1. Տեխնիկական աջակցության պահանջներ
1.1 Առաջարկվող տվյալների արտահոսքի պաշտպանության ծրագրային արտադրանքը պետք է ունենա արտադրողի կողմից հավաստագրված տեխնիկական աջակցության կենտրոն, որը կիրականացնի տեխնիկական աջակցություն օգտագործողներին՝ համաձայն հետևյալ պահանջների՝

- **24x7x365 սպասարկում** – 24 ժամ օրական, 7 օր շաբաթական, տարվա բոլոր 365 օրերին, ներառյալ տոները, հանգստյան և ոչ աշխատանքային օրերը:
- **Ընդլայնված տեխնիկական խորհրդատվություն** տվյալների արտահոսքի պաշտպանության ծրագրային արտադրանքի կարգավորումների և շահագործման վերաբերյալ՝ հեռախոսով (տեղական հեռախոսազանգերի հնարավորությամբ՝ առանց միջազգային կապի ծառայության օգտագործման) և էլեկտրոնային փոստով:

2. Տվյալների արտահոսքի պաշտպանության լուծման պահանջներ
2.1 Ընդհանուր պահանջներ

- MS SQL Server 2016 և ավելի նոր տարբերակների աջակցություն:
- Azure SQL տվյալների բազայի սերվերի աջակցություն:
- Windows 10 և ավելի նոր տարբերակների, macOS 12 և ավելի նոր տարբերակների աջակցություն:
- Windows Server 2016 և ավելի նոր տարբերակների աջակցություն:
- Ինտեգրացիա MS Active Directory-ի հետ:
- Ինտեգրացիա Microsoft 365-ի հետ՝ էլփոստի և ֆայլերի փոխանակման վերահսկման հնարավորությամբ ամպային համակարգում՝ նույնիսկ անապահով սարքերի միջոցով:
- Բովանդակության վավերացման համար OCR տեխնոլոգիա՝ բազմալեզու աջակցությամբ:
- Կառավարման վահանակի անհատականացման հնարավորություն՝ ադմինիստրատորի կարիքներից ելնելով:
- Հաշվետվություններին և կարգավորումներին հասանելիության իրավունքների սահմանման հնարավորություն՝ ադմինիստրատորների կառավարմամբ:
- Թաքնված ռեժիմ՝ գործընթացների և պանակների թաքցմամբ՝ նույնիսկ տեղական կամ դոմեյնի ադմինիստրատորների համար:
- Համակարգի չարաշահման պաշտպանության մեխանիզմներ՝
    - Պաշտպանությունն ակտիվ պետք է լինի բոլոր օգտագործողների, տեղական և դոմեյնի ադմինիստրատորների համար:

    - Բարձր իրավունքներով օգտվողների կողմից գործընթացների դադարեցման դեպքում համակարգը պետք է վերակենդանացնի դրանք կամ օգտագործի այլ մեթոդ:
    - Սարքի վրա համակարգի բաղադրիչների ջնջումը պետք է անհնար լինի՝ առանց հստակ թույլտվության:
    - Գրանցամատյանի, համակարգային բաղադրիչների և DLL գրադարանների խմբագրումը պետք է արգելված լինի:
    - Անթույլատրելի է պաշտպանական կարգավորումների չարտոնված փոփոխությունը:
- Պաշտպանության ապահովում՝ անվտանգ ռեժիմում:
- Ֆունկցիոնալության պահպանում օֆֆլայն ռեժիմում՝ առանց ընկերության ցանցին միացված լինելու:
- Արխիվացված գրառումների հետ աշխատանք:
- Ձեկույցների ուղարկում դեպի SIEM համակարգ:
- API ինտեգրում Power BI-ի և Tableau-ի հետ՝ վերլուծության համար:
- Բաղադրիչների և կարգավորումների պահուստային պատճենների ստեղծման հնարավորություն:
- Տվյալների բազայի կառավարիչի առկայություն՝ պահուստավորում, տարածքի դիտում, առաջադրանքների ստեղծում պահուստավորման համար:
- Արխիվների պլանային ստեղծում և կառավարիչ սերվերի միջոցով դիտելու հնարավորություն:
- Ինցիդենտների մասին ավտոմատ ծանուցումներ էլ.փոստով՝ զգայունության կարգավորման և մանրամասների հստակեցման հնարավորությամբ:
- Մոնիթորինգի վահանակում ադմինիստրատորի գործողությունների աուդիտ:
- Անոմալ ակտիվության հայտնաբերմամբ կանխարգելիչ պաշտպանություն:
- Գաղտնագրված արխիվների հայտնաբերում:
- Գրառումների ավտոմատ արխիվացում:
- Տվյալների փոխանցման սահմանափակումների ժամանակավոր հանման հնարավորություն՝ կենտրոնացված կառավարումով:
- Տեղեկատվության որոնման ֆիլտրերի փոխանակում:

- Զեկույցների ավտոմատ ուղարկում էլ.փոստով՝ ամբողջությամբ կարգավորվող ձևաչափով (տեղեկատվության ծավալ, հետևվող օգտագործողներ, ուղարկման հաճախականություն, ստացողներ):
- Վեբ վահանակի առկայություն՝ անվտանգության ինցիդենտների և աշխատակիցների գործունեության հետևման համար:
- Տպման վերահսկում՝ տեղական, ցանցային և վիրտուալ տպիչների համար:
- Տվյալ արտահոսքի պատճառն առաջացրած ֆայլի ներբեռնման հնարավորություն:
- Քաղաքականության խախտման ժամանակ ոչ միայն գրանցում, այլև ինցիդենտի ձևավորում՝ մեկնաբանելու հնարավորությամբ:
- Քաղաքականությունների կարգավորում՝ դինամիկ գործողություններով, որոնք արձագանքում են օգտագործողի վարքին:
- Օգտագործողի համար վեբ և ծրագրային հասանելիության կարգավորում ըստ կատեգորիաների:
- Գործակալների տեղադրում:

2.2 Անվտանգության աուդիտ
Ընդհանուր պահանջներ՝

- Ծրագրերի գործարկման և ակտիվ օգտագործման ժամանակի մանրամասն հաշվառում՝ կատեգորիաներով:
- Վեբ էջերում անցկացրած ժամանակի տեղեկատվություն՝ ներառյալ URL, պրոտոկոլ, հեդեր, անկախ բրաուզերից:
- Զեկույցների արտահանում CSV, PDF:
  IM ծրագրեր, վեբ փոստի հաճախորդներ՝
- Ուղարկված տվյալների հսկում՝ անկախ ծրագրից:
- Շաբաթական և ամսական ժամանակի օգտագործման ավտոմատ հաշվետվություններ:
  Էլփոստ՝
- POP3, IMAP, MAPI/Exchange, ներառյալ SSL:
- Outlook, Thunderbird, Icewarp և այլ հաճախորդներ՝ անկախ տեսակից:
- Exchange Online – օգտագործողի գործունեության վերահսկում՝ սարքից անկախ:

  Տվյալների հոսք՝

- Ձգայուն ֆայլերի հետ կատարված գործողությունների մանրամասն պատմություն:
- Տեղային ֆայլերի գործողություններ՝ պատճենում, տեղափոխում, ներբեռնում, ջնջում, սարքի տեսակ, աղբյուր և նպատակի ուղի:
- Որոնում օգտագործողի սարքերում պահված՝ մոռացված գաղտնի ֆայլերի:
- Տպագրված տվյալների գրանցում:
- Պանակի բովանդակության պատճենում, սքրինշոթ:
  Վերջակետի ակտիվություն՝
- Միացում/անջատում:
- Մուտք/ելք:
- Քնի ռեժիմի անցում:
  Ցանցային ակտիվություն՝
- Ներբեռնված/փոխանցված տվյալների ծավալ:

2.3 Տվյալների պաշտպանություն
Ընդհանուր պահանջներ՝

- Քաղաքականության խախտման դեպքում ինցիդենտների ավտոմատ ստեղծում:
- Ծրագրային ապահովումից անկախություն, ներառյալ կոդավորված կապերը:
- Ֆայլերի պաշտպանության շրջանցման մեթոդների նկատմամբ դիմադրողականություն:
- Ձգայուն տվյալների դասակարգում՝ ըստ ծրագրի, URL, սկավառակի ուղու կամ բովանդակության:
- Երրորդ կողմի դասակարգիչների օգտագործում:
- Ձգայուն ֆայլերի հայտնաբերում՝ ըստ բովանդակության, ծագման, ֆայլի տեսակի:
- Տեղային և ցանցային պանակների, սկավառակների և ամպային պահոցների հասանելիության աուդիտ:
- Ֆայլերի ստվերային պատճենների ստեղծման հնարավորություն:

Տվյալների գաղտնագրում՝

- Ամբողջ սկավառակի, ներառյալ համակարգայինի, գաղտնագրում:
- USB կրիչների գաղտնագրում:

Տվյալների արտահոսքի կանխարգելում՝

- Զգայուն տվյալների շարժի սահմանափակում՝ ըստ կրիչի, կայքի, էլփոստի հասցեների, ծրագրերի:
- Արգելել, տեղեկացնել, վերահսկել ռեժիմներ:
- Օգտագործողի ինտերնետ ռեսուրսների հասանելիության արգելում՝ ըստ URL, տիրույթի կամ կատեգորիայի:
- Ֆայլերի գործողությունների վերահսկում:
- Հստակ ֆայլի ընդլայնումներով արտահոսքի արգելք:
- Օգտագործողի վարքի վերլուծություն՝ ռիսկային վարքագծի բացահայտմամբ:

Սարքերի վերահսկում՝

- Համընդհանուր սահմանափակումներ՝ USB, Firewire, քարտերի ընթերցիչներ, LPT, COM, Bluetooth, CD/DVD/Blu-ray:
- Արտաքին սարքերի վերահսկում՝ թույլատրելի/արգելված խմբերի ստեղծմամբ:
- Կարդալու միայն ռեժիմի հնարավորությամբ:

---

3. Մասնակցի պահանջներ

3.1 Արտադրողի կողմից տրված լիազորագիր, որը հաստատում է մասնակցի և արտադրողի կամ նրա պաշտոնական ներկայացուցչի գործընկերային հարաբերությունները և լիազորում է մասնակցին ներկայացնել գին, վարել բանակցություններ և կնքել պայմանագիր:

3.2 Հաղթող մասնակիցը պետք է իրականացնի Համակարգի ամբողջական ներդրում եվ հիմնական կարգաբերում գնորդի հարթակում: