IF

QUADRE DE CARACTERÍSTIQUES TÈCNIQUES

Llicències d'ús antivirus d'alta seguretat al núvol programari MDR amb Crowdstrike per 900 llocs de treball (Exp. 2022/6816) (Categoria 3 del SDA)

Codi expedient contracte derivat: 2024/7554
Persona responsable / Suplent: Marc Ferrés / Josep Bosch

1. OBJECTE DEL CONTRACTE. CODI CPV. DURADA.

Un programari de vigilància, detecció i resposta a amenaces de ciberseguretat en el lloc de treball en modalitat de programari al núvol administrat pel proveïdor.

Inclourà totes les tasques d'administració del programari i alerta de seguretat, d'instal·lació, càrrega de dades i formació.

Codi CPV: 48000000-8 Paquets de software i sistemes d'informació
Codi CPV: 48730000-4 Paquets de software de seguretat

Durada Inicial: 2 anys
Pròrroga: No

2. CARACTERÍSTIQUES TÈCNIQUES.

Cobertura per 900 llocs de treball dels següents productes de Crowdstrike instal·lats al núvol amb administració:

- Falcon Prevent
- Falcon Insight
- Falcon Threat Graph Standard on EU Cloud
- Falcon Overwatch
- Falcon Discover
- Falcon Firewall Management
- Falcon Device Control
- Falcon Spotlight

Caldrà disposar d'una estructura multi-tenant a crowdstrike:

- Existirà un tenant pare amb visibilitat i control sobre els subtenants que tindrà per sota. En el tenant pare hi haurà usuaris amb permisos per operar sobre els subtenants
- Existiran 3 subtenants:
  - Dipsalut
  - XALOC
  - Diputació de Girona (subtenant)
- Aquests tres subtenants tindran els seus propis usuaris que només podran veure i actuar sobre els equips qui hi sigui assignats. Aquests usuaris tindran permisos de lectura a la consola de HOSTS i vulnerabilitats i permís de gestió de la configuració de dispositius USB dels equips, per permetre o denegar dispositius.
- A cada subtenant se li assignaran un número determinat de llicències i caldrà controlar que no s'hi puguin afegir més dispositius que llicències tingui assignades.

L'administració dels productes subministrats serà prestada per personal especialista en seguretat i amb disponibilitat 24x7 i en idioma català i/o castellà. Les tasques d'administració inclouran:

- Monitorització d'alerta d'amenaça i resposta
  - Caldrà revisar i donar resposta de forma reactiva a les alertes d'amenaces provocades per la tecnología EDR de Falcon Insight desplegada a cada lloc de treball.
  - Per cada alerta es proporcionarà una visió processable de l'incident. Les investigacions també inclouran les conclusions de l'analista derivades de la investigació, així com recomanacions per mitigar, erradicar, recuperar i prevenir problemes semblants en el futur.
  - Inclourà el bloqueig automàtic de les amenaces potencials per el EDR, la selecció d'alertes i la confirmació d'amenaces, la investigació d'amenaces i la contenció a distància, i la notificació d'aquestes i del compromís quan sigui necessari.
  - Caldrà Investigar cada incident en el moment en què es produeixi i es donarà resposta a l'incident segons la classificació:

- Alertes critiques:
  - horari laboral: menys d'1 hora
  - Fora d'horari laboral: menys 1'5 hores
- Alertes high:
  - horari laboral: menys de 2 hores
  - Fora d'horari laboral: menys de 3 hores
- Alertes high (amb incident medium) o alertes medium:
  - horari laboral: menys de 4 hores
  - Fora d'horari laboral: NBD
- Resta d'alertes:
  - horari laboral: 8 hores
  - Fora d'horari laboral: NBD

- La monitorització i resposta donaran suport a diferents tipologies de 'endpoint':
  - Servidor windows 2012, 2016, 2019
  - Ordinador Personal amb Windows 10 i 11
  - Servidor Linux
  - Ordinador Personal Mac.

- Analisi de vulnerabilitats:
  - Mensualment es realitzarà una revisió de les vulnerabilitats detectades en el modul de spotlight emetent un informe amb la relació de les vulnerabilitats prioritaries per resoldre per part de Diputació.
  - En el moment en que es publiqui una vulnerabilitat considerada critica es farà una comunicació específica afegint la informació pertinent de context de la vulnerabilitat per tal que aquesta sigui prioritzada al màxim.
- Threat Hunting
  - Execució de projectes de threat hunting: selecció i investigació de les amenaces, execució inicial, anàlisi i informe i recomanacions
  - Anualment, es farà l'execució detallada de dos projectes de hunting, adequats a l'entorn de Diputació de Girona, i segons la identificació d'amenaces imminents a considerar. Els exercicis de hunting tindran el proposit de cercar indicadors que permetin detectar evidències de

la presència d'actors maliciosos més enllà de les capacitats de detecció de l'eina. Es tindran en compte els IOCs IOAs i TTPS que se seleccionen configuren i es llancen sobre el conjunt de la infraestructura. Un cop acabats els exercicis, es seleccionarà el conjunt d'indicadors més adequats i efectius i es programarà una cerca setmanal dels mateixos.

- Projecte 1:
  - Activitat (TTP/IOC/IOAs) relacionats amb mostres o tècniques de:
    - Entry points / Droppers
    - Stealers
- Projecte 2:
  - Activitat (TTP/IOC/IOAs) relacionats amb mostres o tècniques de:
    - RATs
    - Exfiltració

- Configuració setmanal de l'exercici de threat hunting amb la consola de crowdstrike mitjançant les "scheduled searches"
- Seguiment mensual dels resultats de threat hunting així com dels falsos positius identificats.

Per l'execució d'aquestes tasques d'administració caldrà que s'implementin les següents mesures de Seguretat:

- Compliment amb el GDPR.
- Connexions i emmagatzematge de dades xifrat.

Tasca d'instal·lació:

- Inicialment es definirà de manera conjunta amb els tècnics de Diputació de Girona:
  - El número d'agents EDR desplegats
  - El llistat detallat dels 'endpoints' basats en la seva tipologia
  - Número d'actius crítics i no crítics protegits.
  - Parametrització de la configuració
  - Detalls dels usuaris i Rols

  - Detalls de l'arquitectura
  - Detalls de les proves
- El desplegament de l'agent de telemetria de Crowdstrike a cada 'endpoint' serà responsablilitat dels tècnics de Diputació de Girona

Informes i reports:

- Per cada amenaça o alerta de seguretat: Cada vegada que es detecti i confirmi una amenaça de seguretat s'entregarà un informe que inclourà els següents punts:
  - Context de l'atac
  - Vectors d'entrada i anàlisi de la causa.
  - Tècniques utilitzades (referit a MITRE)
  - Vulnerabilitats explotades
  - Avaluació de la classificació de severitat i criticitat.
  - Grau de compromís
  - Detall de la intel·ligència operacional i estratègica si procedeix.
  - Cursos d'acció i recomanacions per aplicació de contramesures.
- Setmanalment s'elaborarà un informe que reculli com a mínim:
  - Monitorització d'alerta d'amenaces: numero d'alertes, número d'incidents mitigats, detall de les accions de mitigació.
  - Threat hunting: report de les tasques de threat hunting realitzades amb el seu detall: adversaris, malware, IoC/IoAs trobats, recomanacions.
- Mensualment s'elaborarà un resum executiu i presentació de les dades analitzades i recollides referents a context i tendències de l'estat de seguretat dels 'endpoints':
  - Numero de sensors online per tipus
  - Numero d'alertes de seguretat
  - Hosts amb funcionalitat reduïda
  - Hosts amb versions desactualitzades
  - Hosts amb polítiques desactualitzades
  - Hosts offline

3 IMPORT I PRESSUPOST BASE DE LA LICITACIÓ.

Justificació del preu:

S'ha realitzat una consulta amb diferents empreses del sector, tot valorant diverses possibilitats de llicenciament.

- Amb el següent pressupost de licitació:

  Import sense IVA: 142.200,00€

  Import IVA (21%): 29.862,00 €

  Pressupost de licitació: 172.062,00 €

- Justificar la no divisió Justificar la no divisió en lots:

  Atès que es demana el subministrament de productes d'un mateix fabricant

4 APLICACIÓ PRESSUPOSTÀRIA (Sense tenir en compte les pròrrogues):.

ANY	CONCEPTE	APLICACIÓ PRESSUPOSTÀRIA	IMPORT
2024	Antivirus al núvol d'alta seguretat	310/92010/2060100	86.031,00 €
2025	Antivirus al núvol d'alta seguretat	310/92010/2060100	86.031.00 €

5 VALOR ESTIMAT DEL CONTRACTE:

142.200,00 € (IVA no inclòs)

Càlcul del valor estimat:

Import del contracte (Sense IVA)	Pròrroga	Modificacions	Valor Estimat del contracte
142.200,00 euros	0 euros	0 euros	142.200,00 euros

6 GARANTIA

Sí procedeix la constitució de garantia definitiva per ser el valor estimat del

contracte superior a 60.000 €, d'acord amb l'establert a l'article 159.6 LCSP

7 TERMINI DE GARANTIES:

- Sí, 2 mesos.

8 OBLIGACIONS DE L'ADJUDICATARI.

El producte ha de complir amb els requeriments de la taula de característiques tècniques.

9 LLOC I FORMA DE PAGAMENT.

Caldrà que tot la instal·lació, formació i configuració hagi estat realitzada.
La primera factura es presentarà a l'inici del contracte i la següent a l'inici del segon any de contracte.

10 CRITERIS DE VALORACIÓ.

Preu: s'atorgarà la màxima puntuació a les proposicions que ofereixin el preu més baix, atorgant-se punts a la resta de forma proporcional. Fins a 100 punts.

Per calcular la puntuació de preu s'utilitzarà la formula lineal competitiva:

Fórmula lineal competitiva

$$P_i = P\left(1 - \left(\frac{O_i - O_m}{IL}\right) \cdot \left(\frac{IL - \frac{1}{2}O_m}{IL - O_m}\right)\right)$$

P_i: punts de l'oferta *i*
P: punts del criteri preu
O_i: preu de l'oferta *i*
O_m: preu de la millor oferta
IL: import de licitació