Príloha č. 1 – Opis predmetu zákazky

Predmetom zákazky je dodanie špecializovaných bezpečnostných nástrojov pre vybavenie SOC pracoviska verejného obstarávateľa v rozsahu uvedenom nižšie.
V prípade konkrétnych technických a výrobných označení materiálov a zariadení takto špecifikovaných v tejto výzve, môže hospodársky v zmysle § 42 ods. 3 zákona o verejnom obstarávaní predložiť ponuku i na technický a/alebo funkčný ekvivalent (ak nie je uvedené inak).

1. SOAR monitoring

Predmetom plnenia je dodanie systému pre orchestráciu a automatizáciu bezpečnostných procesov (SOAR) na zefektívnenie a urýchlenie manuálnych a časovo náročných procesov. Automatizácia pri identifikácii a reakcii na riziká.

Účel:
- Automatizácia opakovaných pracovných postupov pracoviska SOC.
- Orchestrácia rôznych bezpečnostných a nebezpečnostných nástrojov.
- Pokročilejšia, zrýchlená, efektívnejšia a automatizovaná reakcia na incidenty.
- Šetrenie času, financií a ľudských zdrojov.
- Posilnenie kybernetickej obrany organizácie.
- Obsahuje verejne dostupnú knižnicu s preddefinovanými workflows.
- Umožňuje zadefinovať vlastné workflows.
- Jednoduchá integrácia so SIEM riešením, manažmentom zraniteľnosti, ticketovacím nástrojom.
- Prehľadný reporting spustených workflows.

SOAR platforma kombinuje funkcie platforiem odozvy na bezpečnostné incidenty, platforiem pre orchestráciu bezpečnosti a automatizácie a platforiem pre spravodajstvo o hrozbách (Threat intelligence platform).
- musí poskytovať súhrnné metriky a upozornenia z externých informačných kanálov a integrovaných bezpečnostných nástrojov na centrálnom paneli. Analytici môžu korelovať údaje z rôznych zdrojov, filtrovať falošné poplachy, uprednostňovať upozornenia a identifikovať konkrétne hrozby, s ktorými sa stretávajú. Potom môžu analytici reagovať spustením príslušných príručiek
- musí automaticky doplniť incident o informácie z interných zdrojov informácií – minimálne z adresárového systému, asset manažment, správa privilegovaných prístupov.
- musí umožniť integráciu s internými aj externými zdrojmi bezpečnostných informácií, minimálne threat intelligence feeds, nástroje existujúcej Centrálneho bezpečnostného, logovacieho a vyhodnocovacieho nástroja, manažmenty používaných bezpečnostných nástrojov.
- musí byť schopné agregovať a konsolidovať výstupy z rôznych riešení tretích strán (vulnerability scannery, risk management nástroje a externé vstupy bezpečnostných informácií z rôznych zdrojov).

Súčasťou predmetu plnenia je aj poskytnutie inštalačných a konfiguračných prác, ako aj integrácia do existujúceho prostredia - SIEM riešenie verejného obstarávateľa (IBM Qradar).
Verejný obstarávateľ požaduje licenčné pokrytie a záruku v trvaní 36 mesiacov.
Počet licencií: pre 15 používateľov.
Licenčné pokrytie musí obsahovať minimálne 100 Resource Unit (virtuálnych serverov).

Súčasťou predmetu plnenia bude aj:
- technický návrh - high a low level design nasadenia do infraštruktúry NCZI,
- školenia administrátorov v elektronickej forme na inštalované technológie v rozsahu 2 MD na každú technológiu,
- školenia používateľov v elektronickej forme použiteľné aj ako praktický návod,

- dodanie používateľskej príručky, inštalačnej príručky a pokynov na inštaláciu (úvodnú/opakovanú),
- prevádzkový opis a pokyny pre servis, údržbu a diagnostiku,
- pokyny na obnovu pri výpadku alebo havárii (Havarijný plán)
- bezpečnostný projekt,

súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou Úradu podpredsedu vlády SR pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov.

Hospodársky subjekt uvedie v ponuke aj zoznam plánovaných technológií (vrátane použitého hardvéru), frameworkov a produktov dodávateľa/hospodárskeho subjektu, resp. tretích strán a tieto samostatne ocení v štruktúrovanom rozpočte tvoriacom jeho indikatívnu cenovú ponuku.

2. Data loss prevention – Štúdia uskutočniteľnosti

Predmetom plnenia je vypracovanie a dodanie štúdie uskutočniteľnosti v rozsahu uvedenom nižšie vrátane vypracovania a dodania podkladov pre manažérske rozhodnutie verejného obstarávateľa o realizovaní (vrátane spôsobu realizácie) Data loss prevention technológie slúžiacej na identifikáciu, monitorovanie a ochranu citlivých dát a informácií pred neautorizovaným používaním alebo odcudzením.

Štúdia uskutočniteľnosti musí byť komplexná, aby z odborného hľadiska:

- poskytla komplexnú analýzu súčasného stavu pripravenosti prostredia verejného obstarávateľa a aktuálnych predpisov
- explicitne uvádzala všetky prínosy implementácie (v porovnaní so súčasným stavom) aj s ich prípadnou kvantifikáciou (ak to je pre daný prínos relevantné), ako aj prípadné nevýhody oproti súčasnému stavu,
- uvádzala iba rámcovo zoznam všetkých činností s uvedením odhadu doby ich trvania a odhadu ich prácnosti a rolí, ktoré sú potrebné na vykonanie týchto činností a tiež odhady rozsahu a prácnosti všetkých súvisiacich aktivít vrátane školení vo forme návrhu rámcového harmonogramu kľúčových úloh budúceho projektu implementácie DLP riešenia spolu s kvalifikovaným odhadom finančných nákladov vykonania takejto náhrady v členení:
  - obstarávacie náklady,
  - náklady na zabezpečenie prevádzky na 1 kalendárny rok,
- identifikovala všetky riziká vyplývajúce z implementácie DLP riešenia a uviedla návrhy opatrení na ich elimináciu vrátane odhadov trvania, spotreby kapacít a nákladov na realizáciu týchto opatrení,
- stanovila technické a organizačné požiadavky na potenciálneho dodávateľa služby pri implementácii DLP riešenia,
- presne stanovila požiadavky na kvalifikačné predpoklady a rozsah personálnych zdrojov NCZI nevyhnutných na zabezpečenie súčinnosti pri implementácii DLP riešenia dodávateľským spôsobom a na budúce zabezpečenie prevádzky DLP systému.
- Stanovila návrh požiadaviek na riešenie (Use Cases) minimálne v tomto rozsahu:
  - Zabrániť úniku chránených alebo citlivých dokumentov z PC a notebookov NCZI pripojených do siete NCZI lokálne alebo prostredníctvom VPN:
    a) Zabrániť ich vytlačeniu neautorizovanou osobou.
    b) Zabrániť ich uloženiu na externé médiá (device control).
    c) Zamedziť ich odoslaniu prostredníctvom emailu neautorizovanou osobou.
    d) Zamedziť ich odoslaniu na nepovolené cloudové úložisko (napríklad Google Drive, Dropbox, Box, atď.).
    e) Zamedziť odfoteniu obrazovky s chránenými dokumentami (screenshot).
  - Zamedziť prístup neoprávneného užívateľa ku klasifikovaným dokumentom a manipulácii s nimi.
  - Navrhnúť nástroj na manuálnu klasifikáciu dokumentov s prihliadnutím na nástroje na klasifikáciu dostupné v NCZI.

Štúdia realizovateľnosti bude základným podkladom, z ktorého sa bude vychádzať pri vypracovávaní súťažných podkladov pre verejné obstarávanie na výber externého poskytovateľa služieb pri implementácii DLP riešenia.

Požiadavky na rozsah a štruktúru štúdie realizovateľnosti

1. Analýza a popis súčasného stavu:
   - 1.1 Analýza a popis platných predpisov zaoberajúcich sa bezpečnosťou a ochranou údajov nevyhnutných pre implementáciu DLP v prostredí NCZI.
   - 1.2 Analýza a popis procesov bezpečnosti a ochrany údajov nevyhnutých pre implementáciu DLP v prostredí NCZI.
   - 1.3 Analýza bezpečnostných požiadaviek na riešenie (Use Cases).
   - 1.4 Analýza funkčných požiadaviek na riešenie.
   - 1.5 Analýza, popis implementovateľných funkcii Microsoft a Azure information protection DLP riešenia v prostredí NCZI, v nadväznosti na už implementované riešenie.
   - 1.6 Analýza závislosti na iných projektoch.
   - 1.7 Analýza, popis implementovateľných funkcii DLP riešenia v prostredí NCZI.
   - 1.8 Podklady pre popis súčasného stavu pre potreby tejto štúdie poskytne NCZI formou konzultácií ako aj formou vyplnenia formulárov resp. dotazníkov pripravených tvorcom štúdie.
   - 1.9 Analýza rizík a obmedzení spojených s nasadením riešenia.
   - 1.10 Analýza dopadov na súvisiace systémy a procesy.
   - 1.11 Analýza ďalších požiadaviek súvisiacich s prípadmi použitia (use cases) DLP:
     - 1.11.1 Klasifikácia dokumentov
       a) Klasifikácia rôznych typov dokumentov nie len MS Office a Pdf ale aj napríklad videí, txt, obrázkov, atď.
       b) Návrh ako pristúpiť s pohľadu klasifikácie k zaheslovaným alebo zazipovaným dokumentom.
       c) Návrh automatickej klasifikácie starších neštruktúrovaných dokumentov na užívateľských PC a laptopoch.
       d) Navrhnúť nástroj a odporučiť postup pri zmene klasifikačného stupňa dokumentu.
       e) Návrh ako vynútiť klasifikáciu dokumentov prichádzajúcich zo zariadení mimo správy NCZI a z externého prostredia.
     - 1.11.2 Návrh zabránenia úniku chránených alebo citlivých dokumentov z mobilných zariadení pod správou NCZI rovnako ako pri PC a notebookoch NCZI.
     - 1.11.3 Návrh procesu a manažmentu udeľovania výnimiek a dočasných výnimiek (preposielanie dokumentov, ukladanie prostredníctvom USB a pre účely prezentácie).
     - 1.11.4 Behaviorálna analýza užívateľov.

2. Závery štúdie realizovateľnosti:
   - 2.1. Návrh požiadaviek na riešenie (Use Cases).
   - 2.2. Návrh a popis procesov a predpisov potrebných/nevyhnutých k implementácii DLP riešenia a tiež úprav, ktoré musia byť vykonané v existujúcich procesoch a predpisoch.
   - 2.3. Špecifikácia požiadaviek na DLP riešenie:
     - 2.3.1. špecifikáciu požiadaviek na potenciálneho externého dodávateľa služieb pri implementácii riešenia DLP,
     - 2.3.2. špecifikáciu technických, technologických, výkonnostných a integračných predpokladov pre zavedenie DLP v prostredí NCZI,
     - 2.3.3. technické a technologické predpoklady HW, SW a licencie,
     - 2.3.4. integračné predpoklady s existujúcimi technológiami v NCZI,
     - 2.3.5. výkonnostné predpoklady a to počty spracovávaných dokumentov, časové odozvy, veľkosť databázy atď.,
     - 2.3.6. špecifikáciu požiadaviek na pracovníkov potenciálneho externého dodávateľa služieb pri implementácii riešenia DLP,

Deleted: McAfee

2.3.7. špecifikáciu požiadaviek na rámcový plán projektu implementácie, ktorý má vypracovať potenciálny externý dodávateľ služieb pri implementácii riešenia DLP,

2.3.8. špecifikáciu požiadaviek na rámcový plán etapovitého nasadzovania v NCZI, ktorý má vypracovať potenciálny externý dodávateľ služieb pri implementácii riešenia DLP.

2.4. Návrh a vyhodnotenie rôznych alternatívnych riešení minimálne v troch úrovniach (low, middle, high). Tieto riešenia musia zohľadňovať mieru pokrytia našich požiadaviek a to funkčných, technických, organizačných, bezpečnostných, výkonnostných, prevádzkových a integračných ako aj náklady na implementáciu riešenia. Návrh riešenia musí obsahovať aj popis výhod a nevýhod jednotlivých alternatív.

Súčasťou predmetu plnenia je aj vytvorenie a dodanie podkladov pre manažérske zhrnutie objednávateľa o realizovaní a spôsobe realizácie DLP.

3. Data loss prevention

Predmetom plnenia je dodanie technológie na identifikáciu, monitorovanie a ochranu citlivých dát a informácií pred ich stratou či odcudzením.

Minimálne požiadavky:

- On-premise riešenie.
- Automatizácia identifikácie, klasifikácie a monitorovania citlivých údajov.
- Zaistenie dodržiavania súladu s regulačnými nariadeniami (GDPR, ZoKB a ich vykonávajúce vyhlášky).
- funkcionality zachované i v offline móde, (ak koncová stanica nie je pripojená k firemnej sieti/ internetu).
- Integrácia na SIEM riešenia verekného obstarávateľa (IBM Qradar) v rozsahu zasielania bezpečnostne relevantných udalostí.
- Zaznamenávanie užívateľských akcií prevedených na Office 365 cloudu (OneDrive for Business, SharePoint Online, MS Teams) - základné súborové operácie ako sťahovanie a zdieľanie.
- Monitorovanie a vyhodnocovanie Office 365 emailové komunikácie (Exchange Online) pre všetkých užívateľov vrátane užívateľov pracujúcich z Outlook Web App, osobných alebo mobilných zariadení.
- Podpora POP3, IMAP, MAPI / Exchange protokolov vrátanie SSL šifrovania, podpora desktopových emailových klientov (Microsoft Outlook, Mozilla Thunderbird,…).
- Riešenie je schopné monitorovať emaily nezávisle od použitej aplikácie, podpora zaznamenávania súborov odoslaných cez web mailových klientov.
- Detailné informácie o práci so súbormi, ako prehľad užívateľov a aplikácií pracujúcich so súbormi, súborové operácie (otvorenie, premenovanie, kopírovanie, mazanie) a informácie o cestách (systémové, externé, webové, cloudové).
- Možnosť úplne blokovať užívateľské akcie, informatívna notifikácia užívateľa či samotné logovanie užívateľských akcií, ochrana citlivých dát, možnosť definície citlivých dát pomocou preddefinovaných slovníkov a algoritmov. Možnosť definície citlivých dát pomocou vlastných reťazcov či regulárnych výrazov. Možnosť importu vlastných slovníkov. 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 (instant messaging) 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 alebo optické disky. Možnosť vynútenia režimu iba na čítanie u pripojených zariadení. Zaznamenávanie všetkých pripojených zariadení.

- Integrácia s MS Active Directory, Podpora pre MS SQL, Podpora operačných systémov Windows, Podpora serverových operačných systémov Windows Server 2008 R2, 2012 a 2016, podpora terminálových prostredí , centrálna administrátorská konzola, multitenantná administrácia v súlade s organizačným členením subjektov na úrovni OU domény, riadené užívateľské práva k nastaveniam konzoly, k výsledným logom a administrácie riešenia a to vrátane lokálnych i doménových administrátorov.
- Kontrola nad tlačou dokumentov, možnosť zablokovať tlač dokumentov s citlivými údajmi.

Súčasťou predmetu plnenia bude aj:
- technický návrh - high a low level design nasadenia do infraštruktúry NCZI,
- školenia administrátorov v elektronickej forme na inštalované technológie v rozsahu 2 MD na každú technológiu,
- školenia používateľov v elektronickej forme použiteľné aj ako praktický návod,
- dodanie používateľskej príručky, inštalačnej príručky a pokynov na inštaláciu (úvodnú/opakovanú),
- prevádzkový opis a pokyny pre servis, údržbu a diagnostiku,
- pokyny na obnovu pri výpadku alebo havárii (Havarijný plán)
- bezpečnostný projekt,
- súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou Úradu podpredsedu vlády SR pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov.

Hospodársky subjekt uvedie v ponuke aj zoznam plánovaných technológií (vrátane použitého hardvéru), frameworkov a produktov dodávateľa/hospodárskeho subjektu, resp. tretích strán a tieto samostatne ocení v štruktúrovanom rozpočte tvoriacom jeho indikatívnu cenovú ponuku.

4. MDM

Predmetom plnenia je dodanie nástroja umožňujúceho správu a monitorovanie mobilných zariadení, ako sú mobilné telefóny a tablety, ktoré sú používané zamestnancami v pracovnom prostredí.

Minimálne požiadavky:
- Zabezpečenie Dát: Zaistiť bezpečnosť firemných dát uložených na mobilných zariadeniach a zabrániť neoprávnenému prístupu alebo úniku citlivých informácií.
- Centralizovaná Správa: Vytvoriť centralizovaný systém pre správu všetkých mobilných zariadení a aplikácií, vrátane možnosti vzdialeného nastavenia a aktualizácií.
- Podpora BYOD: (Bring Your Own Device) - umožniť zamestnancom používať vlastné zariadenia v pracovnom prostredí, pričom zároveň zabezpečí oddelenie pracovných a osobných dát.
- Podpora COPE (corporate-owned, personally enabled) - možnosť zamestnancov používať mobilné zariadenie vo vlastníctve zamestnávateľa na pracovné aj súkromné účely.
- Súlad a Reporting: Vynucovanie nastavených pravidiel a politík spoločnosti a generovanie správ o stave zariadení a aplikácií.
- Registrácia a konfigurácia zariadenia.
- Správa aplikácií a ich distribúcia.
- Riadenie prístupu a práv užívateľov.
- Monitorovanie a logovanie aktivít.
- Vzdialená správa a blokovanie zariadenia v prípade straty alebo krádeže.
- Kompatibilita s rôznymi mobilnými operačnými systémami (iOS, Android, Windows).
- Silné zabezpečenie dát a možnosť vzdialeného vymazania.
- Intuitívne užívateľské rozhranie pre administrátorov.
- **Licencie pre 600 koncových zariadení.**
- Integrácia na SIEM riešenia objednávateľa (IBM Qradar) v rozsahu zasielania bezpečnostne relevantných udalostí.

Súčasťou predmetu plnenia bude aj:

Deleted: 400 zariadení s možnosťou škálovateľnosti až do ...

- technický návrh - high a low level design nasadenia do infraštruktúry NCZI,
- školenia administrátorov v elektronickej forme na inštalované technológie v rozsahu 2 MD na každú technológiu,
- školenia používateľov v elektronickej forme použiteľné aj ako praktický návod,
- dodanie používateľskej príručky, inštalačnej príručky a pokynov na inštaláciu (úvodnú/opakovanú),
- prevádzkový opis a pokyny pre servis, údržbu a diagnostiku,
- pokyny na obnovu pri výpadku alebo havárii (Havarijný plán)
- bezpečnostný projekt,
- súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou Úradu podpredsedu vlády SR pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov.

Hospodársky subjekt uvedie v ponuke aj zoznam plánovaných technológií (vrátane použitého hardvéru), frameworkov a produktov dodávateľa/hospodárskeho subjektu, resp. tretích strán a tieto samostatne ocení v štruktúrovanom rozpočte tvoriacom jeho indikatívnu cenovú ponuku.

5. EDR - Endpoint Detection and Response

Predmetom plnenia je dodanie a implementácia pokročilého riešenia Endpoint Detection and Response (EDR) pre našu spoločnosť. Cieľom je zabezpečiť bezpečnosť a ochranu všetkých koncových zariadení a serverov, ktoré používajú naši zamestnanci, s dôrazom na detekciu, monitorovanie a rýchlu reakciu na kybernetické hrozby.

Minimálne požiadavky:

- Detekcia a prevencia hrozieb: Riešenie musí byť schopné identifikovať a zabrániť rôznym typom kybernetických hrozieb, vrátane malvéru, ransomvéru a iných škodlivých aktivít. Riešenie musí podporovať tzv. samoučiaci režim (machine learning), zero-day ochranu pred neznámymi hrozbami, anti-ramsoware ochranu (aktívne blokovanie neoprávneného šifrovania) a tiež skenovanie všetkých bežných súborov vrátane súborov typu obrázok.
- Monitorovanie a správa: Zákazník musí mať možnosť monitorovať všetky koncové zariadenia v reálnom čase a sledovať ich bezpečnostný stav. Riešenie musí ponúkať centralizovanú správu, vytváranie správ pre bezpečnostných administrátorov, umožňovať real-time správu klientov (serverov) a možnosti špecifických politík pre jednotlivé skupiny administrátorov.
- Rýchla reakcia na incidenty: EDR riešenie musí umožňovať rýchlu reakciu na detegované hrozby, vrátane izolácie postihnutých zariadení, odstránenia hrozieb a obnovy postihnutých systémov. Riešenie musí podporovať schopnosť threathuntingu (vrátane automatizovaného threathuntingu) s funkciou vizualizácie, pričom požadovaná data retention je minimálne 30 dní. Riešenie musí mať schopnosť analyzovať správanie sa administrátora servera a v prípade jeho neštandardného správania odmietnuť overenie.
- Kompatibilita a integrácia: Riešenie by malo byť kompatibilné s existujúcimi bezpečnostnými infraštruktúrami a mala by byť možnosť jeho integrovať s ďalšími bezpečnostnými nástrojmi, ako sú firewally, SIEM systémy atď.
- Výkonnosť a škálovateľnosť: EDR riešenie musí byť dostatočne výkonné a škálovateľné, aby dokázalo spravovať a chrániť veľký počet koncových zariadení bez degradácie výkonu.
- **Licencie pre 1500 koncových zariadení,**
- Aktualizácie a podpora: Dodávateľ musí poskytovať pravidelné aktualizácie bezpečnostných záplat a signatúr, tak ako aj technickú podporu v prípade problémov. Okrem licencie operačného systému musí riešenie obsahovať všetky licencie potrebné pre plnú funkcionalitu všetkých častí riešenia s platnosťou minimálne 12 mesiacov.
- Dátová ochrana a súlad s reguláciami: Riešenie musí spĺňať všetky relevantné normy a regulácie v oblasti kybernetickej bezpečnosti a ochrany dát.

Deleted: 1000

Deleted: s možnosťou škálovateľnosti až do 2000 používateľov

Súčasťou predmetu plnenia bude aj:

- technický návrh - high a low level design nasadenia do infraštruktúry NCZI,
- školenia administrátorov v elektronickej forme na inštalované technológie v rozsahu 2 MD na každú technológiu,

- školenia používateľov v elektronickej forme použiteľné aj ako praktický návod,
- dodanie používateľskej príručky, inštalačnej príručky a pokynov na inštaláciu (úvodnú/opakovanú),
- prevádzkový opis a pokyny pre servis, údržbu a diagnostiku,
- pokyny na obnovu pri výpadku alebo havárii (Havarijný plán)
- bezpečnostný projekt,
- súčinnosť s vytváraním dokumentov a aktivít vyžadovaných vyhláškou Úradu podpredsedu vlády SR pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov.

Hospodársky subjekt uvedie v ponuke aj zoznam plánovaných technológií (vrátane použitého hardvéru), frameworkov a produktov dodávateľa/hospodárskeho subjektu, resp. tretích strán a tieto samostatne ocení v štruktúrovanom rozpočte tvoriacom jeho indikatívnu cenovú ponuku.