SEGON RECULL DUBTES REBUTS PER CORREU ELECTRÒNIC

1. **Pulse Secure PSA5000 S'indica que 900 usuaris concurrents, però quin tipus de llicència: Consec, Polsec, Essentials+? Perpètues o llicenciades?**

   Són llicències perpetues. Estan formades per 3 packs. Un pack de 200, un pack de 200 i un de 500. D'aquest element s'ha de contemplar el manteniment del hardware.

2. **Quants dispositius (punts finals, usuaris, servidors, dispositius de seguretat, encaminadors, commutadors) teniu inscrits a ELK, QRadar i Alien Vault?**

   Tant a nivell de SIEM com de l'ELK hi ha de l'ordre de 12 fonts respectivament. Ambdós casos actualment es troben en procés de noves incorporacions de fonts.

3. **Podeu proporcionar una arquitectura de disseny d'alt nivell de la solució que tingueu desplegada relacionada amb QRadar / ELK / Alien Vault?**

   Es tracten d'arquitectures stàndards. A nivell de SIEM QRADAR hi ha dos appliences físics en HA i un AppNode per recolectar logs. A nivell de Alien Vault hi ha un USM Server, dos sensors (un a cada cpd) i un logger. A nivell de ELK hi ha 6 servidors amb llicència Gold.

4. **Hores d'ara, estan aquestes plataformes monitorades per un sol equip or podríeu compartir com està distribuïda actualment aquesta monitorització?**

   A dia d'avui Qradar es troba monitoritzat per un equip i Alien Vault i ELK per l'actual SOC.

5. **Totes aquestes 3 plataformes QRadar, ELK i Alien Vault s'han de conservar durant tota la durada del contracte o els licitadors podríem proposar millores i reducció de costos respecte a aquestes plataformes, i per tant la cancel·lació del servei d'algunes plataformes?**

   A nivell d'AV, s'haurà de mantenir fins que l'adjudicatari hagi finalitzat la posta a punt i la configuració del SIEM QRADAR, així com haver finalitzat la migració dels casos d'ús definits en AV cap a QRADAR. Tal i com s'especifica al punt 4.1.5.1. Posta a punt i configuració SIEM i ELK pels objectius del SOC del PPT.

6. **Quina eina de ticketing esteu utilitzant hores d'ara? Quines opcions hi han disponibles per a la integració?**

   A dia d'avui les eines de ticketing corporatives més utilitzades son Easyvista, HP Service Manager i Jira, entre d'altres

7. **Disposeu d'alguna plataforma SOAR?**

   No disposem.

8. **Quin tipus de solució d'antivirus disposeu hores d'ara i de quin proveïdor?**
   Disposem d'antivirus de fabricants líders de mercat tant per la part d'estació de treball com de servidors

9. **Feu servir alguna solució EDR o XDR? De quin proveïdor?**

   No disposem.

10. **Capítol 9.2. pàgina 121: "En qualsevol moment durant l'execució del contracte, l'IMI es reserva el dret de sol·licitar a l'adjudicatari la realització de la prestació del servei de forma presencial en les instal·lacions de l'IMI i en els percentatge dels recursos que consideri. L'adjudicatari s'ha d'adaptar a aquests canvis consensuats en el termini acordat " Dubtes concrets:**

    - **Quin serà el període de notificació?**

      Els que l'IMI consideri oportuns per necessitats del servei.

    - **Quin tipus d'esdeveniments desencadenaria aquesta possibilitat de treball presencialment a l'IMI?**

      El que l'IMI consideri oportú per necessitats del servei.

    - **Teniu alguna estimació de quantes vegades podria ser necessari aquest desplaçament de treball a les vostres instal·lacions ? (si les condicions del COVID ho permeten)**

      A dia d'avui no disposem d'aquesta estimació, però arribat el moment podríem requerir presencialitat 100%.

    - **Quants dies calculeu que ha de treballar una persona des de les vostres instal·lacions?**

      El que l'IMI consideri oportú per necessitats del servei (des d'un dia puntual, fins a cinc dies per setmana).

11. **Referent a l'escaneig de vulnerabilitats en compliment amb els Approved Scanning Vendors (ASV) de la norma PCI Data Security Standard o la certificació FedRAMP, quantes IPs espereu escanejar mensualment?**

    Tal i com s'indica a l'apartat 4.1.1.2 Auditories tècniques de seguretat i hacking ètic es demanen escanejos periòdics de vulnerabilitats sobre 800 IPs públiques i 600 Ips internes.

12. **Entenem que els recursos humans esmentats al plec de condicions NO s'han de dedicar en exclusivitat a l'IMI i per tant es poden pertànyer a organitzacions compartides del licitador. Correcte?**

    L'equip de treball s'ha d'organitzar tenint en compte el número mínim de FTEs total i el número mínim de FTEs per perfil definits al PPT.

13. **Podeu explicitar les solucions que hores d'ara esteu utilitzant com a eines de gestió d'accessos i identitats, control d'accés a la xarxa i monitoratge de l'activitat de base de dades?.**

    No considerem que aquesta informació sigui rellevant explicitar-la.

14. **Confirmeu si us plau si NetFlow Analytics està actualment integrat a la solució SIEM actual?**

    De moment no.

15. **Capítol 4.1.2.1 Quan expresseu: "Ha d'incloure tant les alertes de seguretat generades pel SIEM així com les alertes i/o incidències rebudes pels altres canals que ha de proporcionar l'adjudicatari". Podeu detallar a quins canals us esteu referint?**

    IOCs per exemple de fonts públiques o privades.

16. **Per als serveis SOC, podeu proporcionar detalls sobre quin tipus de gràfics configurables s'haurien de desenvolupar? Quin tipus d'informació s'hauria d'incloure a la interfície per IMI i fins a quin punt us cal aprofundir en els detalls? Estaríeu disposar a utilitzar aquesta informació en anglès ?**

    Els gràfics necessaris per proporcionar el servei demandat. El català és la llengua pròpia de l'Ajuntament de Barcelona, com a tal, ha d'ésser la llengua d'ús normal i general en les seves activitats, per tant, no estaríem disposats que fos en anglès.

17. **Al document PCAP, pag. 21 es descriu el que s'ha d'incloure en Sobre C, en concret es requereix: Així mateix el sobre electrònic C haurà de contenir l'acreditació de la part de solvència tècnica en els termes establerts a la clàusula 7a d'aquest plec, i conforme la plantilla de l'empresa licitadora està formada per un mínim de professionals experts amb les següents certificacions (disposar a la plantilla d'un mínim de professional amb les següents certificacions*):**

    - **És correcte on s'indica clàusula 7A que és la solvència financera? o ha d´indicar clàusula 7B com solvència tècnica ?? Quina documentació s'ha d'aportar?**

      El paràgraf assenyalat fa referència a la clàusula setena del PCAP (7a) que engloba tant l'apartat A relatiu a la solvència financera com el B relatiu a la solvència tècnica. En aquest sentit quan ens referim a l'acreditació de la part de solvència tècnica en els termes establerts a la clàusula 7a d'aquest plec, al·ludeix en concret a l'apartat B de dita clàusula. S'haurà de lliurar una declaració responsable emesa pel representant legal de l'empresa en què es faci constar la relació concreta de cada perfil amb la corresponent identificació del nom i cognoms, especificació de la categoria professional, dades d'adscripció a l'empresa i certificació que declara disposar amb vigència actual adjuntant-se dita certificació.

- **Sobre els perfils professionals, s'entén que s'ha d'aportar les certificacions dels mateixos?**

  Tal i com s'ha assenyalat efectivament s'hauran d'aportar dins el sobre requerit les certificacions corresponents.

18. Quin és el CPD principal? CPD1?

A dia d'avui el CPD principal és el CPD1 tot i que hi ha previsió de moviment tal i com s'especifica al PPT apartat 4.2.1 Nus de comunicacions.

19. Quin és el secundari? CPD2 o CPD3?

El CPD secundari és el CPD2, que una vegada fet el moviment passarà a ser el principal.

20. Com estan connectats CPD i BDC? S'utilitza la connectivitat de l'IMI entre els centres per al suport a tots dos centres?

Tal i com s'especifica a l'apartat del PPT 4.2.1.1. Arquitectura del Nus la connectivitat entre ambdós CPD és proveïda per un altre contracte. L'adjudicatari haurà de proveir la solució necessària per complir amb els SLAs demanat.

21. És requisit tenir enllaç entre l'adjudicatari amb CPD i BDC? O queda a criteri de la solució?

L'adjudicatari haurà de proveir la solució necessària per complir amb els SLAs demanats.

22. Entenem que els items del inventari que no estan especificats els llicenciaments, només caldrà oferir el manteniment hardware?

S'ha de mantenir el hardware i mantenir el software associat del parc de l'inventari a excepció de:

- Palo Alto 5220. La seva renovació es farà a banda.
- Pulse: Només manteniment hardware.
- Fluke. Es troba EoS

23. Referent al document PCAP, Clàusula 7B (pag. 15), Solvència Técnica o Professional s'indica:
De les certificacions mínimes que l'empresa ha de declarar disposar, ***en queden excloses les pròpies certificacions del personal que es posarà a disposició del contracte directament****, per tal de tenir major transparència amb les valoracions que es puguin fer de conformitat amb els criteris d'adjudicació d'aquest plec i allò establert en el plec de prescripcions tècniques.*

Això vol dir que els recursos que es dedicaran a aquest contracte no son vàlides les seves certificacions a aportar per cobrir la solvència tècnica???

Com a solvència tècnica mínima de l'empresa licitadora es requereix disposar del nombre mínim de perfils professionals certificats; els quals efectivament no es podran proposar per avaluar-se

com a criteri de millora de la capacitació de l'equip professional a adscriure a l'execució del contracte per sobre de les certificacions mínimes requerides en l'apartat 8.2.1 i 8.2.2 del PPT.

24. **Els certificats que s'aporten a aquesta solvència tècnica es consideren recursos de backup del servei?**

El servei sempre ha de quedar cobert amb tècnics del mateix perfil professional. Per aquest motiu els recursos de backup han de tenir el mateix nivell de certificacions que els tècnics dedicats però en cap cas es complementaran les certificacions.

25. **A l'inventari d'equips on s'ha de proposar la renovació de manteniment de garanties de fabricat, l'equip Infoblox TE-820 es troba End of Support per part del fabricant. Quina solució es vol prendre per donar Support?**

Els Infoblox han entrat en End of Support i no disposen de garantia de fabricant. En cas d'avaria l'adjudicatari haurà de substituir-los per uns iguals/equivalents/superiors de característiques similars amb el seu corresponent llicenciament DDI per incloure'l com a membre del Grid.

26. **Al document PPT, capítol 4.2.4.4. Servidors i Cabines d'OSAT, es demana renovació de manteniment de les llicències VMWare Essential Plus. Ens podeu facilitar els números de sèrie ?**

4160N-6A3E1-P8K9E-08CK6-9DUM1 H5017-4NL9M-28K8J-0Y12M-3HR71

27. **A l'inventari els equips de Fortinet (F60) tenen el mateix serial number, podeu proporcionar el serial que falta?**

FWF60D4615018068

28. **En el document PPT, apartar 4.2.3.2. Eina que doni visibilitat dels entorns cloud i kubernetes, per dimensionar l'eina necessitaríem saber quants nodes de Kubernetes tenim.**

Es requereix com a mínim 100 assets.