

Serverhousing + datové linky + internetové přípojky		
NIPEZ	72410000-7 Poskytovatelské služby	
parametr	hodnota	max./min.
celková cena zakázky bez DPH (server housing, datové linky, internetové přípojky, DDoS ochrana, SOC a EDR) za celé období trvání smlouvy bez plateb za spotřebovanou elektrickou energii.	15 250 000 Kč	max.
délka trvání poskytování služeb (včetně přechodných období na začátku a konci kontraktu)	52 měsíců	max.
počet poptávaných racků v datacentrech dodavatele	2 ks	
počet nezávislých internetových přípojek v datacentru Dodavatele	2 ks (1 pro každý rack)	
počet datových propojů mezi datacentrem Dodavatele a lokalitou Zadavatele (Štěpánská)	2 ks (1 pro každý rack)	
součástí dodávky je i internetová přípojka v lokalitě Zadavatele (Štěpánská)	ne	
lokalita Zadavatele (DC-03)	Štěpánská 567/15, Praha 2	
datacentrum - oba racky musí být ve stavebně oddělených prostorech	ano	
datacentrum - oba racky musí být v požárně oddělených prostorech	ano	
datacentrum - oba racky musí být v klimatizačně oddělených prostorech	ano	
datacentrum - oba racky musí být připojeny oddělenými větvemi elektrického napájení	ano	
datacentrum - oba racky musí mít možnost definovat rozdílné oprávnění přístupu	ano	
termín pro předání všech služeb dle specifikace	31. 10. 2024 od 9:00 hod.	
nejzazší termín, do kdy musí být zadministrvány všechny žádosti o vstup do datacenter Dodavatele vč. vydání vstupních prostředků (např. vstupní karta a klíče od racku)	24. 10. 2024 od 9:00 hod.	max.
datacentrum Dodavatele je na území hlavního města Prahy	ano	
datacentrum Dodavatele - splňuje úroveň (dle normy ANSI/TIA-942)	Tier 3	min.
datacentra Dodavatele - splňují bezpečnostní úroveň eGovernment cloud	2	min.
datacentrum Dodavatele - má odolnost proti přerušení funkčnosti z důvodu	záplavy, vytopení, tornáda	min.
datacentrum Dodavatele - má ochranu proti nepovolanému přístupu do objektu datacentra	ano	
datacentrum Dodavatele - je vybaveno kamerovým systémem	ano	
datacentrum Dodavatele - kamerový systém je vč. systému nočního vidění	ano	
počet požadovaných racků v lokalitě Dodavatele	2 ks	
racky - požadovaný druh	wide rack 48 U	min.
racky - požadovaná šířka	800 mm	min.
racky - požadovaná hloubka	1200 mm	min.
racky - požadovaná nosnost	800 kg	min.
racky - musí být opatřeny pevnými nebo uzamykatelnými bočnicemi	ano	
racky - musí být opatřeny uzamykatelnými předními a zadními dvířky	ano	
racky - přední a zadní dvířka jsou perforovaná	ano	
racky - prostupnost dvířek	75 - 85%	
racky - musí být opatřeny čidly pro detekci a reporting otevření předních a zadních dveří	ano	
racky - čidla otevření dveří odesílají report o otevření a zavření e-mailem na Zadavatele	ano	
racky - požadované volné místo před rackem	1000 mm	min.
racky - požadované volné místo za rackem	1000 mm	min.
racky - požadována instalace UPS v racku	ne	

racky - součástí dodávky je i poskytnutí a instalace PDU lišt v racku	ano	
racky - počet instalovaných PDU v racku	2 ks	min.
PDU - dostupné porty v každém PDU	IEC320 C13 a IEC320 C19	
PDU - počet portů IEC320 C13 na jednom PDU	26 ks	min.
PDU - počet portů IEC320 C19 na jednom PDU	2 ks	min.
PDU - obě PDU umístěné vzadu v racku	ano	
racky - všechna PDU v racích umožňují plynulé vysunutí i vyjmutí všech komponent umístěných v racku oběma (dopředu a dozadu) směry (nezasahují do prostor určených pro rackové komponenty vč. nosné lišty pro rackové komponenty) bez nutnosti jejich natočení/naklonění	ano	
dodávka ele. energie - odhadovaný max. špičkový odebíraný výkon <b>za oba racky</b>	10 kW	
dodávka ele. energie - je požadována dodávka	ano	
dodávka ele. energie - napětí	230 V	
dodávka ele. energie - zabezpečena pomocí UPS	ano	
dodávka ele. energie - jištěna sekundárním zdrojem v podobě motorgenerátoru	ano	
dodávka ele. energie - počet zálohovaných větví elektrické energie v racku	2 větve	
dodávka ele. energie - garantovaná dostupnost elektrické energie z PDU	99,92%	
racky - součástí dodávky je i zařízení, které umožní nepřerušovaný provoz jednozdrojových zařízení v případě výpadku napájení jedné větve (hotswap napáječ, např. Socomec STATYS XS)	ano	
hotswap napáječ - příkon	600 W	min.
hotswap napáječ - počet a druh zásuvek	4x IEC C13	min.
dodávka elektrické energie - součástí nabídkové ceny je i úhrada za spotřebovanou elektrickou energii	ne	
dodávka elektrické energie - spotřebovaná elektrická energie odebraná prostřednictvím PDU v obou racích bude fakturována jako dodatečná položka na pravidelné měsíční faktuře	ano	
dodávka elektrické energie - veškerý fakturovaný odběr elektřiny je doložen měřením skutečné spotřeby	ano	
dodávka elektrické energie - maximální cena za spotřebovanou elektrickou energii po celou dobu platnosti kontraktu	3 150 000 Kč	
dodávka datových propojů mezi racky v datovém centru Dodavatele a Zadavatele je součástí dodávky	ano	
datový propoj Štěpánská 15 - výchozí bod pro propojení uživatelů na datacentra Zadavatele	ano	
datový propoj Štěpánská 15 - rychlost download	10 Gbps	min.
datový propoj Štěpánská 15 - rychlost upload	10 Gbps	min.
datový propoj Štěpánská 15 - dostupnost	99,95%	
datový propoj Štěpánská 15 - cíl propoje 1	Rack 1 Dodavatele	
datový propoj Štěpánská 15 - cíl propoje 2	Rack 2 Dodavatele	
datové propoje mezi racky Dodavatele - typ	nenasvícené vlákno	min.
datové propoje mezi racky Dodavatele - počet	70 ks	
datové propoje mezi racky Dodavatele - druh propoje	SingleMode OS2	
datový propoj z RACK-01 - cíl propoje 1	RACK-02 Dodavatele	
datový propoj RACK-01 - cíl propoje 2	DC-03 (Štěpánská 15)	
datový propoj RACK-02 - cíl propoje 1	RACK-01 Dodavatele	
datový propoj RACK-02 - cíl propoje 2	DC-03 (Štěpánská 15)	
všechny datové propoje - garantují zachování pořadí rámců	ano	

všechny datové propoje - předávací rozhraní	2x singlemode vlákno, zakončeno na patchpanelu konektorem typu LC	
všechny datové propoje - garantovaná odezva	1 ms	max.
všechny datové propoje - filtrované	ne	
všechny datové propoje - transparentní na úrovni L2	ano	
všechny datové propoje - prioritizované (QoS)	ne	
všechny datové propoje - podporují službu VRRP mezi všemi racky a DC-03	ano	
všechny datové propoje - služba VRRP mezi všemi racky a DC-03 je součástí dodávky	ano	
všechny datové propoje - garantovaná dostupnost	99,50%	min.
všechny datové propoje - v případě nutného plánovaného výpadku na některé datové službě je Dodavatel povinen informovat Odběratele písemně předem	ano	
všechny datové propoje - minimální doba, kterou musí Dodavatel poskytnout Odběrateli pro přípravu na plánovaný výpadek datových služeb	2 pracovní dny	min.
Zadavatel umožňuje Dodavateli použít rack unit (RU) v racku pro nutné síťové komponenty (typicky optická vana, patch panely a edge router pro LAN + SAN) pro dodání služeb	ano	
počet rack unit (RU) Dodavatele použitých v pronajatém racku pro nutné síťové komponenty (typicky optická vana, patch panely, edge routery pro LAN, ) pro dodání služeb	5 ks	max.
dodávka dedikovaných internetových přípojek pro každý rack Dodavatele je součástí služby	ano	
celkový počet dedikovaných internetových přípojek v datacentru Dodavatele	2 ks	
dodávka internetové přípojky z datového centra Zadavatele DC-03 (Štěpánská 15) je součástí služby	ne	
internetové přípojky - musí umožňovat online reporting vytíženosti linky na straně Dodavatele (edge router)	ano	
internetové přípojky - součástí dodávky je i přidělení veřejných pevných IP adres Zadavateli	ano	
internetové přípojky - verze přidělených pevných IP adresy	IPv4	
internetové přípojky - celkový počet přidělených pevných IP adres	256	min.
internetové přípojky - součástí dodávky je i zabezpečení transportu internetu do zahraničí (Full BGP table) bez omezení	ano	
internetové přípojky - garantovaná šířka pásma do zahraničí	300 Mbps	min.
internetové přípojky v datacentru Dodavatele - rychlost download	300 Mbps	min.
internetové přípojky v datacentru Dodavatele - rychlost upload	300 Mbps	min.
internetové přípojky v datacentru Dodavatele - rozhraní dostupné v racku	RJ-45	
internetové přípojky v datacentru Dodavatele - agregované	ne	
internetové přípojky v datacentru Dodavatele - full duplex	ano	
internetové přípojky v datacentru Dodavatele - dostupnost	99,50%	min.

ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služby sledování prostor kolem racků	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služby nepřetržitě ostrahy objektů	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb EZS	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb kamerového systému	ano	
kamerový systém - kamery umístěny	vstup do objektu, vstup na chodbu před sálem, v sále, v uličce k rackům Zadavatele	min.
kamerový systém - služba sledování prostor nutných pro přístup k rackům - rozsah	24x7	
kamerový systém - Zadavatel má možnost získat záznam o přístupu zájmových osob k jeho rackům	ano	
kamerový systém - umožňuje uchování záznamu o stáří	14 dní	min.
kamerový systém - pokud nebude Zadavatelem poskytnut přístup k záznamům kamerového systému, musí Dodavatel zajistit předání požadovaného záznamu do	2 pracovní dny	max.
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - pro dosažení přístupu k poskytovaným rackům je požadována nutnost autentizace pracovníků Objednatele více faktory	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - jako jeden z požadovaných autentizačních faktorů musí být použit biometrický prostředek (naplnění principu "something you are")	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - jako jeden z požadovaných autentizačních faktorů musí být použit fyzický bezpečnostní prostředek (naplnění principu "something you have")	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb autorizace	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb autentizace	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služby řízení přístupů do prostor	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služby řízeného přístupu k poskytovaným rackům	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb požární ochrany	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb klimatizování prostorů s racky	ano	
služba klimatizace - v případě, že je klimatizovaný prostor sálů datacentra rozdělen na tzv. "teplou" a "studenou" uličku, tak studená musí být umístěna	v předu	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí služeb Remote Hands Service v režimu 24x7	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje přítomnost uzlu NIX.CZ pro oba racky Zadavatele	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavatel požaduje poskytnutí nezbytné součinnosti při instalaci a provozování umístěné technologie v místech poskytování služeb serverhousingu	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - v prostoru datacentra musí být dostupné parkování pro pracovníky Zadavatele v případě návštěvy	ano	
parkování musí být umožněno pro automobily typu	osobní, dodávka	

ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - datacentru musí umožňovat transport zařízení z dopravního prostředku na sál Dodavatele bez nutnosti zdolávat schody	ano	
ostatní služby v rámci plnění v lokalitách Dodavatele - datacentrum obsahuje chráněný prostor, kde je možné dočasné usazení pracovníka pro plnění nezbytných úkonů spojených s konfigurací zařízení Zadavatele	ano	
chráněný prostor, kde je možné dočasné usazení pracovníka pro plnění nezbytných úkonů spojených s konfigurací zařízení Zadavatele je opatřen přístupem k internetu	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - přístup do datacentra nesmí být časově omezen (provoz datacentra v režimu 24x7)	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - veškeré podpůrné technologie v musí umožňovat jejich opravu bez výpadku služby	ano	
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - podpůrné technologie musí být odolné proti výpadku jednoho prvku	klimatizace, dodávka ele. energie, EZS, EPS	min.
ostatní služby v rámci plnění služby serverhousingu v lokalitě Dodavatele - Zadavateli bude poskytnut pravidelný měsíční reporting o provozních událostech v datacentru a racích	ano	
pravidelný měsíční reporting provozních událostí - obsahuje typy událostí	přístupy oprávněných osob do datacentra, výpadky podpůrných služeb, teplota + vlhkost na sálech, provozně-bezpečnostní události	min.
služby EZS - rozsah	24x7	
služby poskytnutí přístupu k poskytovaným rackům - osoby	pro autorizované pracovníky Zadavatele, jeho servisní partnery a servisní pracovníky poskytovatele serverhousingu	
oprávněné osoby s možností využití služby Remote Hands	pro autorizované pracovníky Zadavatele, jeho servisní partnery a servisní pracovníky poskytovatele serverhousingu	
Zadavatel má možnost definovat různé seznamy a úrovně oprávnění pro výše uvedené služby (přístup k rackům a Remote Hands)	ano	
služby poskytnutí přístupů k poskytovaným rackům jako součást paušálu - předpokládaný počet autorizovaných osob	10	min.
služby požární ochrany - automatická	ano	
služby požární ochrany - redundantní	ano	
služby požární ochrany - prostory racků jsou chráněny automatickým hasicími zařízeními	ano	
služby požární ochrany - automatická hasící zařízení jsou životu nebezpečná	ne	
služby požární ochrany - jsou konstruovány tak, aby zabránily požáru v sále	ano	
služby požární ochrany - jsou konstruovány tak, aby zabránily požáru v podlaze pod racky	ano	
služby klimatizování prostor s racky - zajištění stabilní teploty	20 až 25°C	

služby klimatizování prostor s racky - zajištění stabilní relativní vlhkosti	20 až 55 % při teplotě 20 °C	
součástí nabídky je i dokument popisující jakým způsobem splňuje Dodavatel požadavky na datové centrum a ostatní služby	ano	

DDoS ochrana		
NIPEZ	72410000-7 Poskytovatelské služby	
parametr	hodnota	max./min.
dodávka služby typu DDoS ochrana na internetových přípojkách je součástí služby	ano	
délka trvání poskytování služeb (včetně přechodných období na začátku a konci kontraktu)	52 měsíců	max.
služba DDoS ochrana - bude realizována prostřednictvím služby Dodavatele	ano	
služba DDoS ochrana - je realizována na straně sítě Dodavatele	ano	
služba DDoS ochrana - je provozována takovým způsobem, aby nedošlo ke zhoršení latence o více jak 10% při přístupu z / na Internet z infrastruktury Zadavatele.	ano	
služba DDoS ochrana - poskytuje dostatečný výkon pro obě internetové přípojky (2x 300 Mbps)	ano	
služba DDoS ochrana - bude poskytována na 1x C rozsah IPv4 adres	ano	
služba DDoS ochrana - musí podporovat IPv4 i IPv6 adresy	ano	
služba DDoS ochrana - Dodavatel je členem sdružení Fenix (fe.nix.cz) a toto členství bude zachovávat po celou dobu účinnosti Smlouvy.	ano	
služba DDoS ochrana - Dodavatel zajistí automatickou mitigaci běžných volumetrických útoků (Volume Based Attacs) na z internetu dostupných rozhraních Zadavatele (webové stránky, informační systémy).	ano	
služba DDoS ochrana - automatické zapnutí v případě atypického chování síťové komunikace	ano	
služba DDoS ochrana - SLA automatické detekce a spuštění automatické mitigace	300 sekund	max.
služba DDoS ochrana - Dodavatel zajistí manuální mitigaci útoku v případě, že se jedná o nový / neznámý typ útoku	ano	
služba DDoS ochrana - SLA pro spuštění manuální mitigace (reakční doba operátora)	15 minut	max.
služba DDoS ochrana - Dodavatel je povinen informovat Zadavatele o aktivaci DDoS ochrany	ano	
služba DDoS ochrana - informace o aktivaci DDoS ochrany musí být poskytnuta kontaktním pracovníkům Zadavatele do	15 minut	max.
služba DDoS ochrana - informace o aktivaci DDoS ochrany musí být poskytnuta kontaktním pracovníkům Zadavatele pomocí	telefonického hovoru	
služba DDoS ochrana - umožňuje úpravu parametrů mitigace na základě kontaktu se Zadavatelem	ano	
služba DDoS ochrana - možnost definovat mitigaci na základě	země (stát), typ služby (protokol), Mbps, Pps (packet), IP adresy, ASN	min.
služba DDoS ochrana - definice šířky kanálu (Mbps a Pps) je možno definovat na internetovou přípojku Dodavatele tak i na zdrojovou IP adresu či stát	ano	
služba DDoS ochrana - podporuje definici rozdílných pravidel na každou jednu IP adresu Zadavatele	ano	
služba DDoS ochrana - podporuje odhalování a blokování útoků na základě světově uznávaných systémů (např. arbor.net)	ano	

služba DDoS ochrana - podporuje nastavování pravidel a mitigací na základě pokynů NÚKIB	ano	
služba DDoS ochrana - k vypnutí služby dochází na telefonický nebo e-mailový souhlas Zadavatele	ano	
služba DDoS ochrana - Dodavatel je povinen uchovávat definované šablony mitigací, které vytvořil ve spolupráci se Zadavatelem a v případě potřeby provést jejich okamžitou reaktivaci	ano	
služba DDoS ochrana - součástí řešení musí být portálový online monitoring provozu a reporting pro IT pracovníky Objednatel (s přehledem síťového provozu a s identifikací alertů)	ano	
služba DDoS ochrana - portálový online monitoring provozu obsahuje monitoring aktuálního provozu (download a upload trafic v kbps nebo Mbps) na internetových linkách	ano	
služba DDoS ochrana - portálový online monitoring provozu - obsahuje monitoring aktuálního využití pásma dle jednotlivých typů služeb (TCP/UDP porty)	ano	
služba DDoS ochrana - součástí řešení musí být pravidelný reporting na měsíční bázi, který sumarizuje objem zpracovaných (přenesených či zahozených) dat, přehled zaznamenaných útoků a jejich trend (klesající nebo stoupající četnost a komplexita útoků)	ano	
služba DDoS ochrana - pravidelný měsíční report obsahuje	období aktivace mitigace, způsob mitigace, cíl útoku	min.
služba DDoS ochrana - dostupnost služby	99,50%	min.
služba DDoS ochrana - režim služby	24x7	
služba DDoS ochrana - celková cena za poskytování DDoS ochrany je pro každý měsíc trvání smlouvy neměnná (měsíční paušál za poskytování služby)	ano	
služba DDoS ochrana - součástí celkové ceny je rovněž realizace konzultací s pracovníky Dodavatele pro správné zavedení služby do provozu (konzultace na začátku plnění služby)	ano	
služba DDoS ochrana - součástí celkové ceny je rovněž realizace konzultací s pracovníky Dodavatele pro bezproblémový provoz služby (konzultace během realizace služby)	ano	
služba DDoS ochrana - Dodavatel uchová informace pro zpracování analýz útoků, bezpečnostních incidentů, ochrany a trendů v síťovém provozu po dobu	90 dnů	min.
služba DDoS ochrana - Dodavatel zajistí zpracování písemných zpráv z bezpečnostních incidentů s údaji o příčinách a následcích incidentů	ano	
služba DDoS ochrana - Dodavatel má povinnost poskytnout nezbytnou součinnost při řešení a vyšetřování incidentů orgány činnými v trestním řízení	ano	
služba DDoS ochrana - počet incidentů, které proběhly v minulém období a vyžadovali součinnost Dodavatele	přibližně 5 za 1 rok	

SOC (Security Operation Center)		
NIPEZ	72410000-7 Poskytovatelské služby	
parametr	hodnota	max./min.
délka trvání poskytování služeb (včetně přechodných období na začátku a konci kontraktu)	na objednávku objednatele	
služba SOC - je zajišťována z území EU	ano	
služba SOC - je dostupná v českém nebo slovenském jazyce	ano	
služba SOC - Dodavatel zajistí prostory a hardwarové vybavení pro poskytování služby	ano	

služba SOC - Dodavatel zajistí jednotný kontaktní bod pro poskytování služby a jednotné komunikační kanály (kontaktní e-mail a telefon)	ano	
služba SOC - Dodavatel se zavazuje plnit bezpečnostní požadavky Zadavatele, Zákona o kybernetické bezpečnosti a souvisejících právních předpisů	ano	
služba SOC - Dodavatel disponuje certifikací ISO/IEC 27001	ano	
služba SOC - musí podporovat práci s nástroji a systémy Zadavatele, které slouží ke sběru a uchování logů systémů Zadavatele	ano	
služba SOC - Dodavatel má schopnost a odbornou způsobilost porozumět obsahu logů vytvářených zařízeními a systémy Zadavatele. Logy Zadavatele jsou shromažďovány ze zařízení a systémů předních výrobců v oboru – Cisco, Checkpoint, F5, Extreme Networks, Microsoft, Canonical Ubuntu, CentOS.	ano	
služba SOC - Dodavatel poskytne spolupráci se Zadavatelem a jeho servisními partnery při analýze potenciálních incidentů z bezpečnostních alertů, potažmo detailních logů událostí zachycených systémy SIEM a EDR/XDR, včetně návrhu na protipatření	ano	
služba SOC - počet potenciálně závažných incidentů, které proběhly v minulém období, ve kterých bude vyžadována nadstandardní součinnost Dodavatele se Zadavatelem, NÚKIB nebo Policií ČR při jejich přezkoumání	přibližně 2 za 1 rok	
služba SOC - proces řízení incidentů musí být nastaven v souladu s dobrou praxí (ISO/IEC 27035:2016 Information Security Incident Management, NIST SP 800-61 nebo jinou obdobnou normou)	ano	
služba SOC - v rámci služby Dodavatel navrhne modifikaci relevantních postupů na straně Zadavatele, včetně vybudování sady detekčních pravidel pro stávající SIEM/Logmanager v rámci rozvojových služeb v produkčním provozu	ano	
služba SOC: Dodavatel zajistí realizační tým pro dodávku služeb SOC a to minimálně s následující úrovní kvalifikace: a) L1 operátor - s dostatečnou odborností pro vykonávání činností SOC s prokazatelnou odborností jako SOC operátor L1 (odborná praxe 3 roky doložená CV) b) L2 analytik - s prokazatelnou minimální dvouletou praxí jako SOC operátor L1 či jako SOC operátor L2, nebo analytik kybernetické bezpečnosti. (CV + odborná certifikace CompTIA Security+ nebo Certified SOC Analyst (CSA) nebo obdobná) c) Expertní analytik -L3 - s prokazatelnou minimální pětiletou praxí analytik kybernetické bezpečnosti (CV + odborná certifikace CompTIA Cybersecurity Analyst (CySA+) nebo Certified Information Systems Security Professional (CISSP) nebo obdobná).	ano	
služba SOC - Dodavatel zajistí dostupnost kapacit a odpovídající expertizu pro řešení ad hoc krizových situací (např. kritického incidentu)	ano	
služba SOC - provádí aktivní monitoring síťového provozu mezi Internetem a sítí Zadavatele	ano	
služba SOC - v případě detekce abnormálního provozu automaticky nasazuje opatření pro mitigaci abnormálního provozu	ano	
služba SOC - v případě nasazení opatření pro mitigaci abnormálního provozu kontaktuje Zadavatele	ano	
služba SOC - kontaktování Zadavatele v případě nasazení opatření proti abnormálnímu provozu musí být uskutečněno pomocí	telefonického hovoru	
služba SOC - informace o nasazení opatření proti abnormálnímu provozu musí být poskytnuta do	15 minut	max.
služba SOC - dostupnost služby	99,50%	min.
služba SOC - režim služby	10x5	min.



<p>služba SOC:  Dodavatel se zavazuje zahájit provoz služby do 2 měsíců od doručení (T0) písemné objednávky Zadavatele na službu SOC. V rámci těchto 2 měsíců Dodavatel provede přípravné činnosti:</p> <p>a) Analýza požadavků – termín dokončení T0 + 2 týdny, cílem je ověřit soulad s požadavky Zadavatele a podrobně specifikovat technickou realizaci služby a případně identifikovat technické problémy;</p> <p>b) Implementace – termín dokončení T0 + 4 týdny, cílem je zprovoznění služby, zprovoznění synchronizace s nástrojem sběru logů Zadavatele a nastavení monitorovacích postupů v souladu s Analýzou požadavků;</p> <p>c) Ověřovací provoz – termín dokončení T0 + 8 týdnů, cílem je jednoměsíční poskytování služby k ověření funkčnosti služby, vyladění efektivní detekce potenciálních incidentů z logů Zadavatele.</p>	ano	
služba SOC - předávání dat SOC ochrany nesmí být realizováno přes internetové linky Zadavatele z důvodu resistance proti DDoS útokům	ano	
služba SOC - předávací rozhraní mezi infrastrukturou Zadavatele a Dodavatele	100BASE-TX	

EDR (Endpoint Detection and Response)		
NIPEZ	72410000-7 Poskytovatelské služby	
parametr	hodnota	max./min.
délka trvání poskytování služeb (včetně přechodných období na začátku a konci kontraktu)	na objednávku objednatele	
EDR (Endpoint Detection and Response) ochrana bude realizována formou rozšíření služby SOC	ano	
služba EDR - musí odhalovat a automaticky eliminovat všechny aktuálně popsané typy útoků v rámci Mitre ATT&CK.	ano	
služba EDR - musí mít schopnost útok automatizovaně zastavit a odstranit jeho artefakty	ano	
služba EDR - musí mít schopnost uložit podezřelé soubory v karanténě	ano	
služba EDR - musí mít schopnost odstavit celý koncový bod do karantény	ano	
služba EDR - při potřebě manuální mitigace musí EDR realizátorovi umožňovat vzdálené přesunutí zařízení do karantény a vyjmutí z karantény	ano	
služba EDR - při potřebě manuální mitigace musí EDR realizátorovi umožňovat vzdálený přístup k obsahu koncového bodu	ano	
služba EDR - při potřebě manuální mitigace musí EDR realizátorovi umožňovat spouštět na koncovém bodu specifické skripty	ano	
služba EDR - služba EDR - při potřebě manuální mitigace musí EDR realizátorovi umožňovat přenést vybraná data k další analýze mimo koncový bod	ano	
služba EDR - musí umožňovat dohledání artefaktů útoku / incidentu přes celou chráněnou infrastrukturu a to minimálně podle dohledání souborů se specifickým hash nebo názvem	ano	
služba EDR - musí umožňovat dohledání artefaktů útoku / incidentu přes celou chráněnou infrastrukturu a to minimálně podle výskytu specifických dat	ano	
služba EDR - musí umožňovat dohledání artefaktů útoku / incidentu přes celou chráněnou infrastrukturu a to minimálně podle výskytu specifických procesů	ano	
služba EDR - pro potřeby forenzního šetření útoků, musí být možné doložit celý sled událostí (minimálně spouštěné procesy, zpřístupňované soubory, klíče registru) od okamžiku zjištění zpětně až k místu prvotního průniku	ano	
služba EDR - musí umožňovat nastavení různých pravidel ochrany podle typu chráněného koncového bodu	ano	
služba EDR - musí umožňovat nastavení výjimek z ochrany	ano	

služba EDR - musí zajistit přiměřené logování na chráněných bodech.	ano	
služba EDR - musí umožňovat odesílání dat do SIEM / logmanageru Zadavatele	ano	
služba EDR - musí fungovat prostřednictvím agentů na chráněných zařízeních s operačními systémy Windows 10 a novější a Windows Server 2016 a novější a Linux (minimálně Ubuntu, CentOS a RedHat)	ano	
služba EDR - Dodavatel zajistí spolupráci realizačního týmu na investigaci a mitigaci incidentů identifikovaných chráněných zařízeních Zadavatele	ano	
služba EDR - dostupnost služby	99,50%	min.
služba EDR - režim služby	24x7	
služba EDR - Dodavatel zajistí dostupnost dat pro zpracování analýz útoků, bezpečnostních incidentů a ochrany	ano	
služba EDR - na základě požadavku Zadavatele Dodavatel zajistí zpracování analýz útoků, bezpečnostních incidentů a ochrany	ano	