Transports Metropolitans de Barcelona

Plec de condicions tècniques per l'adquisició, instal·lació, implementació i manteniment de l'ampliació per incloure dos sistemes a la plataforma passiva de monitorització industrial en temps real per sistemes operacionals de FMB

Expedient número 16030901

Versió 1.0
11/2023

ÍNDEX

1. INTRODUCCIÓ 2
2. ABAST DEL SERVEI 3
2.1. De producte 3
2.2. De serveis professionals 5
3. OBLIGACIONS DE L'ADJUDICATARI 6
3.1 Instal·lació i posada en marxa de la solució i implementació 6
3.2 Suport tècnic llicències Nozomi 7
3.3 Formació 7
3.4 Servei d'acompanyament o millora de la plataforma: 7
3.4.1 Suport tècnic L2 8x5 8
3.4.2 Servei evolutiu de l'aplicació amb actualització de versions 8
3.4.3 Bossa d'hores per fine tuning de la plataforma 8
3.5 Altres Obligacions de l'Adjudicatari 9
3.6 Seguretat i Confidencialitat 11
3.7 Compliment de la llei Orgànica de Protecció de Dades de Caràcter Personal 12
4. OBLIGACIONS DE TMB 13
5. COMUNICACIONS ENTRE LES PARTS 13
5.1 Seguiment del contracte 13
6. ANNEXE - SISTEMES OPERACIONALS FMB 14

1. Introducció

L'objecte del present document és definir les condicions per a la presentació d'oferta per l'ampliació per incloure dos sistemes més a la plataforma passiva de monitorització industrial en temps real i intel·ligència que permet detectar i alertar de l'estat dels sistemes operacionals de FMB, amb la detecció continua de les amenaces i vulnerabilitats dels actius, identificant funcionaments anòmals i activitats inusuals que derivin en problemes potencials, per tal de reforçar la seguretat dels sistemes identificats com a infraestructura crítica i/o servei essencial.

El monitoratge de sistemes i xarxes per a detectar el seu funcionament incorrecte i supervisar activitats inusuals resulta fonamental per a una identificació primerenca de potencials problemes En primer lloc, s'ha d'identificar la informació clau requerida, després recopilar-se aquesta informació en la xarxa local i seguidament transferir-la al següent nivell de xarxa disponible, i així successivament fins que arribi al sistema de gestió d'esdeveniments i informació de seguretat SIEM on es sotmetrà a anàlisi per a establir les mesures adequades a adoptar.

L'absència de monitoratge de les xarxes industrials suposa un al·licient per als atacants a l'hora d'atacar un sistema. Si un atacant aconsegueix accés a aquesta xarxa és necessari tenir un correcte monitoratge que permeti una detecció precoç que limiti els danys ocasionats. La implementació d'una sonda que doti de visibilitat sobre les comunicacions que es produeixen dins de les xarxes industrials i la detecció precoç d'anomalies i/o amenaces, així com la connexió de dispositius no autoritzats a la xarxa industrial, pot ajudar a reduir el nivell de risc. Per a aquesta mena de tasques existeixen solucions tecnològiques que funcionen com IDS i realitzen les accions en temps real:

- Detecció de trànsit maliciós o anomalies en l'entorn industrial
- Identificació de nous dispositius i alerta

Actualment ja es disposa d'aquesta eina de monitorització industrial, i es vol ampliar per incloure 2 sistemes més.

2. Abast del Servei

L'abast dels serveis tècnics objecte de la present licitació són:

- De producte
- De serveis professionals

2.1. De producte

Una solució de monitoratge industrial en temps real que permeti detectar i alertar de l'estat dels SCI. Aquesta solució haurà de realitzar anàlisi de tràfic de manera passiva i tenir capacitat de fer les següents tasques en les xarxes de la companyia:

- Solució Full-stack: Solució integral del mateix fabricant, que consta de Hardware, S.O. i aplicatiu
- Descobriment i inventariat d'actius
- Identificació de protocols
- Identificació dels fluxos de comunicació i disponibilitat de la xarxa
- Identificació de les vulnerabilitats existents en els actius desplegats, així com la situació d'aquestes
- Detecció de trànsit maliciós i anomalies en l'entorn industrial
- Anàlisi de riscos i vectors d'entrada
- Detecció d'amenaces avançades que siguin específiques per a xarxes industrials
- Estat de salut i rendiment dels sistemes

- Asset Intelligence: disponibilitat d'enriquir la informació dels Assets descoberts, així com el seu comportament sense necessitat d'aprendre'l
- Capacitat d'extreure els valors de les variables de procés
- Capacitat d'utilitzar els valors de les variables de procés en la generació de la seva baseline de comportament
- Capacitat de detecció d'anomalies
- Capacitat de detecció d'amenaces, almenys de les següents deteccions front amenaces conegudes:
    - Packet rules
    - YARA rules
    - Indicadors STIX

L'equipament haurà de ser on-premise, garantint la no sortida de dades de la organització, derivat de que els sistemes operacionals actualment estan aïllats del exterior.

A incloure:

- Equipament hardware i cablejat necessari per disposar/habilitar la connexió als punts a monitoritzar dels sistemes operacionals de FMB que s'indiquen com a Annexe.
- Sondes físiques on-premise Guardian Nozomi Network per als 2 sistemes operacionals, detallat al Annexe.
- Subministrament de llicències Nozomi Networks, incloent dos anys de subscripció i suport tècnic del fabricant.
- En cas de requerir una solució NPB, aquesta haurà de ser Gigamon, al estar inclòs en el catàleg del CNPIC (CCN STIC 105) amb categoria alta, complint amb l'Esquema Nacional de Seguretat (ENS) i es considera acceptable per ser utilitzada en entitats públiques subjectes al compliment del ENS.
- Subministrament de llicències Gigamon, incloent dos anys de subscripció i suport tècnic del fabricant.

Es requisit de la solució, que aquesta **ha de garantir la seva escalabilitat**, en previsió d'incloure més sistemes operacionals a monitoritzar en següents fases.

Ha de garantir el protocol MOXA sobre UDP.

Per efectuar el llicenciament, s'haurà de tenir en compte que el sistema no disposa de connexió a internet.

2.2. De serveis professionals

- Instal·lació i posada en marxa de la solució i implementació
- Suport tècnic del fabricant
- Formació
- Servei d'acompanyament o millora de la plataforma:
    - Suport tècnic L2 8x5
    - Servei evolutiu de l'aplicació amb actualització de versions
    - Bossa d'hores per un fine tuning de la plataforma

3. Obligacions de l'Adjudicatari

És responsabilitat del Adjudicatari, la realització de la totalitat de les tasques aportant els mitjans tècnics i humans necessaris per mantenir la plataforma de monitorització industrial operativa per acomplir la seva funció i proporcionar els serveis descrits al capítol 2, Abast del Servei, durant la vigència del contracte, amb els nivells descrits a continuació:

3.1 Instal·lació i posada en marxa de la solució i implementació

- Anàlisi, disseny i configuració del producte per:
    - 2 sistemes operacionals, que s'indiquen com a Annexe
    - Sistemes independents entre si
    - Garantir la no afectació a les comunicacions del propi sistema
    - Garantir la escalabilitat de la plataforma de monitorització de sistemes operacionals

- Implementació/desplegament de la solució en TMB (requereix part de l'activitat en mode presencial):
    - Configuració inicial de les sondes, incloent la instal·lació / actualització del firmware, configuració de la xarxa, etc.
    - Instal·lació dels equips als CPDs
    - Integració de les sondes a la consola de gestió de la plataforma de FMB
    - Configuració inicial de la lògica de seguretat dels equips
    - Activació mode aprenentatge
    - Activació mode producció
    - Acreditació del desplegament per part del fabricant

- Posada en marxa de forma escalonada per garantir la continuïtat del negoci, tractant-se de sistemes crítics

3.2 Suport tècnic llicències Nozomi

El suport de 2 anys que està inclòs en la compra de llicències software Nozomi Networks:

- Suport tècnic per resolució de dubtes i consultes
- Accés base de dades de coneixement, manuals d'usuari i documentació tècnica
- Manteniment software: Descàrrega de darreres versions de software amb millores, correcció d'errors i pegats de seguretat
- Manteniment hardware: Substitució d'equips defectuosos
- SLA:
    - RMA: 2 business day
    - Temps de resposta per incidències crítiques / altes / baixes: 1h / 4h / 12h

Previst activar durant la fase d'implementació.

En cas de requerir solució NPB, també s'inclourà el suport tècnic de llicències Gigamon amb les mateixes condicions.

3.3 Formació

Curs de 16hores en format online, on s'explicaren conceptes fonamentals per operar amb les sondes, a més de realitzar tallers pràctics.

3.4 Servei d'acompanyament o millora de la plataforma:

- Suport tècnic L2 8x5
- Servei evolutiu de l'aplicació amb actualització de versions
- Bossa d'hores per la realització d'un fine tuning de la plataforma

3.4.1 Suport tècnic L2 8x5

El servei per 2 anys des de la formalització de la implementació de la plataforma.

Inclou:

- Suport tècnic de nivell 2 (Integrador / Adjudicatari) de la plataforma de monitorització:
    - En horari d'atenció 8x5
    - Idioma castellà / català
    - SLA: temps de resposta 1h
- Escalat a suport tècnic de nivell 3 (fabricant) en cas necessari
- Punt de contacte, qui gestionarà i resoldrà les peticions de TMB, contactant amb fabricants en cas necessari
- Revisió periòdica per assegurar el funcionament òptim de la plataforma
- Resolució d'incidències i apertura de casos a fabricant, incloent manteniment hardware RMA i software
- Execució d'accions programades sobre els equips per a la instal·lació de noves versions de firmware o actualitzacions

3.4.2 Servei evolutiu de l'aplicació amb actualització de versions

Aquest servei compren l'actualització de la versió de la plataforma amb les recomanacions del fabricant Nozomi.

3.4.3 Bossa d'hores per fine tuning de la plataforma

Aquest servei compren una bossa de 250 hores en un període d'1 any per tal de realitzar un fine tuning de la plataforma de monitorització.

Inclou:

- Creació d'usuaris amb control d'accés basat en rols (perfil seguretat, perfil mantenidor, perfil tècnic sistema operacional, etc.)

- Revisió proactiva de la configuració per adaptar-la a les necessitats de FMB
- Personalització de la plataforma. Generació de Built-in reports i dashboards sobre la plataforma, segons capacitat de la mateixa
- Resolució de dubtes sobre el funcionament de la plataforma
- Revisió de les alertes: assessorament, suport en la interpretació
- Definició de la tipologia de logs a recollir de cada font de dades (activitat de dispositius, detecció d'errors, Health checking rendiment del dispositiu, etc.)
- Definició de generació d'alertes personalitzades, per exemple, no comunicació de node, etc.
- Processament d'esdeveniments: Definir casos d'ús específics per a aquests sistemes i que generin alertes quan un comportament maliciós ocorri en l'entorn amb la finalitat d'enviar-ho al SIEM corporatiu (Splunk)
- Integració amb altres eines de seguretat (SIEM / SOC) amb l'objectiu d'establir mètriques de detecció i resposta a possibles incidents de seguretat que siguin detectats
- Suport del fabricant per resolució de tasques complexes
- Anàlisi de logs per detectar i corregir problemes de funcionament o generar propostes de millora en funció del tràfic detectat

L'Adjudicatari a més a més indicarà a l'oferta el preu hora addicional a aquesta bossa per poder ampliar aquest nombre en cas que fos necessari.

3.5 Altres Obligacions de l'Adjudicatari

A part de la realització de les tasques necessàries descrites en els punts anteriors també són obligacions de l'Adjudicatari:

- Formació i capacitació del personal del seu personal assignat a la realització d' aquestes tasques.

  El personal haurà de disposar de la formació tècnica adequada per les tasques específiques del lloc de treball.

  Tota la formació tècnica necessària serà impartida per l'Adjudicatari.

  L'Adjudicatari facilitarà a tot el seu personal la formació necessària en els riscos laborals propis per a la execució de les diferents tasques en la xarxa de Metro.

  L'Adjudicatari haurà de disposar de les següents certificacions:

  - Acreditació o declaració responsable d'estar en procés d'acreditació a l'ENS
  - NNCE (Nozomi Networks Certified Engineer)
  - Certificació ISA/IEC 62443 Cybersecuriy Fundamentals Specialist
  - Experiència demostrable en treballs relacionats amb l'aplicació (total o parcial) pràctica de criteris i recomanacions sobre Seguretat en Sistemes de Control i Automatització Industrial emanats per: INCIBE i CCN
  - Experiència demostrable en consultories i oficines tècniques en Infraestructures Crítiques i entorns industrials (OT)
  - Experiència en projectes similars, demostrant haver realitzat, durant els últims cinc anys 5 o més, projectes en l'àmbit de tecnologies de l'operació. Aquests projectes han d'estar basats en els estàndards industrials IEC 62443 i/o TS 50701.
  - Mínim 2 tècnics en plantilla, certificats en la solució Nozomi Networks, i amb experiència amb el producte. Caldrà demostrar-ho amb els corresponents certificats emesos pel fabricant i el Currículum Vitae que demostri experiència amb altres instal·lacions.

El personal assignat al projecte haurà de disposar de les acreditacions professionals adients per demostrar la seva experiència.

- Vigilància de l'Obsolescència dels equips i components dels sistemes que conformen la plataforma, comunicant a TMB anticipadament qualsevol amenaça per disponibilitat de components del sistema que pugui esdevenir.

- Vigilància de la ciberseguretat: Acompliment de la política de Seguretat de sistemes tecnològics de TMB i el cos normatiu derivat d'aquestes. Suport i execució de les tasques de ciberseguretat necessàries per vetllar per la seguretat.

- El desenvolupament dels treballs ha de garantir que no sigui intrusiu, per tal de no comprometre la continuïtat del negoci, tractant-se de sistemes crítics.

- Evitar en la realització d'aquestes tasques qualsevol impacte sobre la seguretat i salut de les persones i del medi ambient.

No s'admetran càrrecs que no estiguin inclosos en el preu de la oferta referents a desplaçaments, dietes, ni allotjament, en el cas de requerir tasques presencials.

3.6 Seguretat i Confidencialitat

L'Adjudicatari s'obliga a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment de l'actual servei, i a subministrar-la solament al personal autoritzat per TMB.

L'Adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal sota el seu càrrec. Tan

mateix, s'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.

Un cop finalitzat el present servei, l'Adjudicatari 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'Adjudicatari ha de complir amb la Política y Cos Normatiu de Seguretat Tecnològica i de la Informació de TMB.

3.7 Compliment de la llei Orgànica de Protecció de Dades de Caràcter Personal

L'Adjudicatari 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 en el que fa referència 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.

4. Obligacions de TMB

TMB realitzarà les activitats operacionals següents relacionades amb el servei:

- Programació de les peticions de treballs
- Informació a l'Adjudicatari en cas de necessitats de canvis a la programació
- Les peticions i permisos necessaris per a la realització de les activitats

5. Comunicacions entre les parts

L'Adjudicatari facilitarà els noms, els telèfons i correus electrònics de:

1. Gestor del Contracte: és el responsable de la realització de les tasques del contracte i interlocutor en temes administratius
2. Supervisor Coordinador del Contracte: és el responsable del seguiment i supervisió de les activitats descrites al contracte.

Per la seva banda, TMB facilitarà a l'Adjudicatari una llista d'interlocutors i els seus telèfons de contacte.

5.1 Seguiment del contracte

Es mantindran reunions periòdiques, a acordar, per avaluar el funcionament de la plataforma, realitzar propostes de millora, implementacions de millores i seguiment de les implementacions.

6. Annexe - Sistemes operacionals FMB

Es tracta de 2 sistemes independents i amb xarxes aïllades (sense visibilitat entre ells), amb redundància física i lògica:

SISTEMA 1				
EQUIPOS Centro Principal	BOCAS switch	Requiere TAP	Velocidad puerto swicth	Activos (@IPs)
Router 1 - IV	2	SI	Gigabit Ethernet	Estimativo 1000 activos
Switch 1 - IV	2	SI	Gigabit Ethernet	
Router 2 - I/II	4	SI	Gigabit Ethernet	
Switch 2- I/II	2	SI	Gigabit Ethernet	
EQUIPOS Centro Secundario	BOCAS switch	Requiere TAP	Velocidad puerto swicth	
Router 1 - IV	2	SI	Gigabit Ethernet	
Switch 1 - IV	1	SI	Gigabit Ethernet	
Router 2- I/II	4	SI	Gigabit Ethernet	
Switch 2- I/II	1	SI	Gigabit Ethernet	
SISTEMA 2				
EQUIPOS Centro Principal	BOCAS switch	Requiere TAP	Velocidad puerto swicth	Activos (@IPs)
Switch ToR	4	NO	10Gbps	3089 Opción 5000 activos
Switch OOB	2	NO	10Gbps	
EQUIPOS Centro Secundario	BOCAS switch	Requiere TAP	Velocidad puerto swicth	
Switch ToR	2	NO	10Gbps	
Switch OOB	1	NO	10Gbps	

L'ampliació de la plataforma de monitorització per aquests sistemes operacionals ha de disposar d'una sonda per sistema i solució TAP / NPB Gigamon pel sistema 1:

Sistema OT	Fabricant	Equipament proposat (per centre)
1	Nozomi	1 sonda Guardian NS1 250 de 7 ports 7x1000 BASE-T
	Gigamon	Sistema NPB Centre principal: '- 1 servidor gestió GigaVUE-FM, manage up to 5 Physical Visibility Fabric Nodes, mod. GFM-FM005 - 1 chasis G-TAP M Series 1/2 RU chassis. Supports up to 3 M Series TAP modules. TAA Compliant, mod. TAP-M100T - 1 equip TAP G-TAP M Series 1/10/25/40/100Gb TAP module, 70/30 Singlemode, 1310/1550 nm, taps 6 links, requires TAP-M100T or TAP-M200T chassis. TAA Compliant, mod. TAP-M273T - 2 equip TAP G-TAP M Series 1/10/25/40/100Gb TAP module, 70/30 Singlemode, 1310/1550 nm LC, taps 2 1/10/25/40/100Gb links, requires TAP-M100T or TAP-M200 chassis. TAA Compliant, mod. TAP-M273LT - 1 equip GigaVUE-TA25 node, 8 40G/100G QSFP28 cages + 48 1G/10G/25G SFP28 cages, 2 power supplies, 4 fan trays, AC power, 24 10G/25G ports enabled, mod. GVS-TAX21A - 2 transceptors 1G SFP, Copper, UTP with RJ45 interface. Not TAA Compliant, mod. SFP-01 - 20 transceptors 1G SFP, Singlemode LX. Not TAA Compliant, mod. SFP-503 Centre secundari: - 1 chasis G-TAP M Series 1/2 RU chassis. Supports up to 3 M Series TAP modules. TAA Compliant, mod. TAP-M100T - 2 equip TAP G-TAP M Series 1/10/25/40/100Gb TAP module, 70/30 Singlemode, 1310/1550 nm LC, taps 2 1/10/25/40/100Gb links, requires TAP-M100T or TAP-M200 chassis. TAA Compliant, mod. TAP-M273LT - 1 equip GigaVUE-HC1 chassis, 12 1G/10G cages, 4 10/100/1000M Copper, fan tray, 2 power
2	Nozomi	1 Sonda Guardian NS20 750 de 9 ports 9x1000 BASE-T i 4xSFP