LLICÈNCIES I SERVEIS EDR I MDR PER LA DIPUTACIÓ DE TARRAGONA

Plec de Prescripcions Tècniques

Índex de continguts

1. OBJECTE DEL CONTRACTE

Per tal de garantir la seguretat dels equips corporatius de la Diputació de Tarragona i dels ajuntaments i consells comarcals als quals es presta el servei, es requereix renovar les llicències per subscripció de programari EDR *(Endpoint Detection & Response)* i MDR *(Managed Endpoint Detection & Response)*, així com els serveis de suport avançat i una bossa d'hores de tasques d'administració de la plataforma.

2. ANTECEDENTS

Actualment la Diputació de Tarragona té desplegada una solució EDR en les estacions de treball i servidors amb la següent distribució:

- Instal·lat en equips de la Diputació: **1.696**
- Instal·lat en equips d'Ajuntaments: **885**
- Instal·lat en equips de Consells Comarcals: **158**

El servei als ajuntaments es distribueix de la següent manera:

a) Ajuntaments amb EDR: **85**

b) Nombre d'Ajuntaments amb EDR per comarques:
- Alt Camp: **15**
- Baix Camp: **13**
- Baix Ebre: **6**
- Conca de Barberà: **15**
- Montsià: **5**
- Priorat: **17**
- Ribera d'Ebre: **1**
- Tarragonès: **4**
- Terra Alta: **9**

Nombre de Consells Comarcals amb EDR:

c) Consell Comarcal de l'Alt Camp
d) Consell Comarcal del Montsià

La seguretat dels equips dels ens locals esmentats depèn de la disponibilitat real d'una protecció continuada i efectiva. Qualsevol discontinuïtat en la protecció que ofereix l'EDR podria exposar els equips i sistemes a ciberatacs

La solució implantada es tracta d'una solució avançada que ofereix una protecció integral mitjançant components de control (Control de dispositius, Control Web, Control d'anomalies adaptable) i de protecció (Detecció de comportament, Prevenció de vulnerabilitats, Prevenció d'intrusions, Motor de reparació, Protecció davant amenaces en fitxers, Protecció davant amenaces web, Protecció davant amenaces en el correu, Protecció davant amenaces a la xarxa, Tallafocs, Prevenció d'atacs de BadUSB, Proveïdor de protecció AMSI).

3. DETALL DEL CONTRACTE

3.1 Subscripcions i serveis de suport

A l'inici del contracte s'han de subministrar les següents llicències per subscripció:

- 3000 llicències *Endpoint Detection and Response* per 2 anys
- 2000 llicències *Managed Detection and Response* per 2 anys

Durant el contracte la Diputació de Tarragona podrà demanar a l'adjudicatari l'activació llicències addicionals dels següents tipus per **preus unitaris,** segons surti la necessitat:

- *Endpoint Detection & Response*
- *Managed Detection & Response*

El subministrament de les llicències ha d'incloure:

- Les actualitzacions del programari de servidor i clients
- Les actualitzacions dels patrons de *malware* publicat pel fabricant

També es requereix disposar de manteniment per a resolució d'incidències i una bossa d'hores per a la realització de treballs tècnics:

- Activació de servei de suport avançat per la plataforma per 2 anys, amb suport per un mínim de 12 intervencions a l'any en modalitat 24x7
- Activació de servei d'anàlisi forense (DFIR) fins a 50 hores anuals per intervencions en incidents: anàlisi d'origen i detalls exhaustius del succés,

raons per les quals s'ha pogut portar a terme, solució per evitar la reincidència, etc.

 Bossa d'hores addicional de 50 hores per servei d'anàlisi forense en cas de necessitar un anàlisi més exhaustiu

 Bosses d'hores de suport directe del fabricant per a treballs tècnics relacionats amb la plataforma: actualitzacions, canvis en la infraestructura, desplegament de components, reconfiguració, anàlisi de la plataforma, etc. Aquestes bosses d'hores serà per preus unitaris per cada paquet de 8 hores, amb un màxim de 120 hores

3.2 Requeriments tècnics

Requeriments tècnics i funcionals del programari

La solució aportada haurà de complir amb els següents requisits tècnics i funcionals:

a) Funcionalitats de l'Endpoint

 Xifratge del PC i/o carpetes amb BITLOCKER: gestió del xifrat i desxifrat de dades, tant per al PC complet com per a carpetes.

 Desplegament de programari de tercers mitjançant la consola: instal·lació de paquets .MSI, MSP, XE, BAT de manera parametritzable.

 Xifratge USB portable, amb tecnologia propietària: evita copiar dades sense xifrar en els dispositius, ja sigui amb USB Bitlocker o amb una tecnologia propietària.

 Control total d'aplicacions, instal·lació, prohibició i distribució: instal·lar programari de tercers als equips, a més de bloquejar, eliminar o denegar-ne l'ús.

 Prevenció d'exploits (Virtual Patching): bloqueig de l'acció de vulnerabilitats conegudes (CVE publicades).

 Gestió de vulnerabilitats del sistema operatiu i de programari de tercers: detecció d'aplicacions i sistemes operatius vulnerables i aplicació de pegats de manera automàtica o manual.

 Inventari de maquinari (HW): inventari automàtic del hardware.

 Inventari de programari (SW): inventari automàtic del software.

 Control del hardware, bloqueig de ports, càmeres, micròfons (tot el hardware que el dispositiu posseeix): control total del maquinari,

bloqueig o pseudo bloqueig (per exemple, bloqueig de micròfon o USB) i registre d'accions en dispositius USB.

- Control del SW, detecció de vulnerabilitats en programari de tercers: detecció i remediació d'aplicacions de tercers amb vulnerabilitats de forma automàtica o manual.
- Control del SW, detecció de vulnerabilitats del Sistema Operatiu: detecció i remediació d'aplicacions del Sistema Operatiu Microsoft.
- Antiransomware i motor de recuperació (ROLLBACK) en xifrar fitxers de manera automàtica: bloqueig 100% contra ransomware LINK i recuperació de la sessió d'usuari (reg.edit, dll, altres).
- Atac fileless, prevenció i detecció d'atacs sense fitxer adjunt: detectar i bloquejar accions que no són legítimes en una xarxa empresarial.
- Intel·ligència basada en núvol amb veredicte de detecció basada en IA.
- Machine Learning i Behavior Detection: detecció d'amenaces basada en el comportament.
- Detecció d'atacs basats en un comportament anòmal del programari.
- Detecció de comportament IA que bastioni automàticament el comportament de les aplicacions d'usuari: bastionament automàtic del comportament anòmal de les aplicacions realitzades per l'usuari.
- Control de la navegació de l'usuari: filtres de contingut (bloqueig per temes, per exemple, xarxes socials, webs concretes, etc.) i auditoria de la navegació per dispositiu.
- Protecció de xarxa: supervisió de connexions TCP/UDP davant d'amenaces de manera automàtica o parametritzable.
- Determinació de l'entorn de xarxa per usuari: BYOD que permeti bloquejar aplicacions, navegació, tallafocs i controls de dispositius, etc., quan l'usuari utilitza el seu equip fora de la xarxa corporativa.
- Control del tallafocs de l'equip: tallafocs independent del SO, parametritzable amb regles basades en la legitimitat i en les connexions de l'aplicació de manera centralitzada.
- Política d'explotació de malware: accions de resposta automàtiques quan es produeix un cert volum d'atacs, per exemple, aplicant una resposta de restricció agressiva en cas de detectar atacs massius.
- Instal·lació de sistemes operatius en equips nous: ha de permetre llançar una imatge de SO per a un PC nou o per a un equip que es desitgi formatar via PXE, amb integració de Wake On LAN.

- Sandbox: determinar si el fitxer disposa d'elements de malware.
- Compatibilitat amb Windows, Windows Server, Linux, iOS, Mac, Android: compatible amb qualsevol SO amb suport del fabricant.
- Bad USB: mòdul que verifiqui la integritat dels dispositius USB (teclat), per exemple, keyloggers, mitjançant un validador de teclat a la pantalla.
- SIEM: Dades exportables a SIEM extern amb protocols SYSLOG / CEF / LEEF.
- Informes automàtics i configurables: informes d'atacs, inventari, resum d'amenaces, automàtic i personalitzable, i dashboard en temps real / parametritzable.
- Tecnologia d'optimització del rendiment de l'anàlisi complet amb escaneig només en variació.
- Background Scan: optimització del rendiment de l'anàlisi per inactivitat de l'usuari, afavorint l'experiència d'usuari.

b) Funcionalitats de l'EDR

- EDR que permeti conèixer la dimensió d'un incident i obtenir informació detallada sobre el host, l'IP i les comunicacions; un mapa visual complet d'una amenaça o possible amenaça, contextualitzat.
- Anàlisi retrospectiu del motor de reparació (rollback): auto recuperació de fitxers i eliminació de virus, troians o altres payloads, amb informe forense.
- Bloqueig d'execució per hash/SHA: bloqueig d'execució per hash a partir d'IOC per a tots els equips en detectar una amenaça.
- Creació d'IOC a partir d'una amenaça: incorporació d'IOC per a cerques de compromís i aplicació de regles de prevenció automàtica.
- EDR per a l'aïllament de la xarxa del host: detecció i aïllament automàtic de qualsevol host en condicions similars; aïllar els equips de la xarxa fins que es determini el seu reintegració després de la remediació o resposta aplicada.
- Consulta a portal d'intel·ligència: consulta directa al portal d'intel·ligència del fabricant de sobre l'abast i el tipus d'amenaça.

- EDR per a l'automatització de les tasques de neteja i desinfecció: creació de tasques per lots i execució en tots els equips afectats.
- Consola web o consola nativa en núvol a la UE.
- Suport per idioma espanyol.
- Implementació senzilla sense impacte en l'entorn corporatiu: no ha de requerir reinici en activar, ni ser intrusiu amb l'usuari.
- Un únic agent unificat

c) Funcionalitats de l'MDR

- El servei MDR haurà de ser prestat sense la necessitat d'instal·lar agents addicionals. La solució haurà d'operar de manera nativa amb la infraestructura de seguretat ja desplegada, garantint la compatibilitat total i evitant qualsevol impacte en el rendiment, estabilitat o integritat dels sistemes.
- La plataforma haurà d'integrar-se de forma transparent amb les solucions de seguretat del proveïdor, assegurant un nivell de protecció òptim sense requerir modificacions en la configuració dels dispositius o la xarxa.
- La telemetria generada per tots els equips protegits haurà de ser emmagatzemada exclusivament en la infraestructura al núvol del proveïdor del servei MDR, garantint un accés immediat i continu per a la investigació i resposta a incidents. Aquest emmagatzematge haurà de mantenir-se per un període mínim de tres mesos, amb opcions d'ampliació sota demanda. A més, la plataforma haurà de comptar amb mecanismes avançats de correlació i anàlisi de dades dins de l'entorn al núvol del proveïdor, assegurant la màxima seguretat, disponibilitat i compliment normatiu sense dependència de tercers.
- L'arquitectura de la consola de gestió de l'EPP/EDR haurà d'oferir flexibilitat en la seva implementació, permetent el seu desplegament en entorns on-premise, híbrids o completament al núvol, garantint sempre una integració nativa amb les solucions de seguretat del

proveïdor. En el cas d'una arquitectura on-premise, la solució haurà de ser compatible amb sistemes operatius Microsoft Windows i Linux, assegurant un rendiment òptim i un suport complet sense necessitat d'adaptacions o desenvolupaments addicionals.

- Així mateix, el sistema de gestió haurà d'oferir compatibilitat obligatòria amb bases de dades empresarials d'alt rendiment, incloent Microsoft SQL, MariaDB, PostgreSQL o Postgres PRO, assegurant la màxima eficiència en l'administració de grans volums de dades de telemetria i esdeveniments de seguretat. La plataforma haurà de garantir que totes les seves funcionalitats operin de manera nativa en aquests entorns, sense requerir configuracions o solucions externes que comprometin l'estabilitat, escalabilitat o seguretat de la infraestructura.

- La gestió dels incidents detectats pel servei MDR haurà de combinar capacitats avançades d'automatització mitjançant intel·ligència artificial i machine learning amb l'anàlisi expert d'un equip humà altament especialitzat del proveïdor. La detecció, el triatge, la categorització i la correlació amb indicadors d'atac (IoAs) hauran de realitzar-se de manera automatitzada, garantint una avaluació inicial precisa i en temps real amb una reducció important dels falsos positius. Posteriorment, la validació, investigació i resposta als incidents hauran d'estar a càrrec d'analistes del fabricant, els quals aplicaran intel·ligència d'amenaces pròpia i coneixements especialitzats per prendre decisions contextualitzades i mitigar riscos de forma efectiva.

- A més, el servei haurà de garantir que la correlació d'esdeveniments, l'anàlisi d'amenaces i la resposta als incidents es realitzin sense intermediaris externs, assegurant un procés unificat, precís i alineat amb les millors pràctiques del sector. Per a això, tant la creació de nous incidents com la interacció amb incidents ja oberts haurà de realitzar-se a través d'un canal de comunicació segur i bidireccional entre el client i els analistes del fabricant. Aquest canal haurà de garantir la transmissió xifrada d'informació sensible, permetre una gestió eficient dels incidents en temps real i facilitar l'intercanvi de dades tècniques, recomanacions i accions de resposta sense comprometre la seguretat o confidencialitat de la informació.

- El proveïdor del servei MDR haurà de garantir temps de reacció dins dels següents límits, assegurant el compliment d'almenys un 90% dels casos dins dels valors objectiu especificats:

Nivell de Severitat	Temps de reacció	Valor objectiu

Alt (Ex.: atac dirigit)	60 minuts	90%
Mig (Ex.: malware comú)	4 hores	90%
Baix (Ex.: adware, riskware, etc...)	24 hores	90%

- Servei amb Web Portal: inclòs en el servei en format CLOUD o integrat amb la plataforma on-premise.
- Servei 24*7*365: gestió de l'EDR operada pel fabricant 24x7x365.
- Localització dels SOC EU+US+APAC: cobrint l'horari 24x7.
- Play Book de resposta: acords d'abast en servidors i PCs entre el client i el Fabricant.
- Respostes automatitzades davant d'atac dirigit de nivell crític: aplicació automàtica i/o informativa de resposta en cas de patir un incident greu.
- Supervisió de tàctiques en el moment de la detecció: cerques de compromís.
- Accés inicial, moviment lateral, command and control, persistència, execució, evasió de la defensa, accés a credencials, escalat de privilegis, impacte, descobriment, recollida, desenvolupament en recursos, exfiltració de dades.
- Retenció de telemetria de 3 mesos: per a anàlisi forense i per detectar des de quan existeixen amenaces; es poden adquirir més mesos.
- Health Check preventiu: revisió prèvia abans de l'entrega del servei.
- MITRE Mapping: mapeig de regles MITRE per a anàlisi forense.

4. DESPLEGAMENT

La solució desplegada a la infraestructura on-premise de la Diputació de Tarragona en l'actualitat és *Kaspersky Endpoint Security for Bussiness*. La solució proposada ha de complir amb totes les funcionalitats actuals, i donar per 2 anys als més de 2.500 equips actuals amb el mateix nivell de protecció i servei.

En cas que la solució proposada requereixi el canvi de la plataforma actual i no sigui només l'activació de llicències, per tal de no perdre cap de les funcionalitats i serveis, tots els costos associats a les següents tasques necessàries aniran a càrrec de l'adjudicatari:

- Cost de les llicències actuals durant tot el període de migració per tal de no tenir cap tall de servei
- Desplegament del maquinari servidor necessari
- Desplegament del programari servidor i llicències i suport del mateix
- Migració de configuracions i parametrització
- Joc de proves de verificació i compatibilitat amb tots els clients
- Desplegament de l'agent EDR a tots els equips clients, de forma presencial, a Diputació i la seu de cada ens al que es presta servei
- Activació de les llicències corresponents
- Formació oficial del fabricant en la gestió de la plataforma per a 10 tècnics de la Diputació, amb un mínim de 40h

5. PRESSUPOST BASE DE LICITACIÓ

Els pressupost base de licitació s'ha calculat en base als preus orientatius dels fabricants.

Pressupost IVA exclòs	(21% IVA)	**Pressupost base licitació (IVA inclòs)**
348.055,00 €	73.091,55 €	421.146,55 €

El tècnic responsable de la contractació
Emili Badia Cantarero