Ajuntament de
Sant Vicenç de Castellet

PLEC DE CLAUSULES TÈCNIQUES PEL CONTRACTE D'ADQUISICIÓ DE LLICÈNCIES PANDA I DE CARACTERÍSTIQUES D'ADMINISTRACIÓ CENTRALITZADA DE SOFTWARE I CONNEXIÓ REMOTA ALS DISPOSITIUS DEL PARC INFORMÀTIC DE L'AJUNTAMENT DE SANT VICENÇ DE CASTELLET.

1.- OBJECTE DEL CONTRACTE

El objecte del present plec es la contractació de llicències dels antivirus Panda Adaptative 360 per l'Ajuntament de Sant Vicenç de Castellet.

Panda adaptive defense 360 és una solució de seguretat completa per als llocs de treball, portàtils i servidors que a més de protegir contra amenaces conegudes, avançades i zero-day, ransomware i atacs de seguretat fileless (en memòria) i malwareless, inclou firewall personal, ips/ids, antispam, antispam en correu, filtratge i categorització en navegació web i control de dispositius, entre altres tècniques de seguretat i control de productivitat. les seves capacitats de protecció avançada cobreixen totes fases de la seguretat adaptativa: prevenció, detecció, resposta i remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables als endpoints i els serveis de threat hunting i anàlisi forense, que permet un reforçament de la seguretat corporativa contínua.

Ha de permetre la configuració agrupada per perfils, tant per servidors, com per clients, com per smartphones.

El sistema de llicencies d'aquets productes es realitza per el numero d'equips a proteger, per un temps determinat. En el nostre cas serien 85 ordinadors, entre els quals hi han 5 servidors, i 80 equips client, 50 smartphones , a un any.

També inclourem les característiques de administració de sofware, i connexió remota per cada un d'ells.

2.- CLAUSULES TÈCNIQUES ESPECÍFIQUES

2.1- Equips a protegir:

La llicencia d'us del producte es composa de un programa informàtic y una sèrie de serveis associats. Els serveis associats es presenten durant tota la vigència del contracte sense cap increment de cost. El programa informàtic en forma de agent de software, s'instal·la en cada un dels equips a protegir, com bé diem 85 ordinadors entre els quals hi ha 5 servidors i 50 smartphones, indiferentment si és Android versió 9 en endavant, o Iphone versió IOS 15 en endavant. De totes maneres, el sistema ha de ser flexible, ha de permetre re-assignar la mateixa llicencia a diferents dispositius si es requereix, independentment del equip o sistema.

Els sistema de administració, que permet la configuració, a traves de grups segons tipus de dispositius, o sistemes operatius, de les polítiques dels antivirus, (Firewall, configuració avançada, llistes ACL... etc).

Plaça de l'Ajuntament, 10 - 08295 Sant Vicenç de Castellet. Tel. 936930611 - Fax 936930610 - www.svc.cat - svcastellet@svc.cat

Ajuntament de
Sant Vicenç de Castellet

Plaça de l'Ajuntament, 10 - 08295 Sant Vicenç de Castellet. Tel. 936930611 - Fax 936930610 - www.svc.cat - svcastellet@svc.cat

2.2- Ubicació de la plataforma:

Es precisa la solució basa al Clout.

La ubicació de la plataforma ha de estar allotjada dintre de **l'Unió Eurpea.**

La plataforma de gestió ha de cobrir els principals nivells de certificació com son:
ISO 27001 y es valorarà positivament qualsevol altre certificació que disposi la infraestructura.

Es donarà a traves d'un accés a una interfície web segura, que permeti la adició com la segregació de les llicencies als equips, la monitorització en temps real, la instal·lació o la desinstal·lació de software, el control del inventariat del parc informàtic i l'accés remot tant per consola, usuari d'assistència a traves de streaming, i amb credencials d'administradors dels domini sobre els clients destí.

2.3- Components del servei.

- Inrfraestrcutura Cloud.
- Programa informatic, agent a desplegar en els equips.
- Consola de web Management.

2.4- Protecció

2.4.1- Plataforma de protecció:

Es requereix una seguretat completa per als llocs de treball, portàtils i servidors que a més de protegir contra amenaces conegudes, avançades i zero-day, ransomware i atacs de seguretat fileless (en memòria) i malwareless, inclou firewall personal, ips/ids, antispam, antispam en correu, filtratge i categorització en navegació web i control de dispositius, entre altres tècniques de seguretat i control de productivitat. les seves capacitats de protecció avançada cobreixen totes fases de la seguretat adaptativa: prevenció, detecció, resposta i remediació, gràcies als serveis gestionats: servei de classificació del 100% dels programes, processos i executables als endpoints i els serveis de threat hunting i anàlisi forense, que permet un reforçament de la seguretat corporativa contínua.

Ha de permetre la configuració agrupada per perfils, tant per servidors, com per clients, com per smartphones.

Ha de permetre el aïllament forçat dels dispositius, així com també ha de permetre la eliminació segura de les dades en remot, per cassos com robatoris o pèrdues accidentals dels mateixos.

2.4.2- Detecció i Resposta:

Es requereix una solució de tipus EDR (Endpoint detection and response) per protegir de les següents amenaces:

Malware avanzat.

PUP (potential unwanted programs)

Ajuntament de
Sant Vicenç de Castellet

Amenazes zero-day

Trollans de nova generació indetectables per els antivirus.

Aquesta solució haurà d'evitar al màxim possible les infeccions de forma proactiva, mai reactiva. La solució haurà d'aportar contramesures diferents a les següents:

Signatures locals que requereixin constants actualitzacions.

Monitoratge heurístic que emprin us de la CPU i puguin produir falsos positius.

Sistemes de llistes blanques.

Sistemes de sand-boxing.

El sistema ha de recollir el 100% dels registres de processos executats per les maquines, generant classificació de software com malware o goodware, i actuant en conseqüència, bloquejant el classificat com a malware.

Ha de incloure un sistema anti-exploit, que detecti bloqui el us d'exploits coneguts i desconeguts.

2.4.3- Protecció de llocs de treball, servidors i dispositius mòbils.

Ha de protegir equips i servidors Windows, Linux, Mac OS X, Android versió 9 en endavant, o iphone versió IOS 15 en endavant de tot tipus de programes maliciosos, incloent atacs dirigits i APTs (Advanced Persistent Threats).

2.4.4- Altres Proteccions

Plataforma de gestió d'informació auditada

El sistema ha de generar informació forense relacionada amb cada equip de tal forma que pugui ser explotada posteriorment. El sistema haurà d'incloure informe per amenaça detectada així com informes d'estat de les proteccions, de les deteccions de malware. Els informes s'han de poder obtenir de manera immediata.

Servei d'alerta d'amenaces (Threat Hunting)

Es requereix un servei que alerti i prengui les mesures correctives adequades quan sigui detectat una activitat anòmala en els equips.

Servei Zerotrust Application

Servei que classifica les accions com malware o com a de confiança, abans de deixar que només les accions de confiança s'executin en cada endpoint. Permet la supervisió dels endpoint, la detecció i la classificació de tota activitat.

2.5- NETEJA DELS SISTEMES

Es requereix un sistema de neteja dels equips de tal forma que es pugui realitzar a demanda una neteja de rastres d'amenaces o programes no desitjats que l'antivirus no hagi pogut eliminar.

3.- CERTIFICACIONS I ESQUEMA NACIONAL DE SEGURETAT

Plaça de l'Ajuntament, 10 - 08295 Sant Vicenç de Castellet. Tel. 936930611 - Fax 936930610 - www.svc.cat - svcastellet@svc.cat

Ajuntament de
Sant Vicenç de Castellet

La solució ha d'estar inclosa en el "Catàleg de Productes de Seguretat de les Tecnologies de la Informació i la Comunicació." (CPSTIC) Publicat pel CCN (Centre Criptogràfic Nacional), dins de la família de protecció del Lloc de treball com a QUALIFICAT.

La solució ha de tenir la certificació de garantia EAL2+ en avaluació de l'estàndard Common Criteria (https://www.commoncriteriaportal.org/)

Tecnologia Cloud Pública, és obligatòria que tingui la certificació de conformitat enfront del ENS, de categoria alta.

4.- CARACTERÍSTIQUES SUPORT TÈCNIC

S'establirà el manteniment i assistència tècnica que permeti assegurar el correcte funcionament. Mitjançant:

- Servei de suport ofert pel fabricant per telèfon en castellà amb telèfon d'accés prioritari.
- Service Packs i hotfixes: Accés a les millores tècniques del producte durant el temps d'activació del servei
- Web de suport: Accés a fòrums, blogs, informació sobre últimes amenaces, enciclopèdia de virus, etc
- Suport tècnic via email 24x7x365, per tècnics certificats en la solució implementada
- Accés il·limitat al Helpdesk: sense límit d'incidències

Plaça de l'Ajuntament, 10 - 08295 Sant Vicenç de Castellet. Tel. 936930611 - Fax 936930610 - www.svc.cat - svcastellet@svc.cat