

Блок: Информационни
технологии

Система: МА

Подразделение: П

Заличено на осн. ЗЗЛД

УТВЪРЖДАВА

Заличено на осн. ЗЗЛД

ЗАМЕСТНИК И

АЛЕКСАНДЪР

16.05.2022

ТЕХНИЧЕСКО ЗАДАНИЕ

№ 21.П.ТЗ.244/01

За доставка

ТЕМА: Доставка и внедряване на система за мониторинг и управление на активна директория и файлови ресурси.

Настоящото техническо задание съдържа техническа спецификация съгласно Закона за обществените поръчки.

1. Описание на доставката

Доставка и внедряване на система за мониторинг и управление на активна директория и файлови ресурси. Срок за доставка до 60 дни след подписване на договора.

1.1. Материали, консумативи, машини и оборудване (СМЗ-стоково материални запаси), които трябва да се доставят.

Софтуер за мониторинг на промените в ИКТ средите.

Лицензи:

-350 бр. за стандартни акаунти;

-250 бр. за сервизни акаунти.

1.2. Нестандартни/специализирани елементи, резервни части и инструменти към доставката

Няма отношение.

1.3. Изискване към Изпълнителя

Няма отношение.

2. Основни характеристики на оборудването и материалите

I. Изисквания относно събирането и съхранението на данни

| № | Описание |
|-----|---|
| 1. | Тип решение: софтуер |
| 2. | Тип лиценз: вечен (perpetual), с включени 12 месеца поддръжка |
| 3. | Брой лицензи: 350 за стандартни акаунти + 250 за сервизни акаунти |
| 4. | Да работи без да използва агенти, така че да не влияе негативно на производителността на системите и да не спира работния процес. |
| 5. | Да не се използват никакви недокументирани методи за събиране на данни от системите на организацията, тъй като подобни методи могат да доведат до отказване на поддръжка от Microsoft или от други ключови производители. |
| 6. | Да събира сурови машинни данни и да ги преобразува в опростена, ясна информация за всяко потребителско действие, за да се улесни вземането на правилни решения от организацията. |
| 7. | Да обединява данни от множество източници (логове за събития, извадки от настройките на средите, записи на действията, свързани с промени и т.н.), за да се извлече възможно най-пълната и надеждна одитна информация, без пропуски. |
| 8. | Да събира и предоставя пълни детайли за всяка промяна и опит за достъп, включително кога и къде промяната или опита за достъп са направени, кой ги е направил и какво точно е променено или достъпено. |
| 9. | Да извършва цялостно сравнение и да събира стойностите преди и след промяната за всички променени обекти. |
| 10. | Да ползва система за съхранение на две нива (SQL база от данни за отчитане и файлово-базирана система за архивиране на данни в компресиран формат за дълготрайно съхранение). Този архив трябва да съдържа цялостна одитна информация за повече от 10 години, без да намалява производителността на системата, като трябва да осигурява лесен достъп до данните за целият период. |
| 11. | Да събира одитна информация от локални и от облачни приложения и да ги съхранява в защитен, централизиран архив, което да позволява използването на общи аларми, търсене, отчитане и анализ на рисковете по сигурността. |

II. Изисквания относно поддържаните системи и обхвата на одитирането

| № | Описание |
|---|----------|
| | |

| | |
|----|--|
| 1. | <p>За активната директория (Active Directory) и груповите политики:</p> <ul style="list-style-type: none"> • Да докладва за промени в активната директория и в груповите политики; • Да събира информация за промените във времето на активната директория и на груповите политики, включително за участниците в групи с множество домейни и различни права на достъп; • Да одитира вписванията; • Да поддържа доверени и недоверени домейни. |
| 2. | <p>За Windows File Servers:</p> <ul style="list-style-type: none"> • Да докладва за промени по файлове, папки, споделени пространства и права за достъп; • Да докладва за преместени, преименувани или копирани файлове; • Да дава информация за успешни и неуспешни опити за прочитане на данни; • Да дава информация за промените във времето на ефективните права за достъп, включително и кои потребители имат превишени права за достъп; • Да създава отчети за собствеността на данните, използването на данните и обема на данните, отдавна неизползвани файлове и дублирани файлове; • Да докладва за чувствителни данни, включително къде са разположени, кой има активни права да ги достъпва и кой е собственик на данните, както и за успешни и неуспешни опити за достъп до данните и опити за промяна на правата за достъп до тях; • Да поддържа множество файлови сървъри и файлови устройства, разположени в няколко физически обекта, домейна и организации. |

III. Изисквания относно одити и аларми

| № | Описание |
|----|---|
| 1. | Да включва предварително зададени одитни отчети и dashboard-ове, които предоставят детайлна информация за промени, опити за достъп и настройки, представени в четим вид, позволявайки на потребителите да филтрират, сортират и извличат одитните данни. |
| 2. | Да позволява на потребителите лесно да изградят собствен отчет, базиран на конкретни изисквания, включително отчети, които да обхващат множество, разнообразни системи. |
| 3. | Автоматично да изпраща отчети до зададени получатели по email или да ги запазва в споделен файлов дял по зададен график (веднъж дневно, седмично, т.н.). |
| 4. | Да поддържа извличането на отчети в няколко различни формата, включително PDF, XLS(X), DOC(X) и CSV. |
| 5. | Да позволява на потребителите лесно да сортират и филтрират одитната информация чрез Google-подобна интерактивна търсачка, така че те лесно да открият точните данни, които са им необходими. |
| 6. | Да показва настоящите настройки на одитираните среди или как са изглеждали настройките в даден отрязък от миналото, включително активните права за достъп на даден потребител или обект, настройките на груповите политики и детайлите за настройките на Windows сървърите. |

| | |
|----|---|
| 7. | Да включва готови за ползване отчети, които са пригодени за проверяване на съвместимост със стандарти като ISO/IEC 27001, GDPR, PCI DSS, HIPAA, SOX, GLBA, FISMA/NIST800-53, CJIS, FERPA, NERC CIP или еквивалентни. |
| 8. | Да известява чрез email или чрез SMS съобщение отговорните екипи за подозрително поведение или събития, които могат да прерастнат в инциденти по сигурността, включително активност, която надвишава изчислените норми (аларми на базата на повтораемост на едно и също събитие). |
| 9. | Да може да докладва SQL SRS, да може да използва отчетните услуги на SQL сървъра по индустриален стандарт, (да поддържа и безплатната версия SQL Express), за да се предоставя широка гама от одитни отчети. |

IV. Изисквания относно сигурността на информацията

| № | Описание |
|----|--|
| 1. | Да притежава Dashboard-ове за оценяване на ИТ рисковете, които да позволяват на потребителите да идентифицират и оценят рисковете по три ключови показателя: управление на акаунти, права за достъп до системите за сигурност и управление на данни. |
| 2. | Да притежава Dashboard за откриване на аномално поведение, чрез който да се подобрява засичането на зловредни акаунти в ИТ средата, като предоставя агрегирани данни за аномалното потребителско поведение и да поставя съответна оценка на риска. |
| 3. | Да предоставя отчети за потребителско поведение и за анализиране на пропуските в системите за наблюдение. Да предоставя информация за потенциални инциденти, свързани със сигурността, като например действия извън нормалните бизнес часове на деня, необичайни вписвания в системите, голям брой неуспешни опити за действия, достъпване на архивирани данни, действия от досега неактивни потребителски акаунти и наличие на потенциално опасни файлове на файловите сървъри. |

V. Изисквания относно функции от общ характер

| № | Описание |
|----|--|
| 1. | Да има управление на Event logs: Автоматично да се събират, обединяват и архивират данните за настъпили събития, така че администраторите да могат да одитират събития от общ характер, събития, свързани с услуги, вписвания на потребители и състояли се сесии с отдалечен достъп. |
| 2. | Да има Dashboard за здравето на системите и за издаване на ежедневен обобщаващ отчет, който да позволява на потребителите да открият проблеми, които влияят на цялостта на събраните одитни данни, като лесно да може да се достигне до конкретната детайлна информация, която е необходима, за да се отстранят проблемите. Потребителите да могат да получават email отчет веднъж дневно, който да обобщава извършените действия през последните 24 часа. |

VI. Изисквания към интерфейса за управление на системата

| № | Описание |
|----|--|
| 1. | Да има централизирана конзола за управление, която да поддържа множество сървъри, като всеки да може да има собствени, различни настройки. |
| 2. | Да позволява интегрирането с други решения, да поддържа одитирането на множество от системи и приложения, включително системи, които са интегрирани чрез RESTful API, като всичко трябва да бъде обединено, позволявайки използването на dashboard-ове и отчети за комплексни среди от разнообразни системи. |
| 3. | Решението да дава цялостен изглед над средата, като всички функционалности да са част от единна платформа, премахвайки необходимостта от използването на множество отделни решения. |
| 4. | Правата за достъп да са ролево базирани. Платформата трябва да позволява фино разделяне на задълженията по наблюдението на системите от различните потребители, така че всеки от тях да има достъп само до необходимите му системи и настройки. |

VII. Изисквания за възможностите за интегриране с други решения

| № | Описание |
|----|---|
| 1. | Да има напълно документиран RESTful API интерфейс за интеграция с други решения, да може да се интегрира с решения за сигурност, за съответствие с различни сертификати и за автоматизиране на ИТ процесите и на работата на бизнес приложенията, така че да се предостави централизирано одитиране и отчетност или да се улесни управлението на промените и на действията по поддръжката на системите. |
| 2. | Да може да се интегрира със SIEM решения, за да се защитят инвестициите на организацията в SIEM платформи, като се предостави интегриране с определени SIEM решения, обогатявайки събраните от тях данни, предоставяйки контекста на събитията. |
| 3. | Да позволява безплатно да се добавят add-on добавки за интегриране с други решения, да има възможност за добавяне на безплатни, предварително създадени add-on добавки, които да улесняват интегрирането с решения, като например SIEM, ServiceNow ITSM и Linux системи. |

2.1. Класификация на оборудването

Няма отношение.

2.2. Квалификация на оборудването

Няма отношение.

2.3. Физически и геометрични характеристики

Няма отношение.

2.4. Характеристики на материалите

Няма отношение.

2.5. Химични, механични, металургични и/или други свойства

Няма отношение.

2.6. Условия при работа в среда с йонизиращи лъчения

Няма отношение.

2.7. Нормативно-технически документи

Няма отношение.

2.8. Изисквания към срок на годност и жизнен цикъл

Няма отношение.

3. Опаковане, транспортиране, временно складиране

3.1. Изисквания към доставката и опаковката

Ако заявените софтуерни лицензи са на физически носител, то те трябва да бъдат доставени в складовете на „АЕЦ Козлодуй“ ЕАД в оригиналната опаковка на производителя.

3.2. Условия за съхранение

Участникът да посочи условията за кратко, средно и дългосрочно съхранение на софтуерните лицензи, ако са на физически носител.

4. Изисквания към производството

4.1. Правилници, стандарти, нормативни документи за производство и изпитване

Няма отношение.

4.2. Тестване на продуктите и материалите по време на производство

Няма отношение.

4.3. Контрол от страна на „АЕЦ Козлодуй“ ЕАД по време на производството

Няма отношение.

5. Входящ контрол, монтаж и въвеждане в експлоатация

5.1. Тестване на продуктите и материалите при входящ контрол при приемане на доставката, след монтаж и по време на експлоатация.

Приемането на доставените софтуерни продукти се извършва след провеждане на общ входящ контрол без забележки съгласно „Инструкция по качество. Провеждане на входящ контрол на доставените суровини, материали и комплектуващи изделия в "АЕЦ Козлодуй" ЕАД", 10.УД.00.ИК.112. Доставката се приема след положителен резултат от общия входящ контрол.

5.2. Отговорности по време на пуск

Внедряването от страна на Изпълнителят включва следните етапи:

- Изготвяне на План-график за инсталиране на системата и интеграцията и в информационната система на АЕЦ „Козлодуй“;
- Съгласуване на план-графика с АЕЦ "Козлодуй" ЕАД;
- Инсталиране, активиране, начална конфигурация и тестване на системата от Изпълнителят в Информационната система на АЕЦ "Козлодуй" в присъствието и със съдействието на служители на отдел ИСиКТ,.
- Провеждане на тестове на инсталираната система. Тестове завършват с подписване на двустранен протокол, който да отбелязва недвусмислено дали тестовете са преминали успешно. Протокола поставя началото на срока за гаранционна поддръжка.

5.3. Мерки за безопасност против замърсяване с радиоактивни вещества и опасни продукти

Няма отношение.

5.4. Здравни и хигиенни изисквания

Няма отношение.

5.5. Условия за демонтаж, монтаж и частичен монтаж

Няма отношение.

5.6. Условия на състоянията на повърхностите

Няма отношение.

5.7. Полагане на покрития

Няма отношение.

5.8. Условия за безопасност.

Няма отношение.

5.9. Документи, които се изискват при доставка, монтаж и въвеждане в експлоатация

Заедно със софтуерните продукт/и е необходимо е да се доставят:

- Декларация за произход;
- Спецификация на доставения софтуер;
- Техническа документация на доставения софтуер (приема се и в електронен вид);
- Лицензи - ако има такива, включително и хартиено копие. Всички лицензи трябва да са на името на "АЕЦ Козлодуй" ЕАД или при изписване на латиница *Kozloduy NPP Plc*.

6. Гаранции, гаранционно обслужване и следгаранционно обслужване

6.1. Услуги след продажбата

Няма отношение.

6.2. Гаранционно обслужване

Предоставените лицензи да са с включени 12 месеца поддръжка.

7. Изисквания за осигуряване на качеството

7.1. Система за управление (СУ) на Изпълнителя

7.1.1 Изпълнителят следва да прилага система за управление на сигурността на информацията по стандарт ISO/IEC 27001 или еквивалентен, чийто обхват включва предоставяне на услуги в областта на ИКТ /информационни и комуникационни технологии/, анализ, администриране и поддръжка на информационни и комуникационни системи.

7.1.2 Изпълнителят уведомява „АЕЦ Козлодуй“ ЕАД за настъпили структурни промени или промени в документацията на Системата за управление, свързани с изпълняваните дейности по договора.

7.2. Програма за осигуряване на качеството (ПОК)

Няма отношение.

7.3. План за контрол на качеството (ПКК)

Няма отношение.

7.4. Одит от страна на „АЕЦ Козлодуй“ ЕАД (одит от втора страна)

7.4.1 „АЕЦ Козлодуй“ ЕАД има право да извършва одит на Изпълнителя преди започване на работата по сключен договор и по време на изпълнение на дейностите по договора.

7.4.2 „АЕЦ Козлодуй“ ЕАД извършва одити по ред установен с „Инструкция по качество. Провеждане на одити на външни организации”, 10.ОиП.00.ИК.049.

7.5. Управление на несъответствията

Изпълнителят докладва на „АЕЦ Козлодуй“ ЕАД за несъответствията, открити в хода на изпълнение на дейностите по договора.

Несъответствия на продукти и услуги, за които се изисква преработка, се докладват на Възложителя (отговорното лице по договор/ръководителя на структурното звено Заявител на

чиято територия се извършват дейностите), за да се вземе решение за разпореждане с несъответстващия продукт/услуга.

7.6. Специфични изисквания по осигуряване на качеството

Към доставения софтуер /лицензи/, да се доставят оригинални (от производителя) физически носители, ако са предвидени такива. Софтуерните ключове, които са задължителни за валидност на лицензи и за работа с продуктите, да бъдат предоставени на физически носител или с възможност да бъдат изтеглени от портал на производителя на софтуера. Всички лицензи за доставения софтуер да са валидни за срока на договора и на името на: "АЕЦ Козлодуй" ЕАД или при изписване на латиница: Kozloduy NPP Plc.

7.7. Обучение и квалификация на персонала на „АЕЦ Козлодуй“ ЕАД

Провеждане на обучение за инсталиране, конфигуриране и експлоатация на системата. Обучението следва да обхване 5 (пет) служителя от отдел ИСиКТ на АЕЦ "Козлодуй", извършва се на място или online и е за сметка на Изпълнителя.

7.8. Приемане на доставката

Ако заявените софтуерни лицензи са на физически носител, то те трябва да бъдат доставени в складовете на „АЕЦ Козлодуй“ ЕАД в оригиналната опаковка от производителя.

При доставката на софтуера /лицензите/ се проверява съответствието му със заявените параметри по спецификацията от договора за доставка.

Общ входящ контрол се извършва съгласно „Инструкция по качество за провеждане на входящ контрол на доставените суровини, материали и комплектуващи изделия в "АЕЦ Козлодуй" ЕАД, № 10.УД.00.ИК.112.

7.9. Спазване на реда в „АЕЦ Козлодуй“ ЕАД

Изпълнителят е длъжен да спазва изискванията на „Инструкция по качество. Работа на външни организации при сключен договор”, ДБК.КД.ИН.028.

8. Изисквания към Изпълнителя при използване на подизпълнители/трети лица

При използване на подизпълнители/трети лица, основният Изпълнител по договора:

- носи отговорност за изпълнението на изискванията на ТЗ от подизпълнителите/трети лица за изпълняваните от тях дейности, както и за качеството на тяхната работа;

- определя линиите за комуникация и взаимодействие с неговите подизпълнители/трети лица и начините на контрол върху дейностите, които им са превъзложени и отговорните лица за изпълнение на този контрол;

- определя по подходящ начин и в необходимата степен приложимите изисквания на ТЗ за подизпълнители/трети лица по договора, в зависимост от дейностите, които изпълняват;

- определя като минимум изискванията си за СУ на подизпълнители/трети лица, приложими норми и стандарти, ред за управление на несъответствията, обем на документацията, изпитания и проверки и др.;

- включва в документацията на договора с подизпълнители/трети лица, всички определени по-горе изисквания.

Заличено на осн. 33ЛД

РЪКОВОДИТЕЛ УПРАВЛЕНИЕ "ИНФОРМАЦИОН
И КОМУНИКАЦИОННИ ТЕХНОЛОГИИ",
АЛЕКСАНДЪР ЗЛАТАНОВ