**Príloha č. 1 –** Opis predmetu zákazky, tejto Výzvy

**Predmetom zákazky je v 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 o zmene a doplnení niektorých zákonov a vyhlášky NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení predĺžením platnosti licencií na služby centrálneho nástroja pre zaznamenávanie činnosti sietí a informačných systémov s podporu riešenia kybernetických bezpečnostných incidentov - Rapid7 Insight IDR Ultimate a upgrade súčasného riešenia o službu automatického spúšťania testovania zraniteľností zariadení Rapid7 Insight VM**

**Opis predmetu zákazky**

**Úvod**:

Predmetom zákazky je „**Predĺženie platnosti licencií na služby centrálneho nástroja pre zaznamenávanie činnosti sietí a informačných systémov s podporou riešenia kybernetických bezpečnostných incidentov - Rapid7 Insight IDR Ultimate a upgrade súčasného riešenia o automatické spúšťanie testovania zraniteľností zariadení Rapid7 Insight VM s post-implementačnou podporou“ (ďalej ako Rapid7)** ktorého cieľom je ochrana počítačovej siete, koncových zariadení, informačných aktív, zaznamenávanie činnosti sietí a informačných systémov a naplnenie požiadaviek legislatívy na riešenie kybernetických bezpečnostných incidentov a opatrení pre oblasť ochrany, monitorovania, testovania bezpečnosti, riešenia a analýzy incidentov 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.

Poskytovateľ poskytne:

**Dodanie licencií, implementáciu a upgrade komplexného nástroja pre Rapid7 s požadovanými funkciami a službami komplexného nástroja Rapid7, pre zaistenie spoľahlivej, kontinuálnej a bezpečnej prevádzky v súlade s dokumentáciou systému a aktuálnymi požiadavkami Objednávateľa, vrátane post-implementačnej podpory**

**Poskytnuté služby:**

1. Predĺženie licencií **Rapid7 Insight IDR Ultimate** o 24 mesiacov pre 600 zariadení:

|  |  |  |  |
| --- | --- | --- | --- |
| Počet lokalít | Počet kolektorov | Počet NTA zariadení | Počet orchestrátorov zariadení |
| 5 | 2 | 5 | 2 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Lokalita | Počet AD užívateľov | Počet AD administrátorov | Počet AD servisných účtov | Počet serverov (virtualizačné + virtuálne) a počet fyzických serverov | Počet sieťových zariadení | Počet pracovných staníc | Počet iných zariadení pripojených do siete (tlačiarne, skenery, dochádzkový terminál a pod.) |
| OL | 900 | 3 | 40 | 60 | 60 | 230 | 50 |
| TR |  |  |  | 4 | 75 | 160 | 60 |
| PE |  |  |  | 2 | 20 | 50 | 15 |
| HR |  |  |  | 2 | 15 | 30 | 15 |
| KR |  |  |  | 2 | 30 | 60 | 30 |

1. Upgrade licenčného modelu o nový systém **Rapid7 Insight VM** na 24 mesiacov pre 600 zariadení:

Riešenie po upgrade licenčného modelu o nový systém Rapid7 Insight VM musí spĺňa minimálne nasledujúce rozšírené funkcionality:

* vykonáva automatizované testovanie zraniteľnosti zariadení, umožňuje testovanie dynamicky prideľovaných IP adries prostredníctvom služby ako je DHCP a monitorovanie ich histórie a podávanie správ pomocou "DNS name" alebo "Host name",
* konzola pre centrálnu správu ako aj skener podporujú inštaláciu na operačné systémy Windows, Windows Server, alebo Linux,
* podporuje hybridné formy nasadenia ako fyzické, virtualizované a cloud prostredie, umožňuje automatickú aktualizáciu tagov v databáze aktív podľa týchto pravidiel dynamického označovania,
* plne automatizované inštalácie aktualizácii všetkých SW komponentov celej architektúry riešenia s najnovšími dostupnými verziami jednotlivých SW komponentov počas celého obdobia predplatného,
* automatizovaná centralizácia všetkých nájdených aktívnych systémov a ich atribútov: verzií operačného systému, verzií aplikácií, otvorených portov TCP a UDP a sieťových protokolov do jednej databázy aktív s možnosťou definovať statické a dynamické hierarchické tagy a podľa týchto tagov vykonávať filtrovanie aktív, testovanie a vykazovanie výsledkov,
* automatické zisťovanie aktív, pričom sa zohľadnia minimálne tieto parametre adresy IP, adresy MAC a názvu hostiteľa, aby sa zabránilo duplicite. Riešenie podporuje centrálnu správu v geograficky rozptýlenom nasadení skenerov, podporuje možnosť skenovania aktív bez agentským spôsobom, podporuje prístup založený na rolách s preddefinovanými aj vlastnými rolami,
* možnosť skenovania pracovných staníc a notebookov umiestnených mimo sieť LAN prostredníctvom agentskej aplikácie aj bez nutnosti VPN pripojenia,
* automatizácia pracovných postupov, ako je plánovanie skenovania, upozornenia na udalosti a zraniteľnosti skenovania a generovanie a distribúcia správ, upozornenia na udalosti zlyhania testovania zraniteľností,
* podpora neinvazívne aj invazívnej kontroly,
* možnosť určiť rušenie akéhokoľvek skenovania úpravou výkonu skenovania a vykonávaných kontrol,
* administrátorské poverenia možno použiť na hĺbkové autentifikované skenovanie, ktoré kontroluje aktíva na širší rozsah zraniteľností alebo porušení bezpečnostných politík,
* označovanie nebezpečných kontrol a umožňuje používateľom vypnúť ich na základe jednotlivých skenov, podporuje skenovanie s aj bez autentizácie,
* podpora dynamických dashboardov pre potrebu práce so živými dátami,
* skenovanie cez IPv4 dokáže zistiť systémy s podporou IPv6 a naopak, poskytuje pokrytie zraniteľností z NVD, CERT, SANS, Bugtraq a Secunia, automaticky koreluje a konsoliduje jednotlivé zraniteľnosti plánu prostredníctvom nápravného opatrenia,
* vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti,
* automatické zisťovanie a inventarizáciu majetku (pomocou IP adresy, MAC adresy),
* pokrytie a upozornenie na zraniteľnosti v aplikáciách, ktoré poskytujú prístup k back-end systémom,
* poskytuje pokrytie zraniteľností v iných ako webových aplikáciách, podporuje vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti,
* hodnotenie rizík zahŕňa hodnotenie CVSS, CVSSv2, CVSSv3, CVSSv3.1 možnosť zneužitia aktív a náchylnosť k súborom škodlivého softvéru,
* vytváranie vlastných politík určených pre skenovanie,
* hodnotenie kritickosti aktív definované používateľom, ktoré sa musí zohľadniť v hodnotení rizík,
* podpora vlastných modelov hodnotenia rizík definované používateľom,
* podpora inbound a outbound API,
* funkcionalita stanovenia cieľov nápravných opatrení podľa kritérií ako sú: stanovený termín ukončenia realizácie nápravných opatrení, odstránenie zraniteľností podľa závažností, odstránenie konkrétnych zraniteľností, odstránenie aktív s nepodporovaným operačným systémov (formáty správ by mali zahŕňať HTML, PDF, CSV, XML a export pomocou SQL query).

**Konfiguračné práce:**

* inštalácia a upgrade riešenia na už existujúcu SW/HW infraštruktúru objednávateľskej organizácie,
* konfiguráciu riešenia,
* školenie minimálne 2 správcov objednávateľskej organizácie v rozsahu 8 hodín.

**Licencovanie Rapid7:**

**Potrebné softvérové licencie Rapid7 Insight IDR Ultimate a Rapid7 Insight VM sa dodávajú na obdobie 24 mesiacov**

**Implementácia komplexného Rapid7 nástroja v rozsahu:**

* + - nastavenie a konfigurácia prostredí verejného obstarávateľa,
			* konfigurácia Windows systémov
			* overenie funkčných a výkonových parametrov Windows agentov,
			* konfigurácia Linux systémov
			* overenie funkčných a výkonových parametrov Linux agentov,
			* predvedenie vytvorenia a uloženia vlastného dashboardu a reportu,
			* konfigurácia cloudovej služby
		- nastavenie pravidelného zasielania definovaných reportov vybraným zamestnancom verejného obstarávateľa,
		- zaškolenie obsluhy a správy systému pre minimálne 2 zamestnancov verejného obstarávateľa,
		- vytvorenie a odovzdanie prevádzkovej dokumentácie systému, administrátorskej dokumentácie,
1. Post-implementačná podpora v rozsahu

**10 človekodeň na obdobie 24 kalendárnych mesiacov**, ktorá obsahuje:

* Technická  podpora prostredia
	+ inštalácia a konfigurácia
	+ konfigurácia systémových nastavení
	+ konfigurácia komponentov (kolektorov, NTA zariadení, orchestrátorov)
	+ konfigurácia a tvorba alertov
	+ konfigurácia a tvorba queries
	+ konfigurácia a tvorba dashboard
	+ konfigurácia event sources a custom parser (data management)
	+ podpora pri riešení technických problémov s platformou
* Konzultačná podpora pri identifikovaných bezpečnostných incidentoch
* Podpora ďalšieho rozvoja riešenia
	+ zdroje udalostí,
	+ integrácie
	+ využitie funkcionalít systému,
	+ licenčný model
* Komunikácia s výrobcom
	+ hlásenie technických problémov výrobcovi,  dotazy na obchodnú podporu

**Postup pri riešení Problémov/požiadaviek – Helpdesk:**

Na hlásenie problémov zo strany Objednávateľa bude Poskytovateľ prevádzkovať Helpdesk, ktorý bude poskytovať službu, ktorá pozostáva z nasledujúcich činností:

* Identifikácia Problému – poskytnutie pomoci Objednávateľovi s cieľom identifikovať príčinu daného Problému v rozsahu podporovaného systému Objednávateľa,
* Poskytovanie informácií o stave riešenia požiadaviek prostredníctvom on-line vzdialeného prístupu oprávnených osôb Objednávateľa do Helpdesku.

**Postup**

1. Oprávnená osoba Objednávateľa zadáva/hlási problém/požiadavku v systéme Helpdesk na adrese: XXXXXX, v prípade nedostupnosti e-mailom na xxx Oprávnená osoba Objednávateľa nahlasuje problém podľa predchádzajúcej vety Poskytovateľovi až potom, ako nebolo možné vyriešiť tento problém v prvom stupni Oprávnenou osobou Objednávateľa.

Uskutočniť takéto hlásenie môže výlučne Oprávnená osoba Objednávateľa. Každé hlásenie Problému prijaté akýmkoľvek spôsobom sa zaeviduje v Helpdesku. Helpdesk vygeneruje identifikačné číslo požiadavky/problému. Helpdesk eviduje minimálne: čas odoslania hlásenia a oprávnenú osobu, kritickosť , čas prijatia hlásenia oprávnenou osobou Poskytovateľa, čas pridelenia riešiteľovi, čas zahájenia riešenia a čas vyriešenia požiadavky alebo Problému. Akákoľvek budúca komunikácia medzi Poskytovateľom a Objednávateľom sa uskutočňuje použitím priradeného identifikačného čísla požiadavky/Problému. Všetky záznamy, prílohy a komunikácia Oprávnených osôb Poskytovateľa a Objednávateľa sú evidované najmä v Helpdesku dostupnom on-line.

1. Špecialista Poskytovateľa preverí požiadavku/Problém a začne ich prešetrenie. Podľa potreby kontaktuje Oprávnenú osobu Objednávateľa. Komunikácia pracovníka Poskytovateľa prebieha priamo s Oprávnenou osobou Objednávateľa. Špecialista Poskytovateľa oznámi výsledok prešetrenia a odporúčané riešenie Oprávnenej osobe Objednávateľa. Na základe výsledkov prešetrenia bude pokračovať riešenie Problému.
2. Problém bude riešený na základe priority určenej dohodou a definíciou kategórie požiadavky/Problému Oprávnenými osobami Objednávateľa a Poskytovateľa. Oprávnená osoba Objednávateľa má právo zmeniť poradie priorít riešenia otvorených Problémov/požiadaviek po dohode s oprávneným zástupcom zo strany Poskytovateľa dokumentovateľným spôsobom – záznamom v Helpdesku.
3. Oprávnená osoba Objednávateľa po vykonaní služieb pracovníkom Poskytovateľa v priestoroch Objednávateľa alebo na diaľku vzdialeným pripojením, potvrdí poskytnutie služby a funkčnosť riešenia v Helpdesku.
4. Všetky vyriešené požiadavky /Problémy Objednávateľa musia byť potvrdené a ich vyriešenie musí byť zaevidované v Helpdesku. Splnenie požiadavky/Problému bude potvrdené v rozsahu ich riešenia Oprávnenou osobou Objednávateľa. Objednávateľ je povinný potvrdiť vyriešenie každej požiadavky/Problému najneskôr do 5 pracovných dní odo dňa jej vyriešenia. Akceptovanie riešenia požiadavky/Problému bude zaevidované priamo v Helpdesku. V prípade, ak Objednávateľ riešenie požiadavky/Problému neakceptuje, v rovnakej lehote svoje pripomienky a výhrady uvedie v Helpdesku. Ak Objednávateľ bez závažného dôvodu neakceptuje vyriešenie požiadavky/Problému a ani nevznesie pripomienky k riešeniu požiadavky/Problému ani do 5 pracovných dní od ich vykonania, považuje sa riešenie požiadavky/Problému za akceptované a Helpdesk automaticky vykoná mailovú notifikáciu.

Reakčná doba Poskytovateľa na problém Objednávateľa sa určuje na základe príslušnej úrovne spracovania Problémov. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do Helpdesku alebo v prípade nedostupnosti Helpdesku od momentu nahlásenia Problému alternatívnym spôsobom, t. j. od momentu doručenia hlásenia Problému emailom.

**Služby post-implementačnej podpory dodaného komplexného nástroja softvéru**

|  |  |  |
| --- | --- | --- |
| **Popis** | **Parameter** | **Poznámka** |
| Prevádzkové hodiny | 9 hodín | 08:00 – 17:00 hod, počas pracovných dní |

###

**Mimoriadna pohotovosť**

V prípade potreby, na základe žiadosti Objednávateľa, Poskytovateľ zabezpečí mimoriadnu pohotovosť a mimoriadne výkony nespadajúce do bežnej pracovnej doby. Objednávateľ je povinný takéto mimoriadne akcie nahlásiť Poskytovateľovi v predstihu minimálne desať (10) pracovných dní vopred.

|  |  |
| --- | --- |
| **Popis** | **Poznámka** |
| Pohotovosť – nočná | Od 17:00 – 8:00 hod počas pracovných dní |
| Pohotovosť – 24 hod. | 00:00 – 24:00 hod počas pracovných dní |
| 00:00 – 24:00 hod počas pracovných dní počas sviatkov a dní pracovného pokoja |

**Úroveň spracovania požiadaviek/Problémov**

Prevádzkové hodiny Poskytovateľa pre Služby podpory prevádzky a údržby ,Služby podpory aplikačného programového vybavenia a systémového softvéru sú počas pracovných dní od 08:00 do 17:00 hod.

Čas mimo prevádzkové hodiny Poskytovateľa podľa predchádzajúcej vety sa do Reakčnej doby nezapočítava.

Reakčná doba Poskytovateľa na Problém sa určuje na základe príslušnej úrovne Problému. Poskytovateľ poskytuje Služby podpory prevádzky a Služby podpory aplikačného programového vybavenia a systémového softvéru podľa tabuľky uvedenej nižšie. Čas sa vždy meria od momentu, kedy je Problém zaznamenaný do Helpdesku.

|  |  |
| --- | --- |
| **Typ požiadavky** | **Reakčná doba v prevádzkových hodinách**  |
| Kategória A - Kritický problém Kritické poruchy alebo vady spôsobujúce nefunkčnosť komplexného nástroja | do 8 hod. |
| Kategória B - Nekritický problém | do 24 hod. |
| Kategória C – Modifikácia komplexného nástoja, iné požiadavky | do 48 hod. |