Ajuntament de Cubelles

Núm. d'expedient 1428/2024 -12363
Departament CONTRACTACIÓ

PLEC DE PRESCRIPCIONS TÈCNIQUES QUE HA DE REGIR L'ADJUDICACIÓ PER PROCEDIMENT OBERT SIMPLIFICAT SUMARI, TRAMITACIÓ ORDINÀRIA, DEL CONTRACTE MIXT D'UN PARTENER CERTIFICAT DE WATCHGUARD I 200 LLICÈNCIES DE PANDA SYSTEMS MANAGEMENT I EL SEU MANTENIMENT

Capítol I: Disposicions Generals

Clàusula 1. Objecte del contracte

L'objecte de la licitació és la contractació d'un *partner* certificat *Gold* de *Watchguard* per a la provisió del servei *Watchguard EPDR (protecció d'endpoints i detecció de resposta)* i la gestió de 200 llicències de *Panda Systems Management*.

El contracte contempla, també, el servei de suport tècnic i manteniment.

Codificació de l'objecte CPV:

- 48760000 - Paquets de software de protecció antivirus.
- 48761000 - Paquets de software antivirus.
- 72220000 - Serveis de consultoria en sistemes i consultoria tècnica.

Capítol II: Prescripcions Tècniques

Clàusula 2. Característiques de l'objecte del contracte

El proveïdor haurà d'assegurar el subministrament i el desplegament del programari, a més d'oferir suport tècnic i manteniment durant tota la durada del contracte.

Pel que fa a Wachtguard EPDR, les característiques mínimes són:

a) Tecnologies antivirus de darrera generació:
   a. Firewall personal o administrat (IDS).
   b. Control de dispositius.
   c. Intel·ligència col·lectiva i heurística prèvia a l'execució.
   d. Antimalware permanent multivectorial i anàlisi a comanda.
   e. Filtratge d'URL i navegació web.
   f. Filtratge d'URL, navegació web i protecció contra suplantació d'identitat.
   g. Protecció contra alteracions.
   h. Correcció automàtica i capacitat de reversió.
   i. Avaluació de vulnerabilitat.

b) Tecnologies de Seguretat Avançades
   a. Supervisió contínua d'endpoints amb EDR.
   b. Aprenentatge basat en el núvol que classifica el 100% dels processos (APT, ransomware, rootkits, etc.).

c. *Sandboxing* en entorns reals.
d. Protecció *antiexploit*.
e. Protecció contra atacs de xarxa: eviteu que els atacs explotin vulnerabilitats en serveis exposats a Internet.
f. *Threat Hunting*: anàlisi del comportament i detecció de Indicadors d'Atacs (IoA) per detectar els atacs del tipus Living-off-the-Land (LotL).
g. Indicadors d'atacs associats al marc de MITRE ATT&CK.
h. Detecció i prevenció d'atacs de RDP.
i. Capacitats de contenció i correcció, com ara l'aïllament d'ordinadors i el bloqueig de programes per *hash* o nom del programa.

Pel que fa al Panda Systems Management, les característiques mínimes són:

a) Solució basada íntegrament al núvol
b) Solució basada íntegrament al núvol
   - No necessiti infraestructura addicional al client.
   - Permeti gestionar tots els dispositius en qualsevol moment i des de qualsevol lloc.
c) Gestió mitjançant agent per a dispositius compatible amb Windows, Linux, macOS, Android i iOS.
d) Gestió sense agent
   - Gestió simple amb ajuda del protocol SNMP i plantilles de configuració, per a aquells dispositius on no sigui possible la instal·lació de l'agent PCSM (impressores, routers, switches, scanners, centraletes, etc.).
   - Gestió de servidors VMware ESXi (VMware vSphere Hypervisor 4.1, 5.0, 5.1, 5.5, 6.0 i 6.5), Gestió de servidors Microsoft Hyper-V al Windows Server.
e) Detecció automàtica de dispositius connectats a la mateixa xarxa i iniciar la instal·lació desatesa.
f) Auditories programades i extraordinàries.
g) Gestió de llicències de programari.
h) Visualització de la seguretat de l'ordinador.
i) Alertes i monitorització
   - Control de l'ús de CPU, memòria i disc, serveis, cues, gràfics de rendiment, alertes al panell, etc.
   - Qualsevol dispositiu i en temps real.
   - Monitors recomanats de ràpida configuració.
j) Monitorització de les aplicacions més comunes (Exchange, SQL i IIS, serveis de Backup, dispositius de xarxa, etc.,) de forma gratuïta.
k) Creació de scripts i tasques ràpides de forma programada o com a resposta automàtica a una alerta.
l) Automatització del desplegament d'actualitzacions i pegats per als sistemes operatius Windows instal·lats.
m) Desplegament centralitzada de programari en equips Windows, Linux, macOS i iOS de la xarxa.
n) Gestió del programari en els dispositius administrats i actualització a les darreres versions dels programes publicats pels proveïdors del programari.
o) Polítiques
   - Possibilitat d'establir configuracions comunes als dispositius gestionats.

- Disposar de polítiques recomanades per accelerar la gestió de l'entorn IT.

p) Accés remot
   - Gestor de tasques, transferència de fitxers, editor del registre, línia d'ordres, visualitzador d'esdeveniments del sistema, etc.
   - Ha de suportar l'intèrpret d'ordres PowerShell 2.0

q) Control remot
   - Accés compartit a l'escriptori de l'usuari o control total mitjançant l'agent PCSM o des de la consola web d'administració.
   - Compatible amb tallafocs i Network Address Translation (NAT).

r) Xat
   - Ha de permetre convidar l'usuari del dispositiu i altres tècnics a una sessió de xat per facilitar la comunicació i la col·laboració a l'hora de localitzar i solucionar les incidències.

s) Gestió remota de dispositius de xarxa
   - Accés a les eines d'administració incorporades als dispositius de xarxa, impressores i altres equips que no admeten la instal·lació de l'agent PCSM.
   - L'administrador ha de poder gestionar tots els dispositius de la xarxa des del seu lloc.

t) Comunicació segura
   - Totes les comunicacions entre els agents i el Servidor Systems Management estan xifrades (SSL).

u) Control d'accés al servei
   - Màxima seguretat a l'inici de sessió a la Consola d'administració, mitjançant l'autenticació en dues fases i altres recursos que limiten l'accés dels dispositius al servidor Systems Management.

v) Informes
   - Sistema d'informes flexible en format PDF i CSV.
   - Suport de diversos idiomes i abast configurable fins a abastar tot el parc informàtic mitjançant l'agregació d'informes.

w) Entorn col·laboratiu
   - Sistema de tiquets que gestiona l'assignació, estat i documentació de les incidències.
   - Ha de facilitar la creació d'"històrics d'"intervenció amb notes associades als dispositius i millora la comunicació en viu amb l'"usuari mitjançant el servei de missatgeria.

x) Registre d'activitat
   - Ha de permetre emmagatzemar tota l'activitat dels administradors a la consola.

y) ComStore
   - Ha de permetre ampliar les capacitats de la plataforma, en seleccionar i descarregar els components necessaris a cada moment gratuïtament.

Diligència per fer constar que aquest Plec de Prescripcions Tècniques que ha de regir l'adjudicació del contracte mixt d'un partner certificat de Watchguard i 200 llicències de Panda Systems Management i el seu manteniment ha estat aprovat mitjançant Decret d'Alcaldia núm. 2025/78, de data 4 de febrer de 2025.

Cubelles, a data de la signatura electrònica

La Secretària General