QUADRE DE CARACTERÍSTIQUES ADMINISTRATIVES
Subministrament de Serveis de ciberseguretat (Categoria 4 del SDA)

CARACTERÍSTIQUES ADMINISTRATIVES

1. **Objecte del contracte. Codi CPV. Durada del contracte.**

Objecte: Nova contractació del Sistema de protecció antivirus i de seguretat d'endpoints amb capacitats EDR/XDR.

Codi CPV: 48760000-3

Durada del contracte: 09/07/2024 – 08/07/2025

2. **Import i pressupost base de la licitació**.

Justificació del preu: s'ha realitzat una consulta a diferents empreses del sector valorant les possibilitats.

El pressupost base de la licitació és d'un màxim de 21.607,09€ IVA inclòs, sent 17.857,10€ de base imposable i 3.749,99€ d'IVA, tenint en compte que la durada serà d'un any.

Concepte	**Quantitat**	**Preu unitari màxim**	**Total (IVA Exclòs)**	**Total (IVA Inclòs)**
Cost Llicències usuaris MS365	128	31,02€	3.970,56€	4.804,37€
Cost Llicències servidors	94	21,57€	2.027,58€	2.453,37€

Concepte	**Quantitat**	**Preu unitari màxim**	**Total (IVA Exclòs)**	**Total (IVA Inclòs)**
Servei SOC 100 llocs i comptes M365	1	5.653,20€	5.653,20€	6.840,37€
Serveis SOC Servidors	94	49,18€	4.622,92€	5.593,73€
Serveis SOC Usuari amb Office 365	28	56,53€	1.582,84€	1.915,23€

3. Plurianualitats

Es contractarà per un any

Any	Import
2024	**8.928,55€**
2025	**8.928,55€**

4. Valor estimat del contracte

El valor estimat del contracte serà de com a màxim 17.857,10 € IVA exclòs.

5. Garantia definitiva

D'acord amb l' article 107.1 segon paràgraf de la LCSP, l'òrgan de contractació pot exigir la constitució de garantia en els contractes específics.

L'adjudicatària haurà de constituir una garantia definitiva corresponent al 5% del pressupost base de licitació del contracte, IVA exclòs.

El termini de garantia serà de sis mesos un cop finalitzat el contracte d'acord amb l'article 111 de la LCSP.

La devolució de la garantia definitiva tindrà lloc durant els dos mesos següents a què finalitzi el termini i un cop hagi signat l'acta de conformitat.

6. Lloc i forma de pagament

Prèvia presentació de la factura, s'abonarà de la següent manera a l'adjudicatari:

- Primer 50% de la factura a l'inici del contracte
- Últim i segon 50% a l'entrega del projecte

7. Criteris de valoració.

Mitjançant preu: s'atorgarà la màxima puntuació a les proposicions que ofereixen el preu més baix. La resta serà de manera proporcional tenint en compte les següents fórmules:

<u>Cost Llicències usuaris MS365:</u>

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 22\ punts$$

Cost Llicències servidors

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 11\ punts$$

Servei SOC 100 llocs i comptes M365

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 32\ punts$$

Serveis SOC Servidors

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 26\ punts$$

Serveis SOC Usuari amb Office 365:

$$Punts = \frac{Oferta\ més\ econòmica}{Oferta\ que\ es\ puntua} * 9\ punts$$

CARACTERÍSTIQUES TÈCNIQUES

1. Característiques tècniques.

La present sol·licitud tècnica té com a objectiu seleccionar un proveïdor que subministri un Sistema de Detecció i Resposta Ampliada (XDR) amb capacitats de Detecció i Resposta davant Amenaces (EDR) per enfortir la postura de seguretat. La solució ha d'incloure els serveis de desplegament, operació d'un Centre d'Operacions de Seguretat (SOC), anàlisi de la postura de seguretat, funcionalitats XDR i protecció d'endpoint per a usuaris i servidors.

La solució presentada ha de cobrir:

- Programari necessari (llicència anual) que comprengui diversos sistemes operatius (Windows desktop i server, Linux).
- Desplegament substituïnt altres solucions anteriors.
- Serveis gestionats de la solució XDR i acció segons plans de contingència específics en cas d'amenaces (SOC).
- Compliment de la legislació vigent a Espanya i Europa.

Requeriments Específics

La solució proporcionada haurà de cobrir els següents punts:

Serveis de Desplegament de la Solució:

- Inicialització de la consola de gestió i configuració.
- Creació de polítiques segons perfils d'usuaris i servidors.
- Desplegament de nous agents i sondes. En el cas dels servidors de producció de manera no automatitzada.
- Formació a l'equip d'administració.

Serveis SOC:

- Monitorització de seguretat 24/7.
- Servei CERT per a resposta davant incidents.
- Generació d'informes mensuals d'estat de seguretat.

Anàlisi de la Postura de Seguretat:

- Índex de risc desglossat per categories.
- Representació gràfica en un quadre de comandament.
- Generació d'informes executius de riscos.
- Integració d'informació a la plataforma XDR.

Funcionalitats XDR:

- Detecció i correlació avançada d'esdeveniments de seguretat.
- Capacitat d'investigació d'alertes.
- Threat hunting automatitzat.
- Execució d'accions de resposta des de la plataforma.

Protecció d'Endpoint:

- Antimalware avançat.
- Anàlisi de reputació web.
- Firewall de host.
- Control de USBs.

- Monitorització d'integritat.
- Compatibilitat amb el programari.
- Compatibilitat amb les VPN.

Requisits d'expansió

- Allotjament de servidors dins de la Unió Europea.
- Emmagatzematge de telemetria i esdeveniments d'auditoria mínim de 30 dies.
- API per a la gestió programàtica del producte.
- Integració amb serveis de tercers i gestors d'identitats.
- Integració i obtenció de dades d'amenaces a nivell global.
- Suport per a sistemes operatius i aplicacions específiques (Linux, Windows desktop, Windows Server).
- Integració amb l'Active Directory.

Requisits de la Consola de Gestió

La consola de gestió ha de complir amb els següents requisits:

- Autenticació mitjançant SAML.
- Accés basat en rols i doble factor d'autenticació.
- Integració nativa amb vCenter, i opcionalment, Azure.
- Personalització de quadres de comandament i informes automatitzats.

Requisits de Seguretat

- Detecció avançada de malware i anàlisi de comportament.
- Protecció contra ransomware i exploits.
- Anàlisi de reputació web a nivell de kernel.
- Firewall de host amb regles configurables.

Requisits de Suport i Manteniment

- Suport tècnic 24/7 a través de plataforma online i sistema de ticketing
- Actualitzacions regulars de signatures i software.
- Capacitats per a l'equip d'administració.
- Garantia de disponibilitat i rendiment.

Altres criteris

Aplicar els principis de seguretat i complir amb els requisits d'un Esquema Nacional de Seguretat (ENS) en el context d'una solució XDR (Detecció i Resposta Ampliada) o EDR (Detecció i Resposta a Amenaces) implica adaptar aquests aspectes específics a la naturalesa i les funcions d'aquestes tecnologies, la solució ha de tenir algunes funcions habituals:

1. **Classificació de la informació**: Classificar les dades segons el seu nivell de sensibilitat i importància per a la seguretat. Això pot ajudar a prioritzar les alertes i les respostes a amenaces segons el seu impacte potencial.
2. **Política de seguretat**: Establir polítiques de seguretat específiques per a la monitorització, la detecció i la resposta a amenaces mitjançant XDR/EDR. Això pot incloure la configuració de regles d'alerta, la definició de procediments de resposta a incidents i la gestió de l'accés a les funcionalitats de la solució a realitzar en un equip conjunt entre IL3-UB i l'empresa a partir dels procediments habituals i experiència de l'empresa adjudicatària
3. **Gestió de l'accés**: Controlar els privilegis d'accés al sistema XDR/EDR per garantir que només els usuaris autoritzats puguin visualitzar i prendre accions sobre les amenaces detectades.
4. **Gestió de les identitats**: Implementar autenticació de dos factors (2FA) o altres mecanismes forts d'autenticació per protegir l'accés a les consoles de gestió de XDR/EDR.
5. **Cifrat i protecció de dades**: Assegurar que les dades emmagatzemades i transmeses per la solució XDR/EDR estiguin adequadament xifrades per protegir-les de l'accés no autoritzat.
6. **Gestió de riscos**: Realitzar avaluacions periòdiques dels riscos de seguretat associats amb la solució XDR/EDR i prendre mesures per mitigar-los.
7. **Monitoratge i detecció d'incidències**: Configurar les polítiques d'alerta per detectar activitats sospitoses o potencialment malicioses a la infraestructura monitoritzada. A més, implementar funcionalitats de resposta automatitzada o guiada per accelerar la mitigació d'amenaces.
8. **Formació i conscienciació**: Proporcionar formació del funcionament de l'eina als equips encarregats de gestionar la solució XDR/EDR per garantir que estiguin capacitats per utilitzar adequadament les seves funcionalitats i interpretar les alertes generades. La formació es farà un cop implementada la solució aprofitant les incidències que es donin.
9. **Gestió de continuitat del negoci**: Desenvolupar plans de contingència i de recuperació per assegurar la disponibilitat contínua de la solució XDR/EDR en cas d'incidents o fallades del sistema.
10. **Auditoria i revisió**: Realitzar auditories semestrals de la configuració i l'ús de la solució XDR/EDR per garantir el compliment de les polítiques de seguretat establertes i identificar àrees d'ampliació o millora.

Característiques del servei de Centre d'Operacions de Seguretat (SOC)

Servei	Descripció
Monitoratge de seguretat	Supervisió constant dels sistemes, la xarxa i les aplicacions per detectar i respondre a amenaces en temps real
Anàlisi d'incidències	Investigació i anàlisi de les amenaces i incidents de seguretat per determinar l'abast i la gravetat.
Resposta a incidents	Accions immediates per respondre a amenaces actives i incidents de seguretat per minimitzar el seu impacte.

Gestió de vulnerabilitats	Identificació, avaluació i correcció de les vulnerabilitats en els sistemes i les aplicacions.
Anàlisi forense	Recopilació i anàlisi de proves digitals per comprendre l'origen i l'impacte dels incidents de seguretat.
Seguretat de la xarxa	Implementació de mesures per protegir la infraestructura de xarxa contra atacs com ara DDoS o intrusions.
Seguretat de l'endpoint	Protecció dels dispositius finals contra amenaces com malware i ransomware
Auditoria de seguretat	Revisió i avaluació de les polítiques de seguretat, els controls i les pràctiques per garantir el compliment dels estàndards.

Aquests serveis ajuden a protegir les organitzacions contra una àmplia gamma d'amenaces cibernètiques i a respondre eficaçment als incidents de seguretat quan es produeixen.

Certificacions del producte

GDRP	CC
ENS Alta	CSA Level 2
ISO27001	C5
SOC 2 Type II	FedRAMP

S'acreditaran amb una declaració responsable del licitador proposat adjudicatari.

2. Obligacions de l'adjudicatari.

L'adjudicatari haurà de comptar amb la capacitat de re vendre o contractar a nom de tercers (distribuïdor oficial) el producte sol·licitant. El producte ha de complir amb els requeriments de la taula de característiques tècniques. S'acreditaran amb una declaració responsable del licitador proposat adjudicatari.

L'adjudicatari haurà de tenir la solvència contrastada al quadrant Gartner EPP 2023 a la zona de Leaders. S'acreditaran amb una declaració responsable del licitador proposat adjudicatari.

Sr. Ruben Colon
Responsable que promou la necessitat
Reponsable Departament de TIC

Sr. Martin Madueño
Responsable del pressupost
Director Departament de TIC