Пазарна консултация № 45288 с предмет „Доставка и въвеждане в експлоатация на система за наблюдаване и защитата на важна и/или конфиденциална информация в „АЕЦ Козлодуй” ЕАД /Data Loss Prevention - DLP/ и защитата на информацията за физическите лица, свързано с обработването на лични данни”

„АЕЦ Козлодуй” ЕАД уведомява всички заинтересовани лица, че във връзка с подготовката за възлагане на обществена поръчка и определяне на прогнозна стойност, на основание на чл. 44 от ЗОП набира индикативни предложения за „Доставка и въвеждане в експлоатация на система за наблюдаване и защитата на важна и/или конфиденциална информация в "АЕЦ Козлодуй" ЕАД /Data Loss Prevention - DLP/ и защитата на информацията за физическите лица, свързано с обработването на лични данни”.

Предложението следва да включва:

- подробно описание, съгласно приложеното по-долу техническо задание - Приложение №1;
- единични цени и обща стойност без ДДС, валута;
- информация за срокове и условия на доставка и въвеждане в експлоатация на системата, гаранционен срок;
- съпроводителна документация при доставка и въвеждане в експлоатация на системата;
- точен адрес и лице за контакт, телефон, факс, e-mail, интернет адрес;
- ако участникът не е производител да се представи документ за представителство /оторизационен документ от производителя, даващ разрешение за продажба на предлаганата стока.

Запитвания във връзка с провежданите пазарни консултации може да бъдат отправяни до 26.08.2020 г. на e-mail: commercial@npp.bg, като разясненията ще бъдат публикувани на Интернет страницата на „АЕЦ Козлодуй” ЕАД в раздел Актуално / Обществени поръчки / Пазарни консултации.

Краен срок за подаване на индикативни предложения: 03.09.2020 г. на e-mail: commercial@npp.bg

Цялата информация, разменена по повод проведените пазарни консултации, ще бъде публикувана в профила на купувача.

С подаване на индикативно предложение, всеки участник в пазарните консултации се съгласява, че предложението и всякаква друга информация, предоставена като резултат от пазарните консултации, ще бъде публично достъпна в профила на купувача.

Възложителят си запазва правото да използва индикативни предложения, получени при проведени пазарни консултации, за възлагане на обществени поръчки до стойностните прагове на чл. 20, ал. 4 от ЗОП.

Допълнителна информация може да бъде получена от Христо Пачев - Експерт „Маркетинг”, тел. +359 973 7 6140, e-mail: HPatchev@npp.bg

Приложения:

1. Техническо задание - Приложение №1

РД-16585/11.08.20

# "АЕЦ Козлодуй " ЕАД

Блок: **Информационни технологии**

Система:

Подразделение: **П**

**ТЕХНИЧЕСКО ЗАДАНИЕ**

№ 19.П.ТЗ.52/01

За услуга

**ТЕМА: Доставка и въвеждане в експлоатация на система за наблюдаване и защитата на важна и/или конфиденциална информация в АЕЦ Козлодуй ЕАД /Data Loss Prevention - DLP/ и защитата на информацията за физическите лица, свързано с обработването на лични данни.**

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

## 1. Предмет на услугата

1.1 Доставка и въвеждане в експлоатация на система за наблюдение и защита на важна и/или конфиденциална информация в "АЕЦ Козлодуй" ЕАД /Data Loss Prevention - DLP/ и защитата на информацията за физическите лица, свързано с обработването на лични данни.

1.2 Обучение на администратори на системата за наблюдение и защита на важна и/или конфиденциална информация в "АЕЦ Козлодуй" ЕАД /Data Loss Prevention - DLP/

## 2. Обем на извършваната услуга

2.1 Доставка и монтаж на хардуерната част от техническа спецификация (Приложение 1).

2.2 Доставка, инсталация и въвеждане в експлоатация на система за наблюдение и защита на важна и/или конфиденциална информация в "АЕЦ Козлодуй" ЕАД /Data Loss Prevention - DLP/, отговаряща на изискванията към софтуерната част от Приложение 1.

2.3 Обучение на служители на Възложителя за конфигуриране и администриране на DLP системата, съгласно частта за обучение от Приложение 1.

## 3. Организация на работата по изпълнение на услугата

### 3.1. План за изпълнение на дейностите по услугата

3.1.1 Крайният срок за реализиране на задачите по техническото задание описани в Приложение 1 е четири /4/ месеца от сключване на договора.

3.1.2 Дейностите по договора трябва да се изпълнят на три етапа.

**Първият етап обхваща дейностите:**

- доставка, монтаж и въвеждане в експлоатация на хардуерната част по точка 1 от Приложение 1, не по-късно от 45 дни от сключването на договора;

**Вторият етап обхваща дейностите:**

- доставка, инсталиране, активиране и начална конфигурация на софтуера по точка 2 от Приложение 1, не по-късно от 45 дни след приключване на дейностите по първия етап от договора;

**Третият етап обхваща дейностите:**

- обучение за администриране и конфигуриране на софтуера по точка 2, отговарящо на изискванията в точка 3 от Приложение 1, не по-късно от 1 месец след приключване на дейностите по втория етап.

3.1.3 "АЕЦ Козлодуй" ЕАД се задължава да осигури достъп на служители на Изпълнителя след предварително подадени списъци с необходимите данни от страна на Изпълнителя.

3.1.4 Всяка дейност ще се счита за изпълнена след отчет от страна на Изпълнителя и подписване на двустранен приемо-предавателен протокол.

### 3.2. Условия за изпълнение на услугата

3.2.1 Достъпът на персонала на Изпълнителя до "АЕЦ Козлодуй" ЕАД и разрешението за работа се осъществява по реда за разрешение и допускане до работа, съгласно Инструкция по качество. Работа на външни организации при сключен договор, ДБК.КД.ИН.028 и Инструкция за пропускателен режим в „АЕЦ Козлодуй" ЕАД, УС.ФЗ.ИН.015.

3.2.2 При необходимост ще се подсигури контролиран дистанционен достъп на служителите на Изпълнителя, за да се обезпечи процеса по инсталацията и конфигуриране на софтуера.

### 3.3. Нормативно-технически документи

Няма отношение

### 3.4. Критерии за приемане изпълнението на услугата

3.4.1 Критериите за приемане изпълнението на услугата са степента и качеството на изпълнените дейности по съответните етапи описани в т. 3.1.2

3.4.2 Документално става чрез двустранно подписани приемо-предавателни протоколи, съгласно етапите по т. 3.1.2

## 4. Документация

### 4.1. Документи, представени от „АЕЦ Козлодуй" ЕАД

4.1.1 Подаването на данни и информация /ако се налага такова/, собственост на „АЕЦ Козлодуй" ЕАД, ще се осъществява след получаване на писмено искане от страна на Изпълнителя по реда на *„Инструкция по качеството. Предаване на входни данни на външни организации"*, № ДОД.ОК.ИК.1194.

### 4.2. Документи, представени от Изпълнителя

4.2.1 Ръководство за инсталиране, конфигуриране и администриране на закупения софтуер за наблюдение и защита на важна и/или конфиденциална информация в "АЕЦ Козлодуй" ЕАД /Data Loss Prevention - DLP/ и защитата на информацията за физическите лица, свързано с обработването на лични данни.

4.2.2 Лицензите за закупения софтуер трябва да са на името на „АЕЦ Козлодуй" ЕАД, вкл. и хартиено копие (приема се и разпечатка от интернет сайт) и да отговарят на условията за брой лицензи и продължителност /в месеци/, съгласно изискванията към софтуера по точка 2 от Приложение 1;

4.2.3 Декларация за произход на хардуера и софтуера;

4.2.4 Спецификация на доставеното оборудване и софтуер;

4.2.5 Пълен комплект документация за доставения софтуер и хардуер (приема се и в електронен вид);

### 4.3. Отчетни документи

4.3.1 Приемо-предавателен протокол за изпълнението на всяка дейност по съответните етапи от ТЗ

4.3.2 Отчет за изпълнение на договора.

4.3.3 Отчетни документи, удостоверяващи доставката на лицензите по т. 2 от Приложение 1

### 4.4. Ред за влизане в сила на документите

4.4.1 Приемо-предавателните протоколи за изпълнението на дейностите по съответните етапи се подписват от отговорното лице по договора от страна на Възложителя.

4.4.2 Отчетът за изпълнение на договора се приема от директор на Дирекция "Производство".

## 5. Изисквания за осигуряване на качеството

### 5.1. Система за управление (СУ) на ВО-Изпълнител

5.1.1 Изпълнителят да прилага система за управление, сертифицирана по БДС EN ISO 9001:2015 или еквивалентен.

### 5.2. Програма за осигуряване на качеството (ПОК)

Няма отношение

**5.3. План за контрол на качеството (ПКК)/ План за контрол и изпитване (ПКИ).**

Няма отношение

**5.4. Одит от страна на „АЕЦ Козлодуй" ЕАД (одит от втора страна)**

Няма отношение

**5.5. Управление на несъответствията**

5.5.1 Несъответствия на продукти и услуги открити в хода на изпълнение на дейностите по договора, за които се изисква преработка за достигане на изискванията на техническото задание, се докладват от Изпълнителя на ръководителя на структурното звено Заявител, на чиято територия се извършват дейностите, за взимане на решение за разпореждане с несъответстващ продукт.

**5.6. Професионална компетентост (квалификация) на персонала на Изпълнителя**

5.6.1 Изпълнителят трябва да е завършил поне 1 проект за внедряване на система за наблюдение и защита на важна и/или конфиденциална информация /Data Loss Prevention - DLP/ или сходна такава. Опитът се доказва с представяне на списък с реализирани проекти.

5.6.2 Изпълнителят трябва да представи екип от минимум двама експерти, които ще участват в изпълнението на проекта със съответните степени на сертифицираност за продуктите /хардуер и софтуер/ предмет на настоящото ТЗ, съгласно Приложение 1

5.6.3 Екипът за изпълнение на проекта следва да се състои от персонал с компетенции в областта на внедряване на система за наблюдение и защита на важна и/или конфиденциална информация /Data Loss Prevention - DLP/.

**5.7. Специфични изисквания по осигуряване на качеството**

5.7.1 Към доставения софтуер /лицензи/, да се доставят оригинални (от производителя) физически носители. 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 на името на:"АЕЦ Козлодуй" ЕАД или при изписване на латиница: Kozloduy NPP Plc.

**5.8. Обучение на персонал на „АЕЦ Козлодуй" ЕАД**

~~5.8.1 Да се проведе обучение на определените от "АЕЦ Козлодуй" ЕАД лица относно~~ инсталирането, конфигурирането и администрирането на софтуера по точка 2 от Приложение 1, съгласно условията описани в т. 3 от Приложение 1

5.8.2 Обучението да се проведе по одобрена Програма за обучение и осигурени учебни материали от Изпълнителя, съгласно изискванията за обучение по съответния софтуер.

5.8.3 Учебните материали, по които ще се провежда обучението трябва да бъдат предадени на Възложителя.

5.8.4 Обучението да се проведе съгласно изискванията за обучение към съответния софтуер. Ако не са упоменати такива, обучението да се проведе според изискванията на Възложителя, които са предмет на уточняване след приключването на Втори етап от настоящото техническо задание.

5.8.5 На успешно преминалите обучението, да се издаде сертификат.

5.8.6 Обучението е за сметка на Изпълнителя.

**5.9. Необходими лицензии, разрешения, удостоверения, сертификати и др. на Изпълнителя.**

5.9.1 Изпълнителят трябва да е сертифициран от производителя на оборудването за продажба и сервиз на предложеното оборудване по точка 1 от Приложение 1.

5.9.2 Изпълнителят трябва да е оторизиран от производителя на софтуера по точка 2 от Приложение 1 или да е негов официален представител.

5.9.3 Изпълнителят трябва да представи документи, доказващи степента на сертифицираност на служителите на фирмата, които ще осъществяват инсталацията и конфигурирането на софтуера по точка 2 от Приложение 1.

5.9.4 Изпълнителят трябва де е оторизирани от производителя на решението или от негов официален представител за продажба и гаранционна поддръжка.

5.9.5 Изпълнителят трябва да представи документи, доказващи степента на сертифицираност на служителите на фирмата, които ще осъществяват обучението по точка 3 от Приложение 1.

**6. Организационни изисквания**

6.1 По време на реализация на договора, при необходимост, Изпълнителят да осигури за своя сметка присъствие на свой представител на работните срещи, провеждани на площадката на „АЕЦ Козлодуй" ЕАД, имащи отношение към изпълняваните дейности.

**7. Допълнителни изисквания**

7.1 Минимум 36 месеца гаранция (от производителя) за хардуерната част от конфигурацията - точка 1 от Приложение 1

7.2 Допълнителна гаранция с време за отстраняване на повреда на следващия работен ден след заявяването – според приложена техническа спецификация (Приложение 1).

**8. Контрол от страна на „АЕЦ Козлодуй" ЕАД**

8.1 „АЕЦ Козлодуй" ЕАД има право да извършва инспекции и проверки на възложените за изпълнение от ВО дейности. Изпълнителят осигурява достъп до персонал, помещения, съоръжения, инструменти и документи, използвани от външните организации и техни подизпълнители.

**9. Изисквания към ВО-Изпълнител при използване на подизпълнители/трети лица**

9.1 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 са им 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;

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

**ПРИЛОЖЕНИЯ:**

Приложение 1 - Техническа спецификация /Приложение 1/ към ТЗ 19.П.ПРЕТЗ.63

# ПРИЛОЖЕНИЕ 1

## ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

**към Техническо задание за**

Доставка, въвеждане в експлоатация и обучение на система за наблюдение и защита на важна и/или конфиденциална информация в "АЕЦ Козлодуй" ЕАД /Data Loss Prevention - DLP/ и защитата на информацията за физическите лица, свързано с обработването на лични данни със следните минимални изисквания:

| 1. | Хардуерна част от техническа спецификация | |
|---|---|---|
| 1.1 | Server със следните минимални технически характеристики | 2 бр. |
| | | |
| **Описание** | **Минимални изисквания** | |
| Шаси | - Формат макс. 2U, за монтаж в 19" шкаф. Включени аксесоари за монтаж | - |
| Процесор | - Два броя процесори с мин. 18 ядра, мин. 2.6 Ghz базова честота и мин. 24 MB cache, | - |
| Оперативна памет | - Инсталирани мин. 128 GB DDR4-2933, Registered<br>- Мин. 24 слота за памет.<br>- Сървърът да поддържа максимален капацитет 3 TB DDR4 | - |
| Дисков контролер | - RAID контролер.<br>- Да поддържа мин. 12 устройства | - |
| Дискови устройства | - Да има мин. 8 броя слотове за дискове.<br>- Да се достави с инсталирани мин. 4 броя с капацитет на всеки от тях мин. 4 TB, 12G, SAS<br>- Да се достави с инсталирани мин. 2 броя с капацитет на всеки от тях мин. 480 GB, 6G, SSD | - |
| Портове за комуникация и интерфейси | - Мин. 4 x 1Gb Ethernet (RJ-45) порта<br>- необходими кабели и/или модули за свързване на двата порта с комутатор съвместими с Cisco WS-C4500X-16) | - |
| Захранване | - Резервирани Hot-Plug захранвания, мин. 800W, Energy Star Platinum (94%) Compatible. | - |
| Софтуер | - VMware vSphere Essentials | - |
| Поддържани операционни системи | - Microsoft Windows Server; VMware; Red Hat, SUSE | - |
| Гаранционно обслужване | - 3 години, с обслужване на място от производителя на оборудването. Да се посочи с партиден номер. | - |

| 2. | Софтуерна част от техническа спецификация DLP System |
|---|---|
| 2.1 | **Брой DLP лицензи:**<br>**- минимален брой 3000 бр;**<br>**- минимален срок 3 години.** |

| 2.2 | Задължителни основни функционални характеристики: |
|---|---|
| Минимални технически изисквания: | Модулите следва да:<br>- Притежават единна централизирана конзола за контрол и управление на информационната сигурност, която да бъде уеб-базирана, достъпна чрез уеб браузър;<br>- Защитават електронната информация в организацията от неоторизирано изтичане на мрежово ниво, в крайните точки (работни станции, лаптопи и мобилни телефони), както ида открива и класифицира данни;<br>- Притежават централизиран мониторинг и документиране действията на служителите;<br>- Притежават централизирано управление и конфигуриране на политиките за всички продукти (за наблюдение и за превенция, на мрежово ниво и на ниво крайна точка) през уеб-базираната конзола за управление, използвайки еднаква логика за изграждането на политиките им;<br>- Решението трябва да поддържа надграждане в бъдеще, което да включва управлението на решения за уеб защита и защита на електронна поща, както и на решения за защита на облачни приложения<br>- Установяват централизиран административен контрол на потребителския достъп до всички съществуващи входни и изходни канали на информация и периферни устройства в „крайните точки";<br>- Налагат контрол на всички потребителски операции с възможно най-високото им детайлизиране: Кой? От къде? Къде? Кога? Какво?;<br>- Прилагат правила за достъп до устройствата и портовете на „крайната точка";<br>- Осигуряват ненамеса в достъпа на служителя, докато не се нарушат установените правила;<br>- Се интегрират с други решения за ИТ сигурност;<br>- Осигуряват централизирано управление на всички крайни точки;<br>- Предоставят възможност за индексиране на данни;<br>- Да могат да засичат и блокират поверителни данни в email комуникация<br>- Разполагат с технология за откриване на съдържание, която улеснява идентифицирането на неструктурирани, текстови данни, които трудно се намират или описват.<br>- Разполагат с модул за анализ на информацията, който да предоставя отчети включващи анализ на риска спрямо нуждите на ръководството и одиторите в организацията;<br>- Разполагат с възможност за наблюдение на достъпа до различни типове файлове и наблюдение на използването им (File access and usage monitoring);<br>- Разполагат с възможност за създаване на гранулярни политики за следене на конфиденциална информация<br>- Решението да притежава възможност да се използва единна политика, за да сканирате данни, където и да се съхраняват или използват, както на мрежово ниво, така и в крайните точки;<br>- Решението да разполага с автоматична реакция на открита заплаха;<br>- Решението да се синхронизира с активна директория и да предоставя възможност за създаване на правила за създаване на политики по групи и/или потребители; |

| | |
|---|---|
| | - Решението да притежава предварително зададени политики за откриване, да съответстват на законовите рамки и най-добрите практики, включително предварително определени политики изисквани в разпоредби;<br>- Решението трябва да разполага с възможности за обработка на много големи файлове или приложения (90MB и по-големи) по време на процеса за откриване на отпечатъци в съдържанието на файловете;<br>- Решението да включва метод за самообучение на методите за откриване, което изисква малък набор от образци на документи, за да се даде възможност за точно откриване на други подобни документи;<br>- Решението да поддържа метод за откриване, базиран на регулярни изрази, който да подлежи на персонализация;<br>- Решението трябва да притежава списък с ключови думи (за откриване);<br>- Решението да предоставя възможност за засичане на криптирани файлове и прилагане на политики спрямо тях;<br>- Решението да позволява наблюдение, базирано на конкретен файлов тип, независимо дали разширението на файла бива променено;<br>- Решението да позволява конфигурирането за засичане на специфични или нови типове файлове;<br>- Решението да позволява автоматично известяване при настъпването на инцидент по електронна поща на изпращача и/или отговорника по информационната сигурност в организацията;<br>- Решението да предоставя възможност за извеждане на екранни съобщения директно върху работните станции на потребителите след засичане на инцидент. Потребителите трябва да имат възможност да предоставят обратна връзка за инцидента чрез диалогови менюта на български език. Да има възможност за допълнително конфигуриране на диалоговите менюта;<br>- Решението да позволява отварянето на оригиналните прикачени файлове, трансферирани по електронна поща, директно от централния интерфейс на приложението;<br>- Решението да позволява създаването на различни роли за достъп до приложението като системните администратори да нямат достъп до конфиденциалната информация, която е регистрирана в инцидентите. Възможност за създаване на нива на достъп спрямо инцидентите, касаещи определено звено в организацията;<br>- Решението да позволява анализирането на мрежовия трафик в реално време;<br>- Решението да позволява наблюдението на web трафик, включително web електронна поща, публикации в интернет, изпращане на файлове и други протоколи използващи HTTP и HTTPS;<br>- Решението да позволява наблюдението на Instant messaging приложения<br>- Решението да може да блокира конфиденциална информация предавана чрез FTP протокол;<br>- Решението да позволява сканирането на Windows и Linux споделени мрежови ресурси и папки;<br>- Решението да позволява сканирането на NAS масиви;<br>- Решението да поддържа сканирането на MS SQL и Oracle бази данни;<br>- Решението да поддържа сканиране на MS SharePoint сървъри; |

| | |
|---|---|
| | - Решението да предоставя история на достъпа до файловете (от всички потребители), за които има регистриран инцидент;<br>- Решението да позволява блокиране на конфиденциална e-mail кореспонденция изпращана от мобилни устройства;<br>- Решението да предлага възможност за генериране на отчети за инцидентите спрямо различните звена в организацията;<br>- Решението да предлага възможност за генериране на отчети спрямо тенденциите открити в организацията за различни времеви интервали;<br>- Решението трябва да притежава възможност за изпращане по имейл на съобщения директно от интерфейса без ръчно повторно форматиране.Възможност отчетите да бъдат директно изпратени по електронна поща от централната конзола на DLP системата;<br>- Компонента за наблюдение на крайни клиенти да позволява наблюдение на всички действия и файлове копирани в клипборда на операционната система;<br>- Клиентският агент да поддържа следните операционни системи, включително техните модификации:<br>• Microsoft Windows Server 2008;<br>• Microsoft Windows Server 2012;<br>• Microsoft Windows Server 2016;<br>• Microsoft Windows Server 2019;<br>• Microsoft Windows 7;<br>• Microsoft Windows 8;<br>• Microsoft Windows 8.1;<br>• Microsoft Windows 10;<br>• Mac OS.<br>- Да поддържа идентификация и класификация на данни;<br>- Да разполага с единна централизирана конзола (уеб-базирана конзола, достъпна през уеб браузър, без да изисква инсталирането на допълнителен софтуер), от която да могат да се управляват всички компоненти на DLP: за засичане и спиране на изтичане на данни на мрежово ниво и чрез електронни съобщения (мрежово DLP); за засичане и спиране на изтичане на данни на ниво крайна точка (Endpoint DLP); за откриване и класифициране на данни (Discover). |
| | - Решението да има възможност за бъдещо надграждане с цел скалируемост, което да включва управлението на решения за уеб защита и защита на електронна поща, както и на решения за защита на облачни приложения от същия производител.<br>- Решенеито да разполага с минимум 1500 предварително зададени политики, за да не е необходимо отделянето на много време от администраторите в създаване на собствени политики.<br>- Да поддържа интеграция със следните облачни среди: Office365, OneDrive, Box.<br>- Да поддържа имплементация на компонентите в Hyper-V или VMware среда.<br>- Да търси класифицирани данни (Discover) по зададени критерии, като трябва да се запомнят откритите досега данни и при последващо сканиране да се търсят само нови данни, които не са индексирани. |

| | |
|---|---|
| | - Да засича множество случаи на изтичане на данни във времето, породени от един и същ потребител, като да може да създаде общ инцидент при достигане на определено, зададено количество събития. По този начин решението трябва да може да засича опити за частично изнасяне на информация от дадени потребители за дълъг период от време<br>- Решението да може да извлича и обработва съдържанието от графични файлови формати, използвайки OCR технологии като Abbyy FineReader или Nuance. OCR технологията трябва да е вградена в решението, без да е необходимо закупуването на допълнителни лицензи.<br>- Да засича изтичане на данни от структурирани системи, което включва бази данни от типа Microsoft SQL Server, Oracle, IBM DB2, както и да всички други типове бази данни, можещи да използват ODBC или OLE конектори за свързване с трети системи<br>- Да разполага с machine-learning технология (да използва алгоритми и техники, за да може автоматично да се учи от предишни инциденти)<br>- Да засича изтичане на данни от структурирани системи, което включва бази данни от типа Microsoft SQL Server, Oracle, IBM DB2, както и да всички други типове бази данни, можещи да използват ODBC или OLE конектори за свързване с трети системи.<br>- Да се задават автоматични действия от системата по различни параметри, например коя политика е нарушена, степента на риска на инцидента, броя събития, използвания протокол за комуникация и т.н.<br>- Да може автоматично да колира файловете в карантина, да криптира файловете (допуска се използването и на third-party инструменти за криптиране) или да трие файловете, които са засечени при неправомерни действия.<br>- Да дава информация и да изготвя отчети, които да информират кои инциденти и кои потребители носят най-голям риск за организацията и кои инциденти трябва да се разгледат първи, с по-голям приоритет.<br>- Да инспектира криптирана SSL комуникация, без тази функция да изисква закупуването на допълнителни модули или да е зависима от използването на ICAP протокол.<br>- Да може да сканира и блокира (или друго зададено автоматично действие): чувтствителни данни в SMTP трафик, прикачена чувствителна информация към уеб трафик, пренос на чуствителни данни от файлов сървър към работна станция (LAN трафик), пренос на чувствителна информация в PDF формат.<br>- Да може да наблюдава и налага политики на email трафика, включително да се сканират прикачените файлове в съобщенията. Да има интеграция с Microsoft Outlook и IBM Lotus Notes. |
| | - Да засича и блокира (или друго зададено автоматично действие) опити на потребители за копиране на класифицирани данни на преносими устройства (например USB устройства, флопи дискове, CD/DVD, т.н.). Да се блокира преноса на данни, независимо дали потребителската крайна точка се намира в или извън мрежата на организацията.<br>- Да се интегрира напълно с трети решения като Titus, Boldon James или Microsoft Azure Information Protection, с цел поставяне на етикети на класифицираните данни. |
| **3.** | **Обучение по DLP System** |

| 3.1 | Изисквания към обучението |
|---|---|
| | 3.1.1 Обучение на минимум 2 лица определени от Възложителя, относно инсталирането, конфигурирането и администрирането на софтуера по DLP Systems.<br>3.2.2 Изпълнителят да представи Програма за обучение и осигури учебни материали, съгласно изискванията за обучение по съответния софтуер.<br>3.2.3 Учебните материали, по които ще се провежда обучението трябва да бъдат закупени от Изпълнителя и предадени на Възложителя.<br>3.2.4 Обучението да се проведе, съгласно изискванията за обучение към съответния софтуер. Ако не са упоменати такива, обучението да се проведе според изискванията на Възложителя, които са предмет на уточняване след приключването на Втори етап от настоящото техническо задание.<br>3.2.5 На успешно преминалите обучението, да се издаде сертификат.<br>3.2.6 Обучението е за сметка на Изпълнителя. |