Číslo zmluvy Dodávateľa:
Číslo zmluvy Kupujúceho: 2398/2023

KÚPNA ZMLUVA
NA DODANIE SOFTVEROV A ZMLUVA O POSKYTNUTÍ SLUŹIEB

uzatvorená podľa § 409 a nasl. a podľa 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov (ďalej len „Obchodný zákonník“) a v zmysle zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“) medzi zmluvnými stranami: (ďalej len „zmluva“)

Dodávateľ

Obchodné meno:	WDS Solutions s. r. o.
Sídlo:	Mateja Bela 2494/4 911 08 Trenčín
V zastúpení:	Ing. Lukáš Bumbál, Konateľ spoločnosti
Bankové spojenie:	Tatra banka, a.s.
IBAN:	
IČO:	46450424
DIČ:	2023387960
IČ DPH:	SK2023387960
Zápis/Právna forma:	Obchodný register Okresného súdu Trenčín, oddiel: Sro, vložka č. 25419/R

Kontaktná osoba: Ing. Lukáš Bumbál, Konateľ spoločnosti
Tel. číslo:
E-mail:

(ďalej ako „Dodávateľ“ alebo ako „Úspešný záujemca“)

a

Kupujúci

Názov:	**Slovenská správa ciest**
Sídlo:	Dúbravská cesta 1152/3, 841 04 Bratislava
Štatutárny orgán:	Mgr. Norbert Polievka, MA., generálny riaditeľ
IČO:	00 00 33 28
DIČ:	2021067785
Bankové spojenie:	Štátna pokladnica
IBAN:	
Právna forma:	Rozpočtová organizácia zriadená Ministerstvom dopravy, pôšt a telekomunikácií SR, zriaďovacou listinou číslo 5854/M-1995 zo dňa 7.12.1995, v znení neskorších zmien a doplnení

Kontaktná osoba:
Tel. číslo:
E-mail:

Právna forma: (ďalej ako „Kupujúci“ alebo ako „Obstarávateľ“)
(Dodávateľ spolu s Kupujúcim ďalej len „zmluvné strany“, alebo individuálne len „Účastníci zmluvy“)

za vzájomne nasledovne dohodnutých podmienok.

Čl. I.
Predmet zmluvy

1. Predmetom tejto zmluvy sú záväzky zmluvných strán súvisiace s dodaním softvérov a poskytnutím služieb pre zvýšenie kybernetickej bezpečnosti informačných technológii v správe a v užívaní Kupujúceho v zmysle „Požiadavky na obstarávanie“ (ďalej len „Požiadavka SSC“) a to:
   a) záväzok Dodávateľa za podmienok podľa tejto zmluvy dodať Kupujúcemu
      i. softvér pokročilej ochrany koncových bodov vrátane ochrany virtualizačnej platformy a EDR,
      ii. softvér k systému na monitorovanie a analytiky sieťovej komunikácie,
      iii. softvér nástroja na automatické spúšťanie skenovania zraniteľnosti a získavania údajov

      (ďalej len „Tovar“),
   b) záväzok Dodávateľa previesť na Kupujúceho vlastnícke právo k dodanému Tovaru,
   c) záväzok Dodávateľa poskytnúť Kupujúcemu služby súvisiace s dodaným Tovarom, ktorými sú
      i. konfigurovanie Tovaru (softvérov) v informačných technológiách Kupujúceho,
      ii. dopravné služby na dodanie Tovaru a na poskytnutie služieb

      (ďalej len „Služby“),
   d) záväzok Dodávateľa zrealizovať svoje záväzky vyplývajúce z tejto zmluvy výlučne len osobou/bami označenou/nými v Požiadavke SSC ako expert č. 1 - projektový manažér a expert č. 2 – expert pre oblasť kybernetickej bezpečnosti, ktoré musia spĺňať požadovanú odbornú spôsobilosť,
   e) záväzok Dodávateľa pred dodaním Tovaru zabezpečiť pre Kupujúceho udelenie licencie/cií k oprávnenému používaniu Tovaru,
   f) záväzok Kupujúceho Predmet plnenia uvedený v článku II. tejto zmluvy prevziať a za Predmet plnenia uhradiť Dodávateľovi kúpnu cenu podľa čl. III. tejto zmluvy.
2. Predmetom tejto zmluvy je aj úprava vzájomných práv a povinností zmluvných strán vyplývajúcich z tejto zmluvy a z Požiadavky SSC.

Čl. II.
Predmet plnenia a účel plnenia

1. Predmetom plnenia:
   a) je Tovar spolu s akýmkoľvek hmotným/nehmotným príslušenstvom k Tovaru, ktoré spolu tvoria funkčný celok v zmysle Požiadavky SSC,
   b) sú Služby spojené s dodaním, inštaláciou a konfigurovaním (implementačné služby) Tovaru vo vzťahu k informačným technológiám Kupujúceho v zmysle Požiadavky SSC, (Tovar spolu so Službami ďalej len „Predmet plnenia“).

   Rozsah a špecifikácia Predmetu plnenia sú uvedené v Prílohe č. 1, ktorá je neoddeliteľnou súčasťou tejto zmluvy.
2. Účelom plnenia je zvýšenie kybernetickej bezpečnosti a zabezpečenie ochrany údajov, s ktorými Kupujúci disponuje, ako aj zabezpečenie nepretržitej prevádzky informačných systémov verejnej správy prostredníctvom monitorovania, skenovania a ochrany koncových bodov v rozsahu a v kvalite v zmysle Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov v spojení s Vyhláškou č. 364/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Čl. III.
Kúpna cena a platobné podmienky

1. Kúpna cena a súvisiace služby sú stanovené v zmysle zákona č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky Ministerstva financií Slovenskej republiky č. 87/1996 Z. z., ktorou sa vykonáva zákon č. 18/1996 Z. z. o cenách v znení neskorších predpisov, ako cena pevná

(nemenná) počas trvania zmluvy a vychádza z cenovej ponuky Dodávateľa/Úspešného záujemcu. V cene sú zahrnuté akékoľvek náklady Dodávateľa súvisiace s plnením predmetu zmluvy.

2. Kúpna cena za Predmet plnenia je

Celková cena tovaru bez DPH:	97 200,00€
DPH 20%:	19 440,00€
Celková cena tovaru vrátane DPH:	116 640,00€

slovom: jednostošestnásťtisícšesťstoštyridsať Eur s DPH

Podrobná špecifikácia ceny je uvedená v Prílohe č. 1 tejto zmluvy.

3. Právo na zaplatenie kúpnej ceny vzniká Dodávateľovi riadnym a včasným splnením jeho záväzkov, po prevzatí Predmetu plnenia Kupujúcim, ktorý riadne splnenie záväzkov Dodávateľa písomne potvrdí v preberacom protokole. Dodávateľ je povinný v preberacom protokole napísať zoznam dodaného Tovaru s uvedením identifikačných čísel Tovaru, príslušenstva a musí byť uvedená i dodaná verzia Tovaru.
4. Dodávateľ na úhradu kúpnej ceny vystaví faktúru so splatnosťou 30 kalendárnych dní od doručenia faktúry Kupujúcemu; Kupujúci sa zaväzuje zaplatiť kúpnu cenu najneskôr do 30 dní od od riadne vystavenej a doručenej faktúry. Pokiaľ posledným dňom lehoty splatnosti bude sobota, nedeľa, deň pracovného pokoja alebo štátny sviatok, deň splnenia peňažného záväzku bude zmluvnou stranou za rovnako dohodnutých cenových a platobných podmienok akceptovaný nasledujúci prvý pracovný deň. Za deň splnenia peňažného záväzku sa považuje deň odpísania fakturovanej sumy z účtu Kupujúceho v prospech účtu Dodávateľa.
5. Faktúra musí obsahovať všetky náležitosti v zmysle platných právnych predpisov. Ak faktúra nebude obsahovať náležitosti podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov (ďalej len „zákon o DPH“), Kupujúcemu vzniká právo faktúru vrátiť Dodávateľovi na prepracovanie. Splatnosť takto vystavenej a vrátenej faktúry sa ruší a nová splatnosť faktúry začne plynúť dňom doručenia opravenej a v súlade s touto zmluvou vystavenej faktúry.
6. Faktúra bude vystavená v mene euro a jej prílohou bude preberací protokol.
7. V prípade omeškania Kupujúceho s úhradou faktúry v zmysle tejto zmluvy vzniká Dodávateľovi nárok na úrok z omeškania vo výške podľa príslušných ustanovení Obchodného zákonníka.
8. Obidve zmluvné strany vylučujú prevod práva, pohľadávky a/alebo záväzku vyplývajúceho z tejto zmluvy, na tretiu osobu bez predchádzajúcej písomnej dohody zmluvných strán. Dodávateľ nesmie plniť záväzky vyplývajúce mu z tejto zmluvy prostredníctvom tretích osôb bez predchádzajúceho písomného súhlasu Kupujúceho.
9. Dodávateľ, ktorý je platiteľom dane v zmysle zákona o DPH vyhlasuje a podpisom tejto zmluvy potvrdzuje, že ku dňu uzavretia tejto zmluvy u neho nenastali dôvody na zrušenie registrácie pre daň z pridanej hodnoty v zmysle zákona o DPH a/alebo nie je zverejnený v príslušnom zozname platiteľov dane z pridanej hodnoty, u ktorých nastali dôvody na zrušenie registrácie vedenom Finančným riaditeľstvom Slovenskej republiky v zmysle zákona o DPH (ďalej aj ako „zoznam DPH platiteľov vedený Finančným riaditeľstvom Slovenskej republiky“). Dodávateľ vyhlasuje a podpisom tejto zmluvy potvrdzuje, že ku dňu uzavretia tejto zmluvy jeho štatutárny orgán, člen štatutárneho orgánu alebo spoločník nie je štatutárnym orgánom, členom štatutárneho orgánu alebo spoločníkom Kupujúceho. V prípade, ak kedykoľvek po uzavretí tejto zmluvy a pred zánikom tejto zmluvy
   a) nastanú u Dodávateľa dôvody na zrušenie registrácie pre daň z pridanej hodnoty podľa zákona o DPH a/alebo Dodávateľ bude zverejnený v príslušnom zozname DPH platiteľov vedenom Finančným riaditeľstvom Slovenskej republiky, alebo

b) štatutárny orgán, člen štatutárneho orgánu alebo spoločník Dodávateľa sa stane štatutárnym orgánom, členom štatutárneho orgánu alebo spoločníkom Kupujúceho okrem prípadu, ak je Dodávateľom spoločnosť, v ktorej má Kupujúci priamu majetkovú účasť alebo ak je Dodávateľom spoločnosť, ktorá má priamu majetkovú účasť v spoločnosti Kupujúceho, alebo
c) vstúpi Dodávateľ do likvidácie, začne sa voči Dodávateľovi konkurzné konanie alebo reštrukturalizačné konanie,
d) Dodávateľ uvedie v zmluve alebo na faktúre číslo bankového účtu, ktorý nie je uvedený v zozname bankových účtov Dodávateľa, uverejnenom na webovej stránke Finančnej správy,

je Dodávateľ povinný najneskôr do 3 dní od vzniku tejto skutočnosti písomne oznámiť vznik tejto skutočnosti Kupujúcemu. V prípade, ak Dodávateľ v stanovenej lehote neoznámi písomne vznik niektorej zo skutočností uvedených v písm. a), b), c) a d) tohto bodu Kupujúcemu, je Kupujúci oprávnený vyúčtovať Dodávateľovi zmluvnú pokutu vo výške 3 000 € (slovom: tritisíc Eur) za každé porušenie povinnosti Dodávateľa. Dodávateľa Dodávateľ je povinný Kupujúcim vyúčtovanú zmluvnú pokutu zaplatiť Kupujúcemu. Zaplatením zmluvnej pokuty nie je dotknutý nárok Kupujúceho na náhradu vzniknutej škody v celom rozsahu. V prípade, ak kedykoľvek po uzavretí tejto zmluvy a pred zánikom tejto zmluvy vznikne (nastane) ktorákoľvek zo skutočností uvedených v písm. a), b), c) a d) tohto bodu zmluvy, má Kupujúci právo zadržať z ceny plnenia alebo z častí ceny plnenia fakturovaných Dodávateľom podľa tejto zmluvy čiastku vo výške zodpovedajúcej výške dane z pridanej hodnoty uvedenej na príslušnej faktúre (ďalej aj ako „nevyplatená čiastka z ceny“). Vo vzťahu k nevyplatenej čiastke z ceny plnenia sa Kupujúci nedostáva do omeškania ani sa nedopúšťa iného porušenia tejto zmluvy, ak nevyplatenú čiastku z ceny plnenia vysporiada alebo použije podľa ustanovení tohto bodu.

10. Kupujúci má právo odstúpiť od zmluvy v prípade zverejnenia Dodávateľa v zozname DPH platiteľov vedenom Finančným riaditeľstvom Slovenskej republiky, u ktorých nastali dôvody na zrušenie registrácie v zmysle zákona o DPH.

Čl. IV.
Čas, miesto plnenia a dodacie podmienky, prevod vlastníckeho práva

1. Dodávateľ je povinný začať s realizáciou Predmetu plnenia v deň nasledujúci po dni nadobudnutia účinnosti tejto zmluvy; Kupujúci túto skutočnmosť oznámi na e-mailovú adresu kontaktnej osoby Dodávateľa, uvedenú v záhlaví zmluvy.
2. Dodávateľ sa zaväzuje dodať Predmet plnenia Kupujúcemu v mieste Predmetu plnenia v termíne **najneskôr do 22. decembra 2023** (ďalej len „lehota dodania“).
3. Miestom Predmetu plnenia je sídlo Kupujúceho: Dúbravská cesta 1152/3, 841 04 Bratislava.
4. Kupujúci je povinný prevziať Predmet plnenia, ktorý mu bol v zmysle zmluvy a Požiadavky SSC dodaný Dodávateľom.
5. Prípadné zmeny v požadovaných parametroch Predmetu plnenia je Dodávateľ povinný vopred konzultovať s Kupujúcim.
6. Odovzdanie a prevzatie Predmetu plnenia potvrdia zmluvné strany v písomnom Protokole o odovzdaní a prevzatí Predmetu plnenia.
7. Nebezpečenstvo škody na Predmete plnenia prechádza z Dodávateľa na Kupujúceho prevzatím Predmetu plnenia osobou oprávnenou konať v mene Kupujúceho.
8. Zmluvné strany sa záväzne dohodli, že Kupujúci nadobúda Tovar do svojho výlučného vlastníctva len čo mu je Tovar riadne odovzdaný a Kupujúci tento Tovar protokolárne prevezme od Dodávateľa.

Čl. V.
Zodpovednosť za vady

1. Kupujúci si vyhradzuje právo odmietnuť prevziať Predmet plnenia z dôvodu nedodržania akosti, štruktúry alebo množstva podľa tejto zmluvy a/alebo podľa Požiadavky SSC. Ak má Predmet plnenia pri jeho preberaní zjavné vady, Kupujúci uvedie túto skutočnosť v preberacom protokole s tým, že odmieta Predmet plnenia z týchto dôvodov prevziať.
2. Dodávateľ zodpovedá za faktické a aj právne vady, ktoré má Predmet plnenia alebo jeho časť v čase jeho odovzdania Kupujúcemu.
3. Dodávateľ nezodpovedá za vady Tovaru alebo jeho časti, o ktorých Kupujúci v čase prevzatia vedel.

4. Ak Dodávateľ čo aj len v časti dodá vadný Predmet plnenia, má Kupujúci nároky z vád Tovaru, ktoré mu prislúchajú v zmysle ustanovenia § 436 a nasl. Obchodného zákonníka.
5. Dodávateľ vyhlasuje, že Tovar bude Kupujúcemu dodaný v súlade, v rozsahu a kvalite za podmienok dohodnutých touto zmluvou.
6. V prípade nefunkčnosti Predmetu plnenia, resp. v prípade poruchy alebo akejkoľvek inej vady Predmetu plnenia, je Dodávateľ povinný zabezpečiť bezplatne a na vlastné náklady odstránenie porúch alebo akýchkoľvek iných vád Predmetu plnenia, resp. výmenu nefunkčnej časti Predmetu plnenia za identickú časť Predmetu plnenia a to nasledujúci pracovný deň od nahlásenia vadného plnenia Kupujúcim. Pri nahlasovaní vadného plnenia alebo akejkoľvek inej vady Predmetu plnenia uvedie poverený zodpovedný pracovník Kupujúceho príznaky vadného plnenia.
7. Dodávateľ sa zaväzuje prevziať a odovzdať odstránenú vadu Predmetu plnenia v mieste dodania Predmetu plnenia.
8. Kupujúci sa zaväzuje zabezpečiť prístup k vadnému Predmetu plnenia pre Dodávateľa vo vzájomne dohodnutom termíne. Pri nezabezpečení prístupu Kupujúcim sa predlžuje lehota na odstránenie poruchy alebo akejkoľvek inej vady Predmetu plnenia o dobu, po ktorú Predmet plnenia nebol sprístupnený.

Čl. VI.
Doklady a licencie

1. Dodávateľ je povinný odovzdať Kupujúcemu spolu s Predmetom plnenia aj doklady vzťahujúce sa k Predmetu plnenia, ktoré sú potrebné na prevzatie a riadne užívanie Tovaru, a to najmä:
   a) dodací list so základnými údajmi o Tovare,
   b) návod na obsluhu k Predmetu plnenia v slovenskom jazyku.
2. Dodávateľ pred realizovaním dodania Predmetu plnenia je povinný na svoje náklady a v prospech Kupujúceho zabezpečiť licenciu/cie a následne ju/ich Kupujúcemu bezodplatne odovzdať.
3. Nesplnenie povinností Dodávateľa, uvedených v tomto článku zmluvy, sa považuje za podstatné porušenie zmluvy.

Čl. VII.
Zmluvné sankcie

1. V prípade omeškania Dodávateľa s dodaním Predmetu plnenia v termíne podľa čl. IV. bod 2. tejto zmluvy, je Kupujúci oprávnený uplatniť si voči Dodávateľovi nárok na zaplatenie zmluvnej pokuty vo výške 15 % z celkovej ceny plnenia.
2. V prípade nesplnenia zmluvne dohodnutých podmienok k odstráneniu vady Predmetu plnenia v nasledujúci pracovný deň od nahlásenia poruchy Kupujúcim podľa článku V. bod 6. tejto zmluvy, je Kupujúci oprávnený účtovať Dodávateľovi zmluvnú pokutu vo výške 100 eur za každý aj začatý deň omeškania so splnením povinnosti.
3. Zaplatením akejkoľvek zmluvnej pokuty uvedenej v tejto zmluve nie je dotknutý nárok Kupujúceho na náhradu škody, ktorá mu vznikla nesplnením a/alebo porušením povinností Dodávateľa.

Čl. VIII.
Zánik zmluvy

1. Zmluva zaniká splnením všetkých záväzkov zmluvných strán.
2. Zmluva môže zaniknúť aj skôr ako je uvedené v bode 1. tohto článku, a to
   a) písomnou dohodou zmluvných strán,
   b) zánikom niektorej zo zmluvných strán bez právneho nástupcu,
   c) odstúpením od zmluvy.
3. Ktorákoľvek zo zmluvných strán je oprávnená odstúpiť od tejto zmluvy v prípade jej podstatného porušenia druhou zmluvnou stranou a v ostatných prípadoch uvedených v zmluve alebo v zákone. Účinky odstúpenia od zmluvy nastávajú okamihom doručenia písomného oznámenia o odstúpení od zmluvy druhej zmluvnej strane.
   Pre účely tejto zmluvy sa za podstatné porušenie tejto zmluvy považujú prípady, ak
   a) Dodávateľ nedodá Predmet plnenia Kupujúcemu riadne a/alebo včas v lehote plnenia podľa čl. IV. bod 2. tejto zmluvy,
   b) Dodávateľ v zmylse tejto zmluvy nezačne s realizáciou Predmetu plnenia,

c) dodaný Tovar nebude zodpovedať vlastnostiam dohodnutým v zmluve a v Požiadavke SSC a/alebo kúpnej cene uvedenej v zmluve a ak Dodávateľ nevykoná nápravu ani po výzve Kupujúceho, v ktorej Kupujúci poskytne Dodávateľovi dodatočnú primeranú lehotu k náprave a/alebo určené opatrenia k náprave,
d) Dodávateľ poverí dodaním Predmetu plnenia také osoby, ktoré nie sú odborne spôsobilé a/alebo nemajú požadovanú odbornú spôsobilosť uvedenú v článku I. bod 1. písm d) zmluvy na dodanie Predmetu plnenia,
e) Dodávateľ v čase uzavretia zmluvy nebol zapísaný v registri partnerov verejného sektora, ak bol z tohto registra vymazaný alebo ak mu bol právoplatne uložený zákaz účasti podľa zákona o verejnom obstarávaní.

Čl. IX.
Doručovanie

1. Zmluvné strany sa dohodli, že pre účely tejto zmluvy sa za doručenú písomnosť bude považovať (ak doručenie nenastane preukázateľne skôr):
   - písomnosť odoslaná e-mailom na adresu kontaktnej osoby druhej zmluvnej strany - najbližší pracovný deň nasledujúci po dni odoslania písomnosti,
   - písomnosť odoslaná poštovou prepravou - uplynutím lehoty 3 pracovných dní odo dňa uloženia neprevzatej písomnosti na pošte, alebo
   - dňom odmietnutia prevzatia doručovanej písomnosti.
2. Pokiaľ nie je v tejto zmluve výslovne uvedené inak, pod pojmom písomne sa rozumie vyhotovenie a doručenie dokumentu buď v listinnej alebo elektronickej forme.
3. Akékoľvek písomné oznámenie alebo iný písomný dokument, ktorý má byť doručený podľa tejto zmluvy je možné doručovať e-mailom na e-mailové adresy kontaktných osôb zmluvných strán len v prípadoch výslovne uvedených v tejto zmluve; v ďalších prípadoch môže byť doručený osobne, alebo doporučenou poštou s doručenkou, na adresu, uvedenú v záhlaví tejto zmluvy alebo na inú adresu, oznámenú písomne druhej zmluvnej strane v súlade s týmto článkom.
4. V prípade doručovania e-mailom je každá zmluvná strana povinná doručenie e-mailu potvrdiť na e-mailovú adresu, z ktorej jej bol e-mail doručený. Pokiaľ zmluvná strana, ktorej bol e-mail doručený jeho prijatie nepotvrdí do 24 hodín v pracovných dňoch od preukázateľného odoslania e- mailu druhou zmluvnou stranou, má sa za to, že e-mail bol riadne doručený.

Čl. X.
Osobitné ustanovenia

1. Ak Dodávateľom navrhovaný subdodávateľ nespĺňa podmienky účasti týkajúce sa osobného postavenia a existovali u neho dôvody na vylúčenie podľa zákona o verejnom obstarávaní, Kupujúci písomne požiada Dodávateľa o jeho nahradenie. Dodávateľ doručí Kupujúcemu návrh nového subdodávateľa do piatich pracovných dní odo dňa doručenia žiadosti podľa predchádzajúcej vety.
2. Ak sa na Dodávateľa a jeho subdodávateľov vzťahuje povinnosť zapisovať sa do registra partnerov verejného sektora podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov (ďalej len „zákon o registri partnerov verejného sektora“), potom je Dodávateľ, ako aj jeho subdodávatelia, povinní dodržať túto povinnosť po celú dobu trvania tejto zmluvy, pričom Dodávateľ sa zaväzuje zabezpečiť splnenie tejto povinnosti aj zo strany subdodávateľov. V prípade porušenia povinnosti Dodávateľa podľa predchádzajúcej vety je Kupujúci oprávnený od zmluvy odstúpiť v okamihu, čo sa o tomto porušení dozvedel. Ak v súvislosti s porušením vyššie uvedenej povinnosti uloží príslušný orgán Kupujúcemu akúkoľvek sankciu, tak Dodávateľ je povinný túto sankciu Kupujúcemu v plnej výške nahradiť.

Článok XI.
Povinnosti Dodávateľa v súvislosti s priamymi subdodávateľmi a kľúčoví experti

1. Zmluva medzi Dodávateľom a subdodávateľom nesmie byť v rozpore s touto Zmluvou.

2. Dodávateľ zodpovedá za konanie, neplnenie, nedbanlivosť, opomenutie povinností alebo potrebného konania riadne a včas svojich subdodávateľov tak, ako by išlo o konanie, neplnenie, nedbanlivosť, opomenutie povinností alebo potrebného konania riadne a včas samotného Dodávateľa. Súhlas objednávateľa s novým subdodávateľom nezbavuje Dodávateľ žiadneho z jeho záväzkov vyplývajúcich z tejto Zmluvy alebo objednávky zadanej podľa tejto Zmluvy.

3. Dodávateľ je oprávnený a zároveň povinný plniť predmet tejto Zmluvy sám alebo prostredníctvom subdodávateľov, ktorí sú uvedení v zozname priamych subdodávateľov, ktorý tvorí prílohu č. 3 (ďalej len „zoznam priamych subdodávateľov“ alebo „príloha č. 3“) alebo odsúhlasení objednávateľom v zmysle bodu 5 tohto článku.

4. Dodávateľ je oprávnený počas trvania tejto Zmluvy zmeniť a/alebo doplniť subdodávateľa uvedeného v zozname priamych subdodávateľov len s predchádzajúcim písomným súhlasom objednávateľa.

5. V písomnej žiadosti o udelenie súhlasu je Dodávateľ povinný uviesť všetky údaje uvedené v zozname priamych subdodávateľov. Objednávateľ písomne upovedomí Dodávateľa o svojom rozhodnutí v lehote do 5 (slovom: päť) pracovných dní odo dňa prijatia úplnej žiadosti o súhlas, v ktorom v prípade neudelenia súhlasu uvedie príslušné dôvody. Ak sa objednávateľ v lehote podľa predchádzajúcej vety k žiadosti Dodávateľa nevyjadrí, znamená to súhlas objednávateľa so subdodávateľom.

6. Ak objednávateľ zistí, že subdodávateľ si nie je schopný plniť svoje záväzky alebo nevykonáva príslušnú časť plnenia riadne, môže od Dodávateľa okamžite vyžadovať náhradu za subdodávateľa. Dodávateľ je povinný spôsobom podľa bodu 6 tohto článku výzve o náhradu vyhovieť najneskôr do tridsiatich (30) dní odo dňa doručenia žiadosti objednávateľa alebo v tejto lehote objednávateľovi oznámiť, že príslušný predmet plnenia bude plniť sám. Požiadavka objednávateľa na zmenu subdodávateľa podľa tohto bodu, nemá vplyv na povinnosť Dodávateľa splniť predmet zmluvy riadne a včas.

7. Ak počas plnenia tejto Zmluvy dôjde k zmene v subdodávateľoch, Dodávateľ je povinný predložiť objednávateľovi aktuálny zoznam subdodávateľov do 5 (slovom: piatich) pracovných dní odo dňa uzatvorenia Zmluvy s novým subdodávateľom (doplnenie subdodávateľa do zoznamu) alebo odo dňa skončenia Zmluvy so subdodávateľom (vynechanie subdodávateľa zo zoznamu bez náhrady). Aktuálny zoznam bude predložený v rozsahu podľa prílohy č. 3. Na požiadanie objednávateľa je Dodávateľ povinný objednávateľovi preukázať deň uzatvorenia Zmluvy s novým subdodávateľom alebo deň skončenia Zmluvy so subdodávateľom, predložením originálu príslušnej zmluvy alebo dokumentu o ukončení Zmluvy, do 5 (slovom: piatich) pracovných dní odo dňa doručenia žiadosti.

8. Dodávateľ je povinný písomne oznámiť objednávateľovi akúkoľvek zmenu údajov o subdodávateľovi, a to najneskôr do 10 (slovom: desiatich) dní odkedy sa o zmene dozvedel. Pod pojmom údaje o subdodávateľovi sa rozumie údaje uvedené v prílohe č. 3, zmena právnej formy subdodávateľa, zmena základného imania subdodávateľa, začatie konkurzného konania, reštrukturalizačného konania alebo likvidácie subdodávateľa.

9. Dodávateľ je povinný použiť na poskytovanie služieb kľúčových expertov uvedených v prílohe č. 2 Zmluvy a odsúhlasených objednávateľom, resp. kľúčových expertov v súlade s týmto článkom Zmluvy.

10. Po predchádzajúcom písomnom súhlase objednávateľa môže Dodávateľ na poskytovanie služieb použiť iných kľúčových expertov než kľúčových expertov uvedených v prílohe č. 2 Zmluvy, ktorí spĺňajú požiadavky, ktoré boli kladené na daného kľúčového experta vo verejnom obstarávaní a za predpokladu, že taká zmena nebude mať za následok navýšenie ceny.

11. Za účelom zmeny v osobe kľúčového experta je Dodávateľ povinný doručiť objednávateľovi žiadosť o zmenu v prílohe č. 2 Zmluvy, ktorá musí obsahovať identifikačné údaje navrhovaného kľúčového experta, ktorý by mal zastávať kľúčové úlohy pri poskytovaní služieb alebo jeho časti alebo iného plnenia podľa Zmluvy.

12. Dodávateľ je povinný priložiť k žiadosti podľa bodu 11 tohto článku potvrdenia preukazujúce splnenie podmienok podľa bodu 10 tohto článku.

13. Každá žiadosť podľa bodu 11.tohto článku musí byť objednávateľovi odovzdaná včas tak, aby nezdržiavala postup poskytovania služieb a to najneskôr 6 (slovom: šesť) pracovných dní pred navrhovanou zmenou kľúčového experta.

14. Objednávateľ je povinný vyjadriť sa k žiadosti podľa bodu 11 tohto článku s uvedením, či so zmenou súhlasí alebo nie najneskôr do 3 (slovom: troch) pracovných dní odo dňa jej doručenia.

15. Ak sa objednávateľ v lehote podľa bodu 15 tohto článku nevyjadrí, predpokladá sa, že s navrhovanou zmenou zoznamu kľúčových expertov súhlasí. Uvedené ustanovenie Zmluvy neplatí, ak Dodávateľ nepredložil objednávateľovi spolu so žiadosťou o zmenu v prílohe č. 2 Zmluvy potvrdenia podľa bodu 12 tohto článku.

16. Zmluvné strany vyhlasujú, že odsúhlasenie zmeny kľúčových expertov zo strany objednávateľa žiadnym spôsobom nezbavuje Dodávateľ záväzkov vyplývajúcich mu zo Zmluvy a že také zmeny nebudú mať za následok navýšenie celkovej ceny.

17. Pre vylúčenie akýchkoľvek pochybností sa uvádza, že na výmenu subdodávateľov a kľúčových expertov nie je potrebné uzavrieť dodatok k Zmluve.

Čl. XI.
Záverečné ustanovenia

1. Právne vzťahy a právne skutočnosti neupravené touto zmluvou ako aj ďalšie vzťahy z nich vyplývajúce sa riadia príslušnými ustanoveniami Obchodného zákonníka, subsidiárne ustanoveniami Občianskeho zákonníka a všeobecne záväznými právnymi predpismi platnými v Slovenskej republike.
2. V prípade, ak by sa niektoré ustanovenie/nia tejto zmluvy stane/ali neplatným/mi, nie je tým dotknutá platnosť a účinnosť zostávajúcich ustanovení tejto zmluvy.
3. Všetky spory, ktoré sa týkajú realizácie alebo slovného výkladu tejto zmluvy budú predmetom rokovania medzi zmluvnými stranami na návrh niektorej zo zmluvných strán a to tak, aby zmluvné strany dospeli k dohode. Pokiaľ nedôjde k priateľskému urovnaniu, spor bude s konečnou platnosťou vyriešený príslušným súdom Slovenskej republiky.
4. Zmluvu možno zmeniť počas jej trvania bez nového verejného obstarávania iba po splnení obsahu ustanovení zákona o verejnom obstarávaní, pričom zmeny a doplnenia k zmluve je možné vykonať výlučne na základe písomných postupne číslovaných dodatkov k zmluve, ktoré musia byť podpísané obidvoma zmluvnými stranami.
5. Táto zmluva nadobúda platnosť dňom podpísania oprávnenými osobami/zástupcami obidvoch zmluvných strán a účinnosť nadobúda dňom nasledujúcim po dni jej zverejnenia v Centrálnom registri zmlúv podľa ustanovenia § 5a zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov a v súlade s ustanovením § 47a ods. 1 Občianskeho zákonníka.
6. Táto zmluva je vyhotovená v troch (3) rovnopisoch, z ktorých jeden (1) je určený pre Dodávateľa a dva (2) rovnopisy pre Kupujúceho.
7. Neoddeliteľnou súčasťou tejto zmluvy sú prílohy:
   a) Príloha č. 1: Podrobný rozsah a špecifikácia Predmetu plnenia
   b) Príloha č. 2: Zoznam expertov
   c) Príloha č. 3: Zoznam subodádvateľov
8. Zmluvné strany vyhlasujú, že zmluvu a všetky zmluvné dokumenty si pred podpísaním tejto zmluvy prečítali, ich obsah je vyjadrený určito a zrozumiteľne, s obsahom v celom jeho rozsahu

súhlasia, zmluvu uzatvárajú na základe slobodnej a vážnej vôle, bez omylu, na dôkaz čoho oprávnené/ní osoby/zástupcovia obidvoch zmluvných strán pripájajú svoje vlastnoručné podpisy.

Za Kupujúceho:	**Za Dodávateľa:**
V Bratislave dňa	V Bratislave dňa 11.12.2024
_____	_____
Mgr. Norbert Polievka, MA konateľ generálny riaditeľ	Ing. Lukáš Bumbál Konateľ spoločnosti

1. Pokročilá ochrana koncových bodov vrátane ochrany virtualizačnej platforiem a EDR

Názov produktu: BitDefender GravityZone Business Security Enterprise

Popis modulu
Zadávateľ požaduje komplexne zabezpečiť všetky koncové body, vrátane fyzických PC s OS Windows, Mac a Linux, virtuálnych PC (VDI) s OS Windows a Linux, fyzických serverov s OS Windows a Linux, virtuálnych serverov s OS Windows a Linux a mobilných zariadení s OS Android a iOS.

Základné minimálne požadované technické požiadavky na riešenie:
riešenie pre komplexnú ochranu PC, Linux, Mac, mobilných zariadení, fyzické a virtuálne serverové infraštruktúry musia byť spravované z jednej webovej konzoly. Navrhované riešenie musí zabezpečiť viacvrstevnú ochranu proti sofistikovaným bezpečnostným hrozbám s podporou MITRE ATT&CK frameworku, anti-phishing ochranu, anti-malware ochranu, anti-spam ochranu a adaptívnu pokročilú ochranu proti zneužitiu v rátane pokročilého strojového učenia a analýzy chovania. Taktiež musí podporovať content filtering, attachement firltering, connection filtering, message filtering, ransomware mitigation, endpoint risk analytics, a advanced anti-exploit. Výrobca nemohol získať na av-comparatives (https://www.av-comparatives.org/awards/) za posledné 2 roky ani raz menej ako 3 hviezdy v kategórií „Real World Protection“ vo firemných riešeniach.

Detailné požiadavky na správu a funkcionalitu:

1. Všetky komponenty riešenia musia byť v slovenskom alebo českom jazyku – vrátane konzoly správy, klientskych aplikácií a manuálov
2. Konzola pre správu nasadená v cloude výrobcu, ktorý sa stará o jej údržbu a vysokú dostupnosť všetkých jej služieb a funkcií
3. Možnosť kedykoľvek migrovať konzolu pre správu do on-premise prostredia bezplatne, bez zmeny platnosti licencie a za vynaloženia minimálneho času zo strany administrátora riešenia
4. Podpora produktov výrobcom nástroja bude poskytovaná v slovenskom alebo českom jazyku
5. Konzola pre centrálnu správu je kompletne multi-tenantná
6. Možnosť realizovať aktualizácie klientov z iných klientov a tým šetriť šírku prenosového pásma pripojenia k internetu
7. Možnosť zobrazovať upozornenia v konzole pre správu a posielanie upozornení e-mailom
8. Možnosť zasielať upozornenia napojením na Syslog server
9. Možnosť využitia napojení akejkoľvek tretej aplikácie za pomoci zdokumentovanej verejnej API, ku ktorej je možné vytvoriť kľúče priamo z konzoly centrálnej správy bez nutnosti zásahu technickej podpory dodávateľa či výrobcu Úlohy správy bezpečnosti
10. Riešenie musí umožniť integráciu so štruktúrami Microsoft Active Directory za účelom správy ochrany zariadení v týchto inventároch.
11. Riešenie musí byť schopné odhaliť zariadenia, ktoré nie sú vedené v Active Directory pomocou Network Discovery
12. Filtrovanie a riadenie v inventári aspoň podľa mena hostiteľa, operačného systému, IP adries, pridelených pravidiel a podľa času poslednej aktivity
13. Možnosť vzdialenej inštalácie a odinštalácie EPP klienta priamo z konzoly centrálnej správy
14. Možnosť upraviť úroveň skenovacích úloh a ich spúšťania a plánovania priamo z konzoly centrálnej správy
15. Možnosť reštartovania serverov alebo desktopov priamo z konzoly centrálnej správy
16. Centralizované miesto pre zaznamenávanie všetkých úloh
17. Priradenie bezpečnostných pravidiel pre koncové stanice možné granulárne na každej úrovni štruktúry inventáru, vrátane koreňov a listov stromov (tzn. akékoľvek OU, prípadne až priamo konkrétna stanica)
18. Podpora API, SIEM integrácia
19. Viac možností priradenia pravidiel:
    podľa užívateľa či skupiny v Active Directory, podľa sieťovej lokality, v ktorej sa zariadenie nachádza (vrátane identifikácie podľa možnej kombinácie – inklúzia či exklúzia - nasledujúcich znakov: IP adresa,

rozsah IP adries, DNS server, WINS server, default gateway, typ siete, názov hostiteľa, DHCP prípona, či je možné sa pripojiť ku konkrétnemu hostiteľovi alebo či je dostupná konzola centrálnej správy) alebo podľa OU, v ktorej sa nachádza v AD

20. Možnosť nastavenia dedičnosti medzi bezpečnostnými pravidlami granulárne podľa sekcií a pod sekcií nastavenia bezpečnostných pravidiel
21. Možnosť nastavenia intervalu, v ktorom sú reporty generované, možnosť vytvoriť report okamžite
22. Možnosť zasielania vygenerovaných reportov e-mailom
23. Možnosť stiahnuť vygenerované reporty minimálne vo formátoch .pdf či .csv
24. Možnosť upravenia reportov, vyberanie cieľa (skupina staníc, typ staníc atď.) a časového intervalu, z ktorého je report vytvorený
25. Vzdialená obnova či zmazanie súboru v karanténe
26. Možnosť automaticky pridať súbor do výnimky pri obnove z karantény
27. Viacero preddefinovaných rolí:
    - pre správu komponentov riešenia,
    - pre správu bezpečnostných pravidiel a inventár koncových zariadení
    - pre správu a tvorbu reportov
28. Podpora 2FA overenia s možnosťou vynútenia
29. Možnosť vynútiť zmenu hesla používateľa po uplynutí určitej doby od jeho poslednej zmeny
30. Možnosť automatického zablokovania užívateľského účtu pri opakovaných neúspešných pokusoch o prihlásenie
31. Detailné možnosti vybrať, aké služby a aké typy staníc môže používateľ spravovať
32. Zaznamenávanie používateľských aktivít
33. Detailný log pre každú aktivitu
34. Komplexné vyhľadávanie v logovacích záznamoch
    Správa a inštalácia ochrany
35. Administrátor môže pred inštaláciou vybrať, ktoré moduly ochrany majú byť nainštalované
36. Inštalácia môže byť zrealizovaná niekoľkými spôsobmi, a to minimálne:
    - Stiahnutím inštalačného balíčku priamo do pracovnej stanice, kde bude nainštalovaný
    - Inštalácia vzdialene priamo zo správcovskej konzoly
    - Distribúcia inštalačného balíčka cez GPO či SCCM
37. Inštalácia klienta na koncové stanice vo vzdialenej lokalite môže byť zrealizovaná z existujúceho, nainštalovaného klienta v tejto vzdialenej lokalite – účelom je optimalizácia prenosu pre WAN/VPN
38. Konzola centrálnej správy bude reportovať počet chránených koncových staníc a počet koncových staníc, ktoré chránené nie sú
39. Konzola správy obsahuje prispôsobiteľné „widgety“ pre okamžitý prehľad o stave ochrany v organizácií
40. Konzola centrálnej správy obsahuje detailné informácie o chránených zariadeniach: názov, IP adresa, operačný systém, nainštalované moduly, aplikované pravidlá, informácie o aktualizáciách
41. Konzola centrálnej správy umožňuje získanie všetkých informácií potrebných pre riešenie problémov s ochranou koncových staníc vrátane podrobných logov
42. Konzola správy umožňuje hromadne zmeniť nastavenia na všetkých staniciach naraz alebo len selektívne pre konkrétnu skupinu staníc naraz
43. Pre rozdielne skupiny používateľov bude možné granulárne nastaviť aké skupiny zariadení majú právo spravovať
44. Možnosť vytvárať inštalačné balíčky pre 32-bit a 64-bit operačné systémy, vrátane samo i nštalačného balíčku, ktorý obsahuje kompletnú aplikáciu bez nutnosti prístupu k sieti pre jeho inštaláciu.
45. Inštalačný balíček umožňuje tzv. „tichú“ inštaláciu (nezobrazia sa žiadne upozornenia, nevyžaduje sa žiadna používateľská interakcia)
46. Administrátor bude môcť v inventári správcovskej konzoly vytvárať skupiny a podskupiny, kam bude môcť presúvať chránené koncové body
47. Možnosť spustenia Network discovery z akéhokoľvek už nainštalovaného klienta
48. Servisná podpora: 12 mesiacov vrátane starostlivosti o softvér 8x5xNBD.

Vlastnosti a funkcie ochrany fyzických koncových bodov (Windows, Mac, Linux):

Podpora operačných systémov:
Windows 10 1507 a vyšší
Windows 8.1

Windows 8
Windows 7
Windows 10 IoT Enterprise
Windows Embedded 8.1 Industry
Windows Embedded 8 Standard
Windows Embedded Standard 7
Windows Embedded Compact 7
Windows Embedded POSReady 7
Windows Embedded Enterprise 7
Windows Server 2019
Windows Server 2019 Core
Windows Server 2016
Windows Server 2016 Core
Windows Server 2012 R2
Windows Server 2012
Ubuntu 14.04 LTS a vyšší
Red Hat Enterprise Linux
CentOS 6.0 a vyšší
SUSE Linux Enterprise Server 11 SP4 a vyšší
OpenSUSELeap 42.x
Fedora 25 a vyšší
Debian 8.0 a vyšší
Oracle Linux 6.3 a vyšší
Amazon Linux AMI 2016.09 a vyšší
Mac OS X El Capitan (10.11) a vyšší

1. Automatické skenovanie dát, pri ich manipulácií – t.z. otváranie súborov, kopírovanie súborov, prenášanie súborov (LAN, WAN, zdieľané úložisko, prenosné média, pevný disk...)
2. Automatické skenovanie súborov v reálnom čase s možnosťou nastavenia skenovania len špecifických typov súborov
3. Automatické skenovanie súborov v reálnom čase s možnosťou obmedzenia na maximálnu veľkosť súboru
4. Aktualizácia bezpečnostného obsahu minimálne raz za hodinu
5. Detekcia na základe vírusových definícií (tzv. signatúr)
6. Threat Emulation Technológia (v cloudovom prostredí dodávateľa alebo lokálne)
7. Pokročilá analýza spúšťaných procesov ešte pred ich spustením a ich zablokovanie v prípade vykázania škodlivého chovania (vrátane ochrany proti 0-day útokom)
8. Pokročilá analýza bežiacich procesov v reálnom čase a ich zablokovanie v prípade detekcie škodlivého chovania (vrátane ochrany proti 0-day útokom)
9. Detekcia 0-day útokov na základe cloudového i lokálneho (100% funkčnosť i v prípade výpadku pripojenia k internetu) strojového učenia
10. Detekcia 0-day útokov na základe odhaľovanie anomálií
11. Dynamická detekcia 0-day útokov, botnetových sietí, DDoS a exploit útokov v cloudových službách dodávateľa pomocou umelej inteligencie a pokročilých algoritmov strojového učenia
12. Detekcia 0-day bez súborových útokov
13. Detekcia 0-day útokov na úrovni sieťových prenosov (útoky na RDP, pokusy o zistenie dostupnosti, detekcia laterálneho pohybu útočníka)
14. Možnosť automatickej kontroly koncových bodov na nesprávnu konfiguráciu a neaktuálnosť bezpečnostných záplat aplikácií na známe zraniteľnosti
15. Možnosť upozornení pred rizikovým chovaním používateľa (prihlasovanie na nezabezpečených weboch, používanie podobného hesla na rôznych weboch, používanie podobného hesla v interných a externých aplikáciách, apod.)
16. „Risk score“ používateľov a koncových bodov umožňujúcich administrátorom priorizovať pri r iešení detegovaných incidentov
17. Riziká sú ohodnotené podľa závažnosti a pokiaľ sú spájané s konkrétnym CVE, tak je to uvedené
18. Možnosť automatickej opravy vybraných rizík, prípadne uvedenie návodu k odstráneniu rizík, ktoré nemožno odstrániť automaticky
19. Možnosť automatického spustenia podozrivých súborov v Sandboxe
20. Možnosť špecifických nastavenia Sandboxu – dĺžka pozorovania po spustení, počet opakovaných spustení, prístup k internetu počas spustení áno/nie
21. Možnosť manuálneho vloženia vzorky do Sandboxu
22. Sandbox po analýze vygeneruje rozsiahly report o vykonanej forenznej analýze vrátane:
    - sumárna časť zrozumiteľná pre laikov,

- podrobné zhrnutie udalostí diania v systéme pre expertov,
- časové osi spustených procesov a zrealizovaných systémových zmien,
- zoznam a geolokačná analýza sieťových pripojení,
- prehľad všetkých vytvorených, zmenených a mazaných súborov
- snímky obrazovky prípadných chybových hlásení

23. Riešenie musí obsahovať funkcie EDR integrované do jednej klientskej aplikácie spolu s EPP
24. Riešenie musí podporovať možnosť izolácie infikovaných koncových bodov. (Odpojenie od siete s možnosťou komunikácie s konzolou centrálnej správy, automatická dezinfekcia a odstránenie škodlivého obsahu, remote shell)
25. Riešenie musí byť schopné logovania procesov, systémových a sieťových aktivít v dobe detegovania incidentu pre ďalšiu investigáciu
26. Riešenie umožňuje analýzu sieťovej komunikácie
27. Riešenie umožňuje detekciu na základe automatizovaného hľadania IoCs Threat Intelligence v nespracovaných údajoch zbieraných EDR senzorom
28. Riešenie umožňuje ukladať údaje o bezpečnostných incidentoch až 90 dní
29. Možnosť preverovať http traffic
30. Možnosť preverovať traffic šifrovaný pomocou SSL
31. Možnosť nastavenia hesla pre odinštalovanie EPP klientskej aplikácie z koncových staníc
32. Automatické skenovanie emailov na úrovni pracovnej stanice, bez ohľadu na použitie emailového klienta, obidve pre odchádzajúce (SMTP) a prichádzajúce emaily (POP3)
33. Možnosť skenovať archívy, možnosť nastavenia maximálnej hĺbky skenovaných archívov a maximálnu veľkosť skenovaných archívov
34. Riešenie u vytvorených incidentov generuje tzv. full execution tree model a časovú os útoku
35. Riešenie umožňuje analýzu vektoru útoku
36. Riešenie umožňuje logovanie sieťových aktivít v dobe zachyteného incidentu za účelom ďalšieho preverovania
37. Ochrana proti podvodným a phishingovým webovým stránkam
38. Detekcia používaných zariadení (device) na koncových bodoch, možnosť blokovania zariadení podľa typu, možnosť povoliť len konkrétne zariadenie podľa Device ID
39. Všetky vrstvy ochrany implementované do jednej aplikácie (t.z. bez nutnosti inštalácie viac ako jednej aplikácie)
40. Súčasťou riešenia musí byť možnosť bezdotykovej a vzdialenej distribúcie bezpečnostných záplat
41. Automatická distribúcia konkrétnej záplaty pre definovanú zraniteľnosť
42. Distribúcia konkrétnej záplaty pre definovanú zraniteľnosť z konzoly na vyžiadanie administrátorom
43. Riešenie musí mať možnosť definovať úložisko v lokálnej sieti pre zníženie dopadu konektivity do internetu
44. Možnosť zobraziť aktuálny stav nainštalovaných / chýbajúcich / nefunkčných záplat na koncových zariadeniach
45. Súčasťou záplat musí byť popis a detailne informácie (CVE, BuletinID)
46. Riešenie umožňuje distribúciu záplat na fyzické a virtuálne servery platformy windows, Golden Image, pracovné stanice OS windows a aplikácie tretích strán
47. Možnosť odloženia reštartu pre záplaty.
48. Dostupné záplaty pre platformu Windows – desktopy a servery
49. Dostupné záplaty pre aplikáciu MS Office
50. Dostupné záplaty pre aplikácie výrobcov: Adobe Acrobat, Adobe Reader, Google Chrome, Mozilla Firefox, Opera, Zoom client, WinZIP, VMware tools, Cisco WebEx
51. Firewall
52. Možnosť blokovať skenovanie portov
53. Modul musí byť možné voliteľne hocikedy inštalovať a odinštalovať bez nutnosti reštartovať OS
54. Firewall obsahuje systém IDS vrátane funkcie odhaľovania neznámych hrozieb
55. Možnosť vypnutia IDS
56. Možnosť nastaviť profily známych sietí
57. Možnosť blokovania Network Discovery kompletne (vrátane spojenia v LAN), alebo len pre spojenia z internetu
58. Po každej aktualizácii bezpečnostného obsahu sú automaticky znovu preskenované súbory v karanténe
59. Možnosť obnovy súboru do originálnej, alebo do novo zadanej lokality
60. Automatické mazanie súborov v karanténe starších než zadaná maximálna doba životnosti (maximum nemôže byť kratšie než 30 dní)

61. Zablokovanie prístupu na internet pre špecifické stanice / skupiny staníc
62. Zablokovanie prístupu ku konkrétnym webom pre špecifické koncové stanice / skupiny staníc
63. Zablokovanie prístupu na internet v určený čas
64. Obmedzenie prístupu k špecifickým typom webových stránok podľa výrobcom spravovaných kategórií (napr. násilie, hazard a iné)
65. Obmedzenie prístupu ku konkrétnym webovým stránkam (vrátane podpory tzn. „wildcards“ pre možnú inklúziu či exklúziu subdomén)
66. Servisná podpora: 12 mesiacov vrátane starostlivosti o softvér 8x5xNBD.

Ochrana virtualizovaných koncových bodov (Windows, Linux)

1. Riešenie nepotrebuje VMware vShield či NSX, aby poskytol tzv. bez enginové skenovanie – režim klienta, keď na klientskom VM beží len ľahký klient a všetky úlohy skenovania sú realizované iným, špeciálnym „skenovacím“ zariadením; toto „skenovacie“ zariadenie môže byť virtualizované, ale nie je nutné aby bolo umiestnené na samotnom hypervisore ako chránená klientska VM. Počet týchto špeciálnych virtuálnych zariadení nesmie byť licenciou nijako obmedzený
2. „Skenovacie“ zariadenia sú spravované z konzoly centrálnej správy
   – aktualizácie, reštart, priradenie jednotlivých klientov ku „skenovacím“ virtuálnym zariadením
3. „Skenovacie“ zariadenie musí byť možné prevádzkovať v režime vysokej dostupnosti a rovnomerného rozloženia záťaže
5. Produkt musí hlásiť aktuálny stav zabezpečenia
   – VM chránený/nechránený, a stav „skenovacieho“ zariadenia
6. Riešenie musí umožňovať optimalizáciu dátových prenosov medzi VM a „skenovacím“ zariadením pomocou deduplikácie skenovacích procesov – t.z. ten istý súbor (podľa hashu) nebude skenovaný na dvoch rôznych VM (za predpokladu, že sa medzitým nezmenila verzia bezpečnostnej klientskej aplikácie)
7. Automatické skenovanie dát, pri ich manipulácií – t.z. otvorenie súborov, kopírovanie súborov, prenášanie súborov (LAN, WAN, zdieľané úložisko, prenosné média, pevný disk...)
8. Automatické skenovanie súborov v reálnom čase môže byť nastavené ku skenovaniu len špecifických typov súborov
9. Automatické skenovanie súborov v reálnom čase môže byť obmedzené na maximálnu veľkosť súborov
10. Aktualizácie bezpečnostného obsahu minimálne raz za hodinu
11. Detekcie na základe vírusových definícií (tzv. signatúr)
12. Threat Emulation Technologia (v cloudovom prostredí dodávateľa alebo lokálne)
13. Pokročilá analýza spúšťaných procesov ešte pred ich spustením a ich zablokovanie v prípade vykázania škodlivého chovania (vrátane ochrany proti 0-day útokom)
14. Pokročilá analýza bežiacich procesov v reálnom čase a ich zablokovanie v prípade detekcie škodlivého chovania (vrátane ochrany proti 0-day útokom)
15. Detekcia 0-day útokov na základe cloudového i lokálneho (100% funkčnosť i v prípade výpadku pripojenia k internetu) strojového učenia
16. Detekcia 0-day útokov na základe odhaľovanie anomálií
17. Dynamická detekcia 0-day útokov, botnetových sietí, DDoS a exploit útokov v cloudových službách dodávateľa pomocou umelej inteligencie a pokročilých algoritmov strojového učenia
18. Detekcia 0-day bez súborových útokov
19. Detekcia 0-day útokov na úrovni sieťových prenosov (útoky na RDP, pokusy o zistenie dostupnosti, detekcia laterálneho pohybu útočníka)
20. Možnosť automatickej kontroly koncových bodov na nesprávnu konfiguráciu a neaktuálnosť bezpečnostných záplat aplikácií na známe zraniteľnosti
21. Možnosť upozornení pred rizikovým chovaním používateľa (prihlasovanie na nezabezpečených weboch, používanie podobného hesla na rôznych weboch, používanie podobného hesla v interných a externých aplikáciách, apod.)
22. „Risk score“ používateľov a koncových bodov umožňujúcich administrátorom priorizovať pri riešení detegovaných incidentov
23. Riziká sú ohodnotené podľa závažnosti a pokiaľ sú spájané s konkrétnym CVE, tak je to uvedené
24. Možnosť automatickej opravy vybraných rizík, prípadne uvedenie návodu k odstráneniu rizík, ktoré nemožno odstrániť automaticky
25. Možnosť automatického spustenia podozrivých súborov v Sandboxe
26. Možnosť špecifických nastavenia Sandboxu – dĺžka pozorovania po spustení, počet opakovaných spustení, prístup k internetu počas spustení áno/nie
27. Možnosť manuálneho vloženia vzorky do Sandboxu
28. Sandbox po analýze vygeneruje rozsiahly report o vykonanej forenznej analýze vrátane:
    - sumárna časť zrozumiteľná pre laikov,

- podrobné zhrnutie udalostí diania v systéme pre expertov,
- časové osi spustených procesov a zrealizovaných systémových zmien,
- zoznam a geolokačná analýza sieťových pripojení,
- prehľad všetkých vytvorených, zmenených a mazaných súborov
- snímky obrazovky prípadných chybových hlásení

29. Riešenie musí obsahovať funkcie EDR integrované do jednej klientskej aplikácie spolu s EPP
30. Riešenie musí podporovať možnosť izolácie infikovaných koncových bodov. (Odpojenie od siete s možnosťou komunikácie s konzolou centrálnej správy, automatická dezinfekcia a odstránenie škodlivého obsahu, remote shell)
31. Riešenie musí byť schopné logovania procesov, systémových a sieťových aktivít v dobe detegovania incidentu pre ďalšiu investigáciu
32. Riešenie umožňuje analýzu sieťovej komunikácie
33. Riešenie umožňuje detekciu na základe automatizovaného hľadania IoCs Threat Intelligence v nespracovaných údajoch zbieraných EDR senzorom
34. Riešenie umožňuje ukladať údaje o bezpečnostných incidentoch až 90 dní
35. Možnosť preverovať http traffic
36. Možnosť preverovať traffic šifrovaný pomocou SSL
37. Možnosť nastavenia hesla pre odinštalovanie EPP klientskej aplikácie z koncových staníc

38. Automatické skenovanie emailov na úrovni pracovnej stanice, bez ohľadu na použitie emailového klienta, obidve pre odchádzajúce (SMTP) a prichádzajúce emaily (POP3)
39. Možnosť skenovať archívy, možnosť nastavenia maximálnej hĺbky skenovaných archívov a maximálnu veľkosť skenovaných archívov
40. Riešenie u vytvorených incidentov generuje tzv. full execution tree model a časovú os útoku
41. Riešenie umožňuje analýzu vektoru útoku
42. Riešenie umožňuje logovanie sieťových aktivít v dobe zachyteného incidentu za účelom ďalšieho preverovania
43. Ochrana proti podvodným a phishingovým webovým stránkam
44, Detekcia používaných zariadení (device) na koncových bodoch, možnosť blokovania zariadení podľa typu, možnosť povoliť len konkrétne zariadenie podľa Device ID
45. Všetky vrstvy ochrany implementované do jednej aplikácie (t.z. bez nutnosti inštalácie viac ako jednej aplikácie)
46. Riešenie umožňuje ukladať údaje o bezpečnostných incidentoch až 90 dní
47. Servisná podpora: 12 mesiacov vrátane starostlivosti o softvér 8x5xNBD.

2. Systém na monitorovanie a analýzu sieťovej komunikácie

Názov produktu: Progress Flowmon Probe 20000 + Progress Flowmon ADS Business

Zadávateľ požaduje škálovateľné monitorovacie riešenie siete, ktoré umožňuje v reálnom čase sledovať a vyhodnocovať, analyzovať prevádzku dátovej siete. Riešenie ktoré zabezpečí detekciu akejkoľvek bezpečnostnej, či prevádzkovej anomálie, hrozby alebo nerozpoznateľného rizika v rámci komunikačných dátových sietí. Systém plne integrovateľný do SIEM riešení, alebo ďalších bezpečnostných riešení tretích strán.

Základné minimálne požadované technické požiadavky na riešenie
Ucelené škálovateľné riešenie umožňujúce dlhodobé monitorovanie siete. Monitorovací systém musí umožňovať dlhodobé detailné monitorovanie všetkej prevádzky na počítačovej sieti. Získané štatistiky o prevádzke dátovej siete musí umožniť v reálnom čase sledovať a vyhodnocovať objemy a štruktúru prevádzky, analyzovať príčiny prevádzkových alebo výkonnostných problémov na strane siete až po používateľov a jednotlivé aplikácie, odhaľovať vnútorné a vonkajšie neznáme bezpečnostné hrozby a anomálie na základe analýzy chovania siete. Je nevyhnutné, aby monitorovací systém bol úplne nezávislý od použitej sieťovej infraštruktúry a svojou funkciou monitorovanú sieť neovplyvňoval. Zo strany sledovanej siete nesmie byť monitorovací systém detekovateľný.
Detailné požiadavky na správu a funkcionalitu nájdete podľa kategórií a funkcií nižšie.

Minimálne technické požiadavky:

1. Pasívne zapojenie senzoru/sondy bez vplyvu na monitorovanie sieť (SPAN / mirror portami) v 1 lokalite
2. Manažment rozhranie: min. 1 x (administratívne) porty 10/100 / 1000Mb / s pre zabezpečenú vzdialenú správu a prenos dát dohľad a konfigurácia - SSH, HTTPS pre každý senzor/sondu
3. Správa užívateľov a prístupových práv na zariadení prostredníctvom užívateľských rolí.
4. Nastaviteľná rýchlosť monitorovacej linky pre senzor (2x10 Gb / s monitorovacie porty) na optickom fyzickom rozhraní (2x SFP+ transceiver fiber 10GBase-SR, MM, 850nm, 300m
5. Výkon min. 1,2 Mp/s na monitorovací port
6. Prevedenie: HW, 1U so vstavaným kolektorom o kapacite min 1TB
7. Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.
8. Podpora protokolov pre výmenu dát: NetFlow dáta vo formátoch verzii 5, 9 a IPFIX.
9. Integrácia do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov pomocou SNMP
10. Vzorkovanie: Na úrovni paketov a na úrovni tokov.
11. Granularita vizualizácie: min. spracovanie dátových tokov / paketov a vizualizácia v 5-minútových, 1-minútových intervaloch a 30-sekundových intervaloch
12. Podpora štandardov dátových tokov: min. NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite a ich zber z desiatok zdrojov v sieti
13. Možnosť dohľadania ľubovoľnej komunikácie až na úroveň jednotlivých flow záznamov, priebežné grafy prevádzky, top štatistiky, reporty, alerty, databázy aktívnych zariadení na sieti vr. identifikácii zariadení.
14. Jednoduchá konfigurácia pomocou dostupných konfiguračných šablón a ich aplikáciou vytvárať profily, kapitoly, reporty, widgety a dashboardy bez nutnosti manuálnej konfigurácie.
15. Integrácia do dohľadového systému pre kontrolu dostupnosti a vyťaženia zdrojov technológií SNMP.
16. Prijímanie a preposielanie IPFIX dát pomocou spoľahlivého TCP spojenia s možnosťou šifrovania (TCP/TLS) podľa štandardu RFC 7011.
17. Vizualizácia štatistických dát podľa objemu (min . počet prenesených bytov, tokov, paketov), IP prevádzky (min. TCP, UDP, ICMP, ostatné) alebo protokolu (min. HTTP, IMAP, SSH), vrátane plnej konfigurácie grafov a pohľadov užívateľom
18. Podpora autentizácie voči LDAP (Active Directory).
19. Časová synchronizácia zariadenia proti centrálnemu zdroju času na sieti.
20. Použitie DNS cache na zariadení pre rýchlejší preklad IP adries na doménové mená.
21. Monitorovanie rozšírených L3 / L4 informácií: Podpora pre monitorovanie rozšírených L3 / L4 informácií - TTL (Time to live), TCP Window size, TCP SYN
22. Monitorovanie a reportovanie MAC adries vo flow štatistikách. Možnosť použiť MAC adresu ako položku kľúča flow záznamu.
23. Spracovanie dátovej prevádzky min. V rozsahu min. IPv4 a IPv6, IPv6 v IPv4, VLAN, MPLS, ASN, QUIC, HTTP, HTTPS (SNI) VoIP, DNS, DHCP,SMB / CIFS a emailovej prevádzky.
24. Analýza oneskorenia na sieti min. RTT, SRT, delay, jitter, retransmisiu, out-of-order pakety ako súčasť flow štatistík a podpora pre analýzu CISCO AVC
25. Podpora vyplňovania AS na základe vstavaného či dodaného zoznamu.
26. Monitoring aktívnych zariadení na sietí a viditeľnosť do šifrovanej komunikácie SSL/TLS vrátane detekcie hrozieb v šifrovanej prevádzke bez nutnosti jej dešifrácie.
27. Monitoring využívaných externých cloudových služieb ako certifikované riešenie na marketplace pre MS Azure, AWS, GPC s podporou end-to-end visibility dátovej komunikácii
28. Systém musí umožňovať vizualizáciu monitorovaných liniek a prepojov a sieťovej topológie
29. Automatické vyhodnocovanie NetFlow dát a detekcia anomálií na sieti s podporou deduplikácie, vzorkovania na úrovni tokov, identity používateľov, persistencii doménových mien.
30. Architektúra systému umožňuje streamové spracovávanie flow dát pre rýchlu detekciu bezpečnostných alebo prevádzkových anomálií.
31. Sada detekčných metód a algoritmov pre analýzu IPFIX štatistík, detekciu bezpečnostných udalostí, útokov a incidentov v reálnom čase, prevádzkových problémov a sieťových anomálií pre min. 1000fps (dátových tokov / s)
32. Perzistencia doménových mien pôvodcu udalosti spolu s detekciou anomálií
33. Behaviorálne detekčné mechanizmy: Detekcia skenovanie portov, slovníkové útoky, útoky odopretia služieb (DoS), supply chain útoky, malware, ransomware a cryptojacking. Detekcia útokov na sieťové protokoly SSH, RDP, Telnet. Detekcia anomálií v DNS, DoH, DHCP, SMTP a neštandardnej komunikácie. Detekcia P2P sietí, podvrhnutých doménových mien, VPN služieb a anonymizačných služieb (napr. TOR nódy). Detekcia nadmernej záťaže siete, nových a cudzích zariadení pripojených k sieti, výpadkov služieb, chýbajúcich reverzných DNS záznamov. Detekcia NAT.

34. Systém umožňuje Threat Inteligence napojenie a obohatenie detekovaných anomálií v rozsahu min. 750.000 updatovateľných informácií min. každých 6 hodín - identifikácia bezpečnostných udalostí (napr. komunikáciu s botnet command & control centrom, prístup na phishingové servery, apod.) využívaním zdrojov IP a host reputačných databáz poskytovaných výrobcom a aktualizovaných najmenej každých 6 hodín. Systém umožňuje zapojiť ďalšie zdroje IP a host reputačných dát pre automatickú detekciu z cez CSV alebo MISP a zároveň aj obohacovať MISP databáze.
35. Detekcia sieťových anomálií na základe predikcie budúceho správania siete s využívaním znalosti histórie komunikácie.
36. Signatúrne detekčné mechanizmy: Vstavaná funkcionalita IDS (Intrusion Detection System) agregovaná pre každú detekovanú anomáliu s interpretáciou signatúr v rámci danej udalosti (alebo osobitne) pre identifikáciu známeho škodlivého kódu, alebo zraniteľnosti systému (CVE) s pravidelným updatom signatúr min. každých 6 hodín.
37. Mapovanie detekovných udalostí k zdrojom najpoužívanejších SaaS (min 4.500 TOP) aplikácii a platforiem ako zdroj alebo cieľ kybernetickej bezpečnostnej udalosti.
38. Prípadné udalosti, ktoré predstavujú falošné poplachy (false positives) je možné odstrániť prostredníctvom jednoduchej konfigurácie pravidiel vylúčenia falošných poplachov dostupné v používateľskom rozhraní.
39. Preddefinované priority udalostí s možnosťou používateľského nastavenia závažnosti udalostí na základe IP adresných rozsahov, typov udalostí, miest výskytu alebo detailov udalosti. Jedna udalosť môže mať v závislosti na konfigurácii priradených viac priorít.
40. Udalosti je možné automaticky exportovať vo formáte Syslog (CEF) . Predpokladané využitie tejto funkcionality je integrácia so systémami typu SIEM, SOAR alebo log management.
41. Udalosti je možné reportovať do dohľadových systémov prostredníctvom funkcionality SNMP trap.
42. Notifikácia o detekovaných udalostiach prostredníctvom e-mailu s podporou rôznych formátov (HTML, incident handling systém, úsporný textový formát). Možnosť pripojiť vzorku flow dát, na základe ktorých bola udalosť detekovaná k emailovému reportu.
43. Vizualizácia priebehu prevádzky s vyznačením detekovaných udalostí v závislosti od nastavenej závažnosti udalostí.
44. Systém integruje informácie zo služieb DNS, WHOIS, geolokačná služby. Užívateľsky definované externé služby fungujúce na protokole HTTP.
45. Systém detekcie anomálií poskytuje dokumentované RestAPI pre získavanie, odosielanie a spracovanie udalostí. Prostredníctvom RestAPI je možné systém detekcie anomálií takisto konfigurovať (napr. vytvárať filtre, meniť nastavenia detekčných metód, apod.).
46. Systém umožňuje vytvárať správcovi vlastné aplikovateľné detekčné metódy na základe vzorcov chovania siete napr. na báze jednoduchého SQL syntaxu a disponuje vstavanými detekčnými metódami tohto typu.
47. Detekované udalosti musia byť interpretované v rámci MITTRE ATT&CK taktík a techník.
48. Systém musí umožňovať analýzu šifrovanej komunikácie pre potreby detekcie bezpečnostných hrozieb v šifrovane prevádzke a podporu manažment politík používaných šifrovacích mechanizmov
49. Na výskyt udalosti je možné automaticky reagovať spustením užívateľsky definovaných skriptov
50. Automatizovaná analýza sieťovej prevádzku a výsledky analýzy prezentuje v zrozumiteľnej podobe v rámci udalostí, ktoré popisujú, ako jednotlivé komunikácie v zázname prevádzky prebiehali. Udalosti sú rozdeľované podľa závažnosti do niekoľkých úrovní a indikujú problémy vzniknuté v sieťovej prevádzke na podporovaných protokoloch.
51. Webové centrálne užívateľské rozhranie, používateľsky definované (konfigurácia per používateľ), používateľsky definovateľný dashboard aj v rámci manažmentu prístupových rolí, ich zdieľania, plne customizovateľný
52. Centralizovaný dashboard s možnosťou zdieľaná vybraných widgetov, preddefinovaných widgetov pre rôzne náhľady a možnosti tvorby vlastných widgetov
53. Multitenancia riešenia pre správu internými, ale aj externými používateľmi s oddelenými rolami a prístupu do systému
54. Systém musí byť do budúcna jednoducho rozšíriteľný o funkcionalitu záchytu prevádzky v plnom rozsahu (on demand full packet capturing) vo formáte PCAP na základe užívateľom definovaného pravidla záchytu a disponuje možnosťou automatizovaného záznamu prevádzky v plnom rozsahu pri detekcii kritickej bezpečnostnej udalosti s možnosťou záchytu prevádzky v čase spätne podľa definovaných pravidiel
55. Interpretácia záchytu prevádzky v plnom rozsahu na základe vstavanej inteligencie na NetFlow kolektore

56. Webové centrálne užívateľské rozhranie, používateľsky definované (konfigurácia per používateľ), používateľsky definovateľný dashboard
57. Systém loguje všetky zmeny konfigurácie s cieľom zaistiť auditovateľnosť činnosti používateľov a vykonané zmeny s dopadom na detekcie udalostí. Zmeny konfigurácie je možné tiež odosielať protokolom syslog pre auditovanie formou externého systému typu SIEM alebo log management.

58. Reporty min. vo formáte min PDF alebo CSV, email alebo Syslog
59. Servisná podpora: 12 mesiacov vrátane starostlivosti o softvér, zákaznícka podpora po telefóne a emailom v českom alebo slovenskom jazyku min. v pracovnej dobe (8x5), prístup k webovému zákazníckemu centru, vzdialená podpora cez SSH.
Výmena HW 8x5xNBD.

3. Nástroj na automatické spúšťanie skenovania zraniteľností a získavanie údajov

Názov produktu: Rapid7 INSIGHTVM viď tech. príloha

Zadávateľ požaduje identifikáciu, vyhodnotenie, ošetrenie a hlásenie zraniteľností softvéru, aplikácií, operačných systémov.

Základné minimálne požadované technické požiadavky na riešenie
Manažment zraniteľnosti je proces identifikácie, hodnotenia, liečenia a podávania správ o bezpečnostných zraniteľnostiach v systémoch a softvéri, ktorý na nich beží. Toto, implementované spolu s ďalšími bezpečnostnými taktikami, je životne dôležité pre organizácie, aby uprednostnili možné hrozby a minimalizovali svoj „útočný povrch".
Bezpečnostné zraniteľnosti sa zase týkajú technologických slabín, ktoré umožňujú útočníkom kompromitovať produkt a informácie, ktoré uchováva. Tento proces je potrebné vykonávať nepretržite, aby bolo možné držať krok s novými systémami pridávanými do sietí, zmenami, ktoré sa v systémoch vykonávajú, a objavovaním nových zraniteľností v priebehu času.

Technické požiadavky:
1. Riešenie musí vykonávať automatizované testovanie zraniteľnosti zariadení
2. Riešenie musí umožňovať testovanie dynamicky prideľovaných IP adries prostredníctvom služby DHCP a monitorovanie ich histórie a podávanie správ pomocou "DNS name" alebo "Host name."

3. Konzola pre centrálnu správu ako aj skener musia podporovať inštaláciu na Windows alebo Linux operačné systémy.
4. Musí podporovať hybridné formy nasadenia ako fyzické, virtualizované a cloud prostredie.
5. Riešenie musí umožniť automatickú aktualizáciu tagov v databáze aktív podľa týchto pravidiel dynamického označovania.
6. Riešenie musí umožňovať automatické aktualizácie všetkých SW komponentov celej architektúry riešenia s najnovšími dostupnými verziami jednotlivých SW komponentov počas celého obdobia predplatného.
7. Riešenie musí umožniť automatickú centralizáciu 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.
8. Riešenie musí podporovať automatické zisťovanie aktív, pričom sa zohľadnia minimálne tieto parametre adresy IP, adresy MAC a názvu hostiteľa, aby sa zabránilo duplicite.
9. Musí podporovať centrálnu správu v geograficky rozptýlenom nasadení skenerov.
10. Musí podporovať prístup založený na rolách s preddefinovanými aj vlastnými rolami.
11. Musí podporovať automatizáciu pracovných postupov, ako je plánovanie skenovania, upozornenia na udalosti a zraniteľnosti skenovania a generovanie a distribúcia správ.
12. Plánované skenovanie musí podporovať opakované skenovanie v určitých časových oknách a intervaloch.

13. Musí podporovať neinvazívne aj invazívne kontroly. Administratívne poverenia možno použiť na hĺbkové autentifikované skenovanie, ktoré kontroluje aktíva na širší rozsah zraniteľností alebo porušení bezpečnostných politík.
14. Musí označovať nebezpečné kontroly a umožniť používateľom vypnúť ich na základe jednotlivých skenov.
15. Musí podporovať overené skenovanie. Zoznam podporovaných typov poverení.
16. Distribuované skenery musí spravovať centrálna konzola.
17. Pri skenovaní cez IPv4 musí zistiť systémy s podporou IPv6 a naopak.
18. Musí poskytovať pokrytie zraniteľností z NVD, CERT, SANS, Bugtraq a Secunia.
19. Musí automaticky korelovať a konsolidovať jednotlivé zraniteľnosti plánu prostredníctvom nápravného opatrenia.
20. Musí podporovať vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti.
21. Musí podporovať automatické zisťovanie a inventarizáciu majetku.(pomocou IP adresy, MAC adresy).
22. Musí poskytovať dodatočné pokrytie a upozornenie na zraniteľnosti v aplikáciách, ktoré poskytujú prístup k back-end systémom.
23. Musí poskytovať pokrytie zraniteľností v iných ako webových aplikáciách.
24. Musí podporovať vytváranie používateľom definovaných zraniteľností a kontrol zraniteľnosti.
25. Hodnotenie rizík musí zahŕňať hodnotenie CVSS, možnosť zneužitia aktív a náchylnosť k súborom škodlivého softvéru.
26. Riešenie musí podporovať hodnotenie kritickosti aktív definované používateľom, ktoré sa musí z ohľadniť v hodnotení rizík.
27. Riešenie musí poskytovať viacero modelov hodnotenia rizík.
28. Musí podporovať vlastné modely hodnotenia rizík definované používateľom.
29. Musí podporovať identifikáciu a správu výnimiek zo zraniteľnosti.
30. Riešenie musí podporovať integráciu so SIEM riešením.
31. Musí podporovať integráciu s platformami na penetračné testovanie.
32. Musí podporovať integráciu s produktmi na analýzu topológie siete a rizík.
33. Musí podporovať integráciu s virtuálnymi prostrediami.
34. Musí podporovať možnosť 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
35. Detekcia sieťových anomálií na základe predikcie budúceho správania siete s využívaním z nalosti histórie komunikácie.
36. Formáty správ by mali zahŕňať HTML, PDF, CSV a XML. Zoznam podporovaných formátov správ.
37. Servisná podpora: 12 mesiacov vrátane starostlivosti o softvér 8x5xNBD.

4. Implementačné služby pre jednotlivé systémy

Zadávateľ požaduje implementačne služby v tomto rozsahu:

Modul 1: Pokročilá ochrana koncových bodov vrátane ochrany virtualizačnej platformy a EDR:
o Inštalácia a konfigurácia softvéru na ochranu koncových bodov (napr. antivírusový softvér, firewally).
o Implementácia EDR riešenia (Endpoint Detection and Response) na sledovanie a analýzu aktivít na koncových zariadeniach.
o Konfigurácia a správa nástrojov na virtualizačnú ochranu.
o Zaškolenie personálu, aby boli schopní efektívne používať a spravovať tieto nástroje.

Modul 2: Systém na monitorovanie a analytika sieťovej komunikácie:
o Inštalácia a konfigurácia systému na monitorovanie siete, ako napríklad SIEM (Security Information and Event Management).
o Integrovanie rôznych zariadení a systémov pre zber logov a dát z komunikácie.
o Nastavenie pravidiel a upozornení pre identifikáciu neobvyklých aktivít alebo hrozieb.
o Zaškolenie personálu pre monitorovanie a analýzu udalostí v systéme.

Modul 3: Nástroj na automatické spúšťanie skenovania zraniteľností a získavanie údajov:
o Inštalácia a konfigurácia nástroja na automatické skenovanie zraniteľností.

- Nastavenie plánov pre pravidelné skenovanie siete a systémov.
- Integrácia s existujúcimi bezpečnostnými systémami a procesmi pre rýchlu reakciu na zistené zraniteľnosti.
- Zaškolenie personálu, ktorý bude spravovať a interpretovať výsledky skenovania.

Produkt 1: **BitDefender GravityZone Business Security Enterprise**

Produkt 2: **Progress Flowmon Probe 20000 + Progress Flowmon ADS Business**

Flowmon Sonda		
IFP-20000-SFP+	Progress Flowmon Probe 20000 SFP+	1
GS-IFP-20000-SFP+	1Y Progress Flowmon IFP-20000-SFP+ Standard Support	1
10G-SFP-SR	SFP+ transceiver fiber 10GBase-SR, MM, 850nm, 300m	2
SHIP-EU	Progress Flowmon Shipment (Ground, Europe) per hardware appliance	1
Celkom bez DPH		
Anomaly Detection System + Intrusion Detection System		
FPC-ADS-B	Progress Flowmon ADS Business	1
GS-FPC-ADS-B	1Y Progress Flowmon ADS Business Standard Support	1
Celkom bez DPH		

Produkt 3: **Rapid7 INSIGHTVM**

Počet aktív (assets)	SKU	Popis produktu
800	IVM	INSIGHTVM Subscription for the specified asset range. This includes discovery, unlimited scan engines, unlimited templates and up to 3 InsightVM Consoles.

ZOZNAM KĽÚČOVÝCH ODBORNÍKOV

Navrhovaná pozícia kľúčového odborníka	Meno a priezvisko	Identifikačné údaje o zamestnávateľovi kľúčového odborníka
Projektový manažér	Mgr. Bibiána Žigová	WDS Solutions s. r. o.
Expert v oblasti kybernetickej bezpečnosti	Ing. Igor Ficek	WDS Solutions s. r. o.

ZOZNAM SUBDODÁVATEĽOV

P. č.	Obchodné meno a sídlo subdodávateľa	IČO	% podiel na zákazke	Predmet subdodávok
1				
2				
3				