Ajuntament de
Calonge i Sant Antoni

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

SECRETARIA GENERAL
Expedient: 2023/9448
Assumpte: CONTRACTE DE SUBMINISTRAMENT D'UNA SOLUCIÓ DE PROTECCIÓ AVANÇADA AMB XDR (EXTENDED ENDPOINT DETECTION & RESPONSE"

PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DEL SUBMINISTRAMENT D'UNA SOLUCIÓ DE PROTECCIÓ AVANÇADA AMB XDR (EXTENDED ENDPOINT DETECTION & RESPONSE).

1. Objecte i necessitat del contracte

L'objecte és la contractació del subministrament de les llicències, la subscripció del suport i la monitorització dels sistemes informàtics i de comunicacions amb una solució integral de protecció avançada dels sistemes amb capacitats de EPP, EDR i XDR. Aquest sistema ha de comptar amb una sèrie de funcionalitats indispensables que permetin reforçar la seguretat dels actius TIC corporatius davant ciberatacs.

Actualment l'Ajuntament de Calonge i Sant Antoni compta amb una solució d'antivirus EPP (Endpoint Protection Platform) dissenyada per a detectar i bloquejar amenaces a nivell de dispositiu, incloent diferents funcions com antivirus, antimalware, IPS o DLP. Aquestes eines són de tipus preventiu, i utilitzen sistemes de patrons i signatures per identificar amenaces conegudes.
Els sistemes EDR (Endpoint Detection and Response) i les seves evolucions, són eines que proporcionen monitorització i anàlisi continua de l'endpoint i la xarxa (esdeveniments dels usuaris, arxius, processos, registres, memòria i xarxa), per identificar, detectar i prevenir amenaces avançades (APT) incloent la presa de decisions (resposta) immediates i automatitzades. Proporcionen per tant mecanismes per a la cerca i detecció d'amenaces desconegudes, més enllà dels virus informàtics, detectant atacs informàtics en temps real, i permetent prendre mesures immediates, si cal.

La solució ha de permetre la detecció i resposta ampliades o XDR (tecnologia de seguretat multicapa que protegeix la infraestructura de TI). Per això, ha de recopilar i correlacionar les dades de múltiples capes de seguretat, inclosos els endpoints, les aplicacions, el correu electrònic, els núvols i les xarxes, per proporcionar més visibilitat de l'entorn tecnològic d'una organització. Això permetrà que els equips de seguretat detectin, investiguin i responguin a les ciberamenaces amb rapidesa i efectivitat.

Per tant, la solució ha de permetre la protecció d'equips d'usuaris, servidors, xarxa, etc.. i aglutinar les dades de totes aquestes fonts en un sol punt de gestió per tal d'obtenir una visió general de què està passant a cada moment a nivell de seguretat a través de "dashboards" i sistemes d'alerta. La gestió corporativa de l'eina ha de facilitar l'anàlisi, detecció, neteja i investigació, per tal de protegir els entorns de treball i donar una resposta eficaç a les amenaces.

La necessitat de reforçar la ciberseguretat corporativa, afegida a les tasques que es realitzen en el marc del Sistema de Gestió de Seguretat de la Informació, fa necessari disposar d'una solució amb funcionalitats avançades que permeti la detecció, protecció i gestió proactiva en aquesta matèria.

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

2. Especificacions tècniques mínimes

En les prescripcions tècniques que segueixen s'especifiquen els requisits mínims obligatoris de les llicències i serveis requerits. Les propostes que ofereixin característiques inferiors no seran preses en consideració.

La Implantació de la solució serà “100 % claus en mà”, inclòs l’abast de totes les accions, subministraments i prestacions necessàries per a la posada en funcionament conforme a les especificacions tècniques que es recullen en aquest plec. Cada licitador pot plantejar a l'Ajuntament la solució tècnica que consideri més apropiada, acompanyant les prestacions que proporcionaria i els nivells de servei que garantiria.

Els licitadors hauran de ser partners autoritzats del fabricant dels productes involucrats en la solució i comptar amb el màxim nivell de certificació.

2.1 Funcionalitats principals

Les funcionalitats mínimes principals que han de complir la solució son les següents:

- Vista d'alertes 360º.
- Protecció dels punts de connexió.
- Antivirus NGAV: Analitzar els fitxers en repòs i els fitxers no executables per protegir-los contra codi maliciós conegut.
  - Protecció contra codi maliciós mitjançant anàlisi estàtica basada en intel·ligència artificial.
  - Protecció contra l’explotació basada en el comportament.
  - Protecció de macros i scripts contra els atacs sense fitxers basada en el comportament.
  - Identificar i prevenir l'execució de codi maliciós amb firmes conegudes.
- Control de dispositius: Detectar i bloquejar els dispositius d'emmagatzematge externs que s'insereixen al punt de connexió (per exemple, un dispositiu USB o una targeta SD).
- Protecció de recursos crítics: Protegir usuaris, xarxes, endpoints i servidors (físics i virtuals), arxius, processos, components al núvol i configuracions del client, alimentant les dades a un punt centralitzat.
- Detecció estesa d'amenaces: Detecció i resposta per prevenir, detectar i respondre les amenaces a nivell més avançat tant conegudes com desconegudes a tot l'entorn.
  - SSDEEP Scan.
  - Patrons de memòria.
  - Tecnologia de detecció avançada (ADT).
  - Controlador en mode kernel.
- Regles d’anàlisi del comportament de l’usuari (UBA/UEBA): Aprendre el comportament d’usuaris i entitats per detectar activitats inusuals i alertar sobre aquests comportaments sospitosos.
  - Detecció i resposta de xarxa (NDR): Analitzar l'activitat per detectar atacs a la xarxa, incloent-hi.
  - Robatori de credencials basat en la xarxa (suplantació d'ARP, crides DNS).
  - Moviment lateral a la xarxa.
  - Reconeixement basat a la xarxa (atacs d'escaneig).
  - Filtració de dades basada en la xarxa (tunelització a través de diversos protocols).
- Entorn de proves: Enviar fitxers per a la seva inspecció a través de l'entorn de proves Smart Simulation Execution (SSE) Sandbox.
- Gestió de la vulnerabilitat.

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

- Inventari d'actius.
- Protecció de memòria en temps real: Detectar i bloquejar les cadenes de memòria que estan associades amb el ransomware.
  - Filtratge d'arxius en temps real: Detectar i evitar que les aplicacions no aprovades escriguin en diversos tipus d'arxius.
  - Filtratge de components crítics: Protegir la volta de contrasenyes del sistema operatiu perquè el ransomware no pugui recopilar credencials / propagar-se per tota la xarxa.
- 24x7 Threat Hunting: Disponibilitat 24/7, Exclusions, llistes blanques, Anàlisi sota demanda, Instruccions de correcció, Monitorització d'alertes, Caça d'amenaces i Investigacions d'atacs.
- Security Operations Center (SOC): Centre d'Operacions de Seguretat, per prevenir, monitoritzar i controlar la seguretat a la xarxa de l'organització 24x7. El SOC ha de tenir un servei de control d'alertes, resposta remota a incidents (IR) i informes sobre atac.
- La solució ha de permetre: la definició i la creació de rols d'administració amb permisos personalitzats en funció dels tipus d'accions disponibles que es poden assignar a usuaris i grups.
- La solució ha de coexistir:
  - Amb tot el programari comercial instal·lat als endpoints i servidors.
  - Entre Endpoints, fitxers, processos, activitat de l'usuari i trànsit de xarxa de forma totalment autosuficient, eliminant la necessitat de configuració manual de regles o polítiques o la dependència de dispositius addicionals.

2.2 Consola d'administració

La consola d'administració haurà d'estar basada en cloud i serà operada pel fabricant de la solució en un model al núvol, els servidors han d'estar ubicats a la Unió Europea. Es requereix alta disponibilitat garantida i capacitats de creixement i escalabilitat.

La solució ha de complir amb les següents funcionalitats:

- Serà accessible mitjançant diferents navegadors amb doble factor de autenticació i amb distinció de diferents rols segons el tipus d'usuari validat.
- Dashboard que destaqui les alarmes i deteccions actives.
- Configuració d'alertes, avisos i notificacions, possibilitat de configurar els avisos via correu electrònic dels incidents detectats.
- Integració amb Directori Actiu.
- Actualitzacions automàtiques de la plataforma i dels motors de seguretat.
- Generació d'informes pre definits i personalitzables sobre les deteccions de codi maliciós (malware) i l'estat dels Endpoints. (resums d'equips amb deteccions, aplicacions bloquejades, gestió de perifèrics, equips sense agent, etc.).
- Definició d'excepcions que permeti desbloquejar processos catalogats com amenaces. A més, el sistema permetrà bloquejar programes o restringir els seus permisos quan no estiguin inclosos en llistes blanques o es trobin en llistes negres.
- Gestió d'events, tant de seguretat com de configuració. Guardats en consola cloud, com a mínim 90 dies.
- Ha de permetre l'anàlisi de Causa Arrel per identificar l'origen de l'incident de seguretat i identificar els elements del sistema amb què es relaciona un procés sota estudi.
- Ha de permetre l'aïllament d'equips des de la consola
- Categorització dels esdeveniments en base a la seva importància i la possibilitat de fer un filtratge d'esdeveniments.

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

- Capacitat d'obtenir informació detallada per realitzar una anàlisi forense a cas d'infecció. Aquesta informació s'ha de poder descarregar a fitxer per posterior anàlisi.
- Capacitat de configuració de control d'aplicacions mitjançant regles pre definides o personalitzables.
- Capacitat de fer una anàlisi avançada d'amenaces executant codi sospitós en un entorn segur i controlat (sandbox).
- Funcionalitat de virtual patching, que permeti detecció d'equips que continguin software amb vulnerabilitats conegudes, i la seva actualització de forma automàtica i centralitzada.
- Han de quedar registrats tots els events de canvis de configuració.
- Possibilitat d'extreure els logs en local cap a un syslog o SIEM.
- Accés a una plataforma cloud estil "Data lake", amb informació històrica dels equips gestionats de mínim 90 dies enrere, on poder realitzar consultes. Cal que disposi de consultes preexistents i també que es puguin fer a mida. També ha de permetre programar les consultes.
- Enviament al fabricant de mostres per ser analitzades.

2.3 Prevenció i detecció

La solució de protecció de l'endpoint haurà d'incloure i combinar múltiples tecnologies natives de detecció necessàries per identificar i prevenir les amenaces a tot l'entorn, amb capacitats EPP, EDR i XDR regles de detecció de xarxa, regles d'anàlisi de comportament de l'usuari (UBA/UEBA), intel·ligència de detecció d'amenaces, entorn de prova i tecnologies opcionalment d'engany i gestió de la postura de seguretat al núvol i en aplicacions SaaS.

El sistema de protecció ha de ser capaç de protegir qualsevol endpoint amb sistemes operatius Windows, MacOS, Linux i sistema Android, macOs i IOS per a mòbils.

La solució ha d'identificar:

- Arxius maliciosos i evitar-ne l'execució, inclosos virus, troians, ransomware, spyware, cryptominers i qualsevol altre tipus de malware, utilitzant com a mínim les tecnologies següents:
  - ➢ Protecció per signatures.
  - ➢ Anàlisi estàtica de Machine Learning.
  - ➢ Anàlisi dinàmica amb Sandbox a Temps Real.
  - ➢ Intel·ligència d'Amenaces vinculat a VT.
  - ➢ Intel·ligència d'Amenaces externa a VT.
  - ➢ Integració AMSI.
- Comportament maliciós de fitxers executats, processos en execució, modificacions de registre, accés a la memòria i finalitzar-los en temps d'execució, o generar una alerta (exploits, fileless, macros, Powershell, WMI, etc.), utilitzant com a mínim les següents tecnologies:
  - ➢ Supervisió de l'accés a la memòria.
  - ➢ Procés d'anàlisi de comportament (heurística).
  - ➢ Alta similitud (fuzzy hashing).
  - ➢ Intel·ligència d'Amenaces.
- Comportament maliciós del compte d'usuari, indicatiu de compromís previ, utilitzant com a mínim les tecnologies següents:
  - ➢ Configurar polítiques d'activitat d'usuari (infracció de política).
  - ➢ Línia base de perfil de compte d'usuari (detecció d'anomalies).

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

- Interacció maliciosa amb arxius de dades, utilitzant la tecnologia de cimbells, generant fitxers "Decoy".
- Filtració de dades a través de protocols legítims (túnels DNS, túnels ICMP), utilitzant com a mínim les tecnologies següents:
  - ➢ Seguiment de Trànsit de Xarxa (NTA).
  - ➢ Seguiment d'accés a fitxers (File Access Monitoring).
- Atacs d'escalat de privilegis, utilitzant com a mínim la tecnologia de seguiment de processos.
- Atacs de reconeixement (escaneig), utilitzant com a mínim la tecnologia de Seguiment de Trànsit de Xarxa (NTA).
- Intents de robatori de credencials des de la memòria (bolcat de credencials, força bruta) o trànsit de xarxa (suplantació d'identitat ARP, responedor DNS), utilitzant com a mínim les tecnologies següents:
  - ➢ Seguiment de memòria.
  - ➢ Seguiment de comptes d'usuari.
  - ➢ Seguiment de Trànsit, Comportament i Resposta de Xarxa (NDR).
  - ➢ Tecnologia de cimbells, generant usuaris "Decoy".
- Ús d'eines d'atac comunes (Metasploit, Empire, Cobalt, etc.), utilitzant com a mínim la tecnologia de seguiment de processos.
- Moviments laterals (SMB relay, pass the hash, etc.), utilitzant com a mínim les tecnologies següents:
  - ➢ Seguiment de Trànsit de Xarxa (NTA).
  - ➢ Tecnologia de cimbells, generant usuaris o connexions de xarxa o equips "Decoy".
- La solució ha de tenir un mecanisme intern de protecció contra l'accés i la manipulació d'usuaris no autoritzats. Alerta i bloqueig davant de qualsevol intent de manipulació o desactivació.
- La solució ha de disposar d'una funcionalitat de creació de perfils de control de dispositius d'emmagatzematge que permetrà detectar i bloquejar els dispositius d'emmagatzematge externs que s'insereixen al punt de connexió (per exemple, un dispositiu USB o una targeta SD).
- Caldrà que inclogui la capacitat de detectar i bloquejar comunicacions a dominis maliciosos, fent servir com a mínim la tecnologia d'Anàlisi de Dominis.
- La solució ha d'incloure la capacitat de crear cimbells (Decoys, també coneguts com a Honeypots) sense necessitat d'instal·lar cap servidor On-Prem i gestionats per l'agent únic de tota la solució. Els cimbells hauran de ser com a mínim de la tipologia de fitxers, hosts i usuaris.

<u>La solució ha de permetre:</u>

- Protecció en temps real.
- Protecció avançada davant de diferents tipus d'amenaces (malware, ransomware, exploits, phishing, APT, fileless, etc.).
- Protecció avançada davant de la navegació, descàrrega web i phising. Control de navegació web.
- Protecció avançada a nivell de xarxa.
- Monitorització d'integritat d'arxius.
- L'agent i les proteccions es podran actualitzar automàticament des de qualsevol xarxa pública o privada.
- L'accés a internet des de l'Endpoint als serveis oferts pel licitant s'ha de cenyir al protocol https pels ports imprescindibles. Pel que fa a la Urls necessàries per al correcte funcionament de

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

l'Endpoint han de ser exclusivament a dominis del licitant i accés als seus proveïdors de certificats i/o serveis.

- L'entorn ha de tenir un sistema de desplegament de la solució automatitzada i ha de permetre la creació de paquets d'instal·lació per a la seva distribució, tant de l'agent com de la protecció.
- Capacitats d'anàlisi de nous processos amb un baix índex de falsos positius i utilització d'intel·ligència col·lectiva.
- Protecció avançada a nivell de xarxa mitjançant firewall. Aquest firewall tindrà regles pre definides i regles personalitzables, a més d'opcions avançades com a prevenció de DoS, port scan i IP spoofing entre d'altres.
- Es podrà realitzar la instal·lació/desinstal·lació de l'agent mitjançant Scripts o ordres de l'agent. Possibilitat de suspendre temporalment la protecció de l'Endpoint per usuari amb drets d'administració.
- Es podrà realitzar la instal·lació/desinstal·lació de l'agent mitjançant Scripts o ordres de l'agent. Possibilitat de suspendre temporalment la protecció de l'Endpoint per usuari amb drets d'administració.
- Detecció d'intents d'intrusió, moviments laterals, elevació de privilegis, etc.

2.4 Resposta, investigació i remeiació

La solució ha de proporcionar:

- Aïllament, mitigació de presència i activitat maliciosa, localment a l'endpoint amb les següents capacitats i/o funcionalitats mínimes:
  - ➢ Executar una ordre coordinada (com la interfície CMD).
  - ➢ Obrir un Shell remot.
  - ➢ Executar scripts o fitxers des d'una ubicació de xarxa o mapejar una unitat.
  - ➢ Tancar un endpoint i/o un servidor.
  - ➢ Aïllament d'un endpoint/servidor de la xarxa.
  - ➢ Eliminació d'un fitxer (inclosos els fitxers d'execució actius).
  - ➢ Posar un fitxer en quarantena (inclosos els fitxers d'execució actius).
  - ➢ Matar un procés.
  - ➢ Eliminació d'un servei/tasca programada.
  - ➢ Bloqueig d'un compte d'usuari local o d'un usuari de domini.
  - ➢ Reset de la contrasenya d'usuari.
  - ➢ Bloqueig de telecomunicacions en funció de la destinació (adreça de domini o adreça IP).
  - ➢ Desconnexió de targetes de xarxa.
  - ➢ Canvi de direcció IP.
  - ➢ Capacitat d'editar un fitxer HOST.
  - ➢ Funcionament renovat d'un endpoint i/o un servidor.
- Aïllament i mitigació de presència i activitat maliciosa a nivell mundial a tot l'entorn amb les capacitats mínimes següents:
  - ➢ Des habilitar usuari.
  - ➢ Restabliment de contrasenya.
  - ➢ Bloquejar IP.
  - ➢ Bloquejar domini.
  - ➢ Bloquejar port.

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

- Respostes automatitzada:
  - ➢ Playbooks de resposta preestablerts que es proporcionen llestos per utilitzar.
  - ➢ Playbooks de resposta personalitzats creats per l'administrador.
  - ➢ Rollback.
- La solució ha de mostrar la cadena d'esdeveniments, objectes relacionats amb un incident amb una visualització gràfica de l'incident mostrant:
  - ➢ Esdeveniments
  - ➢ Dades relacionades sobre la víctima.
  - ➢ Dades relacionades amb l'agressor.
  - ➢ Dades relacionades sobre la relació dels artefactes.
  - ➢ Dades amb tot l'arbre de processos.
  - ➢ Cadena d'esdeveniments.
- La solució ha d'incloure motor de recerca automàtic sobre els esdeveniments de seguretat detectats que:
  - ➢ Permetrà identificar qualsevol persistència,
  - ➢ Mostrarà la causa arrel
  - ➢ Mostrarà els elements compromesos en tota la infraestructura protegida.
- Capacitat de remeiar, sempre de forma autònoma, allò identificat, eliminant de forma automatitzada els elements maliciosos identificats durant la fase de recerca.

La solució ha de recopilar contínuament dades sobre totes les entitats i les activitats dins de l'entorn:

- Interacció amb arxius:
  - ➢ crear
  - ➢ obrir
  - ➢ re anomenar
  - ➢ eliminar
  - ➢ executar
- Execució de processos (inclosa la visualització de l'arbre de processos)
- Inici de sessió d'usuari
- Trànsit de xarxa
- Canvis al registre
- Software instal·lat

La solució ha d'admetre:

- La visualització de dades d'entitat i activitat:
  - ➢ Cerca basada en patrons de comportament en tots els camps de cobertura (usuaris, arxius, màquines i trànsit de xarxa).
  - ➢ Determinació de les regles i/o creació d'alertes i/o determinació del nivell de risc, basant-se en una resposta al patró de cerca i en temps real.
  - ➢ Habilitació de nombre d'usuaris per realitzar activitats en paral·lel, en base als permisos dels usuaris, i sense necessitat de desconnexió d'un altre usuari per al "execució de l'activitat.
- L'anàlisi dinàmica (és a dir, sandbox) fins i tot pot enviar manualment fitxers per a la seva anàlisi.
- Consultes entre organitzacions permetent cerques d'ocurrències d'activitats de procés, fitxers, xarxa i/o usuaris a tots els equips de l'entorn.

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

La solució ha de sustentar els mitjans per executar la investigació forense, com ara:

- Procés en execució
- Fitxer en execució.
- Nivell de màquina.
- Activitats de memòria.
- Obtenir bolcat de memòria.

3. Migració i Implantació de la solució

La instal·lació de la solució objecte del contracte és responsabilitat de l'adjudicatari, sempre amb la col·laboració, coordinació i vistiplau de la Unitat TIC.
Els licitadors han d'incloure com a mínim el següent:

- L'adjudicatari haurà de planificar i proporcionar tots els serveis necessaris per la migració de la solució actual a la solució oferta, és a dir, la desinstal·lació del producte actual i posterior instal·lació i configuració dels Endpoints associats a la seva plataforma.
- Servei d'implantació integral que inclogui la instal·lació, desplegament i parametrització de la solució en tots els actius, així com el seu seguiment i resolució de qualsevol incident que es pugui originar durant aquest procés.
- El procediment necessari per a la implantació de la nova solució, haurà d'assegurar en tot moment el sistema des del punt de la protecció i de la integritat de les dades, evitant interrupcions en els serveis, sempre que sigui possible. És a dir, s'ha de minimitzar el temps que un equip roman sense protecció. Això implica que no es pot fer primer la desinstal·lació del producte actual de tots els equips i després la instal·lació del nou, sinó que cal plantejar-ho per conjunts d'equips.
- Desplegament de les polítiques necessàries, basades en les "best practices" del fabricant i en la pròpia idiosincràsia del funcionament de l'Ajuntament, tant a nivell de servidor com d'equip personal.
- L'adjudicatari haurà de planificar i proporcionar tots els serveis necessaris per realitzar la instal·lació i configuració de la consola d'administració i gestió, així com la definició de les polítiques de seguretat de l'EPP que millor s'adaptin a l'entorn de l'Ajuntament de Calonge i Sant Antoni, amb l'estudi previ amb els tècnics de la Unitat TIC. Durant la implantació i tunning de la nova solució, l'adjudicatari haurà de proporcionar els serveis de suport necessaris per tal que el procés sigui el més ràpid, eficient i transparent possible.
- Previ a la posada en marxa es realitzarà una sessió formativa per al personal de la Unitat de Tecnologies de la Informació i Comunicacions, encarregat de l'administració del sistema. Aquesta sessió es podrà realitzar per mitjans telemàtics i tindrà una durada mínima de 4 hores, en què s'explicarà amb detall el maneig i configuració de la consola, l'Endpoint així com les eines del fabricant que seran útils per a la resolució d'incidències i/o protocol d'actuació enfront un atac.

4. Serveis monitorització

Els serveis de monitorització han de ser prestats per personal especialista en seguretat i amb disponibilitat 24x7 i en idioma català i/o castellà.

Els serveis mínims de monitorització han de permetre:

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

- File Integrity Monitoring (FIM) que asseguri la política en entorns fixos per alertar sobre qualsevol canvi en un fitxer.
- La descoberta desatesa de diferents tècniques d'atac, cercant fitxers, processos, connexions de xarxa i comptes d'usuari susceptibles de risc amb contrasenyes antigues.
- La solució ha de proporcionar els mitjans per dur a terme la gestió d'inventari permetent mapejar i correlacionar tots els actius dins de l'entorn, com ara punts finals, servidors, aplicacions instal·lades, comptes d'usuari i informes periòdics generats.
- Recopilació i retenció de registres d'activitat i autenticació permetent-ne la conservació durant el període de temps que exigeixen les diferents normatives.
- 24x7 Cerca proactiva d'amenaces global (Threat Hunting).
- 24x7 Cerca Proactiva d'amenaces a Deepweb (Deep Hunting)
- 24x7 Cerca Proactiva d'amenaces a Darkweb (Dark Hunting)
- Avaluació de vulnerabilitats integrada al mateix agent, que descobreixi les actualitzacions de seguretat que falten en els sistemes i aplicacions. Els requisits mínims són:
  - ➢ Revisió automatitzada de pegats de Windows
  - ➢ Control d'aplicacions instal·lades no desitjades.
  - ➢ Control de versió mínima permesa d'aplicacions de tercers
  - ➢ Validació d'operativitat constant d'agents de tercers.

5. Serveis de manteniment i suport tècnic del software

El manteniment i suport tècnic del software haurà de contemplar, almenys, els aspectes següents:

- Informació sobre noves versions.
- Actualització de les versions de programari, a fi de disposar de totes les correccions, revisions i millores del programari, entenent que en cas d'aparèixer noves versions hauran de ser facilitades dins del període en què el contracte tingui el seu efecte i amb la documentació corresponent adaptada als programes suportats.
- Serveis de notificació anticipada.
- Informació i accés preferent a les presentacions de nous productes, noves versions o conferències d'usuaris organitzats per l'empresa adjudicatària.
- L'adjudicatari proporcionarà un suport tècnic que asseguri la resolució de tota mena d'incidències, tant d'instal·lació del programari com d'execució, que puguin sorgir durant el contracte a partir de la data d'inici del mateix.
- Atenció no presencial en suport telefònic, web, correu electrònic davant de problemes o consultes.
- En cas d'incidents crítics, possibilitat de fer un diagnòstic remot.
- Suport a un nombre il·limitat de casos via web, fax, telèfon o correu electrònic

6. Formació i instal·lació

La instal·lació de la solució anirà a càrrec de l'adjudicatari i comptarà amb el suport del departament d'Informàtica de l'organització per al desplegament dels agents. La generació de paquets, polítiques i altres funcionalitats seran consensuades per ambdues parts en reunions periòdiques fins al total desplegament de la solució.

La formació de la solució anirà a càrrec de l'adjudicatari a mesura que la instal·lació vagi avançant.

Plaça de la Concòrdia, 7
17251 Calonge i Sant Antoni
Tel. 972 66 03 75
www.calonge.cat

La instal·lació, implantació i formació s'haurà de desenvolupar en un percentatge d'un 60% de forma presencial a les dependències municipals amb el desplaçament del tècnic qualificat i designat per al projecte.

7. Proves de concepte

L'Organització Contractant demanarà a les empreses licitadores (inicialment a la que s'hagi proposat com a adjudicatària), sense cost addicional, la realització d'una prova de concepte de 7 dies, per tal de validar que la solució tecnològica proposada s'ajusta a les funcionalitats que han estat recollits en aquest plec de prescripcions tècniques.

L'empresa adjudicatària s'encarregarà de preparar l'entorn i facilitar l'accés als tècnics de l'Organització Contractant, de manera que, des d'un lloc de treball corporatiu, que tingui instal·lada la maqueta estàndard corporativa, es pugui fer aquesta comprovació.

Per a la realització de la prova de concepte, els tècnics de l'Organització Contractant proporcionaran a l'empresa proposada com a adjudicatària equips amb sistemes operatius diversos, que podran incloure:
Windows 10
Windows 11
Windows Server 2008
Windows Server 2012
Windows Server 2019
Windows Server 2022
Linux
MacOS

Es considerarà que la solució tecnològica proposada té l'acceptació de l'Organització Contractant, si es constata que els resultats de la prova de concepte han permès garantir, de manera objectiva, que la solució proposada ha complert les especificacions tècniques i els criteris de validació inclosos a la prova de concepte i detallats als paràgrafs precedents d'aquest mateix apartat.

8. Documentació a presentar a l'oferta

Amb l'oferta caldrà entregar una memòria tècnica completa amb la descripció detallada que figurarà al PCAP on incorporarà la solució subministrada. Aquesta documentació serà validada pe la unitat TIC a l'efecte d'acceptar-la i verificar que dona compliment als requeriments tècnics determinats en aquest Plec i les millores que s'hagin ofert. Aquesta memòria tècnica ha de tenir com a guió la justificació de tots els requeriments tècnics d'aquest plec i els punts que es demanen a l'apartat de criteris de valoració subjectius de la Memòria.

La no presentació d'una memòria tècnica serà motiu de desestimació de l'oferta.

9. Certificacions

Les empreses licitadores han tenir les certificacions màximes de les empeses fabricants de la solució presentada que garanteixi que són distribuïdors oficials i que poden donar suport tècnic qualificat de les solucions presentades.