Plec de Prescripcions Tècniques

Manteniment de llicències i serveis Delinea Secret Server (gestió usuaris privilegiats PAM)

Expedient: **15012771**

Gener de 2024

Versió 1.0

Operació Sistemes Tecnològics / Prestació del Servei
Àrea de Tecnologia

Índex de continguts

1. Introducció

En TMB des de 2022 s'utilitza el producte Delinea Secret Server per a la gestió de comptes privilegiats a sistemes crítics (PAM).

La present licitació té com a objectiu renovar el manteniment de les llicències i els serveis de suport associats, així com evolucionar en la integració d'aquest component amb la resta de sistemes que intervenen en el cicle de vida de la infraestructura tècnica de TMB, tenint com a objectiu últim automatitzar al màxim els procediments operatius.

2. Abast

2.1. Manteniment de las llicencies de fabricant

Renovació de les llicencies de fabricant que inclouen el dret d'ús, els serveis de suport del fabricant i l'accés a noves versions i pegats que corregeixen errors i vulneracions de seguretat.

Les llicències a mantenir son:

- 300 x SS - Connection Manager - On Prem Sub T4-S Premium
- 300 x Secret Server - Platinum Edition - IT/Admin User Maintenance T3-M Premium Support
- 2 x Secret Server - Engines - Maint Premium Support

2.2. Serveis professionals.

També és abast de la present licitació la contractació dels serveis professionals necessaris per a l'administració, evolució i suport a l'operació d'aquest component .

A continuació es detallen els diferents aspectes que es consideren imprescindibles per a la cobertura del servei. No obstant, el licitador tindrà en consideració qualsevol altre element que, tot i no estar detallat en el present Plec de Prescripcions Tècniques, sigui necessari per al correcte funcionament del programari i el servei, oferint una solució plenament operativa.

2.2.1. Help Desk de 1er. nivell

Servei de suport telefònic 24x7 en castellà/català que inclou la realització del diagnòstic inicial de la incidència (programari o maquinari) i la resolució directa en primer nivell o escalat a fabricant si es necessari.

Temps de resposta demanats:

- Incidències no crítiques (plataforma inoperativa per a menys del 20% d'usuaris).

  Temps màxim de 4h en horari 8x5 (dies laborables) entre l'avís i la resposta inicial dels tècnics per a casos de baixa prioritat. L'horari serà de 8:00h a 17:00h

- Incidències crítiques (plataforma inoperativa per a més del 20% d'usuaris).

  Temps màxim de 2h en horari 24x7 (dies laborables) entre l'avís i la resposta inicial dels tècnics per a casos de baixa prioritat.

Una vegada s'hagi obert una incidència crítica, el seguiment fins a la seva resolució serà 24x7 dut a terme per un tècnic certificat en l'eina.

La present licitació contempla un màxim de 4 incidències crítiques al mes.

2.2.2. Administració

- Healthcheck inicial de la plataforma i propostes d'evolució.
- Upgrades de la plataforma PAM (major/minor versió). Limitat a 3 actualitzacions de versions menors i 1 canvi d'una versió major a l'any. Pla de marxa enrere i pla de proves per a cada canvi major. Els canvis major es faran en horari 24x7.
- Elaboració de processos i còpies de seguretat de l'eina.
- Desenvolupament d'un pla de recuperació de desastres.
- Aplicació de pegats crítics de seguretat recomanats pel fabricant o els requerits per a resolució d'incidències, a aplicar en horari 8x5 (dies laborables).
- Configuració de l'organització de la plataforma en mode keepass (generació d'estructura de carpetes, dotació de privilegis necessaris).
- Revisions setmanals i mensuals de la plataforma. Serveis recurrents de la plataforma, amb assessorament i planificació evolutiva al costat de TMB.
- Actualització de documentació i guies amb processos detallats d'operació.
- Formacions i transferència de coneixement a personal de TMB. Resolució de dubtes teòrics i funcionals propostes per TMB.
- Sessions de formació, dirigides a nous usuaris que mai hagin usat la plataforma PAM i a operadors per a la realització d'accions d'administrador. Màxim 1 formació cada 2 mesos.
- Elaboració i presentació d'informes mensuals i quadres de comandament integrats en l'eina de splunk de TMB, amb, com a mínim, la següent informació:
  1) Estat de salut de la plataforma
  2) Ús de la plataforma
  3) Llistat d'incidents i resolució

2.2.3. Operació

Servei gestionat d'Operació. L'equip d'operació haurà d'atendre les tasques demandades (incidències i sol·licituds) sobre la plataforma.

A continuació, s'indiquen alguns tipus de sol·licituds que es necessiten tractar:

- Revisió diària de l'estat de la plataforma i resoldre o reportar les fallades trobades en l'execució de les tasques.
- Altes, baixes, modificacions de proveïdors (carpetes), sincronitzacions de grups proveïdor del DA i permisos.
- Altes, baixes, modificacions de grups de servidors Windows.
- Altes, baixes i modificacions de secrets.
- Alta/Modificació/Baixa de secrets.
- Actualització en PAM per a gestió de permisos, rols, i actualització de polítiques.
- Anàlisis de fallades en comptes integrats i fallades de girat o sincronització amb sistemes finals.
- Revisió, actualització i desactivació de comptes en desús (neteja de l'entorn).
- Generació de script per a eliminació massiva de secrets.
- Configuració d'exportació de comptes break-the-glass: comptes que han de ser accessibles en cas de caiguda del servei, per a poder minimitzar del temps d'espera.

L'empresa adaptarà el flux d'entrada sol·licituds a través de l'eina de Footprints de TMB i/o tant a través de la seva Service Desk per Correu electrònic i Número d'atenció telefònica.

2.2.4. Evolució

En l'apartat d'evolució l'oferta contemplarà una quantitat de 200 hores a consumir durant la duració del contracte en les què queden incloses els següents tipus de tasques:

- Desplegament de nova infraestructura.
- Configuració de noves funcionalitats de la plataforma.
- Construcció de nous connectors que no siguin OOTB.
- Generació de desenvolupaments personalitzats, per a aconseguir noves funcionalitats, com per exemple Just in time per a usuaris crítics.
- Integració amb altres solucions (SIEM, ITDR, Ticketing…).
- Onboarding de comptes de servei. Treball d'anàlisi de dependències i proves de funcionament.
- Configuració de "challenges": mecanismes de seguretat llançats automàticament davant un comportament no normatiu dins del PAM fent ús del mòdul Privileged Behavior Analytics.

Addicionalment, comentar que en aquests moments TMB està submergida en un profund canvi cultural cap a l'automatització de tots els seus processos i serveis tecnològics, usant metodologia DevOps i el control de versions mitjançant GitHub. Es pretén que totes les accions que es realitzen sobre els diferents sistemes es facin a partir d'un model declaratiu, obtenint així el mateix entorn – amb el seu corresponent estat – cada vegada que s'aplica, i establint de facto la seva documentació.

Alineats amb aquesta estratègia, **durant el primer any** s'haurà d'adaptar l'operació i administració del PAM seguint els criteris d'aquest marc cultural. Per a això és necessari afegir les següents funcionalitats, ja sigui usant facilitats pròpies del producte o inclús, si és necessari desenvolupant-les. En aquest últim cas, preferiblement seguint les premisses d'aquesta mena d'integracions que estableix TMB:

- Detecció i onboarding automàtic de comptes locals en Windows i Linux.
- Onboarding automàtic de proveïdors (carpetes, permisos, grups de màquines Windows i secrets Linux).
- Onboarding automàtic de comptes admin, en cas de windows la default administrator, en cas de linux comptes rootXXX.
- Configuració de Discovery per a la detecció i onboarding automàtic de comptes de domini.
- Anàlisi de comptes de domini pertanyents als dominis integrats en PAM.
- Onboarding automàtic de comptes amb nomenclatura de tots els proveïdors.
- Baixes i modificacions automàtiques de secrets de proveïdors.
- En aquest primer any es faran totes les configuracions, scripts, … necessaris per a automatitzar aquestes tasques d'operació.

3. Requeriments organitzatius

3.1. Tasques genèriques

Els treballs s'executaran en els sistemes i programes propietat de TMB i responsabilitat de l'Àrea de Tecnologia.

3.2. Aspectes funcionals

La prestació del servei objecte d'aquesta contractació ha de complir amb els ítems següents:

1. La execució de les tasques es durà a terme principalment de forma remota. No obstant això, si TMB ho considera, per la naturaleza de la invenció o incidència, pot demanar realitzar les tasques de forma presencial. En aquet cas, de no indicar una altra cosa, es faran a l'oficina de TMB situada a la següent adreça:

   Centre de Suport Tecnològic
   C/Josep Estivill, 47
   08027, Barcelona

2. La sol·licitud dels serveis es realitzarà, en els casos que no es tracti d'incidència, amb un període d'antelació, a convenir entre les parts, mai superior a una setmana natural.
3. El servei disposarà d'un referent que serà l' interlocutor amb el responsable del servei de TMB i es disposaran dels recursos necessaris per finalitzar les tasques en les dates acordades.
4. Es presentarà una planificació dels treballs a realitzar per acordar amb TMB la durada del treball en cas que es tracti de tasques que permetin aquesta planificació.
5. L'horari de les jornades serà de 8h a 14h els dies laborables.

4. Confidencialitat

L'empresa col·laboradora ha d'acceptar la Política de Seguretat Tecnològica i de la Informació de TMB. L'adjudicatari es compromet a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del servei actual i a la qual només el personal autoritzat per TMB. L' adjudicatari serà responsable de les violacions del deure de secret que es puguin produir pel personal sota el seu càrrec.

Se l'obliga a aplicar les mesures necessàries per garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer per part del personal que participi en el desenvolupament del servei.

Una vegada finalitzat el present servei es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per TMB, així com qualsevol altre producte obtingut com a resultat del present contracte.

L'empresa col·laboradora ha d'acceptar el compromís de confidencialitat respecte a les dades a les quals tindrà accés i que són propietat de TMB.

Els permisos d' accés als sistemes i aplicació, en cas de ser necessari, tindran el nivell necessari per al treball a realitzar i assignats a usuaris personals. En cas de precisar de l'accés amb un usuari amb privilegis elevats en el sistema es durà a terme a través de l' eina que disposa TMB per a aquest fi, de manera que quedin traçades les accions que es realitzin.

5. Compliment de la llei Orgànica de Protecció de Dades de Caràcter Personal

L'adjudicatària es compromet a complir quantes obligacions li són exigibles en matèria de protecció de dades personals tant pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE ("RGPD") com per la llei Orgànica 3/2018, de 5 de desembre, de Protecció de dades de Caràcter Personal així com totes les altres normes legals o reglamentàries incideixin, desenvolupin o substitueixin les anteriors en aquest àmbit.

6. Seguiment del contracte

Per facilitar la bona marxa del contracte cal tenir en compte els següents punts:

- Es realitzaran reunions periòdiques entre el responsable del servei de l'empresa adjudicatària i el responsable d'aquest a TMB.
- La periodicitat es fixarà en funció de la marxa del servei, essent la proposta inicial d'una vegada cada tres mesos. En aquestes reunions es tractaran temes de la marxa del contracte, així com el consum i saldo de jornades.

Jesús Aguilar Morales

Responsable de Sistemes de Seguretat TIC