ZMLUVA O DIELO

uzatvorená podľa ustanovenia § 536 a nasl. Obchodného zákonníka,
medzi zmluvnými stranami

Objednávateľ:

Názov:	Trenčianska univerzita Alexandra Dubčeka v Trenčíne
Sídlo:	Študentská 2, 911 50 Trenčín
IČO:	31 118 259
DIČ:	2021376368
IČ DPH:	SK2021376368
V zastúpení:	doc. Ing. Jozef Habánik, PhD., rektor
Bankové spojenie:	Štátna pokladnica
IBAN:	SK

Zriadená zo zákona NR SR č. 155/1997 Z.z. z 15. mája 1997 v znení a doplnení zákona NR SR č. 209/2002 Z.z. z 5. apríla 2002.

a

Dodávateľ

Obchodné meno:	DATALAN, a.s.
Sídlo:	Krasovského 14, 851 01 Bratislava – mestská časť Petržalka
IČO:	35 810 734
DIČ:	2020259175
IČ DPH:	SK2020259175
Spoločnosť zapísaná v Obchodnom registri Mestského súdu Bratislava III, oddiel: 2704/B, vložka číslo: Sa	
V mene spoločnosti koná:	Ing. Juraj Zelko, predseda predstavenstva

PREAMBULA

a) Dňa ...10.04.2025.... bola zo strany Objednávateľa vystupujúceho v právnom postavení verejného obstarávateľa podľa zákona č. 343/2015 Z.z. o verejnom obstarávaní v platnom znení (ďalej len „Zákon o verejnom obstarávaní") vyhlásené verejné obstarávanie postupom podlimitnej zákazky podľa § 110 Zákona o verejnom obstarávaní na predmet zákazky: **„Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v prostredí Trenčianskej univerzity II.",** zverejnením vo Vestníku verejného obstarávania č. 73/2025 pod označením . 6590 - WYT (ďalej aj „Verejné obstarávanie");Účelom realizácie Verejného obstarávania, a teda i účelom za ktorým sa uzatvára táto Zmluva je vytvoriť u Objednávateľa podmienky kybernetickej bezpečnosti, zvýšenej sieťovej a komunikačnej bezpečnosti, kontrolu dátových tokov, integrované prostredie u Objednávateľa, a splnenie povinností Objednávateľa ako prevádzkovateľa základnej služby podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „ZoKB") a podľa zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe, a to všetko v súlade so súťažnými podkladmi k Verejnej súťaži a ponukou Dodávateľa predloženou do Verejnej súťaže;

b) Ponuka Dodávateľa predložená do Verejného obstarávania bola na základe kritéria na vyhodnotenie ponúk stanoveného vo Verejnom obstarávaní vyhodnotená ako úspešná a Objednávateľ túto Ponuku Dodávateľa prijal;

c) Predmet zákazky má byť financovaný z nenávratného finančného príspevku poskytnutého Objednávateľovi, ako verejnému obstarávateľovi Ministerstvom investícii, regionálneho rozvoja a informatizácie Slovenskej republiky, (ďalej len „Poskytovateľ NFP") pre projekt: **Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v prostredí Trenčianskej univerzity II, Kód ITMS: NFP401101FLY9, (akronym: KIBUNI)",**

d) Vzhľadom na vyššie uvedené sa Zmluvné strany dohodli a uzatvárajú túto Zmluvu v nasledovnom znení:

1. ÚVODNÉ USTANOVENIA

1.1 Definície

V tejto Zmluve budú mať nasledovné výrazy a slová napísané s veľkým začiatočným písmenom nižšie uvedený význam:

„Autorský zákon" znamená zákon č. 185/2015 Z. z. Autorský zákon v znení neskorších predpisov.

„Dielo", pozostáva z dodania tovaru a poskytnutia služieb definovaných v Špecifikácii predmetu zákazky konkretizovaných v Ponuke Dodávateľa, ktorých účelom je dobudovanie, rozšírenie a čiastočná výmena existujúcej infraštruktúry určenej pre prevádzku produkčných systémov Objednávateľa tak, aby tvorila jeden funkčný celok.

„Dodávateľ" znamená osobu menovanú ako Dodávateľ v záhlaví tejto Zmluvy.

„Dokumentácia Dodávateľa" znamená všetky doklady á dokumentáciu (technická dokumentácia LAN/SAN infraštruktúry, návrhy konfigurácie a pod.) vzťahujúce sa na Dielo, ktoré je Dodávateľ povinný odovzdať Objednávateľovi na základe Špecifikácie predmetu zákazky, tejto Zmluvy a Ponuky Dodávateľa.

„Funkčné skúšky" znamenajú každé skúšky funkčnosti dodaného Diela vykonané podľa bodu 3.6 tejto Zmluvy.

„Lehota plnenia" znamená lehotu na dodanie Diela uvedenú v bode 3.4.1 tejto Zmluvy.

„Občiansky zákonník" znamená zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.

„Obchodný zákonník" znamená zákon č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov.

„Objednávateľ" znamená osobu menovanú ako Objednávateľ v záhlaví tejto Zmluvy.

„Ponuka Dodávateľa" znamená ponuku, ktorú Dodávateľ predložil do Verejnej súťaže, a na základe ktorej bol Dodávateľ úspešný vo Verejnej súťaži. Pokiaľ sa v tejto Zmluve nachádza odkaz na Ponuku Dodávateľa, má sa tým namysli podľa kontextu Ponuka z verejného obstarávania, Zoznam Subdodávateľov a/alebo Zoznam Odborníkov, poprípade ktorákoľvek z časti Ponuky Dodávateľa (aj celá Ponuka Dodávateľa) tak, ako bola predložená do Verejnej súťaže.

„Poskytovateľ NFP" má význam uvedený v bode c) Preambuly tejto Zmluvy.

„Právne predpisy" znamenajú všetky všeobecne záväzné právne predpisy Slovenskej republiky a Európskej únie, vrátane všetkých smerníc a nariadení každej legálne ustanovenej verejnej správy. Právne predpisy zahŕňajú aj Technické normy.

„Preberací protokol" má význam uvedený v bode 3.7.1 tejto Zmluvy.

„Subdodávateľ" je hospodársky subjekt, ktorý uzavrie alebo uzavrel s Dodávateľom písomnú odplatnú zmluvu na plnenie určitej časti tejto Zmluvy.

„Súťažné podklady" znamenajú súťažné podklady pre Verejnú súťaž.

„Špecifikácia predmetu zákazky" znamená Prílohu č. 1 tejto Zmluvy. Špecifikácia predmetu zákazky špecifikuje účel, rozsah a technické a iné kritériá a požiadavky na dokumentáciu k Dielu a ostatné plnenia tejto Zmluvy tak, ako ich Objednávateľ definoval v prílohe č. 1 Výzvy na predloženie cenovej ponuky.

„Technické normy" znamenajú technické normy (STN, EN) vzťahujúce sa na akékoľvek práce na Diele, samotné Dielo a Materiály, a ostatné normy uvedené v Špecifikácii predmetu zákazky alebo normy definované Právnymi predpismi.

„Verejná súťaž" má význam uvedený v bode a) Preambuly tejto Zmluvy.

„Vyššia moc" má význam uvedený v bode 4.2.5 tejto Zmluvy.

„Zákon o verejnom obstarávaní" znamená zákon č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

„Zmluva" znamená túto zmluvu o dielo v znení všetkých jej príloh a doplnení.

„Zmluva o NFP" má význam uvedený v bode c) Preambuly tejto Zmluvy.

„Zmluvná cena" znamená konečnú pevnú cenu, za dodanie Diela na základe tejto Zmluvy vrátane DPH uvedenú v bode 4.1.2 tejto Zmluvy.

„Zmluvná strana" znamená Objednávateľa alebo Dodávateľa podľa kontextu. V prípade označenia ako Zmluvné strany, zahŕňa tento pojem aj Objednávateľa aj Dodávateľa.

1.2 Výklad Zmluvy a pojmov

Ak z kontextu Zmluvy nevyplýva niečo iné alebo v Zmluve nie je vyslovene uvedené inak, pre výklad Zmluvy a pojmov platia nasledovné pravidlá:

a) slová v jednotnom čísle zahŕňajú aj ich množné číslo a naopak;
b) slová v mužskom rode zahŕňajú aj ich ženský rod a naopak;
c) názvy bodov alebo nadpisy alebo vysvetľujúce poznámky, ktoré sa uvádzajú v tejto Zmluve, slúžia iba pre lepšiu orientáciu a pri vysvetľovaní podstatných podmienok a ustanovení tejto Zmluvy sa nebudú brať do úvahy;
d) deň sa rozumie kalendárny deň, pokiaľ Zmluva neurčuje inak;
e) osobou sa rozumie aj právnická aj fyzická osoba, vrátane jej právneho nástupcu.

1.3 Predmet Zmluvy

1.3.1 Predmetom tejto Zmluvy je úprava najmä, nie však výlučne, nasledovných záväzkov Dodávateľa:

a) dodať na vlastnú zodpovednosť Dielo v zmysle špecifikácie, ktorá je Prílohou č. 1 tejto zmluvy, a uviesť ho do riadnej prevádzky,

b) dodať Dokumentáciu Dodávateľa, ktorá sa k Dielu vzťahuje,

c) umožniť Objednávateľovi nadobudnúť vlastnícke právo k hmotným tovarom dodávaným ako súčasť Diela a nadobudnúť užívacie práva k softvéru dodávaným ako súčasť Diela v súlade s touto Zmluvou a všeobecne záväznými právnymi predpismi relevantnými vo vzťahu k dodaniu Diela podľa tejto Zmluvy.

1.3.2 Predmetom tejto Zmluvy je tiež najmä, nie však výlučne, úprava nasledovných záväzkov Objednávateľa:

a) Objednávateľ je povinný Dodávateľovi poskytnúť súčinnosť definovanú touto Zmluvou tak, aby Dodávateľ mohol Dielo a/alebo ktorúkoľvek časť plnenia na základe tejto Zmluvy dodať, uviesť riadne a včas;

b) Objednávateľ je povinný za riadne dodané Dielo a ostatné plnenia na základe tejto Zmluvy Dodávateľovi zaplatiť Zmluvnú cenu v súlade s touto Zmluvou;

c) Objednávateľ je riadne vykonané Dielo povinný v súlade s ustanoveniami tejto Zmluvy prevziať.

1.3.3 Predmetom tejto Zmluvy je aj úprava všetkých ostatných práv a povinností Zmluvných strán spojených s riadnym plnením tejto Zmluvy alebo v súvislosti s ňou.

1.3.4 V prípade neposkytnutia dostatočného finančného krytia zo strany Poskytovateľa NFP na celý predmet plnenia podľa tejto Zmluvy alebo v prípade nedostatku vlastných finančných zdrojov, Objednávateľ má právo neobjednať si vybrané hmotné tovary, užívacie práva k softvéru alebo služby tvoriace jednotlivé položky Ceny Diela. V takomto prípade je Objednávateľ oprávnený v záväznej objednávke / pokyne na dodanie Diela uviesť predmet plnenia / rozsah Diela len v rozsahu podľa jeho aktuálnych potrieb a jeho finančných možností. Dodávateľ je povinný plniť Zmluvu / dodať (zhotoviť) Dielo v rozsahu uvedenom v záväznej objednávke / pokyne na dodanie Diela.

2. DOKUMENTÁCIA DODÁVATEĽA

2.1 Dokumentácie Dodávateľa

2.1.1 Dodávateľ vypracuje a bude zodpovedný za všetku Dokumentáciu Dodávateľa, ktorú je povinný dodať podľa tejto Zmluvy, Špecifikácie predmetu zákazky alebo Právnych predpisov. Každá Dokumentácia Dodávateľa bude vyhotovená v súlade s Ponukou Dodávateľa, Špecifikáciou predmetu zákazky, Zmluvou a Právnymi predpismi. Pokiaľ táto Zmluva neustanovuje vo vzťahu k určitej časti Dokumentácie Dodávateľa inak, Dodávateľ je povinný odovzdať finálne znenie (po príslušnom preskúmaní zo strany Objednávateľa v prípadoch, v ktorých sa vyžaduje) akejkoľvek Dokumentácie Dodávateľa v dvoch (2) vyhotoveniach v tlačenej forme a v jednom (1) vyhotovení v elektronickej forme.

2.1.2 Každý dokument, ktorý znamená Dokumentáciu Dodávateľa a vyžaduje sa jeho schválenie alebo odsúhlasenie zo strany Objednávateľa podľa tejto Zmluvy (ak sú takto označené) bude predložený Objednávateľovi na preskúmanie 1x v tlačenej forme a 1x v elektronickej forme. Odo dňa kedy Objednávateľ obdrží takýto Dokument Dodávateľa má Objednávateľ 10 dní na preskúmanie Dokumentu Dodávateľa, ak nie je v Zmluve osobitne uvedené inak. V rámci lehoty na preskúmanie má Objednávateľ povinnosť vydať Dodávateľovi oznámenie, že

Dokument Dodávateľa spĺňa požiadavky podľa Zmluvy alebo nespĺňa požiadavky podľa Zmluvy s konkrétnym uvedením všetkých požiadaviek, ktoré nespĺňa. Ak Dokument Dodávateľa nespĺňa požiadavky Zmluvy, bude na náklady Dodávateľa opravený, znova predložený a znova preskúmaný v súlade s týmto bodom. Opätovné preskúmanie opraveného Dokumentu Dodávateľa nezbavuje zodpovednosti za omeškanie s odovzdaním Dokumentu Dodávateľa a/alebo za omeškanie s iným súvisiacim plnením podľa tejto Zmluvy. Pre vylúčenie pochybností platí, že v prípade, ak k dátumu odovzdania Dokument Dodávateľa nespĺňa požiadavky tejto Zmluvy, má sa za to, že Dodávateľ sa dostal do omeškania s riadnym odovzdaním Dokumentu Dodávateľa ku dňu, kedy mal Dodávateľ podľa tejto Zmluvy odovzdať Dokument Dodávateľa Objednávateľovi (ak taký dátum je), a to bez ohľadu na jeho následnú opravu.

2.1.3 Ak Dokument Dodávateľa spĺňa požiadavky tejto Zmluvy Objednávateľ o tom v lehote na preskúmanie podľa bodu 2.1.2 Dodávateľovi vydá potvrdenie. Pokiaľ Objednávateľ v príslušnej lehote na preskúmanie Dodávateľovi nevydá oznámenie, že Dokument Dodávateľa nespĺňa požiadavky tejto Zmluvy, postupom podľa bodu 2.1.2 tejto Zmluvy alebo Dodávateľovi nevydá potvrdenie podľa tohto bodu, má sa za to (platí fikcia), že toto potvrdenie bolo vydané v posledný deň lehoty na preskúmanie.

2.1.4 Vydanie potvrdenia alebo akékoľvek iné schválenie, či súhlas Objednávateľa vo vzťahu k Dokumentácii Dodávateľa nezbavuje Dodávateľa žiadnej zodpovednosti. Ak sa v Dokumentácii Dodávateľa nájdu chyby, opomenutia, nejasnosti, rozpory, nedostatky alebo akékoľvek iné vady, tieto budú spolu s Dielom opravené na náklady Dodávateľa, nehľadiac na súhlasy alebo schválenia Objednávateľa podľa tohto bodu 2.1.

2.2 Príručky pre prevádzku a údržbu a zaškolenie obsluhy

Najneskôr k Preberaciemu konaniu Dodávateľ dodá Objednávateľovi všetky návody a príručky pre prevádzku a údržbu akýchkoľvek častí Diela (servery, switche, softvér) vrátane akýchkoľvek nevyhnutných dokumentov pre riadne užívanie, prevádzku a údržbu, ktorú má vykonávať Objednávateľ pre dodržanie záručných podmienok výrobcov jednotlivých zariadení alebo záruky Dodávateľa za Dielo. Dodávateľ zároveň zabezpečí a vykoná zaškolenie personálu Objednávateľa v súlade so Špecifikáciou predmetu zákazky. O zaškolení obsluhy Objednávateľa Zmluvné strany vyhotovia osobitný protokol, ktorý musí byť podpísaný oprávnenými zástupcami oboch Zmluvných strán.

3. DODANIE DIELA

3.1 Miesto plnenia

Miestom plnenia je Trenčianska univerzita Alexandra v Trenčíne, Študentská, 911 50 Trenčín.

3.1.1 Objednávateľ poskytol Dodávateľovi v rozsahu, v akom ich má k dispozícii, všetky dôležité a potrebné údaje a informácie o faktickom stave jestvujúcej infraštruktúry Objednávateľa. Za interpretáciu všetkých týchto údajov zodpovedá Dodávateľ.

3.1.2 Dodávateľ vyhlasuje, že v rozsahu v akom to bolo prakticky možné, sa oboznámil s infraštruktúrou Objednávateľa.

3.1.3 Objednávateľ je povinný Dodávateľovi poskytnúť, resp. zabezpečiť právo prístupu na Miesto plnenia tak, aby Dodávateľ mohol Dielo riadne dodať a odovzdať Objednávateľovi v Lehote plnenia. Objednávateľ poskytne prístup na Miesto plnenia Dodávateľovi najneskôr do piatich (5) dní odo dňa doručenia výzvy na sprístupnenie Miesta plnenia Objednávateľovi zo strany Dodávateľa. O poskytnutí prístupu Dodávateľa na Miesto plnenia Zmluvné strany vyhotovia protokol o sprístupnení Miesta plnenia. Tento protokol musí byť podpísaný oboma Zmluvnými stranami. Dodávateľ nie je v omeškaní s plnením podľa tejto Zmluvy po dobu, po ktorú mu Objednávateľ neposkytol právo prístupu na Miesto plnenia podľa tohto bodu.

3.2 Podmienky dodania Diela

3.2.1 Dodávateľ je zodpovedný za to, že Dielo bude vyhovovať Špecifikácii predmetu zákazky, Ponuke Dodávateľa, Zmluve a Právnym predpisom.

3.2.2 Dodávateľ a Objednávateľ sú povinní vzájomne si poskytnúť akúkoľvek a všetku súčinnosť nevyhnutnú k riadnemu dodaniu a prevzatiu Diela vrátane súčinnosti pri spoločnom postupe voči orgánom verejnej moci a akýmkoľvek iným subjektom. V prípade, ak niektorá Zmluvná strana bude považovať poskytnutie súčinnosti

druhej Zmluvnej strany za nedostatočné, je povinná o tom písomne informovať druhú Zmluvnú stranu. V opačnom prípade sa bude mať za to, že súčinnosť podľa tejto Zmluvy bola poskytnutá riadne.

3.2.3 Dodávateľ nesie zodpovednosť za správne umiestnenie všetkých častí Diela v súlade so Špecifikáciou predmetu zákazky a Dokumentáciou Dodávateľa.

3.2.4 Objednávateľ poskytne Dodávateľovi možnosť napojenia na odberné miesta elektriny a všetkých energií a ďalších služieb, ktoré môže pri dodávke Diela potrebovať, ak sa s Objednávateľom nedohodne inak. Všetky náklady na spotrebu nevyhnutne spotrebovaných energií znáša Objednávateľ.

3.2.5 Dodávateľ okrem iného zabezpečí na vlastné riziko a zodpovednosť najmä:

a) Všetky materiály (prepojovacie káble, koncovky, či nástroje potrebné pre realizáciu Diela), zariadenia, softvér definovaný Špecifikáciou predmetu zákazky prípadne iný softvér potrebný pre zhotovenie Diela;
b) dopravu a vykládku zariadení Diela v Mieste plnenia;
c) akékoľvek technické úpravy na ním dodaných zariadeniach nevyhnutné pre inštaláciu, umiestnenie a sprevádzkovanie Diela;
d) všetky potrebné konfigurácie, parametrizácie a customizácie potrebné pre vykonanie Diela v súlade so Špecifikáciou predmetu zákazky a Ponukou Dodávateľa;
e) uvedenie Diela do riadnej prevádzky vrátane vykonania Funkčných skúšok celého Diela a zabezpečenia všetkých vstupov potrebných pre vykonanie Funkčných skúšok;
f) vykonanie úspešného Preberacieho konania
g) dodanie všetky požadovanej dokumentácie.

3.2.6 Dodávateľ počas celej platnosti tejto Zmluvy nesie zodpovednosť za všetky činnosti smerujúce k dodaniu a sprevádzkovaniu Diela a akýmikoľvek inými prácami a činnosťami, ktoré je Dodávateľ povinný vykonať na základe tejto Zmluvy. Dodávateľ zabezpečí najmä, nie však výlučne:

a) bezpečnosť a ochranu zdravia pri práci tak pokiaľ ide o vlastných zamestnancov prostredníctvom ktorých dodáva Dielo, a to najmä, nie však výlučne, zabezpečením bezpečnostných a zdravotných požiadaviek podľa zákona č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci a o zmene a doplnení niektorých zákonov a ostatných právnych predpisov bezpečnosti a ochrany a bezpečnosti pri práci;
b) rešpektovanie predpisov bezpečnosti a ochrany a bezpečnosti pri práci a protipožiarnych predpisov Objednávateľa v Mieste plnenia;
c) poriadok a čistotu v Mieste plnenia, pokiaľ ide o činnosť zamestnancov Dodávateľa prípade iné osoby, ktoré použije na dodanie Diela;
d) aby sa všetky osoby realizujúce Dielo v mene Dodávateľa zdržali fajčenia na Mieste plnenia;
e) predchádzanie škodám na majetku tretích osôb.

3.2.7 Dodávateľ sa zaväzuje zabezpečiť všetky materiály, krabicový softvér, hardvér, nevyhnutné pre dodanie Diela a dopraviť ich podľa ich povahy na Miesto plnenia. Dodávateľ zabezpečí ochranu všetkých materiálov a hardvéru pred poškodením alebo zničením a ich skladovanie tak, aby tieto nestratili predpísané, resp. požadované vlastnosti. Dodávateľ zodpovedá za súlad všetkých materiálov, softvéru a hardvéru tvoriacich Dielo, s príslušnými Právnymi predpismi a touto Zmluvou. Nebezpečenstvo vzniku škody na Dielo znáša výlučne Dodávateľ a to až do úplného prevzatia Diela zo strany Objednávateľa v súlade s bodom 3.7 tejto Zmluvy.

3.2.8 Dodávateľ je zodpovedný za nakladanie s odpadmi vrátane prípadných stavebných odpadov podľa príslušných ustanovení zákona č. 79/2015 Z. z. o odpadoch v znení neskorších predpisov, ktoré vzniknú v súvislosti s plnením tejto Zmluvy. Dodávateľ nesie zodpovednosť za plnenie a plní za Objednávateľa aj všetky povinnosti pôvodcu odpadu v zmysle príslušných ustanovení zákona o odpadoch. V prípade ak Objednávateľovi vznikne akákoľvek škoda v dôsledku porušenia povinností Dodávateľa podľa tejto Zmluvy alebo zákona o odpadoch v súvislosti s (ne)plnením akýchkoľvek povinností podľa zákona o odpadoch a príslušných vykonávacích predpisov, Dodávateľ odškodní Objednávateľa za akékoľvek takéto škody.

3.2.9 Dodávateľ sa zaväzuje akékoľvek zmeny týkajúce sa hmotných tovarov dodávaných ako súčasť Diela (a to najmä, nie však výlučne ukončenie výroby tovaru) oznámiť Objednávateľovi bezodkladne, od kedy sa o tejto skutočnosti preukázateľne dozvedel, a to e-mailom s následným písomným doručením oznámenia Objednávateľovi. V prípade, ak Dodávateľ oznámi Objednávateľovi ukončenie výroby tovaru alebo nedoručenie tovaru prepravcom, súčasťou oznámenia bude písomné potvrdenie výrobcu tovaru o ukončení výroby tovaru alebo potvrdenie prepravcu tovaru o nedodaní tovaru prepravcom v požadovanej lehote dodania v súlade s bodom 3.4.1 tejto Zmluvy. V prípade, ak sa oznámenie Dodávateľa o ukončení výroby tovaru a/alebo potvrdenie výrobcu tovaru o ukončení výroby tovaru resp. oznámenie Dodávateľa o nedoručení tovaru a/alebo potvrdenie prepravcu tovaru o nedodaní tovaru v požadovanej lehote dodania, dodatočne preukáže ako nepravdivé, zodpovedá Dodávateľ Objednávateľovi za škodu, ktorá mu v dôsledku toho vznikne.

V prípade uvedeného ukončenia výroby tovaru uzatvoria Zmluvné strany na základe výzvy Objednávateľa dodatok k tejto Zmluve podľa § 18 ods. 1 písm. a) zákona o verejnom obstarávaní a postupom v tejto Zmluve dohodnutým, predmetom ktorého bude zmena zariadenia, ako súčasť predmetu tejto Zmluvy (pričom nové zariadenie bude spĺňať všetky technické požiadavky v zmysle Prílohy č. 1 tejto Zmluvy) v dôsledku ukončenia výroby pôvodne dohodnutého zariadenia.

Bez uzatvorenia dodatku k tejto Zmluve nie je Dodávateľ oprávnený dodať Objednávateľovi iné zariadenie ako to, ktoré je predmetom tejto Zmluvy. Postup podľa tohto bodu 3.2.9 Zmluvy, (t. j. doručiť oznámenie o ukončení výroby tovaru resp. oznámenie o nedoručení tovaru a dohodnutým postupom dodať iný ako pôvodne dohodnutý tovar), môže Dodávateľ uplatniť len jedenkrát počas trvania právneho vzťahu založeného touto Zmluvou.

3.2.10 Pre vylúčenie pochybností, podmienkami vykonania Diela uvedenými v tomto bode nie sú dotknuté ostatné podmienky uvedené v ostatných častiach Zmluvy, najmä v Špecifikácií predmetu zákazky.

3.3 Spolupráca počas dodania Diela

3.3.1 Dodávateľ berie na vedomie, že v Mieste plnenia budú prítomné aj iné osoby odlišné od personálu Dodávateľa, keďže dodanie Diela môže prebiehať paralelne s výukou a bežnou prevádzkou Objednávateľa. Podpisom Zmluvy Poskytovateľ prehlasuje, že berie na vedomie túto skutočnosť, a že táto skutočnosť ako taká nebude brániť riadnemu dodaniu Diela. Pokiaľ by činnosť osôb Objednávateľa v Mieste plnenia mala znemožňovať alebo brániť Dodávateľovi v prístupe na Miesto plnenia a/alebo v dodaní Diela, alebo ak by takáto činnosť mala spôsobiť škodu na akýchkoľvek zariadeniach Dodávateľa potrebných k dodaniu Diela, Objednávateľ sa zaväzuje vynaložiť všetko primerané úsilie na zabránenie tejto škody a na zabránenie alebo zmiernenie následkov takejto činnosti. Dodávateľ sa zaväzuje v čo najvyššej možnej miere poskytnúť akúkoľvek súčinnosť Objednávateľovi a/alebo ostatným osobám prítomným v Mieste plnenia v záujme zachovania plynulej paralelnej výučby a bežnej prevádzky Objednávateľa (napr. pri realizácii výskumu). Zmluvné strany sú povinné si tiež vzájomne poskytnúť akúkoľvek a všetku súčinnosť nevyhnutnú k riadnemu dodaniu Diela.

3.3.2 V prípade, ak niektorá Zmluvná strana bude považovať poskytnutie súčinnosti druhej Zmluvnej strany za nedostatočné, je povinná o tom písomne informovať druhú Zmluvnú stranu. V opačnom prípade sa bude mať za to, že súčinnosť podľa tejto Zmluvy bola poskytnutá riadne.

3.4 Lehota plnenia

3.4.1 Lehota na dodania Diela je do troch mesiacov odo dňa doručenia objednávky / pokynu na dodanie Diela. Objednávateľ vystaví objednávku / vydá pokyn na dodanie Diela po ukončení ex post kontroly zadávania zákazky poskytovateľom finančného príspevku, nie však neskôr ako dva mesiace pred ukončením realizácie projektu na základe ktorého je predmet zmluvy spolufinancovaný (t.j. Objednávateľ má právo vystaviť Objednávku aj pred skončením ex post kontroly, ak by dodanie Diela v lehote podľa prvej vety ohrozovalo ukončenie projektu na základe ktorého je predmet zmluvy spolufinancovaný). Dodávateľ je povinný Dielo v súlade s Plánom dodania Diela v Lehote plnenia dodať tak, aby vyhovelo Funkčným skúškam, bolo pripravený na Preberacie konanie podľa bodu 3.7 tejto Zmluvy.

3.4.2 Dodávateľ bude mať nárok na predĺženie Lehoty plnenia pokiaľ oneskorenie s dodaním Diela bude spôsobené niektorou z nasledovných okolností:

a) príčina, ktorá dáva Dodávateľovi nárok na predĺženie Lehoty plnenia podľa niektorého z bodov tejto Zmluvy,

b) omeškanie alebo obmedzenie na strane Objednávateľa, ktoré je priamou príčinou omeškania Dodávateľa, a ktoré nebolo odstránené v primeranej lehote na základe výzvy Dodávateľa na odstránenie takéhoto omeškania alebo obmedzenia,

c) dôvody Vyššej moci, ktoré sú priamou príčinou omeškania Dodávateľa.

3.5 Plán dodania Diela

3.5.1 Dodávateľ najneskôr do desiatich (10) dní odo dňa nadobudnutia účinnosti tejto Zmluvy predloží Objednávateľovi grafický Plán dodania Diela s uvedením miesta plnenia. Plán dodania Diela bude zodpovedať požiadavkám Špecifikácie predmetu zákazky, Ponuke Dodávateľa a tejto Zmluve. Po odovzdaní Plánu dodania Diela patrí Objednávateľovi lehota na preskúmanie Plánu dodania Diela v trvaní desiatich (10) dní. Na preskúmanie Plánu dodania Diela platia primerane podmienky podľa bodov 2.1 tejto Zmluvy. Po preskúmaní Plánu dodania Diela Objednávateľom sa tento stáva Prílohou č. 3 tejto Zmluvy.

3.5.2 Dodávateľ vyhotoví Plán dodania Diela tak, aby Dodávateľovi umožňoval prepravu, dodanie a uvedenie Diela do prevádzky a vrátane úspešného absolvovania Funkčných skúšok celého Diela v Lehote plnenia.

3.5.3 Grafický Plán dodania Diela bude obsahovať vyjadrenie časovej náročnosti a nadväznosti jednotlivých úkonov, činností a prác vyjadrenú v dňoch potrebných na dodanie Diela vrátane plánu Funkčných skúšok. Plán dodania Diela bude obsahovať stručný popis všetkých činností a prác (najmä no nie výlučne inštaláciu hardvéru, nasadenie softvéru, resp. dodanie, montáž hardvéru), ich vzájomnú postupnosť a časovou nadväznosť.

3.5.4 Kedykoľvek to bude potrebné z dôvodu predĺženia Lehoty plnenia alebo kedykoľvek Plán dodania Diela nebude zodpovedať Zmluve, alebo ak sa skutočný postup prác nezhoduje s Plánom dodania Diela, alebo ak sa v porovnaní s predpokladmi Plánu dodania Diela, Dodávateľ predloží Objednávateľovi revidovaný Plán dodania Diela na preskúmanie za rovnakých podmienok ako sú uvedené v bode 3.5.1, a to najneskôr do piatich (5) dní odo dňa, kedy Objednávateľ vyzve Poskytovateľa na predloženie takéhoto revidovaného Plánu dodania Diela na preskúmanie. Pre vylúčenie pochybností platí, že revízia Plánu dodania Diela podľa tohto bodu nemôže mať sama o sebe vplyv na predĺženie Lehoty plnenia, pokiaľ okolnosť vyvolávajúca potrebu revízie Plánu dodania Diela zároveň nedáva Dodávateľovi právo na predĺženie, resp. úpravu Lehoty plnenia podľa iného bodu tejto Zmluvy.

3.6 Funkčné skúšky

3.6.1 Pred odovzdaním celého Diela je Dodávateľ za účasti Objednávateľa a v súlade s Plánom dodania Diela povinný vykonať Funkčné skúšky Diela. Na základe Funkčných skúšok musí Dodávateľ preukázať, že Dielo je spôsobilé a pripravené pre riadnu prevádzku, a že spĺňa všetky podmienky a požiadavky vyplývajúce zo Špecifikácie predmetu zákazky, vyhovuje Ponuke Dodávateľa a spĺňa ostatné požiadavky na základe Zmluvy vzťahujúce sa na Dielo. Funkčnými skúškami sa rozumie najmä testovanie funkčnosti riešenia a testovania vysokej dostupnosti riešenia, odolnosti voči výpadkom jednotlivých komponentov riešenia formou simulácie chybových stavov vytypovaných komponentov.

3.6.2 Dodávateľ pre účely Funkčných skúšok zabezpečí a poskytne všetko potrebné vybavenie, asistenciu, dokumenty a iné informácie (testovacie scenáre a pod.) personál a všetko ostatné tak, aby Funkčné skúšky prebehli v súlade so Zmluvou.

3.6.3 Harmonogram Funkčných skúšok Dodávateľ doručí Objednávateľovi v dostatočnom časovom predstihu, najneskôr však štrnásť (14) dní pred plánovaným termínom Funkčných skúšok. Harmonogram Funkčných skúšok bude obsahovať časový harmonogram jednotlivých plánovaných úkonov testovania.

3.6.4 Funkčné skúšky budú prebiehať v súlade s harmonogramom Funkčných skúšok a budú zahŕňať všetky prevádzkové skúšky za účelom preukázania, že Dielo môže byť prevádzkovaný správne a bezpečne za všetkých dostupných prevádzkových podmienok.

3.6.5 O výsledku Funkčných skúšok bude vyhotovený samostatný protokol. Ak Dielo nevyhovie Funkčným skúškam, Objednávateľ môže požadovať, aby Dodávateľ napravil vady Diela, a aby Dodávateľ vykonal opakované Funkčné skúšky za rovnakých podmienok. To sa vzťahuje na ktorúkoľvek časť Funkčných skúšok. Ak Dielo nevyhovie ani opakovaným Funkčným skúškam, Objednávateľ môže nariadiť ďalšie opakovanie Funkčných skúšok alebo Dielo odmietnuť prevziať a odstúpiť od Zmluvy.

3.6.6 Odstránenie nedostatkov po neúspešných Funkčných skúškach, resp. úspešné vykonanie opakovaných Funkčných skúšok nezbavuje Dodávateľa zodpovednosti za omeškanie s riadnym dodaním Diela v Lehote plnenia a Objednávateľa nezbavuje nároku na náhradu škody a zaplatenie zmluvnej pokuty podľa tejto Zmluvy.

3.7 Preberacie konanie

3.7.1 Preberacie konanie je konanie, v ktorom Objednávateľ v nadväznosti na Funkčné skúšky preverí, že Dielo ako celok a k tomu zodpovedajúca Dokumentácia Dodávateľa nemá vady a spĺňa požiadavky Špecifikácie predmetu zákazky a Ponuky Dodávateľa, Právnych predpisov, Zmluvy, ktoré sa končí vydaním protokolu, ktorým Objednávateľ deklaruje splnenie záväzkov Dodávateľa dodať Dielo riadne (konanie podľa tohto bodu ďalej aj ako „**Preberacie konanie**" a protokol vydaný v Preberacom konaní ďalej aj ako „**Preberací protokol**").

3.7.2 Samotné Preberacie konanie sa uskutoční až po Funkčných skúškach celého Diela a odovzdaní všetkej požadovanej Dokumentácie Dodávateľa. Dodávateľ je povinný k Preberaciemu konaniu predložiť Objednávateľovi nasledovné doklady:

a) Žiadosť o vydanie Preberacieho protokolu;

b) dodacie listy, licencie k softvéru;

c) všetky protokoly o Funkčných skúškach;

d) príslušné oprávnenia Dodávateľa na dodanie Diela, ak sú potrebné;

e) všetku Dokumentáciu Dodávateľa, ak ešte nebola Objednávateľovi podľa tejto Zmluvy odovzdaná;

f) všetky protokoly o realizovaných školeniach;

g) akékoľvek ďalšie dokumenty, ktoré majú byť Objednávateľovi odovzdané na základe tejto Zmluvy;

h) vyjadrenie Dodávateľa, že Dielo bolo vyhotovené v súlade so Špecifikáciou predmetu zákazky, touto Zmluvou a Ponukou Dodávateľa.

3.7.3 Preberacie konanie sa začína dňom predloženia žiadosti o vydanie Preberacieho protokolu spolu so všetkými dokumentami podľa bodu 3.7.2 vyššie. Predloženie žiadosti o vydanie Preberacieho protokolu Objednávateľovi znamená, že podľa názoru Dodávateľa je Dielo dodané riadne v súlade so Zmluvou, nemá vady brániace riadnemu užívaniu, a je pripravené k úspešnému Preberaciemu konaniu. Za riadne dodané Dielo sa považuje Dielo dodané bez vád a v súlade s Ponukou Dodávateľa, Špecifikáciou predmetu zákazky, Zmluvou a Právnymi predpismi.

3.7.4 Ak sa zmluvné strany nedohodnú inak, tak do štrnástich (14) dní odo dňa začatia Preberacieho konania je Objednávateľ povinný:

a) vydať Dodávateľovi Preberací protokol s uvedením dátumu, kedy bolo Dielo dodané v súlade so Zmluvou, s výnimkou drobných nedorobkov a vád, ktoré nebránia užívaniu Diela pre zamýšľaný účel; alebo

b) zamietnuť žiadosť o vydanie Preberacieho protokolu s uvedením vád Diela, ktoré musí Dodávateľ odstrániť, aby bolo Dielo v súlade so Zmluvou.

3.7.5 V prípade, ak Objednávateľ nevydá Preberací protokol alebo žiadosť o vydanie Preberacieho protokolu nezamietne v lehote podľa bodu3.7.4, má sa za to, že Preberací protokol bol vydaný k poslednému dňu tejto lehoty. Vydaním Preberacieho protokolu alebo uplynutím lehoty podľa bodu 3.7.4 v prípade fikcie vydania Preberacieho protokolu podľa predchádzajúcej vety sa končí Preberacie konanie. Vydanie Preberacieho protokolu Dodávateľ Objednávateľovi potvrdí podpisom Preberacieho protokolu. Pokiaľ Dodávateľ podpisom nepotvrdí Objednávateľovi vydanie Preberacieho protokolu do troch (3) pracovných dní odo dňa, kedy bol Dodávateľovi doručený, má sa za to, že vydanie Preberacieho protokolu Dodávateľ podpisom potvrdil v posledný deň tejto lehoty.

3.7.6 Dňom podpisu Preberacieho protokolu oboma Zmluvnými stranami podľa bodu 3.7.4 prechádza na Objednávateľa vlastníctvo, resp. užívacie práva k Dielu a nebezpečenstvo škody na Dielo v zmysle tejto Zmluvy.

3.7.7 Pre vylúčenie pochybností, ak bude mať Dielo k dátumu uplynutia Lehoty plnenia zjavné vady zistené v rámci Preberacieho konania podľa tohto bodu 3.7 tejto Zmluvy, má sa za to, že Dodávateľ sa dostal do omeškania s riadnym a včasným plnením k dátumu uplynutia Lehoty plnenia, a to bez ohľadu na to, či boli vady v rámci Preberacieho konania zistené po tomto dátume (resp. týchto dátumoch). Odstránenie vytknutých vád Dodávateľom a následné vydanie Preberacieho protokolu podľa tohto článku Dodávateľa nezbavuje zodpovednosti za škodu a omeškanie a Objednávateľa nezbavuje nároku na zmluvnú pokutu za omeškanie Dodávateľa s povinnosťou plniť riadne a včas v Lehote plnenia.

3.7.8 V prípade, že Objednávateľ odmietne vydať Preberací protokol postupom podľa bodu 3.7.4b), Dodávateľ po odstránení vytknutých vád opätovne predloží žiadosť o vydanie Preberacieho protokolu podľa bodu 3.7.1, resp. 3.7.3 tejto Zmluvy a Objednávateľovi plynie lehota v zmysle bodu 3.7.4 tejto Zmluvy, pričom bod 3.7.5 sa aplikuje primerane. Opätovným vykonaním Preberacieho konania nie je dotknutý tento bod 3.7.8. Pre vylúčenie pochybností, bez ohľadu na to, kedy Objednávateľ vydá Preberací protokol napr. aj pre prípad opakovaného Preberacieho konania (pokiaľ neplatí fikcia vydania Preberacieho protokolu podľa bodu 3.7.5) platí, že pokiaľ k uplynutiu Lehoty plnenia nebolo Dielo spôsobilé na úspešné ukončenie Preberacieho konania (t. j. bez vád, resp. bez vád, ktoré bránia užívaniu Diela pre dohodnutý účel), Dodávateľ sa dostal do omeškania ku dňu nasledujúcemu po uplynutí Lehoty plnenia. Vyššie uvedené znamená, že odstránenie vytknutých vád Dodávateľom a následné vydanie Preberacieho protokolu v Preberacom konaní Dodávateľa nezbavuje zodpovednosti za škodu a omeškanie a Objednávateľa nezbavuje nároku na zmluvnú pokutu za omeškanie Dodávateľa s riadnym a včasným plnením v Lehote plnenia.

3.7.9 V prípade, ak Objednávateľ vydá Preberací protokol podľa bodu 3.7.4a) s výnimkou drobných vád, ktoré nebránia užívaniu Diela, Objednávateľ v Preberacom protokole určí alebo sa s Dodávateľom dohodne na primeranej lehote

na odstránenie týchto vád. O úplnom odstránení vád Zmluvné strany vyhotovia protokol o úplnom odstránení vád. Tento protokol musí byť podpísaný oboma Zmluvnými stranami.

3.7.10 Pokiaľ Dodávateľ neodstráni vady Diela v dodatočnej primeranej lehote určenej v Preberacom protokole podľa bodu 3.7.4a)vzniká Objednávateľovi nárok na zaplatenie zmluvnej pokuty podľa bodu 4.5.1a) tejto Zmluvy. V prípade, ak vznikne Objednávateľovi škoda v dôsledku užívania Diela s vadami a nedorobkami uvedenými v Preberacom protokole, Dodávateľ Objednávateľa za túto škodu odškodní v plnom rozsahu.

4. SPOLOČNÉ USTANOVENIA

4.1 Zmluvná cena a platobné podmienky

4.1.1 Zmluvná cena za plnenie predmetu Zmluvy je stanovená dohodou Zmluvných strán v súlade so zákonom č. 18/1996 Z. z. o cenách v znení neskorších predpisov a vyhlášky MF SR č. 87/1996 Z. z., ktorou sa vykonáva zákon o cenách a je rozčlenená nasledovne:

4.1.2 Celková Zmluvná cena za dodanie Diela a za všetky súvisiace plnenia podľa tejto Zmluvy je nasledovná:

Cena bez DPH:	192 700,00 EUR
Sadzba DPH:	44 321,00 EUR
Cena s DPH:	237 021,00 EUR

(slovom: dvestotridsaťsedemtisícdvadsaťjeden EUR)

(ďalej aj ako „**Zmluvná cena**")

4.1.3 Zmluvná cena je cena maximálna a je totožná s cenou, ktorú Dodávateľ predložil vo svojej Ponuke Dodávateľa. Zmluvná cena je premietnutá v Cene Diela, ktorá tvorí Prílohu č. 2 Zmluvy. Zmluvná cena a Cena Diela zahŕňa všetky náklady nevyhnutné na riadne dodanie Diela a odstránenie všetkých vád, a zahŕňa v sebe všetky ostatné plnenia v rozsahu a na základe tejto Zmluvy, Špecifikácie predmetu Zákazky a Ponuky Dodávateľa. Zmluvná cena pokrýva všetky zmluvné záväzky a všetky povinnosti nevyhnutné pre riadne dodanie Diela, vrátane všetkých materiálov, súčiastok, cla, daní, personálneho zabezpečenia, dopravy a akýchkoľvek iných poplatkov, ktoré bude nutné vynaložiť podľa tejto Zmluvy.

4.1.4 Faktúru za Cenu za Dielo je Dodávateľ oprávnený vystaviť Objednávateľovi po dodaní a prevzatí predmetu Zmluvy v súlade s bodom 3.7 Zmluvy.

4.1.5 Faktúra doručená Objednávateľovi na zaplatenie bude obsahovať náležitosti podľa zákona č. 222/2004 Z. z. o dani z pridanej hodnoty v znení neskorších predpisov a musí obsahovať minimálne nasledovné údaje:

a) číslo faktúry;

b) identifikáciu Objednávateľa podľa Zmluvy;

c) identifikáciu Dodávateľa podľa Zmluvy (údaj o obchodnom mene, sídle alebo mieste podnikania, identifikačnom čísle, údaj o zápise v obchodnom registri alebo inej evidencii vrátane spisovej značky, ak je v nich Dodávateľ zapísaný, daňové identifikačné číslo a identifikačné číslo pre DPH);

d) označenie banky a čísla účtu, na ktorý ma byť platba zaplatená, vrátane konštantného a variabilného symbolu v súlade so Zmluvou;

e) deň vystavenia faktúry, deň splatnosti a deň dodania;

f) rozsah a druh plnenia;

g) základ dane;

h) výška dane;

i) celkovú čiastku vrátane DPH;

j) dôvod fakturácie s odkazom na Zmluvu;

k) názov Projektu;

l) akékoľvek ďalšie údaje vyžadované pre takéto doklady Právnymi predpismi;

4.1.6 Splatnosť každej faktúry podľa tejto Zmluvy je šesťdesiat (60) dní od doporučeného doručenia faktúry bez nedostatkov do sídla Objednávateľa v zmysle Zmluvy, a to bezhotovostným prevodom na účet Dodávateľa uvedený v záhlaví Zmluvy, pokiaľ nie je v zmluve uvedené inak.

4.1.7 Ak faktúra nebude obsahovať vyššie uvedené údaje alebo k nej nebudú priložené prílohy, alebo ak nebude obsahovať správne údaje, Objednávateľ je oprávnený takúto faktúru vrátiť Dodávateľovi spolu s označením nedostatkov, pre ktoré bola vrátená. V tomto prípade sa plynutie lehoty splatnosti takejto faktúry prerušuje a nová lehota splatnosti začne plynúť dňom nasledujúcim po dni doporučeného doručenia opravenej alebo doplnenej faktúry do sídla Objednávateľa.

4.2 Riziko a zodpovednosť za škodu

4.2.1 Dodávateľ zodpovedá bez obmedzenia za všetky škody, ktoré vzniknú jeho zavinením, ktoré vzniknú Objednávateľovi a iným osobám v Mieste plnenia, na samotnom Diele, na veciach, ako aj na osobách, pri prácach, ktorými bol poverený bez ohľadu na to, či tieto práce budú vykonané jeho zamestnancami alebo pracovníkmi, alebo ním poverenými Subdodávateľmi.

4.2.2 Škodou sa rozumie aj škoda spočívajúca v povinnosti Objednávateľa vrátiť časť nenávratného finančného príspevku na financovanie predmetu Diela Poskytovateľovi NFP, resp. sankcia uložená Objednávateľovi Poskytovateľom NFP v prípade, ak Dielo nebude vykonané riadne a/alebo v Lehote plnenia z dôvodov na strane Dodávateľa. Nárok na náhradu škody nevylučuje právo Objednávateľa uplatniť zmluvnú pokutu v súlade s podmienkami Zmluvy.

4.2.3 Škodou sa rozumie aj akákoľvek sankcia alebo pokuta uložená Objednávateľovi zo strany orgánov verejnej správy alebo orgánov štátnej správy za porušenia akýchkoľvek povinností súvisiacich s plnením Zmluvy, za ktoré nesie zodpovednosť Dodávateľ.

4.2.4 Dodávateľ odškodní Objednávateľa od všetkých nárokov, škôd, strát a nákladov v súvislosti s poškodením alebo stratou akéhokoľvek majetku, nehnuteľného alebo hnuteľného v rozsahu, v akom toto poškodenie alebo strata vyplýva z dôvodov Dokumentácie Dodávateľa, vyhotovenia alebo dodania Diela a odstránenia akýchkoľvek vád alebo ak sa dá pripísať akejkoľvek nedbanlivosti, úmyselnému činu alebo porušeniu Zmluvy Dodávateľom.

4.2.5 Dodávateľ nezodpovedá podľa tejto Zmluvy za nároky, škody, straty a náklady v prípadoch, kedy ich vznik možno pričítať okolnosti Vyššej moci. Za okolnosť Vyššej moci sa má namysli taká okolnosť, pri ktorej sú kumulatívne splnené všetky nižšie uvedené znaky:

a) je mimo kontroly Zmluvnej strany;

b) proti jej vzniku sa Zmluvná strana nemohla primerane zabezpečiť;

c) Zmluvná strana sa jej po jej vzniku nemohla primerane vyhnúť alebo ju prekonať; a zároveň

d) Zmluvná strana ju v čase uzavretia tejto Zmluvy objektívne nemohla predvídať.

(okolnosti podľa tohto bodu ďalej aj ako „**Vyššia moc**")

4.2.6 Kedykoľvek ktorákoľvek Zmluvná strana zistí akúkoľvek prekážku, ktorá jej bráni alebo je odôvodnené predpokladať, že jej bude brániť, v plnení akýchkoľvek povinností podľa tejto Zmluvy, najmä tak prekážku podľa bodu 4.2.5 a bodu 3.4.2 tejto Zmluvy, ale aj podľa akéhokoľvek iného ustanovenia tejto Zmluvy, je povinná jej vznik alebo existenciu bezodkladne písomne oznámiť druhej Zmluvnej strane. Pri riešení vzájomných nárokov spôsobených výskytom takýchto prekážok sú Zmluvné strany povinné postupovať vo vzájomnej súčinnosti tak, aby do najvyššej možnej miery zabránili následkom alebo zmiernili následky Vyššej moci.

4.3 Záručná doba a zodpovednosť za vady

4.3.1 Dodávateľ zodpovedá za zabezpečenie Záruky v súlade so Špecifikáciou predmetu zákazky. V prípade ak nie sú v Špecifikácii predmetu zákazky uvedené osobitné požiadavky na záruku, Dodávateľ poskytne záruku na tieto tovary v trvaní stanovenom výrobcom daného zariadenia, najmenej však 24 mesiacov. Záručná doba pri všetkých zariadenia začína plynúť prevzatím nainštalovaného zariadenia.

4.3.2 Výslovne sa dojednáva, že Dielo alebo ktorákoľvek časť Diela musia byť bez právnych vád. Existencia právnych vád predstavuje kritickú vadu. Za stav bez právnych vád sa na účely tejto zmluvy považuje situácia, kedy Dielo alebo časti Diela nie sú zaťažené právami tretích osôb, ktoré znemožňujú užívať Dielo alebo ktorúkoľvek jeho časť v súlade s touto zmluvou. V prípade, ak má Dielo a/alebo časť Diela právne vady, je Dodávateľ povinný tieto

nároky na vlastné náklady vysporiadať. V prípade ak sa tak nestane je povinný uhradiť Objednávateľovi všetky náklady s tým vzniknuté, vrátane trov právneho zastúpenia (účelne vynaložených).

4.4 Práva duševného vlastníctva a softwarové vybavenie

4.4.1 V prípade, že Dielo a/alebo akákoľvek časť predmetu plnenia podľa tejto Zmluvy, ktorá bude vytvorená a/alebo dodaná Dodávateľom alebo jeho zamestnancami na účely splnenia jeho záväzkov podľa tejto Zmluvy bude mať povahu autorského diela v zmysle Autorského zákona, tak Dodávateľ udeľuje Objednávateľovi v súlade s ustanovením § 65 a nasl. Autorského zákona licenciu, resp. sublicenciu na použitie takto chráneného autorského diela, a to nevýhradnú, neobmedzenú (bez časového a teritoriálneho obmedzenia) v rozsahu nevyhnutnom na riadne fungovanie a užívanie Diela prípadne inej časti plnenia Objednávateľom v súlade s účelom tejto Zmluvy. Za týmto účelom a v tomto rozsahu je Objednávateľ oprávnený udeliť sublicenciu tretím osobám. Zmluvné strany sa dohodli, že odmena Dodávateľa za poskytnutie licencie/sublicencie podľa tohto bodu 4.4 je zahrnutá v Cene Diela.

4.4.2 Dodávateľ prehlasuje, že dodaním (i) akéhokoľvek softwarového, či systémového vybavenia poskytnutého na základe tejto Zmluvy a (ii) akéhokoľvek technického alebo akéhokoľvek iného zariadenia alebo dokumentácie, ktoré je súčasťou Diela nedochádza k porušovaniu ani ohrozovaniu žiadnych práv duševného vlastníctva tretích osôb vrátane práv priemyselného vlastníctva a iných obdobných práv. Dodávateľ odškodní a ochráni Objednávateľa pred akýmikoľvek prípadnými nárokmi tretích strán voči Objednávateľovi v súvislosti s dodaním a prevádzkou Diela.

4.4.3 Dodávateľ sa zaväzuje, že zabezpečí akékoľvek a všetky potrebné licencie či iné súhlasy od akýchkoľvek, výrobcov a prevádzkovateľov systémov, softwarov, zariadení Diela, či akýchkoľvek iných osôb, potrebné pre riadne užívanie Diela.

4.4.4 Objednávateľ prevzatím Diela nepreberá žiadnu zodpovednosť za prípadne porušenie akýchkoľvek majetkových a/alebo autorských a priemyselných práv tretích osôb Dodávateľom v súvislosti s plnení tejto Zmluvy.

4.4.5 Dodávateľ sa zaväzuje Objednávateľa odškodniť pred každým nárokom tretej osoby z porušenia akéhokoľvek patentového práva, registrovaného návrhu, autorského práva, ochrannej známky, obchodného záväzku, obchodného tajomstva, alebo iných duševných a priemyselných práv súvisiacich s Dielom, ktorý vznikne z alebo v súvislosti s Dokumentáciou Dodávateľa, výrobou alebo vyhotovením Diela alebo používaním Diela Objednávateľom. Dodávateľ v plnej miere zodpovedá za škodu, ktorá Objednávateľovi vznikne v súvislosti s porušením akýchkoľvek povinností Dodávateľa podľa tohto bodu Zmluvy.

4.5 Zmluvné sankcie

4.5.1 V prípade, že nastane niektorá z nižšie uvedených okolností má Objednávateľ na základe faktúry nárok požadovať od Dodávateľa zaplatenie a Dodávateľ je v prípade uplatnenia takého nároku zo strany Objednávateľa povinný Objednávateľovi zaplatiť nasledovné zmluvné pokuty (pre vylúčenie pochybností, pre každý prípad, kedy nastane akákoľvek z nižšie uvedených okolností, t. j. kedykoľvek aj opakovane):

a) V prípade omeškania Dodávateľa s dodaním Diela v Lehote plnenia má Objednávateľ nárok na zaplatenie zmluvnej pokuty vo výške 0,05 % zo Zmluvnej ceny Diela, a to za každý aj začatý deň omeškania;

b) V prípade, ak Dodávateľ zadá určitú časť plnenia tejto Zmluvy Subdodávateľovi v rozpore s postupom podľa bodu 4.7 tejto Zmluvy má Objednávateľ nárok na zaplatenie zmluvnej pokuty vo výške 100.000,- EUR (slovom: stotisíc euro);

c) V prípade porušenia záväzku ochrany sprístupnených informácií/dát podľa bodu 4.10 má Objednávateľ nárok na zaplatenie zmluvnej pokuty vo výške 100.000,- EUR (slovom: stotisíc euro), a to za každé jednotlivé porušenie povinnosti mlčanlivosti podľa bodu 4.10 tejto Zmluvy.

4.5.2 V prípade omeškania Objednávateľa s úhradou faktúr má Dodávateľ nárok na zaplatenie úroku z omeškania vo výške 0,05 % z dlžnej sumy vrátane DPH za každý aj začatý deň omeškania.

4.5.3 Zaplatením zmluvnej pokuty na základe tejto Zmluvy nezaniká povinnosť splniť zabezpečený záväzok. Rovnako nezaniká ani nárok na náhradu škody príslušnej Zmluvnej strany, ktorá jej vznikne v súvislosti s porušením tejto Zmluvy v plnej výške a nie je dotknutý ani prípadný iný nárok na primerané zadosťučinenie, ktoré môže byť poskytnuté aj v peniazoch, či nárok na vydanie bezdôvodného obohatenia alebo iného nároku vyplývajúceho z akéhokoľvek právneho predpisu.

4.5.4 Splatnosť faktúry za zmluvnú pokutu vystavenej podľa tohto bodu bude minimálne sedem (7) kalendárnych dní.

4.6 Trvanie a ukončenie Zmluvy

4.6.1 Zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni kumulatívneho splnenia nasledovných podmienok:

- schválenie zmluvy zo strany Poskytovateľa NFP, t. j. a doručením stanoviska Poskytovateľa NFP a zároveň,
- zverejnenie tejto Zmluvy v Centrálnom registri zmlúv, vedenom Úradom vlády Slovenskej republiky v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a § 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.

4.6.2 Táto Zmluva trvá až do úplného splnenia všetkých vzájomných povinností a vysporiadania všetkých záväzkov Zmluvných strán na základe tejto Zmluvy, pokiaľ nedôjde k jej predčasnému ukončeniu v súlade s ustanoveniami tejto Zmluvy.

4.6.3 Táto zmluva zanikne okrem splnenia všetkých práv a povinností obidvoch Zmluvných strán aj písomnou dohodou Zmluvných strán alebo písomným odstúpením od Zmluvy jednej zo Zmluvných strán.

4.6.4 V prípade zániku zmluvy dohodou Zmluvných strán, táto zaniká dňom uvedeným v tejto dohode. Dohoda o ukončení Zmluvy musí byť písomná. V tejto dohode sa upravia aj vzájomné nároky Zmluvných strán, ktoré vzniknú z plnenia zmluvných povinností alebo z ich porušenia druhou Zmluvnou stranou ku dňu zániku Zmluvy dohodou.

4.6.5 V prípade odstúpenia od Zmluvy sa Zmluvné strany budú riadiť ustanoveniami § 344 a nasl. Obchodného zákonníka. Odstúpenie od Zmluvy musí mať písomnú formu, musí byť doručené druhej Zmluvnej strane (ktorá svoju povinnosť porušila) a je účinné dňom doručenia odstúpenia Zmluvnej strane, ktorá svoju povinnosť porušila.

4.6.6 Objednávateľ je oprávnený okamžite odstúpiť od Zmluvy v prípade podstatného porušenia Zmluvy Dodávateľom. Na účely tejto zmluvy sa za podstatné porušenie Zmluvy Dodávateľom považuje najmä, nie však výlučne:

a) ak sa preukáže, že Dodávateľ v Ponuke Dodávateľa predložil nepravdivé doklady alebo uviedol nepravdivé, neúplné alebo skreslené údaje;

b) ak Dodávateľ opustí Dielo alebo inak jasne prejavuje úmysel nepokračovať v konaní svojich povinností podľa Zmluvy (platí obdobne aj v prípade ak Dodávateľ tieto povinnosti plní iba vo veľmi obmedzenom rozsahu);

c) ak nedôjde k úspešnému absolvovaniu Funkčných skúšok, ani pri opakovaných Funkčných skúškach;

d) ak Dodávateľ postúpi Zmluvu bez súhlasu Objednávateľa;

e) ak je Dodávateľ v omeškaní s dodaním Diela v Lehote plnenia o viac ako 30 kalendárnych dní;

f) ak nastane iná okolnosť uvedená v tejto Zmluve oprávňujúca Objednávateľ odstúpiť od Zmluvy.

4.6.7 Objednávateľ môže odstúpiť od Zmluvy tiež v súlade s § 19 Zákona o verejnom obstarávaní.

4.7 Subdodávatelia

4.7.1 Dodávateľ je oprávnený plnením vybraných častí tejto Zmluvy poveriť svojich Subdodávateľov. Zoznam Subdodávateľov tvorí Prílohu č. 4 tejto Zmluvy. V zozname subdodávateľov sa uvádza podiel plnenia každého subdodávateľa vo finančnom vyjadrení z celkovej Ceny diela a údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia. Každý Subdodávateľ, ktorý má takú povinnosť, musí byť zapísaný v registri partnerov verejného sektora podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov.

4.7.2 V prípade, ak má počas plnenia Zmluvy Dodávateľ záujem zmeniť alebo doplniť svojich Subdodávateľov, je povinný rešpektovať nasledovné pravidlá:

a) Subdodávateľ, ktorého sa týka návrh na zmenu, a má takú povinnosť, musí byť zapísaný v registri partnerov verejného sektora podľa zákona č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov,

b) Subdodávateľ, ktorého sa týka návrh na zmenu, musí byť schopný realizovať príslušnú časť Diela v rovnakej kvalite, ako pôvodný Subdodávateľ a musí spĺňať rovnaké podmienky, ako pôvodný Subdodávateľ (ak boli stanovené),

c) Dodávateľ oznámi Objednávateľovi návrh na zmenu Subdodávateľa spolu s predložením dokladov preukazujúcich splnenie podmienok uvedených vyššie.

4.7.3 Návrh na zmenu subdodávateľa spolu s dokladmi podľa bodu 4.7.2c) vyššie a aktualizovaným znením Prílohy č. 4 musí Dodávateľ predložiť Objednávateľovi najneskôr tri (3) pracovné dni pred začatím plánovanej subdodávky. Objednávateľ má právo zmenu odmietnuť, ak nie sú splnené podmienky uvedené v bode 4.7.2 vyššie.

4.7.4 Pre vylúčenie pochybností sa Zmluvné strany dohodli, že z dôvodu zmeny alebo doplnenia Subdodávateľov podľa bodu 4.7 tejto Zmluvy je potrebné uzatvárať dodatok k tejto Zmluve.

4.7.5 V prípade, ak Dodávateľ využije na plnenie ktorejkoľvek povinnosti podľa tejto Zmluvy Subdodávateľa, Dodávateľ za konanie Subdodávateľa voči Objednávateľovi zodpovedá, ako keby plnenie vykonával sám.

4.8 Experti

4.8.1 Dodávateľ sa zaväzuje, že výkon vybraných odborných činností v rámci plnenia tejto Zmluvy bude vykonávať výlučne prostredníctvom expertov, prostredníctvom ktorých preukazoval splnenie podmienok účasti technickej spôsobilosti podľa Súťažných podkladov, a ktorých za týmto účelom identifikoval vo svojej Ponuke Dodávateľa (ďalej aj ako „**Experti**"). Zoznam jednotlivých Expertov s uvedením ich kvalifikácie a doklady preukazujúce ich kvalifikáciu tvoria obsah Prílohy č. 6 tejto Zmluvy.

4.8.2 V prípade, ak chce Dodávateľ nahradiť niektorého z Expertov, takéto nahradenie je možné výlučne so súhlasom Objednávateľa. Objednávateľ takýto súhlas bezdôvodne neodoprie, avšak platí, že novo navrhovaný Expert musí spĺňať rovnakú odbornú spôsobilosť, ako je spôsobilosť, ktorej splnenie preukazoval Expert, ktorý sa nahrádza. Spôsobilosť nového Experta Dodávateľ preukazuje spôsobom, akým preukazoval vo Verejnom obstarávní spôsobilosť Experta, ktorého chce Dodávateľ nahradiť.

4.8.3 Pre vylúčenie pochybností sa Zmluvné strany dohodli, že pre nahradenie Expertov nie je potrebné uzatvárať dodatok k tejto Zmluve, pokiaľ bude dodržaný postup podľa tohto bodu. Po zmene Experta Zmluvné strany aktualizujú Prílohu č. 6 a údaje o novom Expertovi.

4.9 Výzva na nápravu

Objednávateľ je oprávnený kontrolovať plnenie akýchkoľvek povinností Dodávateľa na základe tejto Zmluvy. Ak Dodávateľ porušuje alebo neplní akýmkoľvek spôsobom túto Zmluvu je Objednávateľ oprávnený vyzvať Dodávateľa, aby toto porušenie alebo neplnenie napravil v primeranej lehote na nápravu. Ak s prihliadnutím na dohodu Zmluvných strán nie je primeranou lehotou na nápravu iná lehota, platí, že primeranou lehotou na nápravu je desať (10) kalendárnych dní. Pokiaľ Dodávateľ nenapraví toto porušenie alebo neplnenie Zmluvy v lehote na nápravu určenej podľa tohto bodu, má Objednávateľ právo určiť Dodávateľovi náhradnú lehotu na nápravu. Pokiaľ Dodávateľ nenapraví toto porušenie alebo neplnenie Zmluvy ani v náhradnej lehote na nápravu určenej podľa tohto bodu, má Objednávateľ právo od tejto Zmluvy odstúpiť.

4.10 Mlčanlivosť

4.10.1 Zmluvné strany akceptujú a sú si vedomé skutočnosti, že v priebehu plnenia tejto Zmluvy môže Dodávateľ získať, alebo môžu mu byť poskytnuté informácie/dáta rôznej povahy o činnosti Objednávateľa, bezpečnostnej politike Objednávateľa, resp. niektoré z takto poskytnutých a/alebo sprístupnených informácií/dát za účelom plnenia jeho záväzku podľa tejto Zmluvy v podobe dokumentov, e-mailov či ústne poskytnutých, no nie len, ale najmä, môžu obsahovať informácie/dáta, ktoré si Objednávateľ želá, resp. je povinný utajiť predovšetkým z dôvodu ich

a) dôvernosti,
b) povinnosti ochrany podľa osobitného predpisu, t. j. napríklad, no nielen, zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
c) ale aj z iných dôvodov, ktoré nemusia byť Prijímajúcej strane známe;
d) ochrany, na ktorú je Objednávateľ povinný na základe akéhokoľvek zmluvného či iného právneho vzťahu.

4.10.2 Povinnosť mlčanlivosti sa vzťahuje predovšetkým, no nie však výlučne, na informácie/dáta, resp. iné skutočnosti týkajúce sa výskumných procesov Objednávateľa, a ktoré budú sprístupnené a/alebo poskytnuté Dodávateľovi.

Informácie/dáta, resp. dokumenty ich obsahujúce pritom môžu byť sprístupnené a/alebo poskytnuté v akejkoľvek podobe či forme, predovšetkým ústnej, elektronickej, písomnej, či elektronickej zachytené na akomkoľvek hmotnom, či nehmotnom substráte najmä, no nie výlučne, písomne alebo elektronicky, alebo zistené priamym poznaním pri dodaní Diela v Mieste plnenia, ktorú Objednávateľ odovzdá alebo iným spôsobom sprístupní za účelom definovanom v tejto Zmluve Dodávateľovi. Dodávateľ je zároveň povinný zachovávať mlčanlivosť ohľadne informácií/dát, ktoré obsahujú skutočnosti obchodnej, výrobnej alebo technickej povahy súvisiace s Objednávateľom, ktoré majú skutočnú alebo aspoň potenciálnu materiálnu alebo nemateriálnu hodnotu, nie sú v obchodných kruhoch bežne dostupné, sú utajené a chránené v zmysle § 17 a nasl. Obchodného zákonníka ako predmet obchodného tajomstva Objednávateľa alebo informácie označené ako dôverné, ktoré nesmie strana, ktorej sa tieto informácie poskytli, prezradiť tretej osobe a ani ich použiť v rozpore s ich účelom pre svoje potreby a sú chránené v zmysle § 271 Obchodného zákonníka.

4.10.3 Pod predmet ochrany nespadajú informácie/dáta,

a) ktoré sú všeobecne známe;
b) ktoré v čase uzavretia tejto Zmluvy sú, alebo po uzavretí tejto Zmluvy sa bez porušenia tejto Zmluvy stali bežne dostupnými v príslušných obchodných kruhoch alebo vo verejnosti;
c) o ktorých Dodávateľ bezpochyby preukáže, že s nimi disponoval v čase uzavretia Zmluvy, resp. pri ich poskytnutí a/alebo ich vypracoval samostatne a bez využitia predmetu ochrany;
d) informácie poskytnuté v nevyhnutnom rozsahu príslušným orgánom v rámci plnenia zákonných povinností, pričom prekročenie nevyhnutného rozsahu poskytnutých informácií je sankcionované rovnako ako porušenie ochrany informácií/dát podľa tejto Zmluvy.

4.10.4 Dodávateľ využije získané informácie/dáta len na účely dodania Diela. Dodávateľ nie je oprávnený poskytnúť informácie/dáta tvoriace predmet ochrany inej osobe bez predchádzajúceho osobitného, písomného súhlasu Poskytujúcej strany. Na udelenie takéhoto súhlasu nemá Dodávateľ právny nárok.

4.10.5 Ak je Dodávateľ nútený na účely realizácie Diela informácie/dáta sprístupniť ďalšej osobe, je povinný oboznámiť všetky tieto osoby, so svojimi povinnosťami a záväzkami prevzatými touto Zmluvou a zaviazať ich na dodržiavanie obmedzení používania informácií/dát tvoriacich predmet ochrany v rovnakom rozsahu v akom sa vzťahujú na Dodávateľa. V prípade porušenia záväzku mlčanlivosti osobami, ktorým Dodávateľ informácie/dáta tvoriace predmet ochrany podľa 4.10.2 sprístupnil alebo akýmkoľvek iným spôsobom poskytla, zodpovedá Dodávateľ rovnako ako keby povinnosť mlčanlivosti porušil sám.

4.10.6 Dodávateľ sa zaväzuje oboznámiť a následne zabezpečiť od svojich zamestnancov a/alebo subdodávateľov realizujúcich predmet plnenia Zmluvy dodržiavanie povinností podľa tohto bodu 4.10 Zmluvy, a to aj po skončení ich pracovného alebo služobného pomeru alebo iného vzájomného zmluvného vzťahu. Uvedenú povinnosť sa Dodávateľ zaväzuje zabezpečiť podpísaním vyhlásenia o mlčanlivosti zo strany príslušného zamestnanca a/alebo subdodávateľa.

4.10.7 Všetky podklady a informácie poskytnuté Dodávateľovi musia byť po ukončení plnenia predmetu Zmluvy bez vyzvania odovzdané Objednávateľovi alebo podľa jeho rozhodnutia vymazané alebo skartované. Táto povinnosť sa vzťahuje aj na vyhotovené kópie. Toto ustanovenie neplatí v prípade vzájomných zmlúv a projektovej dokumentácie medzi Zmluvnými stranami, ktoré ale nesmú byť bez súhlasu Objednávateľa sprístupnené tretej strane.

4.11 Komunikácia

4.11.1 Zmluvné strany sa dohodli, že všetky oznámenia, požiadavky, žiadosti a akákoľvek iná komunikácia, ktorá má byť podľa tejto Zmluvy písomná sa bude doručovať doporučene poštovou zásielkou, kuriérom prípadne inou formou registrovaného poštového styku alebo osobne ak nie je v Zmluve výslovne dohodnutá aj iná možnosť doručovania (napr. email). Za deň doručenia sa považuje deň prevzatia písomnosti, ak nie je v Zmluve dohodnuté inak. V prípade, ak adresát odmietne písomnosť prevziať, za deň doručenia sa považuje deň odmietnutia prevzatia písomnosti. V prípade, ak si adresát neprevezme písomnosť v úložnej dobe na pošte, za deň doručenia sa považuje posledný deň úložnej doby na pošte. V prípade, ak sa písomnosť vráti odosielateľovi s označením pošty „adresát neznámy" alebo „adresát sa odsťahoval" alebo s inou poznámkou podobného významu, za deň doručenia sa považuje deň vrátenia zásielky odosielateľovi.

4.11.2 Akákoľvek komunikácia podľa bodu 4.11.1 vyššie bude adresovaná a doručovaná na kontaktné údaje strán uvedené v záhlaví tejto Zmluvy, poprípade na kontaktné údaje, ktoré si Zmluvné strany písomne oznámia.

4.12 Spoločné a záverečné ustanovenia

4.12.1 Práva a povinnosti Zmluvných strán neupravené v tejto Zmluve sa riadia výlučne príslušnými ustanoveniami Obchodného zákonníka a ostatných všeobecne záväzných Právnych predpisov platných a účinných v Slovenskej republike. Zmluvné strany sa dohodli, že v prípade vzniku sporov Zmluvných strán týkajúcich sa tejto Zmluvy a jej aplikácie, ak sa ich nepodarí urovnať iným spôsobom a jednou zo Zmluvných strán je zahraničný subjekt, je daná právomoc súdov Slovenskej republiky, ktoré budú rozhodovať podľa Civilného sporového poriadku.

4.12.2 Dodávateľ nie je oprávnený postúpiť akékoľvek pohľadávky (práva) vyplývajúce z tejto Zmluvy na tretiu osobu alebo sa dohodnúť s treťou osobou na prevzatí jeho záväzkov (povinností) vyplývajúcich z tejto Zmluvy bez predchádzajúceho písomného súhlasu Objednávateľa.

4.12.3 Z dôvodu, že predmet plnenia bude čiastočne financovaný z prostriedkov poskytnutých Objednávateľovi na základe Zmluvy o NFP, zaväzuje sa Dodávateľ strpieť výkon kontroly/auditu súvisiaceho s dodávaným Dielom kedykoľvek počas platnosti a účinnosti Zmluvy o NFP, a to oprávnenými osobami na výkon tejto kontroly/auditu a poskytnúť im všetku súčinnosť. Oprávnené osoby na výkon kontroly/auditu sú najmä:

a) Poskytovateľ NFP a ním poverené osoby,
b) Útvar vnútorného auditu Riadiaceho orgánu alebo Sprostredkovateľského orgánu a nimi poverené osoby,
c) Najvyšší kontrolný úrad SR a ním poverené osoby,
d) Orgán auditu, jeho spolupracujúce orgány (Úrad vládneho auditu) a osoby poverené na výkon kontroly/auditu,
e) splnomocnení zástupcovia Európskej Komisie a Európskeho dvora audítorov,
f) Orgán zabezpečujúci ochranu finančných záujmov EÚ,
g) osoby prizvané orgánmi podľa písm. a) - f) tohto bodu v súlade s príslušnými Právnymi predpismi.

V tejto súvislosti sa výkon kontroly môže vzťahovať aj na Dodávateľa a prípadne i jeho subdodávateľov.

4.12.4 Zmluva je vyhotovená v štyroch (4) rovnopisoch, pričom Objednávateľ obdrží dva (2) rovnopisy a Dodávateľ obdrží dva (2) rovnopisy.

4.12.5 Zmluvné strany berú na vedomie a podpisom tejto Zmluvy potvrdzujú, že sú plne oboznámené so skutočnosťou, že predmet tejto Zmluvy je poskytovaný v súvislosti s realizáciou aktivít Projektu a napĺňajú sa ciele Programu Slovensko 2021-2027 podľa čl. 21 až 23 Nariadenia 2021/1060, ktorý je spolufinancovaný zo zdrojov EÚ.

4.12.6 Zmluvné strany berú na vedomie, že zmena Zmluvy je možná len v súlade s § 18 Zákona o verejnom obstarávaní, a to za predpokladu, že sa nezmenia záväzky Dodávateľa, ku ktorým sa zaviazal v Ponuke. Prípadná zmena tejto Zmluvy je možná len písomnou dohodou Zmluvných strán, a to vo forme číslovaných dodatkov podpísaných oprávnenými zástupcami oboch Zmluvných strán.

4.12.7 Ak niektoré ustanovenia tejto Zmluvy nie sú celkom alebo sčasti účinné alebo platné alebo neskôr stratia účinnosť alebo platnosť, nie je tým dotknutá účinnosť a platnosť ostatných ustanovení. Ak sa niektoré z ustanovení tejto Zmluvy stane neplatným z dôvodu rozporu s Právnymi predpismi, zaväzujú sa Zmluvné strany takéto ustanovenie nahradiť iným, primerane zodpovedajúcim Právnemu významu pôvodného ustanovenia a zmyslu a účelu tejto Zmluvy.

4.12.8 Zmluvné strany vyhlasujú, že sa s obsahom Zmluvy oboznámili, túto uzatvorili slobodne a vážne, že sa zhoduje s ich prejavom vôle a svoj súhlas s jej obsahom potvrdzujú vlastnoručným podpisom.

4.12.9 Neoddeliteľnou súčasťou zmluvy sú prílohy:

Príloha č. 1 Špecifikácia predmetu Zákazky *Príloha č. 1 – Výzvy na predloženie cenovej ponuky]*
Príloha č. 2 Cena Diela *[Príloha č. .2 Výzvy na predloženie cenovej ponuky - predloží uchádzač vo svojej ponuke]*
Príloha č 3 Plán dodania Diela *[Odovzdá Dodávateľ v súlade s bodom 3.5 Zmluvy po podpise tejto Zmluvy]*
Príloha č. 4 Zoznam Subdodávateľov *[predloží úspešný uchádzač najneskôr pri podpise Zmluvy]*
Príloha č. 5 Ponuka Dodávateľa *[Podrobný opis ponúkaného predmetu plnenia - predloží uchádzač vo svojej ponuke]*
Príloha č. 6 Zoznam Expertov *[predloží úspešný uchádzač vo svojej ponuke]*

Objednávateľ
V Trenčíne
Dňa 19. 6. 2025

doc. Ing. Jozef Habánik, PhD.
rektor TnUAD

Trenčianska univerzita
Alexandra Dubčeka v Trenčíne
Študentská 2
911 50 Trenčín

Dodávateľ
V *Bratislava*
Dňa 10.06.2025

Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Príloha č. 1 Špecifikácia predmetu Zákazky

Špecifikácia predmetu zákazky - položka: Dátové úložisko pre potreby záložnej a archivačnej kópie

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĽŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu **TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky**		
Položka predmetu zákazky - Dátové úložisko pre potreby záložnej a archivačnej kópie požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Dátové úložisko pre potreby záložnej a archivačnej kópie)**	**Doplňujúce informácie**
1	Prevedenie	Rackmount
2	Dual kontroler prevedenie v režime active-active s „controller failover"	Diskové pole nesmie obsahovať žiadny SPOF. Redundantné napájanie pre každý modul vrátane kontrolerov.
3	Pripojiteľnosť k existujúcej infraštruktúre diskových polí	Verejný obstarávateľ v súčasnosti prevádzkuje diskové polia NetApp s operačným systémom ONTAP. Vyžaduje sa plná kompatibilita s existujúcimi diskovými poľami – najmä s možnosťou využitia replikácie a vytvárania záloh medzi existujúcim a novým prostredím priamo využitím funkcionalít OS ONTAP.
4	Unified diskové úložisko podporujúce ako sieťové, tak blokové protokoly v rámci jedného kontroleru. Riešenie pridaním tzv. "NAS" gateway nebude akceptované	Áno
5	Plná virtualizácia poľa, vrátane portov (Možnosť vytvárania „virtuálnych diskových polí" s priradením logických portov a definovanými QoS).	Min 250 virtuálnych diskových polí (VDP). Možnosť bezodstávkového presúvania VDP aj logických portov medzi jednotlivými HW kontrolermi transparentne voči aplikáciám.
6	Pamäť systému	Min 32GB/Ctrl ochrana batériou pre prípad výpadku napájania,
7	On board flash cache	áno
8	Spôsob pripojenia on board cache	NVMe M.2
9	Veľkosť on board flash	Min. 2 TiB
10	Možnosť využitia SSD ako dodatočnú cache	Áno - min. do veľkosti 22 TiB
11	Architektúra	PCIe Gen 3 12Gb SAS-3 architektura
12	Počet diskových pozícií	Min. 24, rozšíriteľnosť minimálne na 144 ks diskov pre jeden HA pár kontrolerov.
13	Rozhranie pre pripojenie diskov	SAS-3, 12 Gbps, PCIe Gen 3 alebo rýchlejšie

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie		
áno/nie		
áno/nie		
áno/nie		
hodnota		
hodnota		
áno/nie		
áno/nie		
hodnota		
áno/nie		
áno/nie		
hodnota		
áno/nie		

14	Podporované disky	2,5" HDD/SSD, 3,5" NL-SAS/SSD	áno/nie		
15	Požadovaný počet diskov	24 x 1,8TB SAS	hodnota		
16	Podporované RAID	RAID-4, RAID-DP (RAID-6), RAID-TEC (alebo podobná ochrana proti výpadku 3 diskov súčasne v tej istej RAID skupine)	áno/nie		
17	Požiadavky na RAID skupiny	SAS/SSD – ochrana proti výpadku min 2 diskov so zápisom bez RAID penalty – obdobne ako RAID10 NL-SAS ochrana proti výpadku min 3 diskov	áno/nie		
18	Podpora pre volumy do veľkosti	Aspoň 100 TiB	hodnota		
19	Možnosť pridávania ďalších kontrolerov a kapacity. Pridávané kontrolery môžu byt aj odlišného typu ako je požadovaný	Áno. Pre NAS min. 24 kontrolerov. Pre SAN min. 12 kontrolerov. Pridávanie a odoberanie kontrolerov je možné počas plnej prevádzky diskového poľa bez potreby odstávky.	áno/nie		
20	Podporované protokoly	FC; FCoE; iSCSI; NFS; pNFS; CIFS/SMB, S3	áno/nie		
21	Požadovaná pripojiteľnosť k hostom	Min. 8 portov 10Gb s káblami Twinax	hodnota		
22	Škálovateľnosť pripojenia k hostom	možnosť zmenit výmenou na porty 16GbE možnosť kombinovať porty FC 16Gb/10GbE	áno/nie		
23	Napájacie káble	rack káble, C14-C13 koncovka	áno/nie		
24	Podporované funkcionality	Možnosť vytvárania priestorovo efektívnych snapshotov a klonov s možnosťou vytvárania viacerých konzistentných skupín na úrovni jednotlivých aplikácií	hodnota		
25	Podpora sync a async replikácie	Áno	áno/nie		
26	Podpora Geo clustera cez IP	Áno	áno/nie		
27	Licenčné pokrytie	Funkcionalitu poskytuje s kapacitne a časovo neobmedzeným licenčným pokrytím. Možnosť vytvárania väčších LUN ako 2TB, pričom uvedenú funkcionalitu poskytuje s kapacitne, časovo neobmedzenou licenciou	áno/nie		
28	Bezodstávková prevádzka	Diskové pole musí umožňovať upgrade firmware diskového poľa (vrátane firmware diskov) bez odstávky diskového poľa.	hodnota		
29	Bezodstávkové presúvanie dát	Zariadenie musí dovoliť presúvať dátové volumy a LUNy medzi rôznymi skupinami diskov, bez ohľadu na to, akým protokolom sú dáta sprístupňované. Presuny musia byť transparentné voči pripojeným aplikáciám a serverom, t.j. celá činnosť musí byť bez dopadu na servery a aplikácie.	áno/nie		
30	Podpora cachingu medzi SSD a HDD	Áno, na celú ponúkanú kapacitu.	áno/nie		
31	Thin Provisioning vrátane zero detect space reclamation.	Áno, bez potreby externej aplikácie.	áno/nie		
32	Podpora snapshotov	1023 per volume	hodnota		
33	Fast Drive Zeroing	Áno	áno/nie		
34	Podpora QoS	Áno	áno/nie		

35	Podpora SMB Multichannel	Áno	áno/nie		
36	Microsoft VSS support	Áno	áno/nie		
37	Plná VAAI podpora (vStorage API for Array Integration)	Áno	áno/nie		
38	Podpora WORM funkcie bez potreby externej aplikácie	Áno	áno/nie		
39	Podpora vytvárania Backup využitím prostriedkov poľa bez potreby externej aplikácie.	Áno	áno/nie		
40	Natívna možnosť integrácie do cloudového prostredia pre Google, AWS, Azure. Podpora vytvárania DR lokalít v cloudovom prostredí. Podpora pre spustenie virtuálneho diskového poľa v privátnom cloude s podporou vzájomnej replikácie využitím SW prostriedkov poľa.	Áno	áno/nie		
41	Backup do cloudoveho prostredia pomocou snapshotov	Áno	hodnota		
42	Podpora automatického vyhodnocovania a presúvania nepoužívaných dát do privátneho cloudu (cloud tiering) pre SSD	Áno	áno/nie		
43	Plná podpora „HW a SW Data At Rest Encryption"	Áno, s možnosťou použitia ako interného („OnBoard"), tak aj externého key manageru	áno/nie		
44	Deduplikácia,komprimácia a kompakcia dát	Áno, na celú ponúkanú kapacitu.	áno/nie		
45	Podpora RBAC	Áno	áno/nie		
46	Podpora Nativnej ochrany poľa proti Ramsomware.	Áno	áno/nie		
47	Integrácia do aplikačného prostredia	Minimálne VMware, SQL, Oracle, Splunk, Docker, Active Directory	áno/nie		
48	Funkcia File servera	Na úrovni NAS schopnosť poskytovať služby file servera s integráciou do MS Active Directory	áno/nie		
49	Popora operačných systémov:	Minimálne Windows® 2000, Windows Server® 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Linux®, Oracle® Solaris, AIX, HP-UX, Mac® OS, VMware®, ESX®	áno/nie		
50	Napájanie a chladenie	Plne redundantné, zdroje a ventilátory typu hot-swap	áno/nie		
51	Požiadavky na tovar / dodávku	Dodaný tovar bude nový, nepoužitý, nerepasovaný. Dodávateľ preukáže, že dodaný tovar pochádza z predajného kanála autorizovaného výrobcom.	áno/nie		
52	Výrobca diskového poľa musí byť zároveň výrobcom jeho obslužného softvéru (operačného systému).	Áno	áno/nie		
53	Podpora výrobcu	„call home" podpora výrobcu diskového poľa. Proaktívny monitoring stavu kapacitného a výkonového vyťaženia, upozornenia na dostupné updaty a bugfixy. Automatizovaná emailová notifikácia pri poruchách jednotlivých komponentov. Automatizované otváranie ticketov pri poruchách. Informácie o stave diskového poľa a o dostupnosti aktualizácií a proaktívnych notifikácií prostredníctvom mobilnej aplikácie.	áno/nie		
54	Kompatibilita	Z dôvodu ochrany investície sa vyžaduje dodanie rozširúcej diskovej police s diskami pre pripojenie k existujúcemu diskovému poľu NetApp FAS2552.	áno/nie		

Osobitné požiadavky na plnenie:				**Osobitné požiadavky na plnenie:**		
55	Servisná podpora na hardvér aj softvér diskového poľa priamo od výrobcu diskového poľa počas trvania 2 roky a s doručením pokazeného komponentu nasledujúci pracovný deň	Záruka, SLA		áno/nie		
56	Implementačné a konfiguračné práce v rozsahu 10 MD	Práce		áno/nie		
57	2 ročná licencia zabezpečujúca záruku a prémiovú technickú podporu 24x7	Licencia		áno/nie		

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

Špecifikácia predmetu zákazky - položka: Vypracovanie kompletných podrobných plánov kontinuity prevádzky 3 systémy. Vypracovanie postupov zálohovania na obnovu siete a informačného systému

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné uchádzačom ponúkaný produkt musí SPĽŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu **TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky**	
Položka predmetu zákazky - Vypracovanie kompletných podrobných plánov kontinuity prevádzky 3 systémy. Vypracovanie postupov zálohovania na obnovu siete a informačného systému požadovaný počet: 40 človekohodín	
P. č.	**Parameter/časť položky**
1	Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu s ohľadom na relevantnú legislatívu vzťahujúcu sa na BCM: Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe , Vyhláška č. 179/2020 Z. z..
2	Vypracovanie dekompozície dôležitých služieb a vypracovanie BIA pre tieto služby, resp. systémy. Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP pre tri vybrané kritické systémy, bude obsahovať krízové plány na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu na základnú službu, plány havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu, postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej:
3	• frekvenciu a rozsah jej dokumentovania a schvaľovania,
4	• určenie osoby zodpovednej za zálohovanie,
5	• časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní,
6	• požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom,
7	• požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,
8	• požiadavku na vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov.
9	Kľúčové kapitoly BCM plánu:
10	• Účel a rozsah BCM v ktorom budú zadefinované ciele a rozsah pôsobnosti v rámci organizácie
11	• Identifikácia kritických procesov (BIA), ktoré môžu mať vplyv na chod organizácie
12	• Hodnotenie a riadenie rizík potenciálnych hrozieb a zraniteľností, ktoré môžu ovplyvniť kontinuitu činností.
13	• Vypracovanie stratégií obnovy (DRP) v ktorom budú zadefinované postupy na obnovu prevádzky a služieb po incidente.
14	• Implementácia komunikačného plánu s definovaním interných a externých komunikačné kanálov a zodpovedností počas krízových situácií.
15	• Pravidelné testovanie a aktualizácia plánu, zadefinovanie časových rámcov a intervalov
16	• Riadenie zdrojov pre kontinuitu prevádzky s opisom personálnych, finančných a technických zdrojov na zvládanie kríz.

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		

.....

Špecifikácia predmetu zákazky - položka: Next generation firewall

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĽŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky		
Položka predmetu zákazky - Next generation firewall požadovaný počet: 2 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Next generation firewall)**	**Doplňujúce informácie**
1	HW appliance NGFW/UTM firewallu v režime vysokej dostupnosti (dve fyzické zariadenia rovnakého typu zapojené do funkčného clustra); Platforma postavená na HW akcelerovanej architektúre (t.j. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií ; HW appliance do racku s veľkosťou 1RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu; Možnosť doplniť druhý napájací zdroj (interný alebo externý), alebo zariadenie vybavené dvoma zdrojmi;	
2	Rozhrania na každom firewalle využiteľné pre management	min. 2x GE RJ45
3	Rozhrania na každom firewalle využiteľné pre spracovanie komunikácie	min. 18x GE RJ45 Ports, 8x GE SFP Slots, 8x 10 GE SFP+ Slots
4	Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky.	
5	Podpora VLAN	min. 4000
6	Podpora LACP	
7	Počet FW pravidel	min. 8000
8	Možnosť definície FW pravidel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je:	min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.
9	Celková priepustnosť firewallu	min. 79.5 / 78.5 / 70 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B)
10	Latencia firewallu	nepresahuje 5 µs (merané na malých UDP paketoch (64B))
11	Počet nových spojení za sekundu (setup-rate)	min. 480 000
12	Celkový počet súčasných TCP spojení firewallu	min. 7 500 000
13	PPS (počet spracovaných paketov za 1 sekundu)	min. 45 000 000
14	Funkcia detekcie aplikácií na L7 (Application Control)	
15	Detekcia známych aplikácií na základe signatúr	min 3500 preddefinovaných aplikácií/signatúr

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie		
hodnota		
hodnota		
áno/nie		
hodnota		
áno/nie		
hodnota		
áno/nie		
hodnota		
hodnota		
hodnota		
hodnota		
hodnota		
áno/nie		
hodnota		

16	pre populárne cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii)		áno/nie		
17	aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu		áno/nie		
18	priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response)	min. 27 Gbps	hodnota		
19	podpora použitia Application control aj formou profilov priradených k pravidlám		áno/nie		
20	Funkcie detekcie a zamedzenia narušení (IPS/IDS)		áno/nie		
21	počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom	min. 11000	hodnota		
22	funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám		áno/nie		
23	možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS		áno/nie		
24	priepustnosť funkcie IPS vrátane logovania	min. 12 Gbps	hodnota		
25	Funkcie antivírovej kontroly		áno/nie		
26	Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom		áno/nie		
27	AV kontrola rozšírená o inšpekciu tzv. sandbox technikou	Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky	áno/nie		
28	Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním	min. 9 Gbps	hodnota		
29	Podpora služby výrobcu umožňujúca detekovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hash-ov		áno/nie		
30	Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky		áno/nie		
31	Podpora SSL dešifrovania/SSL inšpekcie	min. 8 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou)	hodnota		
32	Funkcia DNS filtra		áno/nie		
33	Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii		áno/nie		
34	Možnosť definovať vlastný tzv. blacklist domén		áno/nie		
35	Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL		áno/nie		
36	Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos		áno/nie		
37	Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri		áno/nie		
38	Podpora SSL VPN		áno/nie		
39	Priepustnost SSL VPN	min. 3,5 Gbps	hodnota		
40	Popora IPSEC VPN v režime site-2-site aj client-2-site		áno/nie		
41	Priepustnosť IPSEC VPN (AES256-SHA256, UDP packet size 512B)	min. 55 Gbps	hodnota		
42	Podpora izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod.		áno/nie		
43	FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu;		áno/nie		

44	Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky		áno/nie		
45	Podpora SNMP vrátane SMPB MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete		áno/nie		
46	Požaduje sa certifikácia ICSA Labs minimálne pre Firewall		áno/nie		
47	Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať.		áno/nie		
48	Možnosť kombinovať akcie pre automatizačné pravidlá	min. webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy.	áno/nie		
49	Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel	min. schopnost parsovat vstupy z logov a z predchádzajúcich vykonaných akcií	áno/nie		
50	Podpora otvoreného API pre ďalšie možnosti integrácie		áno/nie		
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
52	2 roky priamo od výrobcu zariadenia, odozva najneskôr do 4h od nahlásenia, vrátane víkendov a sviatkov. Servis bude poskytovaný v mieste inštalácie. Nahlasovanie poruchy v režime 24x7. Nahlasovanie porúch priamo u výrobcu zariadenia. .	Záruka	áno/nie		
53	Implementačné a konfiguračné práce s otestovaním, zaškolením a dokumentáciou riešenia, Implementácia MFA pre vzdialený prístup do siete v rozsahu 18 človekohodín	Práce	áno/nie		
	Implementačné práce pre MFA Implementačné práce pre nasadenie MFA na navrhovaných technológiách s existujúcim systémom M365 pre všetkých užívateľov s vytvoreným VPN pripojením :		áno/nie		
	Analýza a identifikácia požiadaviek: o Analýza existujúcej infraštruktúry a identifikácia systémov, kde bude MFA nasadené. o Definovanie bezpečnostných požiadaviek a politík prístupu.		áno/nie		
	Nasadenie MFA na next generation firewall: o Konfigurácia autentifikátora ako zdroja MFA. o Nastavenie RADIUS servera pre autentifikáciu používateľov. o Aktivácia MFA na SSL VPN, IPsec VPN a administrátorských prístupoch. o Testovanie funkčnosti MFA s rôznymi scenármi prístupu.		áno/nie		
	Nasadenie MFA na Microsoft 365: o Aktivácia MFA v Microsoft 365 Admin Centre. o Konfigurácia Conditional Access Policies pre riadenie prístupov. o Registrácia používateľských zariadení pre MFA (mobilné aplikácie, SMS, e-mail). o Testovanie prihlásení a overenie správnosti nastavení.		áno/nie		
	Vzdelávanie a podpora: o Školenie zamestnancov o používaní MFA a postupoch v prípade problémov s prístupom. o Vytvorenie dokumentácie s postupmi pre koncových používateľov.		áno/nie		
	Monitorovanie a optimalizácia: o Pravidelné monitorovanie prístupových logov a analýza bezpečnostných incidentov. oÚprava politík na základe spätnej väzby a nových bezpečnostných požiadaviek		áno/nie		
54	1 ročná licencia zabezpečujúca záruku a prémiovú technickú podporu 24x7 a nasledovné služby aktualizácií firmware, a komponentov a služieb firewallu ako (IPS, Advanced Malware Protection, aplikačná kontrola, Web a Video filtrovanie, Antispam služba)	Licencia	áno/nie		

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

Špecifikácia predmetu zákazky - položka: Dohľadový nástroj na hranici siete

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vyplňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky		
Položka predmetu zákazky - Dohľadový nástroj na hranici siete požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Dohľadový nástroj na hranici siete**	**Doplňujúce informácie**
1	Systém pre ukladanie a koreláciu logov v sieti obstarávateľa.	
2	Systém musí byť plne kompatibilný s dodávanými riešeniami pre NGFW/UTM, Switche, 2FA AUTHENTICATION, Mailova ochrana, Sandbox riesenie	
3	Riešenie vo forme subskribcnej licencie	
4	Schopnost spracovávať logy v objeme GB/deň	min. 5 GB za deň
5	Možnosť škálovateľného navýšenia objemu spracovávaných logov pomocou licencií	
6	Podpora SYSLOG, podpora šifrovaného prenosu dát/logov	
7	Riešenie musí obsahovať konfigurovateľné prehľady s drill down funkcionalitou	
8	Filtrovanie správ/logov na základe roznych parametrov, ich kombinácií. Podpora AND, OR logiky pri vytváraní filtrov	
9	Možnosť ukladania definícií filtrov pre rýchle opätovné použitie	
10	Možnosť prehliadania logov v historickom alebo realtime režime	
11	Možnosť zobrazovania logov v RAW alebo štruktorovanom formáte	
12	Korelácia logov	
13	Možnosť automatického vytvárania incidentov	
14	Možnosť automatického vyšetrovania incidentov pomocou definovateľných playbookov	
15	Podpora Indication of Compromise - Systém musí obsahovať reputačné databázy nebezpečných IP/URL adries a musí vykonávať spätné prehľadávanie historických logov pri update reputačných DB za účelom detekcie napadnutia systémov a koncových staníc	min. 7 dní do minulosti
16	Licencia umožňuje ďalšiu automatizáciu reakcií na incidenty s vylepšeným monitorovaním a eskaláciou, vstavanými pracovnými postupmi správy incidentov, konektormi, príručkami	
17	Licencia poskytuje automatické sťahovanie balíkov obsahu na detekciu najnovšieho malvéru, vrátane súhrnu prepuknutia a mapovania reťazca utoku, aby sa zistilo, ako malvér funguje. Licendia dalej obsahuje správu o vzniku utoku, detail udalosti a šablónu správy o detekovani vzniku utoku	
18	Podpora vytvárania reportov v formátoch PDF, HTML, CSV, XML	
19	Možnosť generovania reportov v pravidelných intervaloch	
20	Možnosť vytvárania vlastných požiadaviek voči databáze a ich použitie ako zdroj dát v reportoch	
21	Podpora SNMP	
22	Podpora REST API	
23	GUI a CLI administračné rozhranie dostupné pomocou HTTPS a SSH protokolov	
24	Podpora LDAP, RADIUS, Tacacs+ pre administrátorské účty	
Osobitné požiadavky na plnenie:		
25	Inštalácia na zdrojoch poskytnutných obstarávateľom v rozsahu 2 človekodní Zoznam implementačných prác pre nasadenie dohľadového nástroja na hranici siete Analýza požiadaviek a plánovanie: o Zhodnotenie existujúcej infraštruktúry, bezpečnostných potrieb a požiadaviek na logovanie. Príprava prostredia: o Overenie virtuálnych zdrojov potrebných pre inštaláciu dohľadového nástroja na hranici siete. Inštalácia dohľadového nástroja na hranici siete: o Nasadenie dohľadového nástroja vo virtuálnom prostredí (VMware, Hyper-V). Základná konfigurácia systému: o Nastavenie sieťových parametrov (IP adresy, DNS, NTP), zabezpečenie prístupov a definovanie admin účtov. Integrácia s kompatibilnými zariadeniami: o Konfigurácia dodaných NGFW a iných zariadení na odosielanie logov do dohľadového nástroja na hranici siete. Nastavenie politiky uchovávania logov: o Definovanie retenčných politik pre efektívne spravovanie dát a súlad s legislatívou. Konfigurácia analýzy a reportingu: o Vytvorenie prispôsobených dashboardov, reportov a upozornení pre sledovanie incidentov. Bezpečnostné opatrenia: o Nastavenie šifrovania logov, správa prístupových práv a implementácia autentifikačných mechanizmov. Testovanie a validácia: o Overenie funkčnosti prenosu logov, správnosti reportov a výkonu systému. Školenie administrátorov a používateľov: o Zaškolenie tímu na správu dohľadového nástroja na hranici siete, tvorbu reportov a riešenie incidentov. Dokumentácia: o Vypracovanie technickej a prevádzkovej dokumentácie pre budúcu správu systému.	Práce
26	1 ročná subscription licencia zabezpečujúca záruku a technickú podporu	Licencia

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie		
áno/nie		
áno/nie		
hodnota		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
hodnota		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
Osobitné požiadavky na plnenie:		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

Špecifikácia predmetu zákazky - položka: Sonda detekcie a prevencie prieniku - HW + licencia

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu

TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky

Položka predmetu zákazky - Sonda detekcie a prevencie prieniku - HW + licencia
požadovaný počet: 1 ks

P. č.	Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Sonda detekcie a prevencie prieniku - HW + licencia)	Doplňujúce informácie	Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke parametre ponúkaného produktu (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov" – Požadovaný formát ponúkaných parametrov	1. TU UVEĎTE ponúkané parametre	POZNÁMKA (napr. doplňujúce informácie k uvedeným parametrom a pod.) 2.
1	Systém pre analýzu sieťovej prevádzky		áno/nie		
2		Systém zložený z hardvérových zariadení musí monitorovať sieťovú aktivitu v reálnom čase a identifikovať potenciálne kybernetické hrozby, bezpečnostné riziká a anomálne správanie a musí o nich v reálnom čase vytvárať upozornenia.	áno/nie		
3		Dodaný systém musí analyzovať sieť na základe zrkadlenej sieťovej prevádzky zo SPAN portov alebo TAPov (nie len na základe štatistických protokolov typu NetFlow) a zároveň bez potreby nasadzovať agentov na koncové stanice alebo ďalšie zariadenia v sieti.	áno/nie		
4		Systém musí analyzovať obsah dátových paketov v reálnom čase a detekovať protokol alebo aplikáciu na základe obsahu prevádzky prostredníctvom DPI (Deep Packet Inspection), nie iba čísla portu.	áno/nie		
5		Dodaný systém musí byť schopný analyzovať sieť aj na základe spracovania štatistických protokolov typu NetFlow, IPFIX, NetStream, Cisco NSEL a prípadne ďalších.	áno/nie		
6		Systém musí byť plne funkčný v offline prostredí objednávateľa bez využitia cloudového prostredia na zber, ukladanie a spracovanie dát a všetky konfigurácie a reporting sú k dispozícii priamo v systéme.	áno/nie		
7		Aktualizácia systému musí byť možné vykonávať užívateľsky v offline režime.	áno/nie		
8	Spracovanie a ukladanie sieťových tokov		áno/nie		
9		Systém ukladá sieťové toky vo formáte, ktorý umožní analýzu sieťovej komunikácie na úrovni jednotlivých tokov, vrátane vyhľadania informácií o aplikačných transakciách a ich metadátach z L2 až L7, obsiahnutých v danom sieťovom toku.	áno/nie		
10		Požadované protokoly pre ukladanie aplikačných metadát z jednotlivých transakcií sú: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAP, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP , FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapuzdrenie.	áno/nie		
11		Vyžaduje sa vysokorýchlostné úložisko pre uchovanie histórie dátových tokov na dobu minimálne 12 mesiacov zloženej z SSD alebo NVMe diskov.	áno/nie		
12	Analýza aplikačných a systémových logov		áno/nie		
13		Systém musí byť schopný zbierať a analyzovať aplikačné a systémové logy vo formáte syslog z dohľadovaných zariadení a identifikovať nebezpečné alebo potenciálne škodlivé aktivity.	áno/nie		
14	Používateľské rozhranie		áno/nie		
15		Systém musí poskytovať jednotné grafické používateľské rozhranie pre všetku prácu používateľov, vrátane všetkých detekcií, analýzy sieťových štatistík, nastavenia systému, konfiguráciu alertov, reportov a dashboardov.	áno/nie		
16		Systém musí byť schopný vytváranie profilov a skupín užívateľov pre obmedzenie funkcionality produktu a viditeľnosti uložených dát s podporou minimálne:	áno/nie		
17		• granulárneho nastavenia prístupu k analytickým aj konfiguračným/administratívnym komponentom systému s definovanými úrovňami prístupu (aspoň read, write, execute),	áno/nie		
18		• granulárneho nastavenia prístupu k dátam z rôznych segmentov siete organizácie s definovanými úrovňami prístupu (aspoň read, write, execute),	áno/nie		
19		• vytváranie vlastných filtrov všetkých dát a ich zdieľanie medzi užívateľmi a skupinami užívateľov,	áno/nie		
20		• vytváranie vlastných užívateľských pohľadov, reportov, dashboardov a pod.	áno/nie		
21	Automatické hlásenie (alerty) a reporting		áno/nie		
22		Systém musí byť schopný upozorňovať užívateľa prostredníctvom minimálne emailu a logu o všetkých identifikovaných udalostiach a ďalej o udalostiach filtrovaných minimálne podľa IP a MAC adresy, podsiete, závažnosti udalosti, kategórie udalosti, krajiny, užívateľa, sieťové služby, čísla portu, prevádzky do/z internetu .	áno/nie		
23		Tieto alerty musí byť systém schopný dodávať aj v strojovo čitateľnom formáte pre využitie v nástrojoch typu SIEM a musí obsahovať minimálne kompletné informácie o detegovanej udalosti vrátane URL odkazu na danú udalosť v reportovanom období do grafického rozhrania systému.	áno/nie		
24		Systém musí mať možnosť vytvárania automatizovaných manažérskych reportov o stave kybernetickej bezpečnosti z pohľadu správy kybernetických incidentov ideálne podľa oblastí ich vznikov (napr.: doména, web, email a pod.).	áno/nie		
25		Je požadované vytváranie automatizovaných reportov v slovenskom jazyku.	áno/nie		
26	Integrácia systému		áno/nie		
27		Systém musí poskytovať hotové nástroje umožňujúce integráciu so softvérom tretích strán bez použitia API systému, a to minimálne:	áno/nie		
28		• syslog, CEF a LEEF pre export udalostí vrátane plnej podpory filtrov (exportovanie iba požadovaných dát)	áno/nie		
29		• priame url odkazy na ľubovoľnú obrazovku grafického používateľského rozhrania a filtrované zobrazenia v grafickom používateľskom rozhraní	áno/nie		
30		• export informácií o toku vo formáte IPFIX alebo podobnom formáte vrátane plnej podpory filtrov (exportovať je možné iba požadované dáta) vrátane aplikačných metadát aspoň pre protokoly HTTP, HTTPS a SMTP	áno/nie		
31		• integrácia so službami identity užívateľov bez nutnosti konfigurácie zasielania logov do systému – minimálne Cisco ISE a Microsoft Active Directory	áno/nie		
32		• integrácia s firewallmi, aspoň Cisco, Palo Alto, Fortinet a Checkpoint, pre automatické a manuálne reakcie vyvolané systémom	áno/nie		
33		• integrácia s nástrojmi pre riadenie prístupu k sieti minimálne Cisco ISE, pre automatickú a manuálnu reakciu systému.	áno/nie		
34	Podpora EDR		áno/nie		
35		Systém musí poskytovať nástroje umožňujúce priamu integráciu so softvérom EDR tretích strán pre získanie informácií a skvalitnenie detekcie.	áno/nie		
36	Podpora SDN (softvérovo definovanej siete)		áno/nie		
37		Systém musí poskytovať integráciu s technológiou CISCO ACI pre získanie informácií o EPG (endpoint groups) a EPSG (endpoint security groups)	áno/nie		
38		Systém musí poskytovať aktuálne informácie o členstve jednotlivých zariadení v skupinách EPG a EPSG. Systém musí umožňovať ľubovoľné filtrovanie a vyhľadávanie zariadenia.	áno/nie		
39		Systém musí byť schopný vizualizovať prestupy zariadenia a podsietí podľa získaných parametrov EPG a EPSG s možnosťou ľubovoľnej ďalšej užívateľskej filtrácie.	áno/nie		
40	Schopnosť detekcie bezpečnostných udalostí		áno/nie		
41	Monitorovanie zariadení, segmentov siete a využívaných sieťových služieb		áno/nie		
42		Dodaný systém musí identifikovať všetky zariadenia pripojené do siete vrátane koncových zariadení, serverov, IoT, OT zariadení a pod. Zároveň musí byť systém schopný identifikovať zmeny v sieti – minimálne:	áno/nie		
43		zmena IP/MAC adresy host,	áno/nie		
44		duplicitná IP/MAC adresa,	áno/nie		
45		zmena na VLAN,	áno/nie		

46		vytvorení novej podsiete,	áno/nie		
47		pripojenie nového zariadenia	áno/nie		
48		použití nebo vznik nové služby,	áno/nie		
49		nedostupnosť skôr dostupné a komunikujúce služby alebo skôr dostupného a komunikujúceho zariadenia,	áno/nie		
50		prístup nového zariadenia k službe či zariadeniu	áno/nie		
51		overovanie platnosti interných certifikátov pre validné TLS šifrovanie u HTTPS a upozornenia pred dátumom ich vypršania.	áno/nie		
52		Systém musí užívateľovi umožniť pomocou týchto detekčných metód nastavovať bezpečnostné politiky pre rôzne segmenty siete a pre rôzne zariadenia a na porušenie týchto politik reagovať upozornením.	áno/nie		
53	Samostatné učenie behaviorálnych aktivít a detekcia anomálií		áno/nie		
54		Systém musí používať matematické metódy samostatného učenia pre analýzu sieťovej aktivity, vytvárať av čase automaticky modifikovať modely správania na základe bežného správania jednotlivých zariadení a na nich prevádzkovaných služieb v rámci celej organizácie.	áno/nie		
55		Systém musí mať schopnosť na základe matematického modelu daného zariadenia a jeho služieb identifikovať nešťandardné sieťové správanie, a to najmä odchýlky od modelu normálneho správania pre:	áno/nie		
56		odchýlku od modelu na prenos dát, tokov a paketov	áno/nie		
57		odchýlku od modelu pre počet komunikačných partnerov,	áno/nie		
58		odchýlku od modelu entropie na komunikačných portoch,	áno/nie		
59		odchýlku od modelu pre počet sieťových tokov a využitých sieťových služieb,	áno/nie		
60		odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy),	áno/nie		
61		Samostatné učenie je požadované na všetkých sieťových zariadeniach a na nich prevádzkovaných službách (port číslo 0 až 65535 pri TCP aj UDP) na IPv4 a IPv6 a ďalších protokoloch L3 a L4 sieťovej vrstvy.	áno/nie		
62	Identifikácia neznámych hrozieb a podozrivých správaní		áno/nie		
63		Systém musí byť schopný detekovať neznáme hrozby, ktoré nemožno identifikovať prostredníctvom detekčných signatúr, ako sú trójske kone, botnety a pod. Najmä musia byť identifikované tieto príznaky potenciálne škodlivého správania:	áno/nie		
64		prieskumné aktivity v sieti,	áno/nie		
65		detekcia podozrivého strojového správania, ktoré nevytvárajú ľudskí používatelia siete,	áno/nie		
66		detekcia repetitívnych vzorcov správania na sieti,	áno/nie		
67		detekcia botnetov a ovládanie kompromitovanej stanice,	áno/nie		
68		detekcia príznakov ťažení kryptomien,	áno/nie		
69		útoky hrubou silou a enumerace dat,	áno/nie		
70		rozpoznanie tunelovanej sieťovej prevádzky – aspoň IPv4 prostredníctvom IPv6 a DNS tunelov.	áno/nie		
71	Detekcia na základe databázy známych hrozieb		áno/nie		
72		Systém musí byť schopný identifikovať hrozby a reportovať udalosti na základe	áno/nie		
73		detekčnú databázu známych hrozieb, tj malware (trójske kone, vírusy, červy, rootkity, apod.), známych útokov (exploity) a zraniteľnosti, porušenie bezpečnostných pravidiel a „best practices" a ďalších rizík	áno/nie		
74		reputačná databáza známych škodlivých IP adries, TLS certifikátov, záznamov DNS a hostname, URL adries a hashov súborov.	áno/nie		
75		Tieto databázy musia byť aktualizované minimálne na hodinovej báze. Nesmie ísť len o voľne dostupné/open-source databázy, ale musí ísť o komerčnú databázu renomovaného vendora alebo poskytovateľa túrbto služieb.	áno/nie		
76	Užívateľ musí byť schopný importovať vlastné záznamy.		áno/nie		
77		Systém musí využívať túto detekciu pre všetku monitorovanú prevádzku (na perimetri aj v internej sieti medzi všetkými segmentmi), nie iba pre obmedzený segment alebo podmnožinu celkovej komunikácie.	áno/nie		
78		Databáza detekčných pravidiel (signatúr) musí byť založená na pokročilých regulárnych výrazoch pre spracovanie reťazcov, ktoré dokážu vykonávať inšpekciu všetkej sieťovej komunikácie od L2 (Ethernet a pod.) po L7. Systém musí detekovať udalosti na základe vysokého počtu signatúrnych pravidiel (minimálne niekoľko desiatok tisíc).	áno/nie		
79		Užívateľ musí byť schopný prostredníctvom webovej aplikácie pridávať vlastné detekčné pravidlá v praktickom a všeobecne využívanom formáte bez nutnosti znalosti syntaxe a sémantiky pravidiel.	áno/nie		
80		Príklad možnej syntaxe detekčného pravidla:	áno/nie		
81		alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b*;)	áno/nie		
82	Analýza šifrovanej komunikácie		áno/nie		
83		Okrem samostatného učenia musí systém používať ďalšie metódy na analýzu šifrovanej komunikácie, minimálne TLS fingerprinting as ňou spojenú detekciu známych hrozieb.	áno/nie		
84	Asistované učenie		áno/nie		
85		Je požadovaný užívateľsky privetivý proces vytvárania pravidiel pre spresnenie detekcie a eliminácia falošne pozitívnej detekcie, a to na základe minimálne nasledujúcich parametrov:	áno/nie		
86		IP adresa,	áno/nie		
87		MAC adresa,	áno/nie		
88		hostname,	áno/nie		
89		segment siete / podsiete,	áno/nie		
90		lokalita – ASN, krajiny, apod.	áno/nie		
91		smer komunikácie – určenie klienta, alebo servera,	áno/nie		
92		detekovaná udalosť – kategorie, názov apod.	áno/nie		
93		použité služby, protokolu, portu,	áno/nie		
94		ľubovoľnej kombinácii vyššie popísaných.	áno/nie		
95		Systém musí byť schopný eliminovať falošné alarmy aj pre udalosti detegované v histórii.	áno/nie		
96	Detekcia s využitím Sandboxu		áno/nie		
97		Systém musí umožňovať integráciu so systémom Sandbox za účelom statickej aj dynamickej analýzy, tzv. „detonace" vo virtuálnom prostredí.	áno/nie		
98		V prípade integrácie, systém musí byť schopný odovzdávať do Sandboxu súbory a url adresy, pre ďalšiu analýzu.	áno/nie		
99		Systém musí byť schopný zobraziť výsledok analýzy Sandboxu vo svojom vlastnom grafickom prostredí, spoločne s ostatnými udalosťami.	áno/nie		
100			áno/nie		
101	Vyhledávání, filtrování a vizualizace dat		áno/nie		
102		Systém musí byť schopný okamžitého (v priebehu sekúnd) vyhľadávania a vizualizácie pre forenznú analýzu a podporu threat hunting bez zvláštneho dotazovacieho jazyka.	áno/nie		
103		Ide o možnosť okamžite filtrovať a vyhľadávať v plnej histórii všetkých uložených dát, tj bezpečnostných udalostí, sieťových tokov a agregovaných sieťových štatistikách (tabuľky a grafy), a to minimálne:	áno/nie		
104		• podľa parametrov IP a MAC adresa, hostname, username (identita užívateľa), prichádzajúca a odchádzajúca prevádzka, sieťová služba, lokálna alebo vzdialená služba (služba z pohľadu klient alebo server), číslo portu, VLAN, krajina, ASN,	áno/nie		
105		• prostredníctvom full-textového vyhľadávania v dátach a vyhľadávania na základe definície smeru (zdroj, cieľ) a logických výrazov and, or, not.	áno/nie		
106		Systém musí pre vyhľadávanie poskytovať už predpočítané hodnoty výkonnostných a behaviorálnych charakteristík pre každé zariadenie v sieti a pre všetky na ňom prevádzkované služby, bez nutnosti spracovania surových dát zo sieťových logov.	áno/nie		
107		Systém musí byť schopný filtrovať a vizualizovať výsledky v grafoch, výpočtových tabuľkách s možnosťou radenia a TOP N štatistikách.	áno/nie		
108		Systém musí byť schopný ukladať a následne vyhľadávať aplikačné metadáta (vždy dotaz aj odpoveď všetkých transakcií v toku) minimálne z nasledujúcich protokolov, ktoré sú alebo môžu byť využívané vo vnútornej sieti organizácie: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SCU, SIP, Kerberos, SSL/TLS.	áno/nie		

109		Metadatá sú v tomto prípade chápané ako prenášané aplikačné metadáta alebo vlastné dáta servisných protokolov. Pri protokole HTTP napríklad http hlavička s metódou, URI, host, user-agent, cookies a pod. V odpovedi potom návratový kód a ďalšie http parametre.	áno/nie		
110		Systém umožňuje vykonávať užívateľsky jednoduché a okamžité vizualizácie sieťových prestupov medzi zariadeniami a podsiete. Využitím užívateľského dátového filtra je možné vizualizačné pohľady ľubovoľne modifikovať.	áno/nie		
111	Kontextuálne informácie		áno/nie		
112		Systém musí byť schopný pre každé zariadenie získavať, vizualizovať av jednom grafickom pohľade zobrazovať kontextuálne informácie:	áno/nie		
113		• meno užívateľa a ďalšie jeho parametre z doménového radiča (MS Active Directory), vrátane jej histórie	áno/nie		
114		• hostname zariadenia a jeho história na základe spracovania relevantných dát z DNS a DHCP prevádzky	áno/nie		
115		• IP geolokácia	áno/nie		
116		• IP reputácia, vr. údaje, či je IP adresa na blackliste alebo podozrivá	áno/nie		
117		• história použitých MAC adresa a výrobca zariadenia	áno/nie		
118		• operačný systém a jeho história na zariadení	áno/nie		
119		• užívateľom zadané poznámky a informácie k zariadeniu	áno/nie		
120		• automaticky priradené značky/tagy zariadení, ktoré popisujú ich účel a správanie – aspoň server doménového radiča, webový server, poštový server, server DNS, server SSH, databázový server, tlačiareň, administrátorské zariadenie, dátové úložisko, aktívne dohľady, skenery zraniteľnosti a technologické systémy.	áno/nie		
121		• zoznam prevádzkovaných a využívaných služieb (klient a server) u daného zariadenia a množstvo na nich prenesených dát.	áno/nie		
122		• zoznam detekovaných bezpečnostných a prevádzkových udalostí daného zariadenia.	áno/nie		
123	Zaznamenávanie, ukladanie a spätná analýza plnej prevádzky		áno/nie		
124		Je požadované voliteľné nahrávanie plnej sieťovej prevádzky (full packet capture) vo formáte PCAP na všetkých dodaných zariadeniach minimálne na základe parametrov: cieľová a zdrojová IP/MAC adresa, podsieť, využitý protokol, IPv4 alebo IPv6. Zaznamenávanie je možné zapínať automaticky podľa detekovaných udalostí, alebo užívateľskou aktiváciou.	áno/nie		
125		Je požadovaná schopnosť importu vlastného PCAP súboru prostredníctvom webového rozhrania a jeho spätná analýza všetkými detekčnými a analytickými prostriedkami kolektora.	áno/nie		
126		Je požadovaná schopnosť zobrazenia plného obsahu PCAP súboru v prostredí webového rozhrania aplikácie a ďalej potom automatizovaná analýza surových dát za účelom identifikácie prevádzkových nedostatkov zachytených iba v dátovom PCAP súbore.	áno/nie		
127	Monitorovanie politík kybernetickej bezpečnosti		áno/nie		
128		Systém musí umožňovať vytváranie komplexných komunikačných a bezpečnostných politík, a to minimálne:	áno/nie		
129		• monitorovať definovanú komunikačnú maticu a detekovať, kedy sú tieto matice porušené – aspoň aké zariadenie smie komunikovať s akým zariadením, cez aký protokol, v akom čase.	áno/nie		
130		• detekcia zmien v sieti – prinajmenšom nové komunikačné vektory, nové alebo zmenené zariadenia a podsiete, obchádzanie perimetra.	áno/nie		
131		Na účely monitorovania politík kybernetickej bezpečnosti musí systém poskytovať užívateľský rámec na definovanie pravidiel pomocou:	áno/nie		
132		• užívateľom definované podsiete na základe rozsahov IP adries	áno/nie		
133		• užívateľsky ľubovoľne definovaných skupín zariadení	áno/nie		
134		• automaticky priradené značky/tagu zariadenia, ktoré popisujú ich účel a správanie – aspoň server doménového radiča, webový server, poštový server, server DNS, server SSH, databázový server, tlačiareň, administrátorské zariadenie, dátové úložisko, aktívne dohľady, skenery zraniteľností a technologické systémy.	áno/nie		
135	Manažment bezpečnostných udalostí a incidentov		áno/nie		
136		Systém musí poskytovať funkcionalitu pre reporting bezpečnostných incidentov (vyhlásenie identifikovanej udalosti za bezpečnostný incident), vrátane:	áno/nie		
137		• spoluprácu a zdieľanie informácií pri analýze identifikovaných bezpečnostných incidentov vrátane potrebného workflow medzi jednotlivými užívateľmi s podporou automatizovaných oznámení o zmene stavu udalosti či priradení riešiteľa,	áno/nie		
138		• jednoduché zdieľanie informácií o bezpečnostných incidentoch, vrátane užívateľom zadaných komentárov,	áno/nie		
139		• možnosť vyhľadávania a filtrovania nad všetkými udalosťami z pohľadu workflow bezpečnostného incidentov (reportovaná udalosť, udalosť v riešení, vyriešená udalosť, udalosti v riešení daného užívateľa a pod.)	áno/nie		
140		• možnosť exportovania dát do emailu, csv, pdf, syslogu a podobne,	áno/nie		
141		• možnosť exportu bezpečnostných udalostí a incidentov do systémov typu ticket management tretích strán.	áno/nie		
142	Detekcia úniku dát		áno/nie		
143		Systém musí byť schopný detekovať prenosy citlivých súborov a dát definovaných pomocou ich názvov, hashov, špecifického binárneho obsahu (vodoznaku) alebo regulárnych výrazov (napr. rodné číslo).	áno/nie		
144		Systém musí byť schopný detekovať prenosy citlivých súborov a dát aspoň pri nasledujúcich protokoloch: HTTP, FTP, SMTP, SMB, NFS.	áno/nie		
145		V rámci historických metadát pri HTTP, FTP, SMTP, SMB a NFS je požadované ukladanie informácií o všetkých po sieti prenášaných súboroch aspoň v rozsahu:	áno/nie		
146		• názov súboru,	áno/nie		
147		• veľkosť súboru,	áno/nie		
148		• HASH súboru.	áno/nie		
149	Monitoring výkonu aplikácií a siete		áno/nie		
150		Systém v celej monitorovanej sieti, medzi všetkými zariadeniami a na všetkých službách meria a vytvára automaticky (bez nutnosti nastavovať manuálne limitné hodnoty) model normálneho správania pre výkonnostné parametre minimálne:	áno/nie		
151		• prenosová rýchlosť siete,	áno/nie		
152		• rýchlosť odozvy aplikácie,	áno/nie		
153		• odozva systému z pohľadu užívateľa.	áno/nie		
154		Výpočet uvedených výkonnostných parametrov a automatickej detekcie anomálií na základe odchýlky od modelu normálneho správania sa musí vykonávať pre:	áno/nie		
155		• všetky porty a služby TCP,	áno/nie		
156		• pre všetky kombinácie služieb a zariadení.	áno/nie		
157		Systém musí v celej monitorovanej sieti, medzi všetkými zariadeniami a na všetkých službách merať informácie o retransmission paketoch, out of order paketoch, TTL, QoS a komunikácii blokovanej firewally.	áno/nie		
158	Monitoring cloudových služieb		áno/nie		
159		Systém musí byť schopný monitorovať prístupy zariadení a užívateľov ku cloudovým službám, a to minimálne Google Workspace a Microsoft Office 365, vr. monitoringu operácií so súbormi, zmien oprávnenia a nastavenia a neúspešných prístupov.	áno/nie		
160		Systém musí byť schopný tieto informácie autonómne a priebežne získavať z aplikačných rozhraní týchto cloudových služieb bez nutnosti využitia riešenia tretích strán.	áno/nie		
161	Inventarizácia siete a grafická vizualizácia topológie		áno/nie		
162		Systém musí byť schopný zobraziť celý inventár monitorovanej siete s počtom zariadení v jednotlivých lokalitách, segmentoch, alebo podsietiach. Vrátane detailného prehľadu zariadenia.	áno/nie		
163		Systém musí byť schopný graficky vykresliť celú topológiu siete, podľa zaznamenanej komunikácie.	áno/nie		
164		Systém musí byť schopný zobraziť inventár jednotlivých lokalít, prehľady zariadení, prehľady výrobcov, tagy zriadenia, užívateľa.	áno/nie		
165		Systém umožňuje všetky inventarizačné informácie zoradiť podľa rôznych parametrov.	áno/nie		
166	Minimálne parametre HW zariadenia:		áno/nie		

167	Procesory	Model servera umožňujúci osadiť dva procesory, osadený jedným procesorom typu x86, disponujúcim 8-mimi jadrami a so základnou taktovacou frekvenciou 2,8 GHz.	hodnota		
168	Pamäť	64 GB, DDR5 Registered min. 4800MTs, server musí obsahovať 4 DDR5 DIMM sloty a podporovať aspoň 128 GB RAM	hodnota		
169	Ethernet adaptér	Minimálne 2 x 1Gb/s pripojenie k externému prostrediu, a 2 x 10/25Gb/s SFP28 zabezpečujúce redundantné a vysoko dostupné pripojenie servera na externú LAN infraštruktúru.	hodnota		
170	Diskový radič	HW diskový radič s rozhraním 12Gb/s, s podporou RAID 0/1/5/6/10/50/60, cache min. 8GB zálohovaná batériou alebo ekvivalentným spôsobom.	hodnota		
171	Pevné disky	Minimálne 8 pozícií SAS/SATA/NVMe pre disky veľkosti 2.5", osadené min: 2x 1.92TB SSD SATA read-intensive	hodnota		
172	USB port	Minimálne tri USB porty prístupné zvonku.	áno/nie		
173	PCI sloty (okrem slotov dedikovaných pre RAID radič, OCP/LOM karty, SD karty a M2 disky)	Min. 1 x 16 Gen4 a 1 x 8 Gen4 pri osadení jedným CPU	hodnota		
174	Grafický adaptér	Integrovaný grafický adaptér, minimalne 1x VGA graficke rozhranie,	áno/nie		
175	Správa a manažment	Musí byť zabezpečené: - hardvérový komponent nezávislý od operačného systému formou vzdialenej grafickej KVM konzoly - dedikovaná IP adresa a separátnym RJ45 portom - časovo neobmedzený prístup na obraz vzdialenej plochy servera a to aj bez spusteného OS, vrátane plnohodnotného pripojenia vzdialených médií - možnosť štartu, reštartu a shutdown serveru cez sieť LAN, nezávisle od OS - možnosť automaticky registrovať servisné incidenty priamo u výrobcu - rozšírená bezpečnostná ochrana na úrovni BIOSu servera - verifikácia autenticity FW - automatická obnova poškodeného / neautentického FW servera - možnosť zasielania a vyhodnocovania telemetrických údajov v cloud nástroji výrobcu HW, vrátane porovnania bezpečnostných nastavení servera voči všeobecne platným bezpečnostným normám, - možnosť zobrazenia konfigurácie a zmeny nastavení servera pomocou bluetooth alebo wi-fi protokolu na mobilnom zariadení - dedikovaný USB port pre priame pripojenie na manažment servera zpredu. Licencie, resp. softvér potrebný na prevádzku, konfiguráciu a správu servera uvedenú funkcionalitu poskytuje s kapacitne a časovo neobmedzeným licenčným pokrytím pre daný server	áno/nie		
176	Napájanie	Redundandné za behu meniteľné, schopné napájať server požadovanej konfigurácie (aj s definovanými rozšíreniami) jedným napájacím zdrojom.	áno/nie		
177	Prevedenie	Max 1U montovateľné do 19" racku, vrátane kolajníc a zariadenia na vedenie káblov	áno/nie		
178	Trvalý prietok dát za sekundu	min. 500 Mbps	hodnota		
179	Netflow toky za sekundu z iných zdrojov	min. 1000	hodnota		
180	Počet monitorovaných IP adries	min. 1500	hodnota		
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
181	Min. 5 rokov servisná podpora v mieste inštalácie, 24x7 nahlasovanie výrobcovi hardvéru, výmena dielu NBD. Oprava zariadenia musí byť realizovaná priamo výrobcom alebo jeho lokálnym autorizovaným servisným partnerom (zastúpením). Obstarávateľ požaduje možnosť bezplatného sťahovania updatov firmvérov a ovládačov aj po uplynutí definovanej servisnej podpory a to priamo obstarávateľom priamo zo stránky výrobcu.	Záruka	áno/nie		
182	Implementačné a konfiguračné práce s otestovaním, zaškolením a dokumentáciou riešenia v rozsahu 6 človekohodín	Práce	áno/nie		
	Implementačné práce pre Sondu detekcie a prevencie prieniku do siete:		áno/nie		
	Návrh architektúry nasadenia sondy detekcie a prevencie prieniku do siete s návrhom optimálneho umiestnenia v existujúcej sieťovej architektúre. Implementácia a zapojenie a integrácia s existujúcimi sieťovými prvkami, prípadne so SIEM platformou. Prispôsobenie detekčných pravidiel pre efektívnu identifikáciu hrozieb. Testovanie nasadenia a správnosti zachytávania hrozieb. Vyškolenie personálu na používanie systému a interpretáciu výsledkov. Dodanie technickej dokumentácie nasadenia.		áno/nie		
	Analýza požiadaviek organizácie: o Zhodnotenie existujúcej sieťovej infraštruktúry, identifikácia kritických bodov a definovanie cieľov nasadenia.		áno/nie		
	Návrh architektúry riešenia: o Plánovanie umiestnenia senzorov, sieťových tapov alebo SPAN portov pre optimálne pokrytie siete.		áno/nie		
	Príprava infraštruktúry: o Zabezpečenie hardvéru alebo virtuálnych prostredí, konfigurácia sieťových prvkov na zrkadlenie prevádzky.		áno/nie		
	Inštalácia sond detekcie a prevencie prieniku: o Nasadenie softvéru na fyzické servery, vrátane základnej konfigurácie systému.		áno/nie		
	Integrácia so sieťovou infraštruktúrou: o Pripojenie k sieťovým zariadeniam (switche, routre, firewally) a systémom na správu logov (SIEM).		áno/nie		
	Konfigurácia detekčných pravidiel: o Prispôsobenie pravidiel na detekciu hrozieb podľa špecifík organizácie a aktuálnych bezpečnostných požiadaviek.		áno/nie		
	Testovanie funkčnosti: o Overenie správnosti zachytávania a analýzy sieťovej prevádzky, testovanie detekcie simulovaných hrozieb.		áno/nie		
	Zaškolenie personálu: o Školenie bezpečnostného tímu a administrátorov na prácu so systémom, interpretáciu výstupov a reakciu na incidenty.		áno/nie		
	Optimalizácia a ladenie výkonu: o Úprava konfigurácie pre zlepšenie výkonu a minimalizovanie falošných poplachov.		áno/nie		
	Záverečné odovzdanie a dokumentácia: o Odovzdanie projektu vrátane dokumentácie k implementácii, prevádzke a správe systému.		áno/nie		
183	1 ročná licencia zabezpečujúca aktualizácie a upgrady všetkých komponentov produktu a technickú podporu 8x5 a a to telefonicky, emailom a helpdeskom.	Licencia	áno/nie		

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

Špecifikácia predmetu zákazky - položka: Nástroj na centrálny manažment logov

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky		
Položka predmetu zákazky - Nástroj na centrálny manažment logov + licencia požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Nástroj na centrálny manažment logov + licencia)**	**Doplňujúce informácie**
1	Centrálny logovací systém má pracovať ako fyzická appliance s jedným uceleným webovým rozhraním pre všetky administrátorské i operátorské činnosti. Nevyžaduje inštaláciu ďalších systémov a aplikácií okrem podpory zberu na iných lokalitách (mimo centrálu) a agenta pre zber Windows logov.	
2	Konfigurácia systému sa musí vykonávať v grafickom rozhraní jednotnej užívateľskej konzoly, Systém poskytuje podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát.	
3	Systém má umožňovať doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľov bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému - užívateľsky definované parsery. Dokumentácia systému musí obsahovať prehľadný návod na vytváranie zákazníckych parserov a systém musí obsahovať možnosť testovania a ladenia parserov bez vplyvu na ostatné produkčné funkcie systému.	
4	Prijaté logy má systém štandardizovať do jednotného formátu a logy sú rozdeľované do príslušných polí podľa ich typu. Systém musí zároveň uchovávať originálne verzie správ.	
5	Pre hodnoty jednotlivých parsovaných polí musí byť možné v definícii parseru zmeniť typ a štandardizovať minimálne na tieto základné druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými dátami typu číslo je možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšia/najväčšia hodnota a pod.).	
6	Centrálny logovací systém musí zachovávať pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, ktorá vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi.	
7	Všetky polia a položky prijaté systémom musia byť automaticky indexované. Nad všetkými položkami musí byť možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom. Centrálny logovací systém musí umožňovať zber udalostí vo formátoch RAW, Syslog.	
8	Centrálny logovací systém neumožňuje mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log musí mať unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.	
9	Centrálny logovací systém musí umožňovať konfiguráciu filtrácie nerelevantných správ, konsolidáciu logov na vlastnom storage priestore, jednoduché vyhľadávanie udalostí a okamžité vytváranie grafických reportov (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. Reportovací nástroj musí byť integrálnou súčasťou systému a aj súčasťou jednotného rozhrania.	
10	V prípade krátkodobého preťaženia systému nemôže dochádzať k strate logov. Všetky prijaté nespracované logy/udalosti sú ukladané do vyrovnávacej pamäte.	
11	Centrálny logovací systém musí umožňovať jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurácie systému alebo parametrov uložených dát. Historické dáta v požadovanej dĺžke retencie uložené v systéme je možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nevyžaduje manuálnu konfiguráciu a zásahy používateľa.	
12	Systém musí podporovať natívne získavanie logov z Office365.	
13	Centrálny logovací systém musí umožňovať unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí a musí spĺňať požiadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov.	
14	Centrálny logovací systém má mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie.	
15	Centrálny logovací systém musí obsahovať reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov.	
16	Centrálny logovací systém musí umožňovať kapacitnú i výkonovú škálovateľnosť.	
17	Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP alebo Syslog.	
18	Centrálny logovací systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)	
19	Centrálny logovací systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému, vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní.	
20	Centrálny logovací systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Systém má automaticky zaznamenávať užívateľské meno ku každej akcii užívateľom.	
21	Aktualizácie systému by mali byť distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. Všetky aktualizácie by mali byť vykonávané z webového rozhrania systému bez potreby asistencie výrobcu/dodávateľa.	
22	Systém musí podporovať downgrade, napríklad pri problémoch s novou verziou systému po upgrade.	
23	Licenčne musí byť neobmedzený počet zariadení pre príjem zasielaných udalostí. Licenčne musí byť neobmedzený počet udalostí v GB za deň. Integrovaná databáza musí podporovať kompresiu ukladaných dát.	
24	Centrálny logovací systém musí podporovať zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém a taktiež musí podporovať zálohovanie dát na externý systém, požadované je plánované aj ad-hoc zálohovanie.	
25	Centrálny logovací systém musí byť schopný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert. Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti.	
26	Centrálny logovací systém by mal obsahovať výrobcom predpripravené sety/vzory alertov a korelácií.	
27	Užívateľská konfigurácia alertov musí byť možná pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nemôže byť prezentovaný čisto textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie umožňuje okamžitú kontrolu.	

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		

28	Ako výstupné pravidlo alertu systém musí vedieť odoslať udalosť, ktorá alert vyvolala na externý systém prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol musí byť možnosť definície formátu dát pre jednoduchšiu integráciu so systémami tretích strán.		áno/nie		
29	V alertoch by mala byť možnosť využívať značky.		áno/nie		
30	Systém musí podporovať funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel má mať možnosť vloženia testovacej správy a výsledku testu vykonanej akcie		áno/nie		
31	Centrálny logovací systém by mal získavať udalosti z Microsoft prostredia buď pomocou agenta inštalovaného priamo na koncovom zariadení s Windows systémom, alebo iným spôsobom. Agent súčasne musí podporovať monitoring interných Windows logov, a aj monitoring textových súborových logov.		áno/nie		
32	Agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovanie auditných informácií.		áno/nie		
33	Agent musí podporovať nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.		áno/nie		
34	Filtrácia odosielaných udalostí agentom sa musí konfigurovať pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Nerelevantné logy majú byť filtrované na strane agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk nesmie byť prezentovaný textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku.		áno/nie		
35	Agent nesmie vyžadovať administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizácia agenta sa nevykonáva z Group Policy.		áno/nie		
36	Komunikácia Windows agenta a centrálneho logovacieho systému je šifrovaná.		áno/nie		
37	Agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale aj zber všetkých ostatných logov v zložke protokoly aplikácií a služieb. Agent musí podporovať centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu.		áno/nie		
38	Agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v prehliadači udalostí (Event Viewer) na koncovom systéme.		áno/nie		
39	Počet inštalácií agenta nemôže byť licenčne ani časovo obmedzený.		áno/nie		
40	Počet udalostí za sekundu pri priemernej veľkosti jednej udalosti 1kB	min. 2000	hodnota		
41	Počet udalostí počas útoku (min. 10 minút)	min. 4000	hodnota		
42	Retencia logov	min. pol roka	hodnota		
43	Veľkosť diskového subsystému s čistou dostupnou kapacitou v RAID5	min. 12TB	hodnota		
44	Veľkosť operačnej pamäte	min. 64 GB	hodnota		
45	Redundantné napájacie zdroje vymeniteľné za chodu		áno/nie		
46	Prevedenie	Max 1U montovateľné do 19" racku, vrátane kolajníc a zariadenia na vedenie káblov	áno/nie		
47	Virtuálne KVM, tj. prevzatie textovej i grafickej konzoly serveru a prenos povelov z klávesnice a myši vzdialeného počítača		áno/nie		
48	Systém pre vzdialenú správu serveru vrátane potrebnej licencie		áno/nie		
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
49	5 rokov priamo od výrobcu zariadenia. Nahlasovanie poruchy v režime 24x7, výmena náhradného dielu NBD.	Záruka	áno/nie		
50	Implementačné a konfiguračné práce s otestovaním, zaškolením a dokumentáciou riešenia v rozsahu 10 človekohodín.	Práce	áno/nie		
	Implementačné práce pre centrálny manažment logov:		áno/nie		
	Analýza požiadaviek a plánovanie: o Identifikácia potrieb organizácie v oblasti logovania, bezpečnosti a súladu s legislatívou.		áno/nie		
	Príprava infraštruktúry: o Overenie hardvérových zdrojov, príprava serverov a siete pre nasadenie centrálneho manažmentu logov.		áno/nie		
	Inštalácia centrálneho manažmentu logov: o Nasadenie softvéru na fyzické alebo virtuálne servery s ohľadom na výkonové požiadavky.		áno/nie		
	Základná konfigurácia systému: o Nastavenie sieťových parametrov, zabezpečenie prístupu a konfigurácia administrátorských účtov.		áno/nie		
	Integrácia so zdrojmi logov: o Konfigurácia serverov, sieťových zariadení, aplikácií a databáz na odosielanie logov do centrálneho manažmentu logov v celkovom počte 50 vzorových zdrojov.		áno/nie		
	Nastavenie politiky uchovávania logov: o Definovanie retenčných politík pre dlhodobé a bezpečné uchovávanie dát podľa noriem (napr. GDPR).		áno/nie		
	Korelácia udalostí a správa alertov: o Nastavenie pravidiel pre automatickú detekciu incidentov a notifikácie o bezpečnostných hrozbách.		áno/nie		
	Reporting a vizualizácia: o Vytvorenie prispôsobených reportov, dashboardov a prehľadov pre rôzne úrovne používateľov.		áno/nie		
	Bezpečnostné opatrenia: o Implementácia šifrovania logov, správa prístupových práv a auditovanie činností.		áno/nie		
	Testovanie a validácia: o Overenie funkčnosti systému, správnosti logov a efektivity detekcie incidentov.		áno/nie		
	Školenie používateľov a administrátorov: o Zaškolenie tímu na prácu s centrálnym manažmentom logov vrátane správy systému a interpretácie reportov.		áno/nie		
	Dokumentácia: o Vypracovanie technickej a prevádzkovej dokumentácie pre interné potreby organizácie.		áno/nie		
51	Licencia zariadenia	1 rok	Hodnota		

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

Špecifikácia predmetu zákazky - položka: Monitorovací nástroj prevádzkových parametrov

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné uchádzačom ponúkaný produkt musí SPĽŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
TU UVEĎTE názov výrobcu /značku / typové označenie /obchodný názov ponúkaného produktu predmetu zákazky		
Položka predmetu zákazky - Monitorovací nástroj prevádzkových parametrov požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Monitorovací nástroj prevádzkových parametrov**	**Doplňujúce informácie**
1	Dodané riešenie podporuje centrálne spravovanú konfiguráciu z webovej administrátorskej konzoly.	
2	Dodané riešenie umožňuje monitoring serverov, sietí, aplikácií a cloudových riešení.	
3	Komunikácia medzi serverom a agentmi je šifrovaná pomocou TLS.	
4	Dodané riešenie podporuje automatické objavovanie nových zariadení v sieti.	
5	Dodané riešenie umožňuje konfigurovateľné prahové hodnoty pre upozornenia.	
6	Dodané riešenie podporuje monitoring v reálnom čase s intervalom od niekoľko sekúnd.	
7	Dodané riešenie je open-source riešenie bez licenčných obmedzení.	
8	Dodané riešenie podporuje ukladanie historických metrík pre dlhodobé analýzy.	
9	Dodané riešenie má webové rozhranie pre zobrazenie statusov a metrík v reálnom čase.	
10	Dodané riešenie podporuje monitoring pomocou SNMP, ICMP, IPMI a JMX.	
11	Minimálna verzia databázového servera podporovaná je MySQL 5.7/PostgreSQL 10.	
12	Dodané riešenie podporuje beh v Docker kontejnery.	
13	Dodané riešenie umožňuje filtrovať upozornenia podľa kritickosti.	
14	Dodané riešenie podporuje generovanie reportov o stave systému a incidentoch.	
15	Dodané riešenie podporuje eskaláciu upozornení na viaceré úverstvenia.	
16	Dodané riešenie umožňuje definovať vlastné metriky a sledované parametre.	
17	Dodané riešenie podporuje ukladanie logov zmien v konfigurácii.	
18	Dodané riešenie podporuje monitoring IoT zariadení.	
19	Dodané riešenie je kompatibilný s OS Linux (RHEL, Ubuntu, Debian) aj Windows.	
20	Dodané riešenie podporuje LDAP autentifikáciu.	
21	Dodané riešenie umožňuje export reportov vo formátoch CSV a JSON.	
22	Dodané riešenie podporuje integráciu s cloudovými poskytovateľmi (AWS, Azure, GCP).	
23	Dodané riešenie podporuje multi-tenant riešenie.	

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		
áno/nie		

24	Dodané riešenie umožňuje integráciu s existujúcimi SIEM riešeniami.		áno/nie		
25	Dodané riešenie podporuje detekciu anomálií v sledovaných parametroch.		áno/nie		
26	Dodané riešenie podporuje notifikácie cez e-mail, SMS, webhooky a iné kanály.		áno/nie		
27	Dodané riešenie podporuje agentless monitoring.		áno/nie		
28	Dodané riešenie podporuje vlastné pravidlá na filtrovanie udalostí.		áno/nie		
29	Dodané riešenie umožňuje full-text vyhľadávanie v logoch.		áno/nie		
30	Dodané riešenie podporuje vizualizáciu historických záznamov metrík.		áno/nie		
31	Dodané riešenie ponúka REST API.		áno/nie		
32	Dodané riešenie podporuje cross-platform integráciu.		áno/nie		
33	Dodané riešenie obsahuje dashboard pre prehľad o stave monitorovanej infraštruktúry.		áno/nie		
34	Dodané riešenie podporuje autentifikáciu pomocou OAuth2.		áno/nie		
35	Dodané riešenie umožňuje vytváranie vlastných skriptov na rozšírenie funkcionality.		áno/nie		
36	Dodané riešenie má podporu pre auditovanie a logging aktivít.		áno/nie		
37	Dodané riešenie má komunitnú podporu cez GitHub Issues a fóra.		áno/nie		
38	Dodané riešenie podporuje multi-language UI.		áno/nie		
39	Dodané riešenie je škálovateľný pre veľké infraštruktúry.		áno/nie		
40	Dodané riešenie umožňuje nastaviteľné prístupové práva.		áno/nie		
41	Dodané riešenie podporuje pravidelné aktualizácie.		áno/nie		
42	Dodané riešenie podporuje šifrovanie uložených informácií.		áno/nie		
43	Dodané riešenie možno nasadiť on-premise aj v cloude.		áno/nie		
44	Dodané riešenie podporuje jednoduchú inštaláciu a konfiguráciu.		áno/nie		
45	Dodané riešenie má podporu pre automatické testovanie.		áno/nie		
46	Dodané riešenie podporuje centralizovanú distribúciu konfigurácií.		áno/nie		
47	Dodané riešenie podporuje sledovanie SLA a reportovanie dostupnosti služieb.		áno/nie		
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
48	Inštalácia na zdrojoch poskytnutých objednávateľom v rozsahu 10 človekodní	Práce	áno/nie		
	Implementačné práce pre nasadenie monitorovacieho nástroja prevádzkových parametrov v organizácii:		áno/nie		
	Analýza požiadaviek a plánovanie: o Identifikácia monitorovacích potrieb organizácie (servery, siete, aplikácie, služby) a definovanie metrík.		áno/nie		
	Príprava infraštruktúry: o Overenie hardvérových/virtuálnych zdrojov, výber vhodného OS (napr. Linux), príprava databázového servera (MySQL/PostgreSQL).		áno/nie		
	Inštalácia monitorovacieho nástroja: o Nasadenie monitorovaniceho nástroja vo virtuálnom prostredí organizácie, webového rozhrania a databázového backendu.		áno/nie		
	Základná konfigurácia systému: o Nastavenie sieťových parametrov, zabezpečenie prístupov a konfigurácia administračných účtov.		áno/nie		
	Inštalácia a konfigurácia monitorovacích agentov: o Nasadenie agentov na monitorované zariadenia (servery, PC, sieťové prvky) a ich konfigurácia v celkovom počte 20 vzorových kusov.		áno/nie		
	Integrácia s externými systémami: o Pripojenie externých zariadení a služieb pomocou SNMP, IPMI, JMX, API alebo prispôsobených skriptov.		áno/nie		
	Nastavenie šablón a monitorovacích položiek: o Vytvorenie alebo prispôsobenie šablón pre rôzne zariadenia a služby na efektívne monitorovanie.		áno/nie		

	Konfigurácia alertov a eskalácií: o Definovanie prahových hodnôt, nastavenie notifikácií (e-mail, SMS, webhook) a eskalačných politík.			áno/nie		
	Bezpečnostné opatrenia: o Implementácia šifrovania komunikácie medzi serverom a agentmi, správa prístupových práv.			áno/nie		
	Testovanie a validácia: o Overenie správnosti monitorovania, testovanie alertov a výkonu systému.			áno/nie		
	Školenie používateľov a administrátorov: o Zaškolenie tímu na prácu s monitorovacím nástrojom prevádzkových parametrov, interpretáciu údajov a správu systému.			áno/nie		
	Dokumentácia: o Vypracovanie technickej a prevádzkovej dokumentácie na podporu budúcej údržby a rozvoja systému.			áno/nie		
49	1 ročná podpora od dodávateľa riešenia v režime 8x5			áno/nie		

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

Príloha č. 2: Cena Diela

Príloha č. 2. - Cenová ponuka

Obchodné meno uchádzača: **DATALAN a.s.**	Kontaktná osoba uchádzača Pavol Rosa	
Sídlo a miesto podnikania: Krasovského 14, 851 01 Bratislava 5	Kontakt: vo@datalan.sk	
IČO: 35810734		
IČ DPH: SK2020259175		

Súhrnná cenová ponuka - návhr na plnenie

Pol. č.	Číslo aktivity v ŽoNFP	Názov aktivity v ŽoNFP	Názov Podaktivity	Názov položky predmetu zákazky	Merná jednotka (MJ)	Poľad. počet MJ	Obchodný názov ponúkaného produktu	Názov výrobcu ponúkaného produktu	Jednotková cena za MJ v EUR bez DPH	Sadzba DPH v %	DPH v EUR	Celková cena za požadovaný počet MJ v EUR bez DPH	Celková cena za požadovaný počet MJ v EUR s DPH
1	1.2.1 - 3. Zvýšenie bezpečnosti pri prevádzke - dátové úložisko a 4. Zvýšenie sieťovej a komunikačnej bezpečnosti - perimetrový firewall	3. Zvýšenie bezpečnosti pri prevádzke - dátové úložisko	Bezpečnosť pri prevádzke informačných systémov a sieti	Dátové úložisko pre potreby zálohnej a archivačnej kópie	ks	1	NetApp FAS2750	NetApp, Inc.	60 000,00 €	23%	13 800,00 €	60 000,00 €	73 800,00 €
2	1.1.3 (MRR), 1.1.2 (VRR)- 3. Zvýšenie bezpečnosti pri prevádzke dobudovaním záložných dátových kapacít, a 4. Zvýšenie sieťovej a komunikačnej bezpečnosti implementáciou perimetrového firewallu	3. Zvýšenie bezpečnosti pri prevádzke - dátové úložisko	Bezpečnosť pri prevádzke informačných systémov a sieti	Dátové úložisko pre potreby zálohnej a archivačnej kópie - Práce	MD	10	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	5 000,00 €	6 150,00 €
3	1.1.3 (MRR), 1.1.2 (VRR)- 3. Zvýšenie bezpečnosti pri prevádzke dobudovaním záložných dátových kapacít, a 4. Zvýšenie sieťovej a komunikačnej bezpečnosti implementáciou perimetrového firewallu	3. Zvýšenie bezpečnosti pri prevádzke dobudovaním záložných dátových kapacít,	Kontinuita prevádzky	Vypracovanie kompletných podrobných plánov kontinuity prevádzky 3 systémy. Vypracovanie postupov zálohovania na obnovu siete a informačného systému	MD	40	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	20 000,00 €	24 600,00 €
4	1.3.1 - 3. Zvýšenie bezpečnosti dobudovaním záložných dátových kapacít, a 4.Zvýšenie sieťovej a komunikačnej bezpečnosti - perimetrový firewall	3. Zvýšenie bezpečnosti dobudovaním záložných dátových kapacít, a	Bezpečnosť pri prevádzke informačných systémov a sieti	Dátové úložisko pre potreby zálohnej a archivačnej kópie - support licencia	ks	1	Licencia netapp FAS2750	NetApp, Inc.	2 900,00 €	23%	667,00 €	2 900,00 €	3 567,00 €
5	1.2.1 - 3. Zvýšenie bezpečnosti pri prevádzke - dátové úložisko a 4. Zvýšenie sieťovej a komunikačnej bezpečnosti - perimetrový firewall	4. Zvýšenie sieťovej a komunikačnej bezpečnosti - perimetrový firewall	Sieťová a komunikačná bezpečnosť	Next generation firewall	ks	2	Fortigate FG400f - SKU-FG-400F - FG-400G-BDL-950-12	Fortinet, Inc.	13 200,00 €	23%	3 036,00 €	26 400,00 €	32 472,00 €
6	1.3.1 - 3. Zvýšenie bezpečnosti dobudovaním záložných dátových kapacít, a 4.Zvýšenie sieťovej a komunikačnej bezpečnosti - perimetrový firewall	4.Zvýšenie sieťovej a komunikačnej bezpečnosti - perimetrový firewal	Sieťová a komunikačná bezpečnosť	Next generation firewall - Licencia	ks	2	Fortigate FG400f UTP licencia je súčasťou ceny firewallu	Fortinet, Inc.	8 500,00 €	23%	1 955,00 €	17 000,00 €	20 910,00 €
7	1.1.3 (MRR), 1.1.2 (VRR)- 3. Zvýšenie bezpečnosti pri prevádzke dobudovaním záložných dátových kapacít, a 4. Zvýšenie sieťovej a komunikačnej bezpečnosti implementáciou perimetrového firewallu	4. Zvýšenie sieťovej a komunikačnej bezpečnosti implementáciou perimetrového firewallu	Sieťová a komunikačná bezpečnosť	Next generation firewall - práce	MD	18	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	9 000,00 €	11 070,00 €
8	1.2.3 (MRR), 1.2.2 (VRR) - 5.Implementácia systémov na nepretržitú kontrolu dátových tokov (hardvérové zariadenie) a 6 centrálny log manažment systém	5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity	Sieťová a komunikačná bezpečnosť	Sonda detekcie a prevencie prieniku - HW	ks	1	HW server Dell All-in-one model S-25 / 4x1GbE monitorovací rozhraní / 2x10/25GbE / 2x 1.92TB SSD datové úložiště / 5 roků DELL HW On-Site NBD support	GREYCORTEX s.r.o.	7 200,00 €	23%	1 656,00 €	7 200,00 €	8 856,00 €
9	1.3.3 (MRR), 1.3.2 (VRR) - 5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity a 6. Implementácia centrálneho log manažment systému	5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity	Sieťová a komunikačná bezpečnosť	Sonda detekcie a prevencie prieniku /licencia	ks	1	GreyCortex Mendel SW + licencia na 12 mesiacov	GREYCORTEX s.r.o.	9 300,00 €	23%	2 139,00 €	9 300,00 €	11 439,00 €
10	1.1.5 (MRR), 1.1.3 (VRR) - 5. Implementácia systémov na nepretržitú kontrolu dátových tokov, 6. Implementácia centrálneho log manažment systému a 7. Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.	5. Implementácia systémov na nepretržitú kontrolu dátových tokov	Sieťová a komunikačná bezpečnosť	Sonda detekcie a prevencie prieniku - práce	MD	6	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	3 000,00 €	3 690,00 €
11	1.3.3 (MRR), 1.3.2 (VRR) - 5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity a 6. Implementácia centrálneho log manažment systému	5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity	Sieťová a komunikačná bezpečnosť	Dohľadový nástroj na hranici siete - licencia	ks	1	FortiAnalyzer-VM Subscription License with Support - SKU-FC1-10-AZVMS-465-01-12	Fortinet, Inc.	1 400,00 €	23%	322,00 €	1 400,00 €	1 722,00 €
12	1.1.5 (MRR), 1.1.3 (VRR)- 5. Implementácia systémov na nepretržitú kontrolu dátových tokov, 6. Implementácia centrálneho log manažment systému a 7. Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.	5. Implementácia systémov na nepretržitú kontrolu dátových tokov	Sieťová a komunikačná bezpečnosť	Dohľadový nástroj na hranici siete - práce	MD	2	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	1 000,00 €	1 230,00 €
13	1.2.3 (MRR), 1.2.2 (VRR) - 5.Implementácia systémov na nepretržitú kontrolu dátových tokov (hardvérové zariadenie) a 6 centrálny log manažment systém	6 centrálny log manažment systém	Zaznamenávanie udalostí a monitorovanie	Nástroj na centrálny manažment logov	ks	1	Logmanager M	Logmanager a.s.	17 500,00 €	23%	4 025,00 €	17 500,00 €	21 525,00 €
14	1.3.3 (MRR), 1.3.2 (VRR) - 5.Implementácia systémov na nepretržitú kontrolu dátových tokov v interných sieťach univerzity a 6. Implementácia centrálneho log manažment systému	6. Implementácia centrálneho log manažment systému	Zaznamenávanie udalostí a monitorovanie	Nástroj na centrálny manažment logov - licencia	ks	1	Logmanager M licencia	Logmanager a.s.	3 000,00 €	23%	690,00 €	3 000,00 €	3 690,00 €
15	1.1.5 (MRR), 1.1.3 (VRR)- 5. Implementácia systémov na nepretržitú kontrolu dátových tokov, 6. Implementácia centrálneho log manažment systému a 7. Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.	6. Implementácia centrálneho log manažment systému	Zaznamenávanie udalostí a monitorovanie	Nástroj na centrálny manažment logov - práce	MD	10	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	5 000,00 €	6 150,00 €
16	1.1.5 (MRR), 1.1.3 (VRR)- 5. Implementácia systémov na nepretržitú kontrolu dátových tokov, 6. Implementácia centrálneho log manažment systému a 7. Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov.	7. Implementáciou systému na sledovanie prevádzkových parametrov a kapacít využívaných systémových prostriedkov	Zaznamenávanie udalostí a monitorovanie	Monitorovací nástroj prevádzkových parametrov	MD	10	Práce	DATALAN a.s.	500,00 €	23%	115,00 €	5 000,00 €	6 150,00 €
											Za ponúknuté produkty spolu:	192 700,00 €	237 021,00 €

Dátum: 10.6.2025

Miesto: V Bratislave

Podpis oprávnenej osoby: .....

Ing. Juraj Želko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Príloha č 3: Plán dodania Diela

Príloha č. 4: Zoznam Subdodávateľov

Príloha č. 4 Zoznam Subdodávateľov

ZOZNAM SUBDODÁVATEĽOV

„Realizácia opatrení na zvýšenie úrovne informačnej a kybernetickej bezpečnosti v prostredí Trenčianskej univerzity II“

p. č.	Obchodné meno a sídlo subdodávateľa	IČO	údaje o osobe oprávnenej konať za subdodávateľa v rozsahu meno a priezvisko, adresa pobytu, dátum narodenia	% podiel na zákazke	Predmet subdodávok
1.	Alanata,a.s., Krasovského 14, 851 01 Bratislava	54 629 331	Ing. Andrej Bališ, nar. 29.11.1986, 505 Voderady 919 42, Slovenská republika	5 %	plnenie experta
2.	ALEF Distribution SK, s.r.o. Galvaniho 17/C, 821 04 Bratislava	35 703 466	Ing. Martin Čársky, nar. 26.05.1976, Janotova 6234, 2E, Bratislava 841 04	5 %	plnenie experta
3.	-	-	-	-	-

.....

Ing. Juraj Zelko

predseda predstavenstva

DATALAN

DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020253175

Príloha č. 5: Ponuka Dodávateľa

Špecifikácia predmetu zákazky - položka: Dátové úložisko pre potreby záložnej a archivačnej kópie

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
NetApp FAS2750		
Položka predmetu zákazky - Dátové úložisko pre potreby záložnej a archivačnej kópie požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Dátové úložisko pre potreby záložnej a archivačnej kópie)**	**Doplňujúce informácie**
1	Prevedenie	Rackmount
2	Dual kontroler prevedenie v režime active-active s „controller failover"	Diskové pole nesmie obsahovať žiadny SPOF. Redundantné napájanie pre každý modul vrátane kontrolerov.
3	Pripojiteľnosť k existujúcej infraštruktúre diskových polí	Verejný obstarávateľ v súčasnosti prevádzkuje diskové polia NetApp s operačným systémom ONTAP. Vyžaduje sa plná kompatibilita s existujúcimi diskovými poľami – najmä s možnosťou využitia replikácie a vytvárania záloh medzi existujúcim a novým prostredím priamo využitím funkcionalít OS ONTAP.
4	Unified diskové úložisko podporujúce ako sieťové, tak blokové protokoly v rámci jedného kontroleru. Riešenie pridaním tzv. "NAS" gateway nebude akceptované	Áno
5	Plná virtualizácia poľa, vrátane portov (Možnosť vytvárania „virtuálnych diskových polí" s priradením logických portov a definovanými QoS).	Min 250 virtuálnych diskových polí (VDP). Možnosť bezodstávkového presúvania VDP aj logických portov medzi jednotlivými HW kontrolermi transparentne voči aplikáciám.
6	Pamäť systému	Min 32GB/Ctrl ochrana batériou pre prípad výpadku napájania,
7	On board flash cache	áno
8	Spôsob pripojenia on board cache	NVMe M.2
9	Veľkosť on board flash	Min. 2 TiB
10	Možnosť využitia SSD ako dodatočnú cache	Áno - min. do veľkosti 22 TiB
11	Architektúra	PCIe Gen 3 12Gb SAS-3 architektura
12	Počet diskových pozícií	Min. 24, rozšíriteľnosť minimálne na 144 ks diskov pre jeden HA pár kontrolerov.
13	Rozhranie pre pripojenie diskov	SAS-3, 12 Gbps, PCIe Gen 3 alebo rýchlejšie
14	Podporované disky	2,5" HDD/SSD, 3,5" NL-SAS/SSD
15	Požadovaný počet diskov	24 x 1,8TB SAS
16	Podporované RAID	RAID-4, RAID-DP (RAID-6), RAID-TEC (alebo podobná ochrana proti výpadku 3 diskov súčasne v tej istej RAID skupine)
17	Požiadavky na RAID skupiny	SAS/SSD – ochrana proti výpadku min 2 diskov so zápisom bez RAID penalty – obdobne ako RAID10 NL-SAS ochrana proti výpadku min 3 diskov
18	Podpora pre volumy do veľkosti	Aspoň 100 TiB
19	Možnosť pridávania ďalších kontrolerov a kapacity. Pridávané kontrolery môžu byť aj odlišného typu ako je požadovaný	Áno. Pre NAS min. 24 kontrolerov. Pre SAN min. 12 kontrolerov. Pridávanie a odoberanie kontrolerov je možné počas plnej prevádzky diskového poľa bez potreby odstávky.
20	Podporované protokoly	FC; FCoE; iSCSI; NFS; pNFS; CIFS/SMB, S3
21	Požadovaná pripojiteľnosť k hostom	Min. 8 portov 10Gb s káblami Twinax
22	Škálovateľnosť pripojenia k hostom	možnosť zmenit výmenou na porty 16GbE možnosť kombinovať porty FC 16Gb/10GbE
23	Napájacie káble	rack káble, C14-C13 koncovka
24	Podporované funkcionality	Možnosť vytvárania priestorovo efektívnych snapshotov a klonov s možnosťou vytvárania viacerých konzistentných skupín na úrovni jednotlivých aplikácií
25	Podpora sync a async replikácie	Áno
26	Podpora Geo clustera cez IP	Áno
27	Licenčné pokrytie	Funkcionalitu poskytuje s kapacitne a časovo neobmedzeným licenčným pokrytím. Možnosť vytvárania väčších LUN ako 2TB, pričom uvedenú funkcionalitu poskytuje s kapacitne, časovo neobmedzenou licenciou
28	Bezodstávková prevádzka	Diskové pole musí umožňovať upgrade firmware diskového poľa (vrátane firmware diskov) bez odstávky diskového poľa.
29	Bezodstávkové presúvanie dát	Zariadenie musí dovolíť presúvať dátové volumy a LUNy medzi rôznymi skupinami diskov, bez ohľadu na to, akým protokolom sú dáta sprístupňované. Presuny musia byť transparentné voči pripojeným aplikáciám a serverom, t.j. celá činnosť musí byť bez dopadu na servery a aplikácie.
30	Podpora cachingu medzi SSD a HDD	Áno, na celú ponúkanú kapacitu.
31	Thin Provisioning vrátane zero detect space reclamation.	Áno, bez potreby externej aplikácie.
32	Podpora snapshotov	1023 per volume
33	Fast Drive Zeroing	Áno
34	Podpora QoS	Áno
35	Podpora SMB Multichannel	Áno
36	Microsoft VSS support	Áno
37	Plná VAAI podpora (vStorage API for Array Integration)	Áno
38	Podpora WORM funkcie bez potreby externej aplikácie	Áno
39	Podpora vytvárania Backup využitím prostriedkov poľa bez potreby externej aplikácie.	Áno
40	Natívna možnosť integrácie do cloudového prostredia pre Google, AWS, Azure. Podpora vytvárania DR lokalít v cloudovom prostredí. Podpora pre spustenie virtuálneho diskového poľa v privátnom cloude s podporou vzájomnej replikácie využitím SW prostriedkov poľa.	Áno
41	Backup do cloudoveho prostredia pomocou snapshotov	Áno
42	Podpora automatického vyhodnocovania a presúvania nepoužívaných dát do privátneho cloudu (cloud tiering) pre SSD	Áno
43	Plná podpora „HW a SW Data At Rest Encryption"	Áno, s možnosťou použitia ako interného („OnBoard"), tak aj externého key managera

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	512	
hodnota	32GB/Ctrl ochrana batériou pre prípad výpadku napájania	
áno/nie	áno	
áno/nie	áno	
hodnota	áno	
áno/nie	áno	142 TiB
áno/nie	áno	
hodnota	áno	
áno/nie	áno	
hodnota	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	áno	300TiB
áno/nie	áno	
áno/nie	áno	
hodnota	áno	
áno/nie	áno	
áno/nie	áno	
hodnota		
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	1023	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	áno	
áno/nie	áno	
áno/nie	áno	

44	Deduplikácia,komprimácia a kompakcia dát	Áno, na celú ponúkanú kapacitu.	áno/nie	áno	
45	Podpora RBAC	Áno	áno/nie	áno	
46	Podpora Nativnej ochrany poľa proti Ramsomware.	Áno	áno/nie	áno	
47	Integrácia do aplikačného prostredia	Minimálne VMware, SQL, Oracle, Splunk, Docker, Active Directory	áno/nie	áno	
48	Funkcia File servera	Na úrovni NAS schopnosť poskytovať služby file servera s integráciou do MS Active Directory	áno/nie	áno	
49	Popora operačných systémov:	Minimálne Windows® 2000, Windows Server® 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016, Linux®, Oracle® Solaris, AIX, HP-UX, Mac® OS, VMware®, ESX®	áno/nie	áno	
50	Napájanie a chladenie	Plne redundantné, zdroje a ventilátory typu hot-swap	áno/nie	áno	
51	Požiadavky na tovar / dodávku	Dodaný tovar bude nový, nepoužitý, nerepasovaný. Dodávateľ preukáže, že dodaný tovar pochádza z predajného kanála autorizovaného výrobcom.	áno/nie	áno	
52	Výrobca diskového poľa musí byť zároveň výrobcom jeho obslužného softvéru (operačného systému).	Áno	áno/nie	áno	
53	Podpora výrobcu	„call home" podpora výrobcu diskového poľa. Proaktívny monitoring stavu kapacitného a výkonového vyťaženia, upozornenia na dostupné updaty a bugfixy. Automatizovaná emailová notifikácia pri poruchách jednotlivých komponentov. Automatizované otváranie ticketov pri poruchách. Informácie o stave diskového poľa a o dostupnosti aktualizácií a proaktívnych notifikácií prostredníctvom mobilnej aplikácie.	áno/nie	áno	
54	Kompatibilita	Z dôvodu ochrany investície sa vyžaduje dodanie rozširúcej diskovej police s diskami pre pripojenie k existujúcemu diskovému poľu NetApp FAS2552.	áno/nie	áno	
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
55	Servisná podpora na hardvér aj softvér diskového poľa priamo od výrobcu diskového poľa počas trvania 2 roky a s doručením pokazeného komponentu nasledujúci pracovný deň	Záruka, SLA	áno/nie	áno	3 roky
56	Implementačné a konfiguračné práce v rozsahu 10 MD	Práce	áno/nie	áno	
57	2 ročná licencia zabezpečujúca záruku a prémiovú technickú podporu 24x7	Licencia	áno/nie	áno	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

.....
Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Špecifikácia predmetu zákazky - položka: Vypracovanie kompletných podrobných plánov kontinuity prevádzky 3 systémy. Vypracovanie postupov zálohovania na obnovu siete a informačného systému

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"	**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
DATALAN smernice a BCM plány			
Položka predmetu zákazky - Vypracovanie kompletných podrobných plánov kontinuity prevádzky 3 systémy. Vypracovanie postupov zálohovania na obnovu siete a informačného systému požadovaný počet: 40 človekohodín			
P. č.	**Parameter/časť položky**	**Požadovaný formát ponúkaných parametrov**	**1.** TU UVEĎTE ponúkané parametre	**2.**
1	Vypracovanie stratégie a krízových plánov prevádzky na základe analýzy vplyvov kybernetického bezpečnostného incidentu na základnú službu s ohľadom na relevantnú legislatívu vzťahujúcu sa na BCM: Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe , Vyhláška č. 179/2020 Z. z..	áno/nie	áno	
2	Vypracovanie dekompozície dôležitých služieb a vypracovanie BIA pre tieto služby, resp. systémy. Politika BCM vrátane stratégie obnovy a návrh pred-vyplnenej šablóny pre BCP a DRP pre tri vybrané kritické systémy, bude obsahovať krízové plány na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu na základnú službu, plány havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu, postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu obsahujú najmenej:	áno/nie	áno	
3	• frekvenciu a rozsah jej dokumentovania a schvaľovania,	áno/nie	áno	
4	• určenie osoby zodpovednej za zálohovanie,	áno/nie	áno	
5	• časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní,	áno/nie	áno	
6	• požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom,	áno/nie	áno	
7	• požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,	áno/nie	áno	
8	• požiadavku na vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov.	áno/nie	áno	
9	Kľúčové kapitoly BCM plánu:	áno/nie	áno	
10	• Účel a rozsah BCM v ktorom budú zadefinované ciele a rozsah pôsobnosti v rámci organizácie	áno/nie	áno	
11	• Identifikácia kritických procesov (BIA), ktoré môžu mať vplyv na chod organizácie	áno/nie	áno	
12	• Hodnotenie a riadenie rizík potenciálnych hrozieb a zraniteľností, ktoré môžu ovplyvniť kontinuitu činností.	áno/nie	áno	
13	• Vypracovanie stratégií obnovy (DRP) v ktorom budú zadefinované postupy na obnovu prevádzky a služieb po incidente.	áno/nie	áno	
14	• Implementácia komunikačného plánu s definovaním interných a externých komunikačné kanálov a zodpovedností počas krízových situácií.	áno/nie	áno	
15	• Pravidelné testovanie a aktualizácia plánu, zadefinovanie časových rámcov a intervalov	áno/nie	áno	
16	• Riadenie zdrojov pre kontinuitu prevádzky s opisom personálnych, finančných a technických zdrojov na zvládanie kríz.	áno/nie	áno	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Špecifikácia predmetu zákazky - položka: Next generation firewall

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu	Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu**	**POZNÁMKA**
Fortinet / Fortigate FG400f / 18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 8 x GE SFP slots, 8 x 10GE SFP+ slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies, Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium) / FG-400G-BDL-950-12	(áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"	(napr. doplňujúce informácie k uvedeným parametrom a pod.)
Položka predmetu zákazky - Next generation firewall **požadovaný počet: 2 ks**	**Požadovaný formát ponúkaných parametrov**	**1.** TU UVEĎTE ponúkané parametre	**2.**
P. č. **Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Next generation firewall)** **Doplňujúce informácie**			
1	HW appliance NGFW/UTM firewallu v režime vysokej dostupnosti (dve fyzické zariadenia rovnakého typu zapojené do funkčného clustra); Platforma postavená na HW akcelerovanej architektúre (t.j. zariadenia vybavené špecializovanými obvodmi FPGA/ASIC pre spracovanie komunikácie a vybraných výpočtovo náročných funkcií ; HW appliance do racku s veľkosťou 1RU; Kompletné príslušenstvo (montážne prvky) pre montáž do RACKu; Možnosť doplniť druhý napájací zdroj (interný alebo externý), alebo zariadenie vybavené dvoma zdrojmi;	áno/nie	áno	Fortigate FG400F + UTP licencia
2	Rozhrania na každom firewalle využiteľné pre management min. 2x GE RJ45	hodnota	2x GE RJ45	
3	Rozhrania na každom firewalle využiteľné pre spracovanie komunikácie min. 18x GE RJ45 Ports, 8x GE SFP Slots, 8x 10 GE SFP+ Slots	hodnota		
4	Podpora režimu vysokej dostupnosti (režim L2 cluster s využitím virtuálnych MAC adries; celý cluster sa prezentuje z pohľadu L3 ako jedno zariadenie) v režime active-active (A/A) a active-passive (A/P). Ak táto funkcia vyžaduje licenciu, tak táto musí byť súčasťou dodávky.	áno/nie	áno	
5	Podpora VLAN min. 4000	hodnota		
6	Podpora LACP	áno/nie	áno	
7	Počet FW pravidiel min. 8000	hodnota	10 000	
8	Možnosť definície FW pravidiel v tzv. NGFW režime (tj. súčasťou základnej definície FW pravidla) je: min. zdrojové a cieľové rozhranie, zdrojová a cieľová adresa, služba, čas, aplikácia, používateľ, kategórie URL filteringu ako kritérium zhody, nie ako profil aplikovaný na dané pravidlo.	áno/nie	áno	
9	Celková priepustnosť firewallu min. 79.5 / 78.5 / 70 Gbps (merané na UDP paketoch s veľkosťou 1518B/512B/64B)	hodnota	79.5 / 78.5 / 70 Gbps	
10	Latencia firewallu nepresahuje 5 µs (merané na malých UDP paketoch (64B))	hodnota	4.19 µs	
11	Počet nových spojení za sekundu (setup-rate) min. 480 000	hodnota	500 000	
12	Celkový počet súčasných TCP spojení firewallu min. 7 500 000	hodnota	7 800 000	
13	PPS (počet spracovaných paketov za 1 sekundu) min. 45 000 000	hodnota	45 000 000	
14	Funkcia detekcie aplikácií na L7 (Application Control)	áno/nie	áno	
15	Detekcia známych aplikácií na základe signatúr min 3500 preddefinovaných aplikácií/signatúr	hodnota	3500	
16	pre populárne cloud aplikácie (minimálne Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) sa požadujú pokročilé funkcie typu blokovanie upload/download súborov, blokovanie hier v rámci aplikácie, blokovanie login, atď. (relevantné k danej aplikácii)	áno/nie	áno	
17	aplikácie je možné: povoliť, monitorovať, blokovať, obmedziť šírku pásma pre danú aplikáciu	áno/nie	áno	
18	priepustnosť funkcie Application Control vrátane logovania (merané s HTTP 64K response) min. 27 Gbps	hodnota	28 Gbps	
19	podpora použitia Application control aj formou profilov priradených k pravidlám	áno/nie	áno	
20	Funkcie detekcie a zamedzenia narušení (IPS/IDS)	áno/nie	áno	
21	počet rozpoznávaných hrozieb (signatúr) definovaných výrobcom min. 11000	hodnota	11000	
22	funkcia IPS sa konfiguruje v rámci IPS profilov, ktoré sú následne priradené konkrétnym FW pravidlám	áno/nie	áno	
23	možnosť tvorby vlastných signatúr pre aplikačnú kontrolu a IPS	áno/nie	áno	
24	priepustnosť funkcie IPS vrátane logovania min. 12 Gbps	hodnota	12 Gbps	
25	Funkcie antivírovej kontroly	áno/nie	áno	
26	Ochrana pred škodlivým kódom, vrátane ochrany pred polymorfným kódom	áno/nie	áno	
27	AV kontrola rozšírená o inšpekciu tzv. sandbox technikou Cloud alebo on-premise Sandboxing. Súčasťou dodávky musia byť aj všetky potrebné licencie alebo HW prostriedky	áno/nie	áno	
28	Priepustnosť FW pri zapnutí IPS, Application Control, Antivirus, Web Filtering a zapnutým logovaním min. 9 Gbps	hodnota	10 Gbps	
29	Podpora služby výrobcu umožňujúca detekovať malware, ktorý bol objavený v dobe od poslednej aktualizácie AV signatúrovej databázy pomocou globálnej a rýchle sa aktualizujúcej databázy hash-ov	áno/nie	áno	
30	Podpora funkcie odstránenia aktívneho obsahu z dokumentov kancelárskych aplikácií – AV engine na firewalle v reálnom čase odstráni aktívny obsah z dokumentu pričom tento zostáva v pôvodnom formáte, ale sú z neho odstránené všetky aktívne prvky	áno/nie	áno	
31	Podpora SSL dešifrovania/SSL inšpekcie min. 8 Gbps (HTTPS prevádzka, merané v kombinácii s IPS kontrolou)	hodnota	8 Gbps	
32	Funkcia DNS filtra	áno/nie	áno	
33	Možnosť blokovať DNS dotazy na základe príslušnosti k URL kategórii	áno/nie	áno	
34	Možnosť definovať vlastný tzv. blacklist domén	áno/nie	áno	
35	Možnosť presmerovať komunikáciu so zakázanými doménami na vlastný portál/URL	áno/nie	áno	
36	Podpora funkcie explicit proxy s možnosťou aktivovania požadovaných ochranných profilov (AV, IPS, AppCtrl, DLP, Web Filtering) a podpora transparentného overovania používateľov voči MS AD protokolom Kerberos	áno/nie	áno	
37	Funkcia transparentného overovania používateľov pomocou domény (MS Active Directory) vrátane podpory autentifikácie používateľov na terminálovom serveri	áno/nie	áno	
38	Podpora SSL VPN	áno/nie	áno	
39	Priepustnost SSL VPN min. 3,5 Gbps	hodnota	3.6 Gbps	
40	Popora IPSEC VPN v režime site-2-site aj client-2-site	áno/nie	áno	
41	Priepustnosť IPSEC VPN (AES256-SHA256, UDP packet size 512B) min. 55 Gbps	hodnota	55 Gbps	
42	Podpora izolovaných virtuálnych kontextov (virtualizácia FW na danom HW). Každý virtuálny kontext musí byť plnohodnotné riešenie vrátane oddeleného managementu účtov, objektov, politík, smerovania a pod.	áno/nie	áno	
43	FW cluster je možné plnohodnotne spravovať pomocou lokálneho GUI a CLI, bez nutnosti inštalovať klienta na koncovú (management) stanicu;	áno/nie	áno	
44	Jedno manažment rozhranie pre celý cluster, akákoľvek zmena je medzi jednotlivými uzlami klastra synchronizovaná automaticky	áno/nie	áno	
45	Podpora SNMP vrátane SMPB MIB súboru dodávaného výrobcom, možnosť začlenenia do existujúceho systému dohľadu siete	áno/nie	áno	
46	Požaduje sa certifikácia ICSA Labs minimálne pre Firewall	áno/nie	áno	
47	Možnosť automatizácie na základe udalostí ktoré je Firewall schopný zaznamenať.	áno/nie	áno	
48	Možnosť kombinovať akcie pre automatizačné pravidlá min. webhook s definovateľnými parametrami, CLI script, Email, MS-TEAMS notifikácia, Slack notifikácia, Karanténa na základe IP, MAC adresy.	áno/nie	áno	
49	Možnosť použitia dynamických vstupných parametrov v rámci automatizačných pravidiel min. schopnost parsovat vstupy z logov a z predchádzajúcich vykonaných akcií	áno/nie	áno	
50	Podpora otvoreného API pre ďalšie možnosti integrácie	áno/nie	áno	

Osobitné požiadavky na plnenie:				**Osobitné požiadavky na plnenie:**		
52	2 roky priamo od výrobcu zariadenia, odozva najneskôr do 4h od nahlásenia, vrátane víkendov a sviatkov. Servis bude poskytovaný v mieste inštalácie. Nahlasovanie poruchy v režime 24x7. Nahlasovanie porúch priamo u výrobcu zariadenia.	Záruka		áno/nie	áno	
53	Implementačné a konfiguračné práce s otestovaním, zaškolením a dokumentáciou riešenia, Implementácia MFA pre vzdialený prístup do siete v rozsahu 18 človekohodín	Práce		áno/nie	áno	
	Implementačné práce pre MFA Implementačné práce pre nasadenie MFA na navrhovaných technológiách s existujúcim systémom M365 pre všetkých užívateľov s vytvoreným VPN pripojením :			áno/nie	áno	
	Analýza a identifikácia požiadaviek: o Analýza existujúcej infraštruktúry a identifikácia systémov, kde bude MFA nasadené. o Definovanie bezpečnostných požiadaviek a politík prístupu.			áno/nie	áno	
	Nasadenie MFA na next generation firewall: o Konfigurácia autentifikátora ako zdroja MFA. o Nastavenie RADIUS servera pre autentifikáciu používateľov. o Aktivácia MFA na SSL VPN, IPsec VPN a administrátorských prístupoch. o Testovanie funkčnosti MFA s rôznymi scenármi prístupu.			áno/nie	áno	
	Nasadenie MFA na Microsoft 365: o Aktivácia MFA v Microsoft 365 Admin Centre. o Konfigurácia Conditional Access Policies pre riadenie prístupov. o Registrácia používateľských zariadení pre MFA (mobilné aplikácie, SMS, e-mail). o Testovanie prihlásení a overenie správnosti nastavení			áno/nie	áno	
	Vzdelávanie a podpora: o Školenie zamestnancov o používaní MFA a postupoch v prípade problémov s prístupom. o Vytvorenie dokumentácie s postupmi pre koncových používateľov.			áno/nie	áno	
	Monitorovanie a optimalizácia: o Pravidelné monitorovanie prístupových logov a analýza bezpečnostných incidentov. oÚprava politík na základe spätnej väzby a nových bezpečnostných požiadaviek			áno/nie	áno	
54	1 ročná licencia zabezpečujúca záruku a prémiovú technickú podporu 24x7 a nasledovné služby aktualizácií firmware, a komponentov a služieb firewallu ako (IPS, Advanced Malware Protection, aplikačná kontrola, Web a Video filtrovanie, Antispam služba)	Licencia		áno/nie	áno	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

.....
Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Špecifikácia predmetu zákazky - položka: Dohľadový nástroj na hranici siete

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
Fortinet / FortiAnalyzer-VM Subscription License with Support / Subscription license for 5 GB/Day Central Logging & Analytics. Include FortiCare Premium support, IOC, Security Automation Service and FortiGuard Outbreak Detection Service. / FC1-10-AZVMS-465-01-12		
Položka predmetu zákazky - Dohľadový nástroj na hranici siete požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Dohľadový nástroj na hranici siete**	**Doplňujúce informácie**
1	Systém pre ukladanie a koreláciu logov v sieti obstarávateľa.	
2	Systém musí byť plne kompatibilný s dodávanými riešeniami pre NGFW/UTM, Switche, 2FA AUTHENTICATION, Mailova ochrana, Sandbox riesenie	
3	Riešenie vo forme subskribcnej licencie	
4	Schopnost spracovávať logy v objeme GB/deň	min. 5 GB za deň
5	Možnosť škálovateľného navýšenia objemu spracovávaných logov pomocou licencií	
6	Podpora SYSLOG, podpora šifrovaného prenosu dát/logov	
7	Riešenie musí obsahovať konfigurovateľné prehľady s drill down funkcionalitou	
8	Filtrovanie správ/logov na základe roznych parametrov, ich kombinácií. Podpora AND, OR logiky pri vytváraní filtrov	
9	Možnosť ukladania definícií filtrov pre rýchle opätovné použitie	
10	Možnosť prehliadania logov v historickom alebo realtime režime	
11	Možnosť zobrazovania logov v RAW alebo štruktorovanom formáte	
12	Korelácia logov	
13	Možnosť automatického vytvárania incidentov	
14	Možnosť automatického vyšetrovania incidentov pomocou definovateľných playbookov	
15	Podpora Indication of Compromise - Systém musí obsahovať reputačné databázy nebezpečných IP/URL adries a musí vykonávať spätné prehľadávanie historických logov pri update reputačných DB za účelom detekcie napadnutia systémov a koncových staníc	min. 7 dní do minulosti
16	Licencia umožňuje ďalšiu automatizáciu reakcii na incidenty s vylepšeným monitorovaním a eskaláciou, vstavanými pracovnými postupmi správy incidentov, konektormi, príručkami	
17	Licencia poskytuje automatické sťahovanie balíkov obsahu na detekciu najnovšieho malvéru, vrátane súhrnu prepuknutia a mapovania reťazca utoku, aby sa zistilo, ako malvér funguje. Licendia dalej obsahuje správu o vzniku utoku, detail udalostí a šablónu správy o detekovani vzniku utoku	
18	Podpora vytvárania reportov v formátoch PDF, HTML, CSV, XML	
19	Možnosť generovania reportov v pravidelných intervaloch	
20	Možnosť vytvárania vlastných požiadaviek voči databáze a ich použitie ako zdroj dát v reportoch	
21	Podpora SNMP	
22	Podpora REST API	
23	GUI a CLI administračné rozhranie dostupné pomocou HTTPS a SSH protokolov	
24	Podpora LDAP, RADIUS, Tacacs+ pre administrátorské účty	
Osobitné požiadavky na plnenie:		
25	Inštalácia na zdrojoch poskytnutných obstarávateľom v rozsahu 2 človekodni Zoznam implementačných prác pre nasadenie dohľadového nástroja na hranici siete Analýza požiadaviek a plánovanie: o Zhodnotenie existujúcej infraštruktúry, bezpečnostných potrieb a požiadaviek na logovanie. Príprava prostredia: o Overenie virtuálnych zdrojov potrebných pre inštaláciu dohľadového nástroja na hranici siete. Inštalácia dohľadového nástroja na hranici siete: o Nasadenie dohľadového nástroja vo virtuálnom prostredí (VMware, Hyper-V). Základná konfigurácia systému: o Nastavenie sieťových parametrov (IP adresy, DNS, NTP), zabezpečenie prístupov a definovanie admin účtov. Integrácia s kompatibilnými zariadeniami: o Konfigurácia dodaných NGFW a iných zariadení na odosielanie logov do dohľadového nástroja na hranici siete. Nastavenie politiky uchovávania logov: o Definovanie retenčných politik pre efektívne spravovanie dát a súlad s legislatívou. Konfigurácia analýzy a reportingu: o Vytvorenie prispôsobených dashboardov, reportov a upozornení pre sledovanie incidentov. Bezpečnostné opatrenia: o Nastavenie šifrovania logov, správa prístupových práv a implementácia autentifikačných mechanizmov. Testovanie a validácia: o Overenie funkčnosti prenosu logov, správnosti reportov a výkonu systému. Školenie administrátorov a používateľov: o Zaškolenie tímu na správu dohľadového nástroja na hranici siete, tvorbu reportov a riešenie incidentov. Dokumentácia: o Vypracovanie technickej a prevádzkovej dokumentácie pre budúcu správu systému.	Práce
26	1 ročná subscription licencia zabezpečujúca záruku a technickú podporu	Licencia

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	5GB za deň	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
hodnota	áno 7 dní	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
Osobitné požiadavky na plnenie:		
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Špecifikácia predmetu zákazky - položka: Sonda detekcie a prevencie prieniku - HW + licencia

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu			Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
GREYCORTEX Mendel AiO: sensor + collector / 500Mbps sustained throughput / 500 enriched flows per second &1000 NetFlow per second / 1500 monitored IPs / Full feature set + HW server Dell All-in-one model S-25 / 4x1GbE monitorovací rozhraní / 2x10/25GbE / 2x 1.92TB SSD datové úložiště / 5 roků DELL HW On-Site NBD support					
Položka predmetu zákazky - Sonda detekcie a prevencie prieniku - HW + licencia požadovaný počet: 1 ks					
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Sonda detekcie a prevencie prieniku - HW + licencia)**	**Doplňujúce informácie**	**Požadovaný formát ponúkaných parametrov**	**1.** TU UVEĎTE ponúkané parametre	**2.**
1	Systém pre analýzu sieťovej prevádzky		áno/nie	áno	
2		Systém zložený z hardvérových zariadení musí monitorovať sieťovú aktivitu v reálnom čase a identifikovať potenciálne kybernetické hrozby, bezpečnostné riziká a anomálne správanie a musí o nich v reálnom čase vytvárať upozornenia.	áno/nie	áno	
3		Dodaný systém musí analyzovať sieť na základe zrkadlenej sieťovej prevádzky zo SPAN portov alebo TAPov (nie len na základe štatistických protokolov typu NetFlow) a zároveň bez potreby nasadzovať agentov na koncové stanice alebo ďalšie zariadenia v sieti.	áno/nie	áno	
4		Systém musí analyzovať obsah dátových paketov v reálnom čase a detekovať protokol alebo aplikáciu na základe obsahu prevádzky prostredníctvom DPI (Deep Packet Inspection), nie iba čísla portu.	áno/nie	áno	
5		Dodaný systém musí byť schopný analyzovať sieť aj na základe spracovania štatistických protokolov typu NetFlow, IPFIX, NetStream, Cisco NSEL a prípadne ďalších.	áno/nie	áno	
6		Systém musí byť plne funkčný v offline prostredí objednávateľa bez využitia cloudového prostredia na zber, ukladanie a spracovanie dát a všetky konfigurácie a reporting sú k dispozícii priamo v systéme.	áno/nie	áno	
7		Aktualizácia systému musí byť možné vykonávať užívateľsky v offline režime.	áno/nie	áno	
8	Spracovanie a ukladanie sieťových tokov		áno/nie	áno	
9		Systém ukladá sieťové toky vo formáte, ktorý umožní analýzu sieťovej komunikácie na úrovni jednotlivých tokov, vrátane vyhľadania informácií o aplikačných transakciách a ich metadátach z L2 až L7, obsiahnutých v danom sieťovom toku.	áno/nie	áno	
10		Požadované protokoly pre ukladanie aplikačných metadát z jednotlivých transakcií sú: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAP, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP , FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapuzdrenie.	áno/nie	áno	
11		Vyžaduje sa vysokorýchlostné úložisko pre uchovanie histórie dátových tokov na dobu minimálne 12 mesiacov zloženej z SSD alebo NVMe diskov.	áno/nie	áno	
12	Analýza aplikačných a systémových logov		áno/nie	áno	
13		Systém musí byť schopný zbierať a analyzovať aplikačné a systémové logy vo formáte syslog z dohľadovaných zariadení a identifikovať nebezpečné alebo potenciálne škodlivé aktivity.	áno/nie	áno	
14	Používateľské rozhranie		áno/nie	áno	
15		Systém musí poskytovať jednotné grafické používateľské rozhranie pre všetku prácu používateľov, vrátane všetkých detekcií, analýzy sieťových štatistík, nastavenia systému, konfiguráciu alertov, reportov a dashboardov.	áno/nie	áno	
16		Systém musí byť schopný vytváranie profilov a skupín užívateľov pre obmedzenie funkcionality produktu a viditeľnosti uložených dát s podporou minimálne:	áno/nie	áno	
17		• granulárneho nastavenia prístupu k analytickým aj konfiguračným/administratívnym komponentom systému s definovanými úrovňami prístupu (aspoň read, write, execute),	áno/nie	áno	
18		• granulárneho nastavenia prístupu k dátam z rôznych segmentov siete organizácie s definovanými úrovňami prístupu (aspoň read, write, execute),	áno/nie	áno	
19		• vytváranie vlastných filtrov všetkých dát a ich zdieľanie medzi užívateľmi a skupinami užívateľov,	áno/nie	áno	
20		• vytváranie vlastných užívateľských pohľadov, reportov, dashboardov a pod.	áno/nie	áno	
21	Automatické hlásenie (alerty) a reporting		áno/nie	áno	
22		Systém musí byť schopný upozorňovať užívateľa prostredníctvom minimálne emailu a logu o všetkých identifikovaných udalostiach a ďalej o udalostiach filtrovaných minimálne podľa IP a MAC adresy, podsiete, závažnosti udalosti, kategórie udalosti, krajiny, užívateľa, sieťové služby, čísla portu, prevádzky do/z internetu .	áno/nie	áno	
23		Tieto alerty musí byť systém schopný dodávať aj v strojovo čitateľnom formáte pre využitie v nástrojoch typu SIEM a musí obsahovať minimálne kompletné informácie o detegovanej udalosti vrátane URL odkazu na danú udalosť v reportovanom období do grafického rozhrania systému.	áno/nie	áno	
24		Systém musí mať možnosť vytvárania automatizovaných manažérskych reportov o stave kybernetickej bezpečnosti z pohľadu správy kybernetických incidentov ideálne podľa oblastí ich vznikov (napr.: doména, web, email a pod.).	áno/nie	áno	
25		Je požadované vytváranie automatizovaných reportov v slovenskom jazyku.	áno/nie	áno	
26	Integrácia systému		áno/nie	áno	
27		Systém musí poskytovať hotové nástroje umožňujúce integráciu so softvérom tretích strán bez použitia API systému, a to minimálne:	áno/nie	áno	
28		• syslog, CEF a LEEF pre export udalostí vrátane plnej podpory filtrov (exportovanie iba požadovaných dát)	áno/nie	áno	
29		• priame url odkazy na ľubovoľnú obrazovku grafického používateľského rozhrania a filtrované zobrazenia v grafickom používateľskom rozhraní	áno/nie	áno	
30		• export informácií o toku vo formáte IPFIX alebo podobnom formáte vrátane plnej podpory filtrov (exportovať je možné iba požadované dáta) vrátane aplikačných metadát aspoň pre protokoly HTTP, HTTPS a SMTP	áno/nie	áno	
31		• integrácia so službami identity užívateľov bez nutnosti konfigurácie zasielania logov do systému – minimálne Cisco ISE a Microsoft Active Directory	áno/nie	áno	
32		• integrácia s firewallmi, aspoň Cisco, Palo Alto, Fortinet a Checkpoint, pre automatické a manuálne reakcie vyvolané systémom	áno/nie	áno	
33		• integrácia s nástrojmi pre riadenie prístupu k sieti minimálne Cisco ISE, pre automatickú a manuálnu reakciu systému.	áno/nie	áno	
34	Podpora EDR		áno/nie	áno	
35		Systém musí poskytovať nástroje umožňujúce priamu integráciu so softvérom EDR tretích strán pre získanie informácií a skvalitnenie detekcie.	áno/nie	áno	
36	Podpora SDN (softvérovo definovanej siete)		áno/nie	áno	
37		Systém musí poskytovať integráciu s technológiou CISCO ACI pre získanie informácií o EPG (endpoint groups) a EPSG (endpoint security groups)	áno/nie	áno	
38		Systém musí poskytovať aktuálne informácie o členstve jednotlivých zariadení v skupinách EPG a EPSG. Systém musí umožňovať ľubovoľné filtrovanie a vyhľadávanie zariadenia.	áno/nie	áno	
39		Systém musí byť schopný vizualizovať prestupy zariadenia a podsietí podľa získaných parametrov EPG a EPSG s možnosťou ľubovoľnej ďalšej užívateľskej filtrácie.	áno/nie	áno	
40	Schopnosť detekcie bezpečnostných udalostí		áno/nie	áno	
41	Monitorovanie zariadení, segmentov siete a využívaných sieťových služieb		áno/nie	áno	
42		Dodaný systém musí identifikovať všetky zariadenia pripojené do siete vrátane koncových zariadení, serverov, IoT, OT zariadení a pod. Zároveň musí byť systém schopný identifikovať zmeny v sieti – minimálne:	áno/nie	áno	
43		zmena IP/MAC adresy host,	áno/nie	áno	

44		duplicitná IP/MAC adresa,	áno/nie	áno	
45		zmena na VLAN,	áno/nie	áno	
46		vytvorení novej podsiete,	áno/nie	áno	
47		pripojenie nového zariadenia	áno/nie	áno	
48		použití nebo vznik nové služby,	áno/nie	áno	
49		nedostupnosť skôr dostupné a komunikujúce služby alebo skôr dostupného a komunikujúceho zariadenia,	áno/nie	áno	
50		prístup nového zariadenia k službe či zariadeniu	áno/nie	áno	
51		overovanie platnosti interných certifikátov pre validné TLS šifrovanie u HTTPS a upozornenia pred dátumom ich vypršania.	áno/nie	áno	
52		Systém musí užívateľovi umožniť pomocou týchto detekčných metód nastavovať bezpečnostné politiky pre rôzne segmenty siete a pre rôzne zariadenia a na porušenie týchto politik reagovať upozornením	áno/nie	áno	
53	Samostatné učenie behaviorálnych aktivit a detekcia anomálií		áno/nie	áno	
54		Systém musí používať matematické metódy samostatného učenia pre analýzu sieťovej aktivity, vytvárať av čase automaticky modifikovať modely správania na základe bežného správania jednotlivých zariadení a na nich prevádzkovaných služieb v rámci celej organizácie	áno/nie	áno	
55		Systém musí mať schopnosť na základe matematického modelu daného zariadenia a jeho služieb identifikovať neštandardné sieťové správanie, a to najmä odchýlky od modelu normálneho správania pre:	áno/nie	áno	
56		odchýlku od modelu na prenos dát, tokov a paketov	áno/nie	áno	
57		odchýlku od modelu pre počet komunikačných partnerov,	áno/nie	áno	
58		odchýlku od modelu entropie na komunikačných portoch,	áno/nie	áno	
59		odchýlku od modelu pre počet sieťových tokov a využitých sieťových služieb,	áno/nie	áno	
60		odchýlku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy),	áno/nie	áno	
61		Samostatné učenie je požadované na všetkých sieťových zariadeniach a na nich prevádzkovaných službách (port číslo 0 až 65535 pri TCP aj UDP) na IPv4 a IPv6 a ďalších protokoloch L3 a L4 sieťovej vrstvy.	áno/nie	áno	
62	Identifikácia neznámych hrozieb a podozrivých správaní		áno/nie	áno	
63		Systém musí byť schopný detekovať neznáme hrozby, ktoré nemožno identifikovať prostredníctvom detekčných signatúr, ako sú trójske kone, botnety a pod. Najmä musia byť identifikované tieto príznaky potenciálne škodlivého správania:	áno/nie	áno	
64		prieskumné aktivity v sieti,	áno/nie	áno	
65		detekcia podozrivého strojového správania, ktoré nevytvárajú ľudskí používatelia siete,	áno/nie	áno	
66		detekcia repetitívnych vzorcov správania na sieti,	áno/nie	áno	
67		detekcia botnetov a ovládanie kompromitovanej stanice,	áno/nie	áno	
68		detekcia príznakov šifrovania kryptomien,	áno/nie	áno	
69		útoky hrubou silou a enumerace dat,	áno/nie	áno	
70		rozpoznanie tunelovanej sieťovej prevádzky – aspoň IPv4 prostredníctvom IPv6 a DNS tunelov.	áno/nie	áno	
71	Detekcia na základe databázy známych hrozieb		áno/nie	áno	
72		Systém musí byť schopný identifikovať hrozby a reportovať udalosti na základe	áno/nie	áno	
73		detekčná databáza známych hrozieb, tj malware (trójske kone, vírusy, červy, rootkity, apod.), známych útokov (exploity) a zraniteľnosti, porušenie bezpečnostných pravidiel a „best practices" a ďalších rizík	áno/nie	áno	
74		reputačná databáza známych škodlivých IP adries, TLS certifikátov, záznamov DNS a hostname, URL adries a hashov súborov.	áno/nie	áno	
75		Tieto databázy musia byť aktualizované minimálne na hodinovej báze. Nesmie ísť len o voľne dostupné/open-source databázy, ale musí ísť o komerčnú databázu renomovaného vendora alebo poskytovateľa týchto služieb.	áno/nie	áno	
76	Užívateľ musí byť schopný importovať vlastné záznamy.		áno/nie	áno	
77		Systém musí využívať túto detekciu pre všetku monitorovanú prevádzku (na perimetri aj v internej sieti medzi všetkými segmentmi), nie iba pre obmedzený segment alebo podmnožinu celkovej komunikácie.	áno/nie	áno	
78		Databáza detekčných pravidiel (signatúr) musí byť založená na pokročilých regulárnych výrazoch pre spracovanie reťazcov, ktoré dokážu vykonávať inšpekciu všetkej sieťovej komunikácie od L2 (Ethernet a pod.) po L7. Systém musí detekovať udalosti na základe vysokého počtu signatúrnych pravidiel (minimálne niekoľko desiatok tisíc).	áno/nie	áno	
79		Užívateľ musí byť schopný prostredníctvom webovej aplikácie pridávať vlastné detekčné pravidlá v praktickom a všeobecne využívanom formáte bez nutnosti znalosti syntaxe a sémantiky pravidiel.	áno/nie	áno	
80		Príklad možnej syntaxe detekčného pravidla:	áno/nie	áno	
81		alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b";)	áno/nie	áno	
82	Analýza šifrovanej komunikácie		áno/nie	áno	
83		Okrem samostatného učenia musí systém používať ďalšie metódy na analýzu šifrovanej komunikácie, minimálne TLS fingerprinting as ňou spojenú detekciu známych hrozieb.	áno/nie	áno	
84	Asistované učenie		áno/nie	áno	
85		Je požadovaný užívateľsky privetivý proces vytvárania pravidiel pre spresnenie detekcie a elimináciu falošne pozitívnej detekcie, a to na základe minimálne nasledujúcich parametrov:	áno/nie	áno	
86		IP adresa,	áno/nie	áno	
87		MAC adresa,	áno/nie	áno	
88		hostname,	áno/nie	áno	
89		segment siete / podsiete,	áno/nie	áno	
90		lokalita – ASN, krajiny, apod.	áno/nie	áno	
91		smer komunikácie – určenie klienta, alebo servera,	áno/nie	áno	
92		detekovaná udalosť – kategorie, názov apod.	áno/nie	áno	
93		použité služby, protokolu, portu,	áno/nie	áno	
94		ľubovoľnej kombinácii vyššie popísaných.	áno/nie	áno	
95		Systém musí byť schopný eliminovať falošné alarmy aj pre udalosti detegované v histórii.	áno/nie	áno	
96	Detekcia s využitím Sandboxu		áno/nie	áno	
97		Systém musí umožňovať integráciu so systémom Sandbox za účelom statickej aj dynamickej analýzy, tzv. „detonace" vo virtuálnom prostredí.	áno/nie	áno	
98		V prípade integrácie, systém musí byť schopný odovzdávať do Sandboxu súbory a url adresy, pre ďalšiu analýzu.	áno/nie	áno	
99		Systém musí byť schopný zobraziť výsledok analýzy Sandboxu vo svojom vlastnom grafickom prostredí, spoločne s ostatnými udalosťami.	áno/nie	áno	
100			áno/nie	áno	
101	Vyhledávání, filtrování a vizualizace dat		áno/nie	áno	
102		Systém musí byť schopný okamžitého (v priebehu sekúnd) vyhľadávania a vizualizácie pre forenznú analýzu a podporu threat hunting bez zvláštneho dotazovacieho jazyka.	áno/nie	áno	
103		Ide o možnosť okamžite filtrovať a vyhľadávať v plnej histórii všetkých uložených dát, tj bezpečnostných udalostí, sieťových tokov a agregovaných sieťových štatistikách (tabuľky a grafy), a to minimálne:	áno/nie	áno	
104		• podľa parametrov IP a MAC adresa, hostname, username (identita užívateľa), prichádzajúca a odchádzajúca prevádzka, sieťová služba, lokálna alebo vzdialená služba (služba z pohľadu klient alebo server), číslo portu, VLAN, krajina, ASN,	áno/nie	áno	
105		• prostredníctvom full-textového vyhľadávania v dátach a vyhľadávania na základe definície smeru (zdroj, cieľ) a logických výrazov and, or, not.	áno/nie	áno	
106		Systém musí pre vyhľadávanie poskytovať už predpočítané hodnoty výkonnostných a behaviorálnych charakteristík pre každé zariadenie v sieti a pre všetky na ňom prevádzkované služby, bez nutnosti spracovania surových dát zo sieťových logov.	áno/nie	áno	
107		Systém musí byť schopný filtrovať a vizualizovať výsledky v grafoch, výpočtových tabuľkách s možnosťou radenia a TOP N štatistikách.	áno/nie	áno	

108		Systém musí byť schopný ukladať a následne vyhľadávať aplikačné metadáta (vždy dotaz aj odpoveď všetkých transakcií v toku) minimálne z nasledujúcich protokolov, ktoré sú alebo môžu byť využívané vo vnútornej sieti organizácie: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.	áno/nie	áno	
109		Metadatá sú v tomto prípade chápané ako prenášané aplikačné metadáta alebo vlastné dáta servisných protokolov. Pri protokole HTTP napríklad http hlavička s metódou, URI, host, user-agent, cookies a pod. V odpovedi potom návratový kód a ďalšie http parametre.	áno/nie	áno	
110		Systém umožňuje vykonávať užívateľsky jednoduché a okamžité vizualizácie sieťových prestupov medzi zariadeniami a podsiete. Využitím užívateľského dátového filtra je možné vizualizačné pohľady ľubovoľne modifikovať.	áno/nie	áno	
111	Kontextuálne informácie		áno/nie	áno	
112		Systém musí byť schopný pre každé zariadenie získavať, vizualizovať av jednom grafickom pohľade zobrazovať kontextuálne informácie:	áno/nie	áno	
113		• meno užívateľa a ďalšie jeho parametre z doménového radiča (MS Active Directory), vrátane jej histórie	áno/nie	áno	
114		• hostname zariadenia a jeho história na základe spracovania relevantných dát z DNS a DHCP prevádzky	áno/nie	áno	
115		• IP geolokácia	áno/nie	áno	
116		• IP reputácia, vr. údaje, či je IP adresa na blackliste alebo podozrivá	áno/nie	áno	
117		• história použitých MAC adresa a výrobca zariadenia	áno/nie	áno	
118		• operačný systém a jeho história na zariadení	áno/nie	áno	
119		• užívateľom zadané poznámky a informácie k zariadeniu	áno/nie	áno	
120		• automaticky priradené značky/tagy zariadení, ktoré popisujú ich účel a správanie – aspoň server doménového radiča, webový server, poštový server, server DNS, server SSH, databázový server, tlačiarní, administrátorské zariadenie, dátové úložisko, aktívne dohľady, skenery zraniteľností a technologické systémy.	áno/nie	áno	
121		• zoznam prevádzkovaných a využívaných služieb (klient a server) u daného zariadenia a množstvo na nich prenesených dát.	áno/nie	áno	
122		• zoznam detekovaných bezpečnostných a prevádzkových udalostí daného zariadenia.	áno/nie	áno	
123	Zaznamenávanie, ukladanie a spätná analýza plnej prevádzky		áno/nie	áno	
124		Je požadované voliteľné nahrávanie plnej sieťovej prevádzky (full packet capture) vo formáte PCAP na všetkých dodaných zariadeniach minimálne na základe parametrov: cieľová a zdrojová IP/MAC adresa, podsieť, využitý protokol, IPv4 alebo IPv6. Zaznamenávanie je možné zapĺňať automaticky podľa detekovaných udalostí, alebo užívateľskou aktivitou.	áno/nie	áno	
125		Je požadovaná schopnosť importu vlastného PCAP súboru prostredníctvom webového rozhrania a jeho spätná analýza všetkými detekčnými a analytickými prostriedkami kolektora.	áno/nie	áno	
126		Je požadovaná schopnosť zobrazenia plného obsahu PCAP súboru v prostredí webového rozhrania aplikácie a ďalej potom automatizovaná analýza surových dát za účelom identifikácie prevádzkových nedostatkov zachytených iba v dátovom PCAP súbore.	áno/nie	áno	
127	Monitorovanie politík kybernetickej bezpečnosti		áno/nie	áno	
128		Systém musí umožňovať vytváranie komplexných komunikačných a bezpečnostných politík, a to minimálne:	áno/nie	áno	
129		• monitorovať definovanú komunikačnú maticu a detekovať, kedy sú tieto matice porušené – aspoň aké zariadenie smie komunikovať s akým zariadením, cez aký protokol, v akom čase.	áno/nie	áno	
130		• detekcia zmien v sieti – prinajmenšom nové komunikačné vektory, nové alebo zmenené zariadenia a podsiete, obchádzanie perimetra.	áno/nie	áno	
131		Na účely monitorovania politík kybernetickej bezpečnosti musí systém poskytovať užívateľský rámec na definovanie pravidiel pomocou:	áno/nie	áno	
132		• užívateľom definované podsiete na základe rozsahov IP adries	áno/nie	áno	
133		• užívateľsky ľubovoľne definovaných skupín zariadení	áno/nie	áno	
134		• automaticky priradené značky/tagu zariadenia, ktoré popisujú ich účel a správanie – aspoň server doménového radiča, webový server, poštový server, server DNS, server SSH, databázový server, tlačiarní, administrátorské zariadenie, dátové úložisko, aktívne dohľady, skenery zraniteľností a technologické systémy.	áno/nie	áno	
135	Manažment bezpečnostných udalostí a incidentov		áno/nie	áno	
136		Systém musí poskytovať funkcionalitu pre reporting bezpečnostných incidentov (vyhlásenie identifikovanej udalosti za bezpečnostný incident), vrátane:	áno/nie	áno	
137		• spoluprácu a zdieľanie informácií pri analýze identifikovaných bezpečnostných incidentov vrátane potrebného workflow medzi jednotlivými užívateľmi s podporou automatizovaných oznámení o zmene stavu udalosti či priradení riešiteľa,	áno/nie	áno	
138		• jednoduché zdieľanie informácií o bezpečnostných incidentoch, vrátane užívateľom zadaných komentárov,	áno/nie	áno	
139		• možnosť vyhľadávania a filtrovania nad všetkými udalosťami z pohľadu workflow bezpečnostného incidentov (reportovaná udalosť, udalosť v riešení, vyriešená udalosť, udalosti v riešení daného užívateľa a pod.),	áno/nie	áno	
140		• možnosť exportovania dát do emailu, csv, pdf, syslogu a podobne,	áno/nie	áno	
141		• možnosť exportu bezpečnostných udalostí a incidentov do systémov typu ticket management tretích strán.	áno/nie	áno	
142	Detekcia úniku dát		áno/nie	áno	
143		Systém musí byť schopný detekovať prenosy citlivých súborov a dát definovaných pomocou ich názvov, hashov, špecifického binárneho obsahu (vodoznaku) alebo regulárnych výrazov (napr. rodné číslo).	áno/nie	áno	
144		Systém musí byť schopný detekovať prenosy citlivých súborov a dát aspoň pri nasledujúcich protokoloch: HTTP, FTP, SMTP, SMB, NFS.	áno/nie	áno	
145		V rámci historických metadát pri HTTP, FTP, SMTP, SMB a NFS je požadované ukladanie informácií o všetkých po sieti prenášaných súboroch aspoň v rozsahu:	áno/nie	áno	
146		• názov súboru,	áno/nie	áno	
147		• veľkosť súboru,	áno/nie	áno	
148		• HASH súboru.	áno/nie	áno	
149	Monitoring výkonu aplikácií a siete		áno/nie	áno	
150		Systém v celej monitorovanej sieti, medzi všetkými zariadeniami a na všetkých službách meria a vytvára automaticky (bez nutnosti nastavovať manuálne limitné hodnoty) model normálneho správania pre výkonnostné parametre minimálne:	áno/nie	áno	
151		• prenosová rýchlosť siete,	áno/nie	áno	
152		• rýchlosť odozvy aplikácie,	áno/nie	áno	
153		• odozva systému z pohľadu užívateľa.	áno/nie	áno	
154		Výpočet uvedených výkonnostných parametrov a automatickej detekcie anomálií na základe odchýlky od modelu normálneho správania sa musí vykonávať pre:	áno/nie	áno	
155		• všetky porty a služby TCP,	áno/nie	áno	
156		• pre všetky kombinácie služieb a zariadení.	áno/nie	áno	
157		Systém musí v celej monitorovanej sieti, medzi všetkými zariadeniami a na všetkých službách merať informácie o retransmission paketoch, out of order paketoch, TTL, QoS a komunikácii blokovanej firewallu.	áno/nie	áno	
158	Monitoring cloudových služieb		áno/nie	áno	
159		Systém musí byť schopný monitorovať prístupy zariadení a užívateľov ku cloudovým službám, a to minimálne Google Workspace a Microsoft Office 365, vr. monitoringu operácií so súbormi, zmien oprávnenia a nastavenia a neúspešných prístupov.	áno/nie	áno	
160		Systém musí byť schopný tieto informácie autonómne a priebežne získavať z aplikačných rozhraní týchto cloudových služieb bez nutnosti využitia riešenia tretích strán.	áno/nie	áno	
161	Inventarizácia siete a grafická vizualizácia topológie		áno/nie	áno	
162		Systém musí byť schopný zobraziť celý inventár monitorovanej siete s počtom zariadení v jednotlivých lokalitách, segmentoch, alebo podsieťach. Vrátane detailného prehľadu zariadenia.	áno/nie	áno	

163		Systém musí byť schopný graficky vykresliť celú topológiu siete, podľa zaznamenanej komunikácie.	áno/nie	áno	
164		Systém musí byť schopný zobraziť inventár jednotlivých lokalít, prehľady zariadení, prehľady výrobcov, tagy zriadenia, užívateľa.	áno/nie	áno	
165		Systém umožňuje všetky inventarizačné informácie zoradiť podľa rôznych parametrov.	áno/nie	áno	
166	Minimálne parametre HW zariadenia:		áno/nie	áno	
167	Procesory	Model servera umožňujúci osadiť dva procesory, osadený jedným procesorom typu x86, disponujúcim 8-mimi jadrami a so základnou taktovacou frekvenciou 2.8 GHz.	hodnota	Model servera umožňujúci osadiť dva procesory, osadený jedným procesorom typu x86 Intel Xeon E-2478, 2.8 GHz, 8/16 cores	
168	Pamäť	64 GB, DDR5 Registered min. 4800MTs, server musí obsahovať 4 DDR5 DIMM sloty a podporovať aspoň 128 GB RAM	hodnota	64 GB (2x 32GB RAM DDR5), DDR5 Registered 4800MTs, server obsahuje 4 DDR5 DIMM sloty a podporujeň 128 GB RAM	
169	Ethernet adaptér	Minimálne 2 x 1Gb/s pripojenie k externému prostrediu, a 2 x 10/25Gb/s SFP28 zabezpečujúce redundantné a vysoko dostupné pripojenie servera na externú LAN infraštruktúru.	hodnota	2 x 1Gb/s pripojenie k externému prostrediu, a 2 x 10/25Gb/s SFP28 zabezpečujúce redundantné a vysoko dostupné pripojenie servera na externú LAN infraštruktúru.	
170	Diskový radič	HW diskový radič s rozhraním 12Gb/s, s podporou RAID 0/1/5/6/10/50/60, cache min. 8GB zálohovaná batériou alebo ekvivalentným spôsobom.	hodnota	HW diskový radič s rozhraním 12Gb/s, s podporou RAID 0/1/5/6/10/50/60, cache 8GB zálohovaná batériou	
171	Pevné disky	Minimálne 8 pozícií SAS/SATA/NVMe pre disky veľkosti 2.5", osadené min: 2x 1.92TB SSD SATA read-intensive	hodnota	8 pozícií SAS/SATA/NVMe pre disky veľkosti 2.5", osadené 2x 1.92TB SSD SATA read-intensive	
172	USB port	Minimálne tri USB porty prístupné zvonku.	áno/nie	áno	
173	PCI sloty (okrem slotov dedikovaných pre RAID radič, OCP/LOM karty, SD karty a M2 disky)	Min. 1 x 16 Gen4 a 1 x 8 Gen4 pri osadení jedným CPU	hodnota	1 x 16 Gen4 a 1 x 8 Gen4 pri osadení jedným CPU	
174	Grafický adaptér	Integrovaný grafický adaptér, minimalne 1x VGA graficke rozhranie,	áno/nie	áno	
175	Správa a manažment	Musí byť zabezpečené: - hardvérový komponent nezávislý od operačného systému formou vzdialenej grafickej KVM konzoly - dedikovaná IP adresa a separátnym RJ45 portom - časovo neobmedzený prístup na obraz vzdialenej plochy servera a to aj bez spusteného OS, vrátane plnohodnotného pripojenia vzdialených médií - možnosť štartu, reštartu a shutdown serveru cez sieť LAN, nezávisle od OS - možnosť automaticky registrovať servisné incidenty priamo u výrobcu - rozšírená bezpečnostná ochrana na úrovni BIOSu servera - verifikácia autenticity FW - automatická obnova poškodeného / neautentického FW servera - možnosť zasielania a vyhodnocovania telemetrických údajov v cloud nástroji výrobcu HW, vrátane porovnania bezpečnostných nastavení servera voči všeobecne platným bezpečnostným normám, - možnosť zobrazenia konfigurácie a zmeny nastavení servera pomocou bluetooth alebo wi-fi protokolu na mobilnom zariadení - dedikovaný USB port pre priame pripojenie na manažment servera zpredu. Licencie, resp. softvér potrebný na prevádzku, konfiguráciu a správu servera uvedenú funkcionalitu poskytuje s kapacitne a časovo neobmedzeným licenčným pokrytím pre daný server	áno/nie	áno	
176	Napájanie	Redundandné za behu meniteľné, schopné napájať server požadovanej konfigurácie (aj s definovanými rozšíreniami) jedným napájacím zdrojom.	áno/nie	áno	
177	Prevedenie	Max 1U montovateľné do 19" racku, vrátane kolajníc a zariadenia na vedenie káblov	áno/nie	áno	
178	Trvalý prietok dát za sekundu	min. 500 Mbps	hodnota	500 Mbps	
179	Netflow toky za sekundu z iných zdrojov	min. 1000	hodnota	1000	
180	Počet monitorovaných IP adries	min. 1500	hodnota	1500	
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
181	Min. 5 rokov servisná podpora v mieste inštalácie, 24x7 nahlasovanie výrobcovi hardvéru, výmena dielu NBD. Oprava zariadenia musí byť realizovaná priamo výrobcom alebo jeho lokálnym autorizovaným servisným partnerom (zastúpením). Obstarávateľ požaduje možnosť bezplatného sťahovania updatov firmvérov a ovládačov aj po uplynutí definovanej servisnej podpory a to priamo obstarávateľom priamo zo stránky výrobcu.	Záruka	áno/nie	áno	
182	Implementačné a konfiguračné práce s otestovaním, zaškolením a dokumentáciou riešenia v rozsahu 6 človekohodín	Práce	áno/nie	áno	
	Implementačné práce pre Sondu detekcie a prevencie prieniku do siete:		áno/nie	áno	
	Návrh architektúry nasadenia sondy detekcie a prevencie prieniku do siete s návrhom optimálneho umiestnenia v existujúcej sieťovej architektúre. Implementácia a zapojenie a integrácia s existujúcimi sieťovými prvkami, prípadne so SIEM platformou. Prispôsobenie detekčných pravidiel pre efektívnu identifikáciu hrozieb. Testovanie nasadenia a správnosti zachytávania hrozieb. Vyškolenie personálu na používanie systému a interpretáciu výsledkov. Dodanie technickej dokumentácie nasadenia.		áno/nie	áno	
	Analýza požiadaviek organizácie: o Zhodnotenie existujúcej sieťovej infraštruktúry, identifikácia kritických bodov a definovanie cieľov nasadenia.		áno/nie	áno	
	Návrh architektúry riešenia: o Plánovanie umiestnenia senzorov, sieťových tapov alebo SPAN portov pre optimálne pokrytie siete.		áno/nie	áno	
	Príprava infraštruktúry: o Zabezpečenie hardvéru alebo virtuálnych prostredí, konfigurácia sieťových prvkov na zrkadlenie prevádzky.		áno/nie	áno	
	Inštalácia sond detekcie a prevencie prieniku: o Nasadenie softvéru na fyzické servery, vrátane základnej konfigurácie systému.		áno/nie	áno	
	Integrácia so sieťovou infraštruktúrou: o Pripojenie k sieťovým zariadeniam (switche, routre, firewally) a systémom na správu logov (SIEM).		áno/nie	áno	
	Konfigurácia detekčných pravidiel: o Prispôsobenie pravidiel na detekciu hrozieb podľa špecifík organizácie a aktuálnych bezpečnostných požiadaviek.		áno/nie	áno	
	Testovanie funkčnosti: o Overenie správnosti zachytávania a analýzy sieťovej prevádzky, testovanie detekcie simulovaných hrozieb.		áno/nie	áno	
	Zaškolenie personálu: o Školenie bezpečnostného tímu a administrátorov na prácu so systémom, interpretáciu výstupov a reakciu na incidenty.		áno/nie	áno	
	Optimalizácia a ladenie výkonu: o Úprava konfigurácie pre zlepšenie výkonu a minimalizovanie falošných poplachov.		áno/nie	áno	
	Záverečné odovzdanie a dokumentácia: o Odovzdanie projektu vrátane dokumentácie k implementácii, prevádzke a správe systému.		áno/nie	áno	
183	1 ročná licencia zabezpečujúca aktualizácie a upgrady všetkých komponentov produktu a technickú podporu 8x5 a a to telefonicky, emailom a helpdeskom.	Licencia	áno/nie	áno	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Špecifikácia predmetu zákazky - položka: Nástroj na centrálny manažment logov

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné uchádzačom ponúkaný produkt musí SPĹŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu

Logmanager.cz / LOGmanager-M /LOGmanager-M
5 years HW support, 1 year SW renewal, 1x LOGmanager-VF, 12 TB database, Dell server / LOGM-M a Logmanager-M SW support 1 year /SUPP-1Y-LOGM-M

Položka predmetu zákazky - Nástroj na centrálny manažment logov + licencia
požadovaný počet: 1 ks

P. č.	Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Nástroj na centrálny manažment logov + licencia)	Doplňujúce informácie	Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
			Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
1	Centrálny logovací systém má pracovať ako fyzická appliance s jedným uceleným webovým rozhraním pre všetky administrátorské i operátorské činnosti. Nevyžaduje inštaláciu ďalších systémov a aplikácií okrem podpory zberu na iných lokalitách (mimo centrálu) a agenta pre zber Windows logov.		áno/nie	áno	
2	Konfigurácia systému sa musí vykonávať v grafickom rozhraní jednotnej užívateľskej konzoly, Systém poskytuje podporu pre vizuálne programovanie pre všetky kroky spracovania strojových dát.		áno/nie	áno	
3	Systém má umožňovať doplnenie parseru pre zariadenia, aplikácie alebo systémy mimo uvedeného zoznamu užívateľov bez nutnosti spolupráce s výrobcom alebo dodávateľom ponúkaného systému - užívateľsky definované parsery. Dokumentácia systému musí obsahovať prehľadný návod na vytváranie zákazníckych parserov a systém musí obsahovať možnosť testovania a ladenia parserov bez vplyvu na ostatné produkčné funkcie systému		áno/nie	áno	
4	Prijaté logy má systém štandardizovať do jednotného formátu a logy sú rozdeľované do príslušných polí podľa ich typu. Systém musí zároveň uchovávať originálne verzie správ.		áno/nie	áno	
5	Pre hodnoty jednotlivých parsovaných polí musí byť možné v definícii parseru zmeniť typ a štandardizovať minimálne na tieto základné druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými dátami typu číslo je možné pri vyhľadávaní vykonávať matematické operácie (súčty všetkých hodnôt, priemery, najmenšia/najväčšia hodnota a pod.).		áno/nie	áno	
6	Centrálny logovací systém musí zachovávať pôvodné informácie zo zdroju logu o časovej značke udalosti, ale nedôveruje jej a vytvára vlastné dôveryhodné časové razítko ku každému logu, ktorá vzniká v okamihu prijatia logu systémom a ktorým sa systém riadi.		áno/nie	áno	
7	Všetky polia a položky prijaté systémom musia byť automaticky indexované. Nad všetkými položkami musí byť možné ihneď vykonávať vyhľadávanie bez nutnosti dodatočného ručného indexovania administrátorom. Centrálny logovací systém musí umožňovať zber udalostí vo formátoch RAW, Syslog.		áno/nie	áno	
8	Centrálny logovací systém neumožňuje mazanie alebo modifikovanie uložených logov ani konfiguračnou zmenou administrátorovi systému s najvyššími oprávneniami. Každý log musí máť unikátny identifikátor, ktorý umožní jeho jednoznačnú identifikáciu.		áno/nie	áno	
9	Centrálny logovací systém musí umožňovať konfiguráciu filtrácie nerelevantných správ, konsolidáciu logov na vlastnom storage priestore, jednoduché vyhľadávanie udalostí a okamžité vytváranie grafických reportov (ad hoc) bez nutnosti dodatočného programovania alebo aplikovania dopytov v SQL jazyku. Reportovací nástroj musí byť integrálnou súčasťou systému a aj súčasťou jednotného rozhrania.		áno/nie	áno	
10	V prípade krátkodobého preťaženia systému nemôže dochádzať k strate logov. Všetky prijaté nespracované logy/udalosti sú ukladané do vyrovnávacej pamäte.		áno/nie	áno	
11	Centrálny logovací systém musí umožňovať jednoducho vytvárať grafické znázornenie udalostí nad všetkými uloženými dátami za ľubovoľné časové obdobie bez nutnosti modifikácie konfigurácie systému alebo parametrov uložených dát. Historické dáta v požadovanej dĺžke retencie uložené v systéme je možné prehľadávať okamžite bez časových strát opätovného importu alebo dekomprimácie starších dát, prehľadávanie nevyžaduje manuálnu konfiguráciu a zásahy používateľa.		áno/nie	áno	
12	Systém musí podporovať natívne získavanie logov z Office365.		áno/nie	áno	
13	Centrálny logovací systém musí umožňovať unifikované vyhľadávanie naprieč všetkými typmi dát a zariadení podľa normalizovaných polí a musí spĺňať požiadavky normy STN/ISO 27001:2013 pre získavanie auditných záznamov.		áno/nie	áno	
14	Centrálny logovací systém má mať možnosť uloženia užívateľom vytvorených pohľadov na dáta (dashboardov) pre budúce spracovanie.		áno/nie	áno	
15	Centrálny logovací systém musí obsahovať reportovací nástroj s prednastavenými najbežnejšími reportami a možnosťou vlastných úprav a vytváranie nových pohľadov.		áno/nie	áno	
16	Centrálny logovací systém musí umožňovať kapacitnú i výkonovú škálovateľnosť.		áno/nie	áno	
17	Monitoring stavu systému - alertovanie pri prekročení prahových hodnôt alebo chybe systému, preposlanie upozornenia pomocou SMTP alebo Syslog.		áno/nie	áno	
18	Centrálny logovací systém musí obsahovať REST-API pre integráciu s externým monitorovacím systémom (Zabbix, Nagios, PRTG a pod.)		áno/nie	áno	
19	Centrálny logovací systém musí umožňovať jednoduché vytváranie užívateľských rolí definujúcich prístupové práva k uloženým udalostiam a jednotlivým ovládacím komponentom systému, vykonávať parsovanie a normalizáciu prijatých udalostí bez nutnosti inštalovať externé aplikácie alebo systémy a to priamo vo svojom rozhraní.		áno/nie	áno	
20	Centrálny logovací systém musí podporovať overovanie užívateľa systému na externom LDAP serveri. V prípade výpadku externého LDAP systému musí podporovať overenie z lokálnej databázy. Systém má automaticky zaznamenávať užívateľské meno ku každej akcii užívateľom.		áno/nie	áno	
21	Aktualizácie systému by mali byť distribuované v jednotnom balíku a ich inštalácia je vykonávaná cez centrálnu správcovskú konzolu. Všetky aktualizácie by mali byť vykonávané z webového rozhrania systému bez potreby asistencie výrobcu/dodávateľa.		áno/nie	áno	
22	Systém musí podporovať downgrade, napríklad pri problémoch s novou verziou systému po upgrade.		áno/nie	áno	
23	Licenčne musí byť neobmedzený počet zariadení pre príjem zasielaných udalostí. Licenčne musí byť neobmedzený počet udalostí v GB za deň. Integrovaná databáza musí podporovať kompresiu ukladaných dát.		áno/nie	áno	
24	Centrálny logovací systém musí podporovať zálohovania alebo obnovy konfigurácie v jednom kroku a jednom súbore pre celý systém a taktiež musí podporovať zálohovanie dát na externý systém, požadované je plánované aj ad-hoc zálohovanie.		áno/nie	áno	
25	Centrálny logovací systém musí byť schopný na základe zadaných podmienok splnených v prijatých dátach vygenerovať alert. Text emailu vygenerovaného alertom môže byť užívateľsky definovaný s premennými z prijatej rozparsovanej udalosti.		áno/nie	áno	
26	Centrálny logovací systém by mal obsahovať výrobcom predpripravené sety/vzory alertov a korelácií.		áno/nie	áno	

27	Užívateľská konfigurácia alertov musí byť možná pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Vizuálny programovací jazyk nemôže byť prezentovaný čisto textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku. Konfigurácia alertu alebo korelácie umožňuje okamžitú kontrolu.		áno/nie	áno	
28	Ako výstupné pravidlo alertu systém musí vedieť odoslať udalosť, ktorá alert vyvolala na externý systém prostredníctvom SMTP alebo Syslog cez TCP protokol. Pre Syslog protokol musí byť možnosť definície formátu dát pre jednoduchšiu integráciu so systémami tretích strán.		áno/nie	áno	
29	V alertoch by mala byť možnosť využívať značky.		áno/nie	áno	
30	Systém musí podporovať funkcie SIEM - korelácie udalostí a upozornenia s hraničnými limitmi. Definícia korelačných pravidiel má mať možnosť vloženia testovacej správy a výsledku testu vykonanej akcie		áno/nie	áno	
31	Centrálny logovací systém by mal získavať udalosti z Microsoft prostredia buď pomocou agenta inštalovaného priamo na koncovom zariadení s Windows systémom, alebo iným spôsobom. Agent súčasne musí podporovať monitoring interných Windows logov, a aj monitoring textových súborových logov.		áno/nie	áno	
32	Agent musí zaisťovať zber nemodifikovaných udalostí a detailné spracovanie auditných informácií.		áno/nie	áno	
33	Agent musí podporovať nastavenie filtrácie odosielaných udalostí pomocou centrálnej správcovskej konzoly.		áno/nie	áno	
34	Filtrácia odosielaných udalostí agentom sa musí konfigurovať pomocou vizuálneho programovacieho jazyka v centrálnej správcovskej konzole. Nerelevantné logy majú byť filtrované na strane agenta a nie sú odosielané po sieti. Vizuálny programovací jazyk nesmie byť prezentovaný textovo, ale textovo-grafickou formou, ktorá vizualizuje aplikačnú logiku.		áno/nie	áno	
35	Agent nesmie vyžadovať administrátorské zásahy na koncovom systéme – je centrálne spravovaný a automaticky aktualizovaný priamo z centrálnej správcovskej konzoly systému. Správa a aktualizácia agenta sa nevykonáva z Group Policy.		áno/nie	áno	
36	Komunikácia Windows agenta a centrálneho logovacieho systému je šifrovaná.		áno/nie	áno	
37	Agent musí podporovať zber nielen zo základných systémových logov (Aplikácie, Zabezpečenie, Inštalácie, Systém), ale aj zber všetkých ostatných logov v zložke protokoly aplikácií a služieb. Agent musí podporovať centralizované nastavenie z administrátorskej konzoly systému pre zber textových logov vrátane možnosti výberu ich formátu.		áno/nie	áno	
38	Agent musí automaticky dopĺňať ku všetkým odosielaným udalostiam ich textový popis tak, ako je zobrazený v prehliadači udalostí (Event Viewer) na koncovom systéme.		áno/nie	áno	
39	Počet inštalácií agenta nemôže byť licenčne ani časovo obmedzený.		áno/nie	áno	
40	Počet udalostí za sekundu pri priemernej veľkosti jednej udalosti 1kB	min. 2000	hodnota	2000	
41	Počet udalostí počas útoku (min. 10 minút)	min. 4000	hodnota	4000	
42	Retencia logov	min. pol roka	hodnota	230 dní	
43	Veľkosť diskového subsystému s čistou dostupnou kapacitou v RAID5	min. 12TB	hodnota	12 TB	
44	Veľkosť operačnej pamäte	min. 64 GB	hodnota	64GB	
45	Redundantné napájacie zdroje vymeniteľné za chodu		áno/nie	áno	
46	Prevedenie	Max 1U montovateľné do 19" racku, vrátane koľajníc a zariadenia na vedenie káblov	áno/nie	áno	
47	Virtuálne KVM, tj. prevzatie textovej i grafickej konzoly serveru a prenos povelov z klávesnice a myši vzdialeného počítača		áno/nie	áno	
48	Systém pre vzdialenú správu serveru vrátane potrebnej licencie		áno/nie	áno	
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
49	5 rokov priamo od výrobcu zariadenia. Nahlasovanie poruchy v režime 24x7, výmena náhradného dielu NBD.	Záruka	áno/nie	áno	
50	Implementačné a konfiguračné práce s otestovaním, zaškolením a dokumentáciou riešenia v rozsahu 10 človekohodín. Implementačné práce pre centrálny manažment logov: Analýza požiadaviek a plánovanie: o Identifikácia potrieb organizácie v oblasti logovania, bezpečnosti a súladu s legislatívou. Príprava infraštruktúry: o Overenie hardvérových zdrojov, príprava serverov a siete pre nasadenie centrálneho manažmentu logov. Inštalácia centrálneho manažmentu logov: o Nasadenie softvéru na fyzické alebo virtuálne servery s ohľadom na výkonové požiadavky. Základná konfigurácia systému: o Nastavenie sieťových parametrov, zabezpečenie prístupu a konfigurácia administrátorských účtov. Integrácia so zdrojmi logov: o Konfigurácia serverov, sieťových zariadení, aplikácií a databáz na odosielanie logov do centrálneho manažmentu logov v celkovom počte 50 vzorových zdrojov. Nastavenie politiky uchovávania logov: o Definovanie retenčných politík pre dlhodobé a bezpečné uchovávanie dát podľa noriem (napr. GDPR). Korelácia udalostí a správa alertov: o Nastavenie pravidiel pre automatickú detekciu incidentov a notifikácie o bezpečnostných hrozbách. Reporting a vizualizácia: o Vytvorenie prispôsobených reportov, dashboardov a prehľadov pre rôzne úrovne používateľov. Bezpečnostné opatrenia: o Implementácia šifrovania logov, správa prístupových práv a auditovanie činností. Testovanie a validácia: o Overenie funkčnosti systému, správnosti logov a efektivity detekcie incidentov. Školenie používateľov a administrátorov: o Zaškolenie tímu na prácu s centrálnym manažmentom logov vrátane správy systému a interpretácie reportov. Dokumentácia: o Vypracovanie technickej a prevádzkovej dokumentácie pre interné potreby organizácie.	Práce	áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie áno/nie	áno áno áno áno áno áno áno áno áno áno áno áno áno	
51	Licencia zariadenia	1 rok	Hodnota	12 mesiacov	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Špecifikácia predmetu zákazky - položka: Monitorovací nástroj prevádzkových parametrov

Uchádzač je povinný uviesť požadované informácie v stĺpcoch č. 1 a č. 2 údaje v stĺpci vypĺňa ak je to relevantné
uchádzačom ponúkaný produkt musí SPĽŇAŤ všetky požiadavky verejného obstarávateľa v plnom požadovanom rozsahu

Uchádzač uvedie: **názov výrobcu / značku / typové označenie / obchodný názov** ponúkaného produktu		
DATALAN Zabbix VM inštalácia		
Položka predmetu zákazky - Monitorovací nástroj prevádzkových parametrov požadovaný počet: 1 ks		
P. č.	**Parameter/časť položky (požadovaná špecifikácia platí pre 1ks Monitorovací nástroj prevádzkových parametrov**	**Doplňujúce informácie**
1	Dodané riešenie podporuje centrálne spravovanú konfiguráciu z webovej administrátorskej konzoly.	
2	Dodané riešenie umožňuje monitoring serverov, sietí, aplikácií a cloudových riešení.	
3	Komunikácia medzi serverom a agentmi je šifrovaná pomocou TLS.	
4	Dodané riešenie podporuje automatické objavovanie nových zariadení v sieti.	
5	Dodané riešenie umožňuje konfigurovateľné prahové hodnoty pre upozornenia.	
6	Dodané riešenie podporuje monitoring v reálnom čase s intervalom od niekoľko sekúnd.	
7	Dodané riešenie je open-source riešenie bez licenčných obmedzení.	
8	Dodané riešenie podporuje ukladanie historických metrík pre dlhodobé analýzy.	
9	Dodané riešenie má webové rozhranie pre zobrazenie statusov a metrík v reálnom čase.	
10	Dodané riešenie podporuje monitoring pomocou SNMP, ICMP, IPMI a JMX.	
11	Minimálna verzia databázového servera podporovaná je MySQL 5.7/PostgreSQL 10.	
12	Dodané riešenie podporuje beh v Docker kontejnery.	
13	Dodané riešenie umožňuje filtrovať upozornenia podľa kritickosti.	
14	Dodané riešenie podporuje generovanie reportov o stave systému a incidentoch.	
15	Dodané riešenie podporuje eskaláciu upozornení na viaceré úverstvenia.	
16	Dodané riešenie umožňuje definovať vlastné metriky a sledované parametre.	
17	Dodané riešenie podporuje ukladanie logov zmien v konfigurácii.	
18	Dodané riešenie podporuje monitoring IoT zariadení.	
19	Dodané riešenie je kompatibilný s OS Linux (RHEL, Ubuntu, Debian) aj Windows.	
20	Dodané riešenie podporuje LDAP autentifikáciu.	
21	Dodané riešenie umožňuje export reportov vo formátoch CSV a JSON.	
22	Dodané riešenie podporuje integráciu s cloudovými poskytovateľmi (AWS, Azure, GCP).	
23	Dodané riešenie podporuje multi-tenant riešenie.	

Uchádzač do stĺpca č. 1 uvedie ku každej požiadavke **parametre ponúkaného produktu** (áno / nie, resp. konkrétnu hodnotu) v súlade so stĺpcom "Požadovaný formát ponúkaných parametrov"		**POZNÁMKA** (napr. doplňujúce informácie k uvedeným parametrom a pod.)
Požadovaný formát ponúkaných parametrov	**1.** TU UVEĎTE ponúkané parametre	**2.**
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	
áno/nie	áno	

24	Dodané riešenie umožňuje integráciu s existujúcimi SIEM riešeniami.		áno/nie	áno	
25	Dodané riešenie podporuje detekciu anomálií v sledovaných parametroch.		áno/nie	áno	
26	Dodané riešenie podporuje notifikácie cez e-mail, SMS, webhooky a iné kanály.		áno/nie	áno	
27	Dodané riešenie podporuje agentless monitoring.		áno/nie	áno	
28	Dodané riešenie podporuje vlastné pravidlá na filtrovanie udalostí.		áno/nie	áno	
29	Dodané riešenie umožňuje full-text vyhľadávanie v logoch.		áno/nie	áno	
30	Dodané riešenie podporuje vizualizáciu historických záznamov metrík.		áno/nie	áno	
31	Dodané riešenie ponúka REST API.		áno/nie	áno	
32	Dodané riešenie podporuje cross-platform integráciu.		áno/nie	áno	
33	Dodané riešenie obsahuje dashboard pre prehľad o stave monitorovanej infraštruktúry.		áno/nie	áno	
34	Dodané riešenie podporuje autentifikáciu pomocou OAuth2.		áno/nie	áno	
35	Dodané riešenie umožňuje vytváranie vlastných skriptov na rozšírenie funkcionality.		áno/nie	áno	
36	Dodané riešenie má podporu pre auditovanie a logging aktivít.		áno/nie	áno	
37	Dodané riešenie má komunitnú podporu cez GitHub Issues a fóra.		áno/nie	áno	
38	Dodané riešenie podporuje multi-language UI.		áno/nie	áno	
39	Dodané riešenie je škálovateľný pre veľké infraštruktúry.		áno/nie	áno	
40	Dodané riešenie umožňuje nastaviteľné prístupové práva.		áno/nie	áno	
41	Dodané riešenie podporuje pravidelné aktualizácie.		áno/nie	áno	
42	Dodané riešenie podporuje šifrovanie uložených informácií.		áno/nie	áno	
43	Dodané riešenie možno nasadiť on-premise aj v cloude.		áno/nie	áno	
44	Dodané riešenie podporuje jednoduchú inštaláciu a konfiguráciu.		áno/nie	áno	
45	Dodané riešenie má podporu pre automatické testovanie.		áno/nie	áno	
46	Dodané riešenie podporuje centralizovanú distribúciu konfigurácií.		áno/nie	áno	
47	Dodané riešenie podporuje sledovanie SLA a reportovanie dostupnosti služieb.		áno/nie	áno	
Osobitné požiadavky na plnenie:			**Osobitné požiadavky na plnenie:**		
48	Inštalácia na zdrojoch poskytnutých objednávateľom v rozsahu 10 človekodní	Práce	áno/nie	áno	
	Implementačné práce pre nasadenie monitorovacieho nástroja prevádzkových parametrov v organizácii:		áno/nie	áno	
	Analýza požiadaviek a plánovanie: o Identifikácia monitorovacích potrieb organizácie (servery, siete, aplikácie, služby) a definovanie metrík.		áno/nie	áno	
	Príprava infraštruktúry: o Overenie hardvérových/virtuálnych zdrojov, výber vhodného OS (napr. Linux), príprava databázového servera (MySQL/PostgreSQL).		áno/nie	áno	
	Inštalácia monitorovacieho nástroja: o Nasadenie monitorovaniceho nástroja vo virtuálnom prostredí organizácie, webového rozhrania a databázového backendu.		áno/nie	áno	
	Základná konfigurácia systému: o Nastavenie sieťových parametrov, zabezpečenie prístupov a konfigurácia administračných účtov.		áno/nie	áno	
	Inštalácia a konfigurácia monitorovacích agentov: o Nasadenie agentov na monitorované zariadenia (servery, PC, sieťové prvky) a ich konfigurácia v celkovom počte 20 vzorových kusov.		áno/nie	áno	
	Integrácia s externými systémami: o Pripojenie externých zariadení a služieb pomocou SNMP, IPMI, JMX, API alebo prispôsobených skriptov.		áno/nie	áno	
	Nastavenie šablón a monitorovacích položiek: o Vytvorenie alebo prispôsobenie šablón pre rôzne zariadenia a služby na efektívne monitorovanie.		áno/nie	áno	

	Konfigurácia alertov a eskalácií: o Definovanie prahových hodnôt, nastavenie notifikácií (e-mail, SMS, webhook) a eskalačných politík.			áno/nie	áno	
	Bezpečnostné opatrenia: o Implementácia šifrovania komunikácie medzi serverom a agentmi, správa prístupových práv.			áno/nie	áno	
	Testovanie a validácia: o Overenie správnosti monitorovania, testovanie alertov a výkonu systému.			áno/nie	áno	
	Školenie používateľov a administrátorov: o Zaškolenie tímu na prácu s monitorovacím nástrojom prevádzkových parametrov, interpretáciu údajov a správu systému.			áno/nie	áno	
	Dokumentácia: o Vypracovanie technickej a prevádzkovej dokumentácie na podporu budúcej údržby a rozvoja systému.			áno/nie	áno	
49	1 ročná podpora od dodávateľa riešenia v režime 8x5			áno/nie	áno	

Týmto potvrdzujem, že všetky uvedené informácie sú pravdivé.

V: Bratislave
Dňa: 10.6.2025

Ing. Juraj Zelko
predseda predstavenstva

DATALAN
DATALAN, a. s.
Krasovského 14, 851 01 Bratislava
IČO: 35 810 734 IČ DPH: SK2020259175

Príloha č. 6: Zoznam Expertov

Príloha č. 6 Zoznam Expertov

Kľúčový expert navrhovaná pozícia v tíme	**meno a priezvisko**
Expert č. 1. Projektový manažér	Tomáš Dovala
Expert č. 2. Technický pracovník zodpovedný za implementáciu zálohovacieho systému	Igor Juran
Expert č. 3. Technický pracovník zodpovedný za implementáciu firewalu (min. 1 osoba)	Daniel Novotný
Expert č. 4. Technický pracovník zodpovedný za implementáciu monitoring siete (min. 1 osoba)	Peter Čajkovský
Expert č. 5. Technický pracovník zodpovedný za implementáciu logovacieho zariadenia (min. 1 osoba)	Jozek Kolek
Expert č. 6. Technický pracovník zodpovedný za bezpečnosť (min. 1 osoba)	Andrej Vávra