Kúpna zmluva č. Z202313930_Z

uzatvorená v zmysle §409 a nasl. Obchodného zákonníka

I. Zmluvné strany

1.1 Objednávateľ:

Obchodné meno:	Centrum spoločných činností Slovenskej akadémie vied
Sídlo:	Dúbravská cesta 3484/9, 84535 Bratislava - mestská časť Karlova Ves, Slovenská republika
IČO:	00398144
DIČ:	2020894843
IČ DPH:	SK2020894843
Bankové spojenie:	IBAN: SK5781800000007000324349
Telefón:	0232293115

1.2 Dodávateľ:

Obchodné meno:	IXPERTA s. r. o., organizačná zložka
Sídlo:	Dúbravská cesta 4, 84104 Bratislava, Slovenská republika
IČO:	48257591
DIČ:	4020380364
IČ DPH:	SK4020380364
Bankové spojenie:	IBAN: CZ7527000000000513686001
Telefón:	+421232292711

II. Predmet zmluvy

2.1 Všeobecná špecifikácia predmetu Zmluvy:

Názov:	Perimetrový firewall
Kľúčové slová:	Firewall, bezpečnosť
CPV:	48730000-4 - Softvérový balík na zaistenie bezpečnosti
Druh/y:	Tovar; Služba

2.2 Funkčná a technická špecifikácia predmetu Zmluvy:

Položka č. 1: Firewall

Funkcia				
Perimetrový Next Generation Firewall s pokročilými funkcionalitami				
Technické vlastnosti	**Jednotka**	**Minimum**	**Maximum**	**Presne**
Firewall (Check Point CloudGuard Network virtual)	ks			2
Technické vlastnosti	**Hodnota/Charakteristika**			
Požadované funkcionality	Firewall, IPS, Aplikačná kontrola, Malware, Botnet a Zeroday ochrana, HTTPs inšpekcia			
Priepustnosť Firewallu (podľa RFC 3511, 2544, 2647, 1242)	minimálne 18 Gbps			
Priepustnosť IPS (enterprise traffic mix)	minimálne 16 Gbps			
Priepustnosť NGFW (Firewall, IPS, Aplikačná kontrola)	minimálne 15 Gbps			
Priepustnosť Threat ochrana (Firewall, IPS/IDS, Aplikačná kontrola, Antivir, Botnet)	minimálne 7 Gbps			
Počet nových spojení za sekundu (CPS)	minimálne 200.000			
Počet súčasných spojení	minimálne 15.000.000			

Požiadavky na hardvérové vybavenie	Firewall musí byť vo forme virtuálnej appliance pre prostredie VMWARE ESXi, Vsphere 7.x
Vysoká dostupnosť	Požaduje sa dodať dvojicu zariadení zapojenú v HAkonfigurácii. Podpora redundancie dvoch zariadení v režime Active-Standby so stavovou synchronizáciou. Šifrovaná klaster komunikácia.
Zvýšenia výpočtového výkonu	Podpora možnosti zvýšenia výpočtového výkonu navýšením licencovaného počtu jadier CPU bez nutnosti výmeny HW
Počet kritických CVE zraniteľností výrobcu firewallu za posledné 3 roky (2020-2022)	maximálne 15
Spoločné vlastnosti	Preddefinované threat ochrany a profily pre IPS, Antivirus, Anti-botnet a Zero-day ochrana
Spoločné vlastnosti	Zobrazenie užívateľskej notifikácie pri blokovaní aplikácií
Spoločné vlastnosti	Možnosť získavania identít užívateľov z AD bez nutnosti inštalácie softvéru na AD servery
Spoločné vlastnosti	Integrovaný firewall performance analyzer, min. top 10 spojení a ich % konzumácia HW zdrojov/pre každé spojenie/protokol
Spoločné vlastnosti	Podpora linux nástrojov (min. SCP, BASH, VI, TOP), spúšťanie linux skriptov a nástrojov tretích strán
Spoločné vlastnosti	Nasadenie NGTX. Implementácia HW platformy. Inštalácia do virtuálneho prostredia. Dokumentácia a zaškolenie
IPS	Nové IPS signatúry musia byť označené a byť aktivované len v detekčnom režime. Automatické vypnutie IPS ochrany (pre konkrétnu inštanciu FW) v prípade preťaženia HW nad definovanú prahovú hodnotu
Aplikačná kontrola. Detekcia a riadenie sieťových aplikácií.	Počet rozpoznávaných aplikácií minimálne 7500
Malware, Botnet a Zero-day ochrana	Ochrana proti neznámym hrozbám: emulácia súborov vo virtuálnom sandbox prostredí, min. podporované typy súborov: powerpoint, word, excel, pdf, exe, archívy (zip, tar, 7z, rar)
Malware, Botnet a Zero-day ochrana	Podporovaná veľkosť emulovaných súborov v sandbox, až do veľkosti 80MB
Malware, Botnet a Zero-day ochrana	Odstránenie potenciálne škodlivého aktívneho obsahu (makro, javascript...) zo súboru, prípadne konverzie dokumentu do PDF. Podporované protokoly SMTP, SMTPs, HTTP a HTTPs.
Malware, Botnet a Zero-day ochrana	Podporované typy súborov na odstránenie aktívneho obsahu: MS Office, PDF, JPEG, BMP, PNG, TIFF, GIF
Malware, Botnet a Zero-day ochrana	Zablokovanie prvého pokusu o stiahnutie zero-day malware cez protokoly SMTP, SMTPs, HTTP a HTTPs. IMAP, IMAPs, POP3, POP3s, SMB a FTP
Malware, Botnet a Zero-day ochrana	Podpora MTA agenta za účelom skenovania súborov pre Anti-virus a Zero-day ochranu
Malware, Botnet a Zero-day ochrana	Pridávanie vlastných IOC indikátorov (IP, MD5, URL), manuálne alebo cez API
HTTPs inšpekcia	SNI HTTPS klasifikácie a inšpekcie. Ochrana proti SNI spoofing v rámci HTTPs inšpekcie. Blokácia SQL Injection a CSS útokov v celej URL a HTML body
Web Application Firewall	Požadovaný je kontextový Web Application Firewall s podporou automatického učiaceho sa režimu a ML algoritmy pre detekciu hrozieb
Web Application Firewall	Požadované funkcie: antivirus, antibot, ips (s podporou snort signatur), podpora openapi schém, rate limiting, ochrana proti neznámym hrozbám (sandboxing pre file upload security)
Web Application Firewall	Samostatne inštalovateľný ako VM (hardenovaný operačný systém rovnakého typu ako je firewall OS) s podporou on-prem prostredia (nie je žiaduce posielať logy do cloudu)
Web Application Firewall	Podpora offline policy bez nutnosti cloudu
Web Application Firewall	Deployment musí podporovať nasledujúce proxy: KONG, NGINX. Taktiež musí byť schopný fungovať ako nezávislý Web Application Firewall

Web Application Firewall	Možnosť integrácie aj ako ingress pre prostredie kubernetes.
Web Application Firewall	Licencovanie musí byť len podľa počtu http requestov za časovú jednotkou: Je požadovaných minimálne 100 miliónov requestov za rok.Nie je žiaduce licencovanie pomocou priepustnosti.
Web Application Firewall	Produkt musí mať i variant opensource, ktorý v prípade ukončenia licencie umožňuje pokračovať ďalej s limitovaným počtom funkcií.
VPN	Podpora S2S VPN, min. podpora algoritmov pre šifrovanie: AES-128, AES-256 a integritu: SHA-256 a AES-XCBC.Podpora IP kompresie pre S2S VPN. Podpora dekrypcieTLS 1.3. Remote Access VPN pre 50 súbežný
Správa platformy	Centrálna jednotná správa politík z dedikovanej grafickej aplikácie
Správa platformy	Možnosť využitia existujúcej manažment platformy Check Point alebo ekvivalent s licenčným pokrytím na minimálne 5 rokov.
Správa platformy	Rovnaký operačný systém (OS) pre všetky zariadenia (firewall, management, endpointy)
Správa platformy	Centrálny management server musí byť na samostatnom zariadení, prípadne ako licencia pre inštaláciu do VM (Vmware ESXi alebo MS Hyper-V)
Správa platformy	Požadujeme konsolidovaný centrálny management politik firewallov, bezpečnosti endpointov, analýza logov a reporting na jednom zariadení (prípadne jednej VM)
Správa platformy	Podpora pravidelného automatického zálohovania konfigurácie (na základe časového rozvrhu), s možnosťou nahrania zálohy na vzdialený SCP server.
Správa platformy	Podpora služby vlastnej certifikačnej autority pre vydávanie PKI certifikátov pre bezpečné prihlasovanie užívateľov a administrátorov a pre VPN klientský prístup
Správa platformy	Integrácia SAML 2.0 autentizačných služieb pre overovanie a získavanie identít užívateľov
Správa platformy	integrácia na Azure AD a získavanie rolí užívateľov z ich skupín pre politikov
Ďalšie vlastnosti	Management musí byť schopný dohľadať pre každý objekt, jeho výskyt v aktívnych aj neaktívnych pravidlách, alebo v iných objektoch (napr. v objektových skupinách)
Ďalšie vlastnosti	Podpora administrátorských profilov pre delegáciu oprávnení (čítanie, zápis)
Ďalšie vlastnosti	Ochrana vzájomného ovplyvňovania alebo kolízie pri súčasnom pripojení viacerých administrátorov (zamykanie pravidiel a objektov)
Ďalšie vlastnosti	Policy Tracer - vyhľadávanie firewall pravidla podľa kombinácie definovaných atribútov (min. zdrojová IP, cieľová IP, užívateľ, služba, aplikácia ..)
Ďalšie vlastnosti	Vizualizácia a prehľadávané logov priamo v politike na vybranom pravidle (min. zdroj, cieľ, služba, aplikácia, používateľ, čas)
Ďalšie vlastnosti	Zobrazenie histórie a zmien priamo v politike na vybranom pravidle (min. kto, aká zmena a kedy bola na pravidle vykonaná)
Ďalšie vlastnosti	Hit count štatistiky pre jednotlivé pravidlá s cieľom optimalizácie bezpečnostnej politiky
Ďalšie vlastnosti	Integrácia na VMware NSX/vCenter, min. dynamické získavanie VM objektov a ich aplikácia vo firewall politike
Ďalšie vlastnosti	Práca s bezpečnostnými logami - možnosť prehľadávania všetkých typov logov (fw, ips, malware) v jednej záložke s definovaním vlastných permanentných filtrov
Ďalšie vlastnosti	Rekonfigurácia a ladenie threat engine priamo z log výstupov firewallu
Ďalšie vlastnosti	Podpora korelácie bezpečnostných logov a incidentov
Ďalšie vlastnosti	Minimálna podporovaná veľkosť diskovej kapacity pre dlhodobé ukladanie logov na konsolidovanommanagemement servery (licencia pre požadovanú veľkosť musí byť súčasťou ponuky) = min. 10 TB

Ďalšie vlastnosti	Mitre Attack podpora v reportovaných udalostiach
Reportovanie a monitorovanie	Centrálny management server musí obsahovať nástroj pre definíciu a generovanie reportov
Reportovanie a monitorovanie	Musí graficky zobrazovať jednotlivé kategórie udalostí vo forme interaktívnych koláčových a časových grafov
Reportovanie a monitorovanie	Integrovaný monitoring musí poskytovať grafické rozhranie pre sledovanie parametrov v reálnom čase a histórii aspoň 30 dní (RAM, CPU, počet novo-otvorených spojení za sekundu, priepustnosť ...)
Licencie pre zabezpečenie všetkých funkcionalít	5 rokov
Služby	Identifikácia prostredia zákazníka
Služby	Návrh implementácie riešenia
Služby	Implementácia riešenia a testovanie
Služby	Integrácia riešenia do komplexného jednotného funkčného bezpečnostného ekosystému s ostatnými riešeniami
Služby	Nasadenie dodaných tovarov do produkčného prostredia
Služby	Konfigurácia a ladenie do komplexného funkčného bezpečnostného ekosystému
Služby	Spustenie produkčnej prevádzky
Služby	Zaškolenie interných pracovníkov v rozsahu 8 človekohodín
Služby	Odovzdanie technickej a užívateľskej dokumentácie
Služby	Projektové riadenie dodávky a implementácie riešenia

2.3 Osobitné požiadavky na plnenie:

Názov
Vrátane dopravy na miesto plnenia
Vrátane inštalácie na mieste plnenia
Požaduje sa predložiť vlastný návrh na plnenie predmetu zmluvy do 7 dní od uzavretia zmluvy
Uchádzač predloží originál alebo kópiu platného certifikátu systému riadenia kvality podľa normy STN EN ISO 9001:2008 minimálne v oblasti predaj, inštalácia a servis zariadení výpočtovej techniky vydaného nezávislou inštitúciou, ktorým sa potvrdzuje splnenie noriem zabezpečenia kvality uchádzačom.
Uchádzač predloží originál alebo kópiu platného certifikátu systému manažérstva bezpečnosti informácií podľa EN ISO 27001 v oblasti bezpečnosti aktív informačných systémov, infraštruktúry informačných technológií a komunikácií, resp. iný certifikát (doklad) prezentujúci zavedený systém manažérstva bezpečnosti informácií dodávateľa.
Uchádzač predloží platný certifikát PRINCE 2 Practitioner alebo IPMA B na odbornú spôsobilosť pre riadenie projektov alebo ekvivalent daného certifikátu zodpovedajúcej úrovne vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou projektového manažéra implementačného tímu.
Uchádzač predloží platný certifikát ArchiMate, alebo TOGAF, alebo ekvivalent daného certifikátu zodpovedajúcej úrovne vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou pre člena tímu zodpovedného za návrh architektúry riešenia.
Platný technický certifikát minimálne dvoch členov implementačného tímu vydaný výrobcom ponúkaného riešenia pre správu firewallov strednej alebo vyššej úrovne, vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou.
Platný certifikát CCNP Enterprise alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditačnou a certifikačnou autoritou pre člena tímu v role sieťového špecialistu.
Platnosť certifikátov objednávateľ overí po uzatvorení zmluvy, pričom nesplnenie tejto požiadavky objednávateľa sa bude považovať za podstatné porušenie zmluvy.
Obstarávateľ prijme aj iné dôkazy predložené uchádzačom alebo záujemcom, ktoré sú rovnocenné opatreniam na zabezpečenie kvality podľa požiadaviek na vystavenie príslušného certifikátu.
Požaduje sa predložiť funkčná a technická špecifikácia, vrátane technických listov preukazujúcich splnenie minimálnych požadovaných parametrov predmetu zákazky s uvedením presných názvov (obchodných značiek) nacenených výrobkov do 5 pracovných dní od účinnosti Zmluvy
Splatnosť faktúry je 30 dní
Objednávateľ požaduje zaslať tovar celkom nový, nepoškodený, nevystavovaný v prvej akostnej triede, zodpovedajúci požiadavkámObjednávateľa

Nový, doposiaľ nepoužitý tovar
Dodávateľ je povinný na svoje náklady zabezpečiť výmenu tovaru. Ak ide o chybu odstrániteľnú má Objednávateľ právo na bezplatné, riadne a včasné odstránenie chyby. Ak ide o chybu neodstrániteľnú brániacu riadnemu užívaniu tovaru má Objednávateľ právo na výmenu chybného tovaru
Ak sa v opisnom formulári uvádzajú údaje alebo odkazy na konkrétneho výrobcu, výrobný postup, značku, obchodný názov, patent alebo typ, umožňuje sa Dodávateľovi predloženie ponuky s ekvivalentným riešením s porovnateľnými, respektíve lepšími parametrami. Ekvivalent je možné dodať v rovnakej alebo vyššej kvalite podľa Technickej špecifikácie predmetu zákazky len po konzultácii a so súhlasom Objednávateľa
Objednávateľ je oprávnený namietať vecnú a formálnu správnosť a úplnosť faktúry a jej povinných príloh najneskôr do 15 dní odo dňa doručenia faktúry Objednávateľovi vrátením faktúry s uvedením konkrétnych výhrad voči faktúre. Doručením opravenej faktúry Dodávateľa začína plynúť nová lehota splatnosti faktúry
V prípade, že Dodávateľ nie je platcom DPH, pri oceňovaní zákazky v EKS pri položke DPH uvedie nulu

Názov	Upresnenie

2.4 Prílohy opisného formulára Zmluvy:

Popis	Názov súboru

III. Zmluvné podmienky

3.1 Miesto plnenia Zmluvy:

Štát:	Slovenská republika
Kraj:	Bratislavský
Okres:	Bratislava IV
Obec:	Bratislava - mestská časť Karlova Ves
Ulica:	Dúbravská cesta 9

3.2 Čas / lehota plnenia zmluvy:

12.12.2023 11:30:00 - 27.12.2023 09:15:00

3.3 Dodávané množstvo/ rozsah zmluvného plnenia:

Jednotka:	ks
Požadované množstvo:	2,0000

3.4 Práva a povinnosti zmluvných strán podľa tejto Zmluvy sa spravujú Obchodnými podmienkami elektronickej platformy verzia 1.2, účinná odo dňa 3. 11. 2022 , ktoré tvoria neoddeliteľnú prílohu tejto Zmluvy.

IV. Zmluvná cena

4.1 Celková cena predmetu Zmluvy bez DPH: 131 700,00 EUR

4.2 Sadzba DPH: 20,00

4.3 Celková cena predmetu Zmluvy vrátane DPH: 158 040,00 EUR

V. Záverečné ustanovenia

5.1 Táto Zmluva bola uzavretá automatizovaným spôsobom v rámci Elektronického kontraktačného systému a v zmysle Obchodných podmienok elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, ktoré tvoria jej prílohu č. 1.

5.2 Táto Zmluva nadobúda platnosť dňom jej uzavretia a účinnosť za podmienok definovaných v Obchodných podmienkach elektronickej platformy uvedených v bode 5.1 tejto zmluvy.

5.3 Táto Zmluva vrátane jej príloh predstavuje úplnú dohodu zmluvných strán o jej predmete. Vedľajšie dohody k tejto zmluve neexistujú.

5.4 Táto Zmluva je vyhotovená v elektronickej podobe v štyroch vyhotoveniach, po jednom pre každú zmluvnú stranu, jedno vyhotovenie bude zaslané na zverejnenie v Centrálnom registri zmlúv Úradu vlády Slovenskej republiky a jedno bude zverejnené v Centrálnom registri zmlúv Trhoviska.

5.5 Túto Zmluvu bude možné meniť a dopĺňať za podmienok stanovených príslušnými všeobecne záväznými právnymi predpismi len vo forme písomného a číslovaného dodatku podpísaného oboma zmluvnými stranami.

5.6 Táto Zmluva má nasledovné prílohy:
Príloha č.1 Obchodné podmienky elektronickej platformy verzia 1.2, účinná odo dňa 03.11.2022, https://portal.eks.sk/SpravaOpet/Opet/VerejnyDetail/

V Bratislave, dňa 07.12.2023 11:08:01

Objednávateľ:
Centrum spoločných činností Slovenskej akadémie vied
konajúci prostredníctvom osoby poverenej zastupovať Objednávateľa v rámci elektronického trhoviska

Dodávateľ:
IXPERTA s. r. o., organizačná zložka
konajúci prostredníctvom osoby poverenej zastupovať Dodávateľa v rámci elektronického trhoviska