OPIS PREDMETU ZÁKAZKY

V prípade, opis predmetu zákazky odkazovať na konkrétneho výrobcu, výrobný postup, obchodné označenie, patent, typ, oblasť alebo miesto pôvodu alebo výroby, verejný obstarávateľ pripúšťa použitie ekvivalentu.

V prípade uvedenia konkrétnych značiek materiálov a výrobkov, pri ktorých sú uvedené minimálne požiadavky, môže uchádzač predložiť výrobky lepších parametrov. Dôkaz o ich vhodnosti musí byť priložený v ponuke.

TECHNICKÁ ŠPECIFIKÁCIA

Časť 1: Obstaranie a implementácia, nasadenie SW nástroja kybernetickej bezpečnosti. Prostredníctvom tohto nástroja bude možné riadiť a vyhodnocovať jednotlivé procesy a parametre v oblasti kybernetickej bezpečnosti (aktíva, hrozby a zraniteľnosti, rizika, úroveň súladu, dodávateľov a kybernetických bezpečnostných incidentov)

Cieľom verejného obstarávania je najmä naplnenie požiadaviek legislatívy na riešenie kybernetických bezpečnostných incidentov a opatrení pre oblasť monitorovania, testovania bezpečnosti a bezpečnostných auditov, a to najmä:

- zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov, vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

<u>Základná funkčnosť systému:</u>

- Organizácia kybernetickej bezpečnosti,
- Riadenie súladu s požiadavkami zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov,
- Riadenie aktív
- Riadenie hrozieb a zraniteľností
- Riadenie rizík
- Hodnotenie dodávateľov
- Hodnotenie implementácie organizačných a technických bezpečnostných opatrení

Spĺňa

Funkčné požiadavky systému:

- Centrálna konzola pre používateľov systému prístupná cez web prehliadače (Chrome, Firefox, Safari alebo Edge)
- Centrálna konzola lokalizovaná v Slovenskom jazyku,
- Podpora požiadaviek legislatívy SR,
- Centrálny Dashboard pre rýchle vyhodnotenie aktív (primárne a podporné), rizík podľa kategórie, rizík podľa hrozieb a zraniteľností, aktuálne dosahovaná úroveň súladu s požiadavkami zákona č. 69/2018 Z. z. a vyhlášky 362/2018 ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- Parametrizácia systému:
    - Definovanie metódy na výpočet hodnotenia aktív,
    - Definovanie metódy na kategorizáciu rizík,
    - Definovanie bezpečnostnej štruktúry spoločnosti (osoby, organizačné jednotky, role),
    - Definovanie druhov aktív,

    - Definovanie typov aktív,
    - Definovanie vlastných atribútov aktív,
    - Definovanie stupnice pre hodnotenie dôvernosti, dostupnosti, integrity, dopadov, hrozieb a zraniteľností,
    - Definovanie bezpečnostných opatrení
    - Register dodávateľov
    - Definovanie kritérií na hodnotenie dodávateľov
- Register rizík prostredníctvom ,ktorého je možné definovať kombinácie hrozba/zraniteľnosť na konkrétne typy aktív
- Evidencia aktív (manuálne alebo prostredníctvom importu z dátového súboru)
    - Všeobecné (druh, typ, lokalita, garant, administrátor, dodávateľ, prevádzkovateľ, závislosť aktíva na iných aktívach
    - Hodnotenie aktíva (dôvernosť, dostupnosť a integrita)
    - Identifikácia hrozieb/zraniteľnosti manuálne alebo priamo z registra rizík
    - Spôsob používania a manipulácie
    - Vlastné atribúty
- Mapa aktív pre grafické zobrazenie závislostí medzi jednotlivými aktívami
- Hodnotenie rizík
    - Možnosť stiahnuť súbor pdf s identifikovanými rizikami pre jedno alebo viaceré aktíva
    - Hodnotenie dopadu identifikovaných rizík
    - Návrh bezpečnostných opatrení pre zníženie rizika na úrovni aktíva
    - Výpočet rizika pred a po opatrení bezpečnostného opatrenia
    - Rozhodnutie o akceptovaní alebo neakceptovaní rizika
- Hodnotenie opatrení
    - Zoznam rizík, ktoré bezpečnostné opatrenie rieši
    - Aplikovateľnosť bezpečnostného opatrenia
    - Zavedenie bezpečnostného opatrenia
- Plán zvládania rizík pre riadenie implementácie bezpečnostných opatrení
    - Evidencia požiadaviek na ľudské a finančné zdroje
    - Dátum začatia a ukončenie implementácie
    - Diskusný priestor pre riešiteľský tím
- Hodnotenie dodávateľov
    - Hodnotenie atribútov dodávateľov aktív
    - Možnosť evidencie podpornej dokumentácie k dodávateľov (zmluvy, SLA,..)
- Hodnotenie plnenie požiadaviek legislatívy
    - Evidencia plnenie požiadaviek legislatívy
    - Jednotlivé požiadavky môžu byť v stave zavedené, v procese zavádzania, neaplikované alebo nezavedené
    - Ku každej požiadavke je možné pripojiť komentár a záznam zo zoznamu bezpečnostných opatrení
- Auditný log pre zaznamenávanie aktivít v systéme
    - Systém zaznamenáva aktivitu užívateľa (priradenie, zmena, vymazanie) pre konkrétne časti systému (aktívum, atribút aktíva, riziko, ..)
    - Možnosť prezrieť stav pred vykonanou zmenou a po zmene

Spĺňa

Spôsob prevádzkovania:
Riešenie bude inštalované v prostrední obstarávateľa.

Súčasťou dodávky sú:

- potrebné SW licencie pre naplnenie požiadaviek na obdobie 12 mesiacov,
- dodanie a inštalácia,
- jednorazové implementačné služby minimálne v nasledujúcom rozsahu:
- nastavenie a konfigurácia systému v IT prostredí verejného obstarávateľa (on premise),
- zaškolenie obsluhy a správy systému pre min. 2 zamestnancov verejného obstarávateľa, o vytvorenie a odovzdanie prevádzkovej dokumentácie systému, administrátorskej dokumentácie,

- post-implementačná podpora v rozsahu 8 človekodní po dobu 12 mesiacov

Spĺňa

Časť 2: Obstaranie, inštalácia a nasadenie DPL licencií pre 50 koncových staníc.

Predmetom realizácie zákazky bude dodanie v rozsahu:

Všeobecné požiadavky na DLP riešenie:

- ntegrácia s MS Active Directory,
- Podpora pre MS SQL 2012 alebo novšia verzia MS SQL,
- Podpora operačných systémov Windows 8.1, 10 a 11.
- Podpora operačného systému macOS 10.10 a novšieho.
- Podpora serverových operačných systémov Windows Server 2016, 2019 a 2022.
- Podpora terminálových prostredí,
- Centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni OU domény,
- Riadené používateľské práva do nastavení konzoly, k výsledným logom a administrácie riešenia,
- Skrytý režim na koncovej stanici vrátane procesov a zložiek, a to vrátane lokálnych aj doménovýchadministrátorov.
- Ochrana proti zastaveniu systému - musí byť aktívna u bežného používateľa, lokálneho i doménového administrátora.
- Ochrana proti zastaveniu procesov. V prípade vyšších používateľských práv dôjde k reštartuzastavených procesov či k použitiu iných spôsobov pre obnovu služby.
- Ochrana proti odinštalovaniu riešenia bez potrebnej autorizácie.
- Ochrana proti editácii registrov, systémových komponentov či DLL knižníc.
- Ochrana proti zmene nastavenia na koncovej stanici.
- Nutná možnosť ochrany i u operačného systému v režime "safe mode".
- Funkcionality zachované i v offline móde, (ak koncová stanica nie je pripojená k firemnej sieti/ internetu).
- Možnosť pracovať s historickými dátami.
- Riešenie musí podporovať možnosť poskytnúť zálohovanie vlastných komponentov, prevažne všetkých záznamov a nastavení.
- Automatické generovanie emailových varovaní v prípade incidentov, možnosť zmeniť citlivosť a špecifikáciu incidentu.
- Automatické generovanie emailových reportov s možnosťou úprav obsahu (množstvo informácií, množina uzlov, frekvencie odosielanie, príjemcovia).
- Zasielanie logov do SIEM riešenia objednávateľa.

Spĺňa

Dátový audit:

- Detailné informácie o aplikáciách, ako čas spustenia a ich aktívnom využití. Aplikácie sú rozdelené dokategórií pre prehľadnú správu.
- Detailné informácie o weboch, ako ich aktívne využitie, informáciách o URL, použitom protokole, hlavičky webu, a to bez ohľadu na použitý prehliadač. Weby sú rozdelené do kategórií pre prehľadnú správu.
- Detailné informácie o práci so súbormi, ako prehľad používateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové atď.).
- Lokálne súborové operácie – kopírovanie, presúvanie, sťahovanie z webu, FTP, mazanie, vytvorenie, otvorenie, a to vrátanie zdrojovej a cieľovej identifikácie: cesta, typ zariadenia, jedinečný identifikátor,
- Logovanie tlačových úloh a možnosť exportu reportov do XLS, PDF.

SpÍňa

Zaznamenávanie komunikácie:

- Podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania.
- Podpora desktopových emailových klientov (Microsoft Outlook, Mozilla Thunderbird,...) – riešenie jeschopné zaznamenávať emaily nezávisle od použitej aplikácie.
- Podpora zaznamenávania súborov odoslaných cez web mailových klientov.
- Podpora zaznamenávania súborov odoslaných cez IM komunikačné nástroje.

SpÍňa

Aktivita koncových staníc:

- Logovanie o stavoch zapnutie/vypnutie PC.
- Logovanie o prihlásení/odhlásení používateľa.
- Logovanie o uspaní/prebudení PC.
- Logovanie o pripojení akýchkoľvek periférií, logovanie všetkých portov na PC.

SpÍňa

Sieťová aktivia:

- Monitorovanie množstva odoslaných/stiahnutých dát

SpÍňa

Ochrana dát

Všeobecné
požiadavky

- Ochrana nezávisle na použitom SW, protokole, vrátane šifrovaných spojení.
- Riešenie podporuje zabezpečenie dát aj v prípade pokusu o porušenie ochrany, napr. Pomocousymbolických odkazov na zložku s dátami a pod.

SpÍňa

Šifrovanie

- Šifrovanie celých diskov vrátane systémových.
- Šifrovanie externých USB diskov.
- Prehľadná správa šifrovaných diskov, USB diskov / kľúčov.

SpÍňa

Správa zariadení

- Reštrikcie pre USB mass storage zariadenia, pripojenie mobilných telefónov, pamäťové karty, Bluetooth prenosy súborov, optické disky či FireWire.
- Možnosť vynútenia režimu Iba na čítanie u pripojených zariadení.
- Zaznamenávanie všetkých pripojených zariadení vrátane monitorov, myší a klávesníc.
- Schopnosť blokovať iba prenosy dát cez Bluetooth, ale povoliť pripojenie a voľné použitie ďalších Bluetooth zariadení (napr. slúchadiel).
- Klasifikované dáta je možné chrániť pred skopírovaním na chytré telefóny pripojené cez Multimedia Transfer Protocol, tieto zariadenia je možné ale inak neobmedzene používať s necitlivými dátami.
- Reštrikcie pre USB zariadenia sú podporované na systéme macOS

Spĺňa

Správa aplikácií

- Monitoring využitia aplikácií naprieč organizáciou a možnosť riadiť, ktoré aplikácie je možné a ktoré nemožno spúšťať.
- Monitoring navštevovania webových stránok naprieč organizáciou a možnosť riadiť, ktoré webové stránky je možné a ktoré nemožno navštevovať

Spĺňa

Ochrana údajov

- Definícia kategórií citlivých dát dovoľuje obmedzenie pohybu a práce s týmito dátami; určuje, ktoré médiá môžu byť použité pre prenos, ktoré siete môžu byť použité pre upload, na ktoré emailové adresy môžu byť dáta odoslané, ktoré aplikácie môžu s dátami pracovať.
- Možnosť úplnej blokácie používateľských akcií, používateľského schválenia operácie, informatívne notifikácie používateľa či obyčajného zaznamenania používateľských akcií
- Možnosť aplikácie politík pre konkrétne aplikácie – definícia zdroja a cieľa (prístup na externé zariadenie, sieť, tlač, virtuálnu tlač) a správa používateľských operácií (použitie schránky, snímanie obrazovky).
- Možnosť správy nepovolených cloudových úložísk.
- Možnosť správy či blokácie presúvania súborov do Git repozitárov.
- Funkcionalita „shadow copy" umožňujúca administrátorovi prezeranie súborov, ktoré boli súčasťou bezpečnostných incidentov. Funkcia musí sprístupniť súbory, ktoré používateľ odoslal, aj tie, ktoré DLP riešenie zablokovalo.
- Možnosť nastavenia počtu výskytov citlivých údajov. Dynamické reštrikcie nad súbormi a aplikáciami, pokiaľ je detegovaný citlivý obsah.
- Blokácia odoslania dát s citlivým obsahom mimo koncovú stanicu – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenie, IM komunikačné nástroje, synchronizácia s cloudovýmiaplikáciami.

Spĺňa

Ochrana citlivých údajov

- Detekcia citlivých dát v dokumentoch na platformách Windows a macOS.
- Možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov.
- Možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov.
- Možnosť importu vlastných slovníkov a kľúčových slov.
- Možnosť nastavenia počtu výskytov citlivých údajov.
- Možnosť klasifikácie citlivých dát podľa kontextových podmienok, napr. pôvod alebo umiestnenie dát.
- Možnosť klasifikácie kompatibilných typov súborov pomocou perzistentných súborových metadát.
- OCR vyhľadávanie citlivých dát v obrázkových formátoch a skenovaných PDF dokumentoch.
- OCR funkcionalita dostupná aj keď sa počítače odpoja od firemnej siete alebo prepnú do offline režimu.
- OCR podpora pre dvojjazyčné prostredie (napr. citlivé dokumenty v angličtine alebo v slovenčine).
- Dynamické reštrikcie nad súbormi a aplikáciami pri detekcii citlivého obsahu.
- Blokovanie odoslania dát s citlivým obsahom mimo koncovej stanice – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenia, IM komunikačné nástroje, synchronizácia s cloudovými aplikáciami.
- Detekcia dát obsahujúcich citlivý obsah, uložených na koncovej stanici alebo na zdieľanom sieťovom disku. Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.

- Reštrikcie pre USB zariadenia, pamäťové karty, Bluetooth zariadení, optické disky či FireWire.
- Možnosť vynútenia režimu iba na čítanie u pripojených zariadení.
- Zaznamenávanie všetkých pripojených vzdialení vrátane monitorov, myší a klávesníc.
  Centrálna správa aplikácií, prehľad jednotlivých verzií aplikácii

Spĺňa

OCR vyhľadávanie citlivých dát v obrázkových formátoch a skenovaných PDF dokumentoch.

- OCR funkcionalita dostupná aj keď sa počítače odpoja od firemnej siete alebo prepnú do offline režimu.
- OCR podpora pre dvojjazyčné prostredie (napr. citlivé dokumenty v angličtine alebo v slovenčine).
- Dynamické reštrikcie nad súbormi a aplikáciami pri detekcii citlivého obsahu.
- Blokovanie odoslania dát s citlivým obsahom mimo koncovej stanice – správa bežných komunikačných kanálov: e-mail, web upload, externé zariadenia, IM komunikačné nástroje, synchronizácia s cloudovými aplikáciami.
- Detekcia dát obsahujúcich citlivý obsah, uložených na koncovej stanici alebo na zdieľanom sieťovom disku. Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov.
- Reštrikcie pre USB zariadenia, pamäťové karty, Bluetooth zariadení, optické disky či FireWire.
- Možnosť vynútenia režimu iba na čítanie u pripojených zariadení.
- Zaznamenávanie všetkých pripojených vzdialení vrátane monitorov, myší a klávesníc.
- Centrálna správa aplikácií, prehľad jednotlivých verzií aplikácii.

Spĺňa

Integrácie s riešením tretích strán

- Integrácia a zobrazovanie záznamov a reportovanie údajov do riešenia Power BI. Podpora Power BI cezAPI.

Spĺňa

Zaznamenávanie Office 365 cloudu:

- Zaznamenávanie bežných používateľských akcií prevedených na Office 365 cloudu (OneDrive for Business, SharePoint Online) - základné súborové operácie ako sťahovanie a zdieľanie,
- Zaznamenávanie Office 365 emailové komunikácie (Exchange Online) pre všetkých používateľov vrátane
- používateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.
- Možnosť automatického vytvorenia DLP politík pre Office 365 e-mailovú komunikáciu (Exchange Online) pre všetkých používateľov, vrátane používateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.

Spĺňa

Dátová klasifikácia

- Možnosť integrácie s klasifikáciou tretích strán uložených v metadátach súborov – rozpoznanie takýchto dát a vynútenie nastaviteľných DLP politík.
- Možnosť integrácie s Azure Information Protection klasifikáciou, vrátane šifrovanej podoby AIP dokumentov.
- Používateľská klasifikácia a reklasifikácia Office dokumentov z používateľského rozhrania Windows Prieskumníka.

Spĺňa

Výrobca: Safetica
Model: Safetica ONE Enterprise + UEBA 1yr

Poprad, 4. 8. 2023

.....

Ing. Tomáš Habiňák
konateľ CORA GEO, s.r.o.

Je požadované, aby uchádzač uviedol ku každej jeden požiadavke pri:

- Základná funkčnosť systému
- Funkčné požiadavky systému
- Spôsob prevádzkovania
- Súčasťou dodávky sú

či požiadavky na predmet zákazky ***spĺňa*** alebo ***nespĺňa.***

Rovnako je potrebné, aby uchádzač pri požiadavke na Časť 2 Obstaranie, inštalácia a nasadenie DPL licencií pre 50 koncových staníc uviedol pri:

- Všeobecné požadavky na DLP riešenie DLP
- Dátový audit
- Zaznamenávanie komunikácie
- Aktivita koncových staníc:
- Sieťová aktivia:
- Šifrovanie
- Správa zariadení
- Správa aplikácií

Ochrana údajov

- Ochrana citlivých údajov
- OCR vyhľadávanie citlivých dát v obrázkových formátoch a skenovaných PDF dokumentoch
- Integrácie s riešením tretích strán
- Zaznamenávanie Office 365 cloudu:
- Dátová klasifikácia

či požiadavky na predmet zákazky ***spĺňa*** alebo ***nespĺňa*** **a uchádzač uvedie výrobcu/model.**

Pri Časti 2 je požadované, aby uchádzač uviedol výrobcu a model.