Exp. 2023-2842 (B149 2023-22)

PLEC DE PRESCRIPCIONS TÈCNIQUES DEL CONTRACTE DE SUBMINITRAMENT DE LLICÈNCIES SOPHOS INTERCEPT X PER A SERVIDORS I ORDINADORS

1. Objecte del contracte

L'objecte del contracte és el subministrament de 30 llicències Central Intercept X Advanced per als servidors amb XDR i 200 llicències Central Intercept X Endpoint Advanced amb XDR per als ordinadors corporatius.

L'objecte del contracte no es divideix en lots atès que es tracta d'un mateix software tant per servidors com ordinadors i el subministrament de les llicències d'ús ha d'anar a càrrec d'un únic proveïdors per tal de garantir una correcte coordinació i gestió des del punt de vista tècnic

2. Naturalesa del contracte

El contracte tindrà, en tot moment i a tots els efectes, la qualificació de contracte de subministrament, tal i com es defineix a l'article 16.3.b) de la Llei 9/2017, de 8 de novembre, de la Llei de contractes del sector públic per la qual es transposen a l'ordenament jurídic espanyol les directives del Parlament Europeu i del Consell 2014/23/UE i 2014/24/UE, de 26 de febrer de 2014 (en endavant LCSP), atès que les prestacions de addicionals de suport i assistència no impliquen acciones complexes i són necessaris pel desenvolupament normal del programa. La classificació segons el vocabulari comú de contractes públics, CPV té els següent codi:48218000-9 "Paquets de gestió de llicències".

3. Durada del contracte

La durada del contracte serà de tres anys, a comptar des de l'endemà de la data de formalització del contracte. No podrà ser objecte de pròrrogues.

Quan al venciment del contracte no s'hagués formalitzat el nou contracte que garanteixi la continuïtat de les prestacions a realitzar pel contractista com a conseqüència d'incidències resultants d'esdeveniments imprevisibles per a l'òrgan de contractació produïdes en el procediment d'adjudicació i existeixin raons d'interès públic per no interrompre la prestació, es podrà prorrogar el contracte originari fins que comenci l'execució del nou contracte i, en tot cas, per un període màxim de nou mesos, sense modificar la resta de condicions del contracte, sempre que l'anunci de licitació del nou contracte s'hagi publicat amb una antelació mínima de tres mesos respecte a la data de finalització del contracte originari, d'acord amb allò que disposa l'article 29.4 LCSP.

4. Prestacions
Les prestacions són les descrites als annexes 1 i 2 d'aquest plec en funció dels tipus de llicències subministrades.

5. Valor estimat del contracte i pressupost base de licitació
El valor estimat del contracte és de 20.160 € (IVA exclòs). Aquest valor estimat és el resultat de multiplicar les tres anualitats màximes previstes pel valor estimat anual i sumar més l'import del 20% de modificacions contractuals previstes, amb el següent detall:

2023	2024	2025	20% Modificacions	**TOTAL (IVA exclòs)**
5.600 €	5.600 €	5.600 €	3.360 €	**20.160 €**

El pressupost base de licitació és fixa en la quantitat de 20.328 €, IVA inclòs, pels tres anys de durada del contracte. Aquest valor és el resultat de la suma de la base imposable amb un import de 16.800 € més la quota de l'IVA, al tipus impositiu vigent del 21%, amb un import de 3.528 €.

El mètode de càlcul del valor estimat del contracte, d'acord amb el contingut i criteris de l'article 101 LCSP, es determina tenint en compte els preus de mercat en subministraments similars.

ANNEX 1 (Central Intercept X Advanced per servidors amb XDR)

REDUCCIÓ DE SUPERFÍCIE D'ATAC

-Protecció web
-Reputació de descàrregues
-Control web / bloqueig d'URL basat en categories
-Control de perifèrics
-Control d'aplicacions
-Llestes blanques d'aplicacions (bloqueig de servidor)

ABANS QUE S'EXECUTI EN EL DISPOSITIU

-Detecció de malware amb Deep Learning
-Escanejat d'arxius antimalware
-Live Protection
-Anàlisis de comportament previ a l'execució (HIPS)
-Bloqueig d'aplicacions no desitjades
-Sistema de prevenció d'intrusions

DETENIR L'AMENAÇA EN EXECUCIÓ

-Prevenció de pèrdues de dades
-Anàlisis de comportament en temps d'execució (HIPS)
-Interfície d'anàlisi antimalware (AMSI)
-Detecció de trànsit maliciós (MTD)
-Prevenció de exploits
-Mitigacions d'adversaris actius
-Protecció contra arxius de ransomware (CryptoGuard)
-Protecció del registre d'arrencada i disc (WipeGuard)
-Protecció contra Man-in-the-Browser (Navegació segura)
-Bloqueig d'aplicacions millorat

DETECTAR

-Decisions en temps d'execució sobre el comportament i els exploits en hosts i contenidors -Linux
-Live Discover (consultes SQL en tota la infraestructura per a la cerca d'amenaces i la higiene de les operacions de seguretat TU)
-Biblioteca de consultes SQL (consultes ja escrites totalment personalitzables)
-Detecció i priorització d'esdeveniments sospitosos
-Emmagatzematge de dades en disc de ràpid accés (fins a 90 dies)

-Fonts de dades entre productes (p. ex. Firewall, Email)
-Consultes entre productes
-Consultes programades

INVESTIGAR

-Casos d'amenaces (Anàlisis de causa arrel)
-Anàlisi de malware amb Deep Learning
-Informació sobre amenaces avançada de SophosLabs a demanda
-Exportació de dades forenses

SOLUCIONAR

-Eliminació de malware automatitzada
-Seguretat sincronitzada amb Security Heartbeat
-Sophos Clean
-Live Response (investigui i prengui mesures de manera remota)
-Aïllament de endpoints a demanda
-"Netejar i bloquejar" en un sol clic

VISIBILITAT

-Protecció de càrregues de treball en el núvol (Amazon Web Services, Microsoft Azure, Google Cloud Platform)
-Control d'aplicacions sincronitzat (visibilitat d'aplicacions)
-Gestió de la postura de seguretat en el núvol (supervisió dels entorns AWS, Azure, GCP)

CONTROL

-Gestió de polítiques específiques del servidor
-Caixet d'actualització i repetidor de missatges
-Exclusions d'escanejat automàtic
-Monitoratge d'integritat d'arxius

ANNEX 2 (Central Intercept X Endpoint Advanced amb XDR per als ordinadors corporatius)

SUPERFÍCIE D'ATAC

Protecció web
Reputació de descàrregues
Control web / bloqueig d'URL basat en categories
Control de perifèrics
Control d'aplicacions

ABANS QUE S'EXECUTI EN EL DISPOSITIU

Detecció de malware amb Deep Learning
Escanejat d'arxius antimalware
Live Protection
Anàlisis de comportament previ a l'execució (HIPS)
Bloqueig d'aplicacions no desitjades
Sistema de prevenció d'intrusions

DETENIR L'AMENAÇA EN EXECUCIÓ

Prevenció de pèrdues de dades
Anàlisis de comportament en temps d'execució (HIPS)
Interfície d'anàlisi antimalware (AMSI)
Detecció de trànsit maliciós (MTD)
Prevenció de exploits
Mitigacions d'adversaris actius
Protecció contra arxius de ransomware (CryptoGuard)
Protecció del registre d'arrencada i disc (WipeGuard)
Protecció contra Man-in-the-Browser (Navegació segura)
Bloqueig d'aplicacions millorat

DETECTAR

Live Discover (consultes SQL en tota la infraestructura per a la cerca d'amenaces i la higiene de les operacions de seguretat TU)
Biblioteca de consultes SQL (consultes ja escrites totalment personalitzables) Detecció i priorització d'esdeveniments sospitosos
Detecció i priorització d'esdeveniments sospitosos
Emmagatzematge de dades en disc de ràpid accés (fins a 90 dies)
Fonts de dades entre productes, p. ex. Firewall, Email (Sophos XDR)

Consultes entre productes (Sophos XDR)
Emmagatzematge en el núvol en Sophos Data Lake
Consultes programades

INVESTIGAR

Casos d'amenaces (Anàlisis de causa arrel)
Anàlisi de malware amb Deep Learning
Informació sobre amenaces avançada sota demanda de Sophos X-Ops
Exportació de dades forenses

SOLUCIONAR

Eliminació de malware automatitzada
Seguretat sincronitzada amb Security Heartbeat
Sophos Clean
Live Response (investigui i prengui mesures de manera remota)
Aïllament de endpoints a demanda
"Netejar i bloquejar" en un sol clic