Adobe/Java/...) на Windows устройства |
|  | Решението трябва да има възможност за грануларен контрол над одобряваните пачове, на база устройство/компания/класификация |
|  | Решението трябва да има възможност за автоматично одобряване и забраняване на пачове |
|  | Решението трябва да може да прави инвентаризация на периферни устройства (уебкамери, монитори и други) |
|  | Решението трябва да събира информация за всяко активиране на даден софтуер (software launches) от Windows устройствата |
|  | Решението трябва да има възможност за отдалечено инсталиране на софтуер на Windows, Linux и Mac устройства. |
|  | Решението трябва да има възможност за масово инсталиране на софтуерни пакети на множество машини с гъвкав график за стартиране (когато потребителят влезе в операционната система, когато компютърът се рестартира или по предварителен график). |
|  | Решението трябва да има възможност за определяне на директорията на крайното устройство, в която да се поставят файловете на пакета. Софтуерът трябва да се инсталира от тази директория. |
|  | Решението трябва да има възможност за избор на опция за инсталиране на софтуера (от системния, текущия потребителски или друг акаунт). |
|  | Решението трябва да има възможност за отдалечено инсталиране на софтуер (сървърът се свързва с клиента и изпраща софтуера, който да се инсталира). |
|  | Решението трябва да има възможност за изпълняване на vbs скриптове. |
|  | Решението трябва да има възможност за изпълняване на bat скриптове. |
|  | Решението трябва да има възможност за изпълняване на powershell скриптове. |
|  | Решението трябва да има възможност за дистанционно управление и взаимодействие, чрез стартиране на работна сесия към работни станции - лаптопи и сървъри. |
|  | Решението трябва да има възможност за създаване на персонализирана автоматизация за поддръжка на устройствата. |
|  | Решенето трябва да предоставя отчети за инсталирания софтуер на крайните устройства. |
|  | Решението трябва да предоставя отчети за хардуера на крайните устройства. |
|  | Решението трябва да има възможност за отчитане на пачовете на крайните устройства |
|  | Решението трябва да има възможност за одитно отчитане на всяко действие в конзолата за управление  |
|  | Решението трябва да има възможност за създаване на отчети въз основа на всички данни от инвентаризацията в системата. |
|  | Решението трябва да може да генерира филтри за различни устройства на базата на текстови файлове (txt, csv) |
|  | Решението трябва да предоставя централизирана конзола за управление. |
|  | Решението трябва да има възможност за диагностика на състоянието на агентите |
|  | Решението трябва да предоставя съвметимост на всчки системни компоненти с платформите за виртуализация Vmware 6. x, Vmware 7. x, Hyper-V |
|  | Решението трябва да има възможност за мониториране на мрежови устройства без агент |
|  | Решението трябва да има възможност за персонализирано конфигуриране на мониторираните компоненти на различните крайни точки |
|  | Решението трябва да има възможност за конфигуриране на персонализирани табла за управление (dashboards) с мониторираните компоненти (services)  |
|  | Решението трябва да има възможност за персонализирано известяване за грешки, базирано на мониторирането |
|  | Решението трябва да има възможност за планиране на действия по сканиране на мрежата за устройства и визуализиране на мрежовата топология от устройства |
|  | Решението трябва да има възможност за автоматизирани и персонализирани "self-healing" действия на мониторираните устройства |
|  | Решението трябва да има възможност за персонализирано мониториране на мрежовите устройства без агент чрез SNMP/SSH/Telnet |
|  | Решението трябва да има възможност за мониториране чрез syslog |
|  | Решението трябва да има възможност за поддръжка на до 35 хил. устройства |
|  | Решението трябва да има възможност за създаване на бекъп на базата данни. |
|  | Решението не трябва да позволява повредата на отделни устройства да влияе на цялостната му функционалност. |
|  | Решението трябва да има възможност за достъп до своя уеб интерфейс чрез HTTPS |
|  | Решението трябва да спазва следните изисквания за контрол на достъпа:- Решението трябва да има възможност за удостоверяване на потребителите на базата MS AD;- Решението трябва да има възможност за ролеви модел на достъп за управление (достъп за четене, неограничен достъп, достъп за управление на устройства);- Решението трябва да има възможност за създаване на потребителски акаунти от конзолата за управление. |
|  | Решението трябва да има възможност за 24/7 поддръжка. |
|  | Решението трябва да има възможност за наличие на вградени топологични карти. |
|  | Решението трябва да има възможност за интеграция с DNG filtering |
|  | Решението трябва да предоставя възможност за добавяне на допълнителен модул при бъдещо закупуване от същия производител - базов антивирус (native AV) |
|  | Решението трябва да предоставя възможност за добавяне на допълнителен модул при бъдещо закупуване от същия производител - EDR |
|  | Решението трябва да има възможност за интеграция с допълнителни антивирус, EDR и бекъп компоненти |
|  | Решението трябва да има възможност за автоматично инсталиране на Антивирус и EDR на крайните устройства, чрез агента за сигурност |
|  | Решението трябва да има възможност за оптимизирано внедряване на дефиниции чрез локални антивирусни сървъри |
|  | Решението трябва да има възможност за автоматична и планирана поддръжка на Антивируса и EDR |
|  | Решението трябва да има възможност за гъвкавост при инсталиране - локално и облачно |
|  | Решението трябва да има възможност за предоставяне на предварително изградени шаблони (templates) за наблюдение |
|  | Решението трябва да има възможност за прилагане на норми към съответните приложения (application compliance) |
|  | Решението трябва да има възможност за персонализиране на PSA интеграция |
|  | Решението трябва да има възможност за персонализиране на известия по Email  |
|  | Решението трябва да има възможност за интеграция с Intune |

Прилагаме като неразделна част към настоящото предложение всички необходими документи, както следва:

1. ………………………….
2. ………………………….
3. ………………………….

*/Описват се подробно приложените документи, съгласно т. 4 от поканата, както и допълнителни документи, представени по преценка на кандидата* /

**ПОДПИС**

[име и фамилия]

[качество на представляващия участника]

***Забележка:*** *Техническото предложение се представя в електронен вид във формат .pdf, подписано с квалифицирано удостоверение за квалифициран електронен подпис.*