

En relación con el expediente en tramitación denominado “**SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES**”, a adjudicar por procedimiento abierto mediante pluralidad de criterios, nº de expediente **ECON/000237/2023**, se han recibido las siguientes **consultas** referidas al PLIEGO DE CLÁUSULAS ADMINISTRATIVAS y de PRESCRIPCIONES TÉCNICAS por parte de empresas interesadas en la licitación. Estas preguntas se transcriben tal y como han sido redactadas por el licitador, y son las siguientes:

1. Respecto al momento de presentación del “**ANEXO 10.4: MODELO DE CURRÍCULUM VITAE**” del PPT, tanto en el pie de página del modelo como en la pag 71 del PPT se indica que los licitadores propuestos como adjudicatarios aportarán CV según este modelo. No obstante, en el PCAP, en la página 22, “**APARTADO 9. DOCUMENTACIÓN TÉCNICA A PRESENTAR**”, se indica que los licitadores deberán aportar el modelo en el sobre 2º. ¿Nos podrían aclarar si el modelo se presenta en esta fase o únicamente en el momento de ser propuestos adjudicatarios?

Respuesta:

Respondido en la publicación de resolución de corrección de errores del Pliego de Cláusulas Administrativas (PCAP).

2. Referido al lote 4, en el pliego de cláusulas administrativas hay una pequeña contradicción con lo que hay que incluir en los sobres 2 y 3.

En la página 22 se indica “**DOCUMENTACIÓN TÉCNICA A PRESENTAR EN RELACIÓN CON LOS CRITERIOS OBJETIVOS DE ADJUDICACIÓN DEL CONTRATO. En el Sobre Nº 2 deberán aportar, debidamente cumplimentado y firmado, el Documento que se adjunta como ANEXO V al presente pliego, en relación con los Criterios de Adjudicación evaluables de forma automática por aplicación de fórmulas del lote/s a los que presenten oferta.**”

En la página 24 se indica “**C) SOBRE Nº 3 – PROPOSICIÓN ECONÓMICA Y DOCUMENTACIÓN RELATIVA A LOS CRITERIOS DE ADJUDICACIÓN EVALUABLES DE FORMA AUTOMÁTICA POR APLICACIÓN DE FÓRMULAS. La documentación que se especifica en la Cláusula 1 Apartado 9 al presente pliego, en orden a la aplicación de los demás criterios de adjudicación, distintos del precio, valorables de forma automática por aplicación de fórmulas que se presentará redactada conforme a los modelos fijados en el Anexo V de este pliego.**”

Indicar si el Anexo V hay que incluirlo en el sobre 2 ó 3.

Respuesta:

Respondido en la publicación de resolución de corrección de errores del PCAP.

3. Para cumplir la solvencia técnica de los lotes 3 y 4, ¿es viable aportar referencias de proyectos y de CV internacionales?

Respuesta:

Se pueden aportar referencias de proyectos internacionales siempre que cumplan con las condiciones establecidas en el PCAP.

4. En los requisitos de solvencia técnica lote 1 se requiere “*Se exigirá al licitador propuesto como adjudicatario pertenecer a la Red Nacional de Soc creada por el Centro Criptológico Nacional, en adelante CCN-CERT y ser miembro de FIRST*”.

Esta solvencia ¿puede ser completada con medios externos?

Respuesta:

Se deberá tener en cuenta lo establecido en el Artículo 75 de la LCSP.

5. En el apartado 4.1.2.2.2 Análisis avanzado de tráfico – NDR se indica lo siguiente:

“La solución analizará el tráfico este-oeste cursado tanto en los dos CPD’s de Madrid Digital como en los dos CPD’s de la Consejería de Sanidad.

El dimensionamiento del equipamiento a instalar en los CPD’s (sensores) será responsabilidad del adjudicatario, estimándose que el tráfico generado en cada CPD a analizar será como mínimo de 20 Gbit/seg.”

En nuestra experiencia hemos visto que en ocasiones se calcula el Throughput según el ancho de banda de las conexiones, cuando en realidad el Throughput puede ser bastante menor. Por tanto, solicitamos amablemente que nos informen sobre el total de Throughput real sobre la red de Madrid Digital. Como sugerencia se apunta a que si tienen NetFlow activado, este les puede dar una indicación, o si tienen packet brokers, a través de ellos pueden ver el Throughput. El afinar este dato a la situación real puede permitir optimizar la respuesta a la licitación.

Respuesta:

El throughput recogido en el Pliego de Prescripciones Técnicas (PPT) es una estimación basada en análisis previos realizados por una muestra de fabricantes de este tipo de soluciones; por tanto, no es un dato de medición real ya que gran parte del tráfico este-oeste está contenido en los hosts físicos que dan soporte a nuestra infraestructura de máquinas virtuales. En consecuencia, el ancho de banda estimado de 20 Gbit/seg incluye tráfico entre máquinas físicas y el tráfico interno en dichos hosts. El ancho de banda disponible para las máquinas en los CPD’s supera con creces el dato facilitado.

En todo caso, el dimensionamiento de la solución deberá realizarse como mínimo en base al ancho de banda especificado y número de activos a proteger.

6. En el lote 4, en el apartado 7.2.1 del Pliego de prescripciones Técnicas, el número de horas exigidas por año incluye vacaciones. En tal caso, se entiende que habría que cubrir las ausencias de los perfiles propuestos con otras personas adicionales que cumplan con el perfil, es decir, que el equipo de trabajo mínimo superaría las dos personas a tiempo completo, ya que se necesita a un suplente para el periodo vacacional. Por favor, ¿pueden confirmar si es así?, ya que ello afecta a la configuración del equipo.

Respuesta:

Efectivamente, está presupuestado el periodo vacacional, por lo que deben cubrirse las ausencias.

7. En el punto 10.3 PLATAFORMA SIEM ACTUAL DE MADRID DIGITAL, se mencionan sondas IDS, además de las sondas del CCN-CERT ¿pueden detallar qué sondas son, si son equipos con sw comercial? ¿o si son elementos basados en sistemas OpenSource, indicar cuál?

Respuesta:

Las sondas IDS instaladas son Suricata para el entorno de CPD’s de Madrid Digital y AlienVault para el entorno de CPD’s de Sanidad, Hospital 12 Octubre, centros hospitalarios y centros sanitarios.

8. En relación con el servicio Threat Hunting solicitado en el lote 1, se indica en la página 27 del PPT que *“No se requiere adscripción exclusiva de este recurso”*. Sin embargo, en la página 42, en la descripción del perfil de Hunter, se indica *“dedicación al proyecto 100%”*.

¿Se contradicen estas afirmaciones? ¿Cuál sería la correcta?

Respuesta:

Se requiere un recurso dedicado 100% a Madrid Digital en horario 8x5 para la realización de actividades de Hunting. Este recurso no tiene por qué ser exclusivo para este contrato, como se requiere para otros perfiles, sino que puede ser ofrecido por un equipo de recursos con el perfil técnico requerido. Se espera que cada licitador defina la mejor forma de organizar este servicio.

9. En el lote 1 del expediente ECON/000237/2023 Servicios gestionados de ciberseguridad de madrid digital - 4 lotes en el pliego de prescripciones técnicas nos ha surgido una duda. En el PCAP pag 22 habla del sobre nº 2 se debe aportar el ANEXO V cumplimentado. Pero en el ANEXO V se indica que se aportar en el sobre 3. ¿La pregunta es donde aportar el ANEXO V en el sobre 2 o en el sobre 3?

¿Otra pregunta, es obligatorio en esta fase de presentación de oferta incluir los CVs del equipo técnico o se deben entregar cuando se es ya adjudicatario? Parece que en esta fase de presentación de oferta hay que entregar los CV sin DNI, ni nombre y apellidos. Luego en la fase de adjudicación, el adjudicatario final tendrá que incluirlos rellenos con los datos de DNI, nombre y apellidos cuando les sea requeridos. ¿Esto es así?

Respuesta:

Respecto a la primera pregunta, respondida en la publicación de resolución de corrección de errores del PCAP.

En cuanto a la segunda pregunta, consultar también la resolución de corrección de errores del PCAP, los CVs los presenta el licitador propuesto como adjudicatario, según se indica en la cláusula 15 del PCAP.

10. Identificación de amenazas externas y vigilancia digital

¿Podrían proporcionar más información sobre la volumetría aproximada cursada actualmente?. Número de marcas, dominios, direcciones IP o número de personas de interés a vigilar.

Respuesta:

La volumetría actual del servicio es la siguiente:

- Número de marcas: 2 marcas principales: Comunidad de Madrid y Madrid Digital, Agencia para la Administración Digital de la Comunidad de Madrid.
- Dominios y direcciones IP: 10
- Personas de interés: 0

11. Los pagos por facturación trimestral de los servicios de cuota fija (prevención, monitorización/detección, análisis/respuesta, soporte a la gestión, operación y procesos), ¿se harán a trimestre vencido?

Respuesta:

En la *cláusula 1 Apartado 22 REGIMEN DE PAGOS* del PCAP se indica que el pago de estos servicios: *se efectuará mediante certificaciones trimestrales, contra factura conformada y previa aceptación por la Subdirección General encargada de la inspección del servicio.*

En consecuencia, el pago de los servicios se realiza trimestralmente después de que finalice el trimestre de prestación del servicio que se tenga que facturar por la empresa, previa certificación y aceptación por Madrid Digital.

12. Los pagos por facturación semestral de los servicios de cuota fija (suscripción de herramientas), ¿se harán al inicio de cada semestre, o a semestre vencido?

Respuesta:

En la *cláusula 1. Apartado 22 REGIMEN DE PAGOS* del PCAP se indica que el pago de... *las suscripciones de herramientas incluidas en el lote 1 que se efectuarán mediante certificaciones **semestrales**.*

En consecuencia, el pago de estas licencias se hará semestralmente, y se abonará en el momento que se certifique que las licencias están a disposición de Madrid Digital.

13. Sería posible saber los siguientes datos para poder dimensionar correctamente el servicio de vigilancia digital, ya que los mismos no figuran ni en el PPT ni en el PCAP.

Nº de empleados/usuarios de Madrid Digital

Nº de dominios, palabras clave e IPs a monitorizar

Nº de CPEs a monitorizar

Respuesta:

La volumetría actual del servicio es la siguiente:

- Dominios y direcciones IP: 10
- Número de CPEs: 5 (a nivel de “vendor” según la estructura de CPE del NIST)

Para el dimensionamiento del servicio de Vigilancia Digital no se requiere el número de empleados/usuarios a los que presta servicio Madrid Digital.

14. En la CLÁUSULA 1.- CARACTERÍSTICAS DEL CONTRATO, APARTADO 29. PLAZO DE GARANTÍA se indica lo siguiente: "Se establece un plazo de garantía de DOCE MESES, cuyo cómputo se iniciará desde la fecha de recepción o conformidad de los trabajos. Hasta que no tenga lugar la finalización del periodo de garantía, el adjudicatario responderá de la correcta realización de los trabajos contratados y de los defectos que en ellos hubiera, sin que sea eximente ni le otorgue derecho alguno la circunstancia de que los representantes de la Agencia los hayan examinado o reconocido durante su ejecución o aceptado en comprobaciones, valoraciones, certificaciones o recepciones parciales e incluso en la recepción total del trabajo, en previsión de la posible existencia de vicios o fallos ocultos en los trabajos ejecutados. A tal efecto, el contratista deberá atender las incidencias y consultas que se pudieran producir sobre el funcionamiento del producto (vía telefónica y por correo electrónico)." En relación con los productos de terceros reflejados en los pliegos (suministro de licencias o suscripciones de productos e infraestructura para el escaneo de vulnerabilidades, NDR y SIEM/SOAR entre otros) a aportar por el Contratista, Madrid Digital entiende que el Contratista no es el fabricante, sino que simplemente se encarga de su adquisición a los fabricantes para transmitirlos al cliente, de modo que Madrid Digital acepta que los productos y su entrega estarán sujetas a su disponibilidad y a los términos y condiciones del fabricante. Asimismo, Madrid Digital entiende que los productos del fabricante se entregan en el estado en el que se encuentran, sin más garantía que la del fabricante, quedando el Contratista exento de responsabilidad, sin tener obligación alguna de indemnización en relación con los citados productos de terceros, aceptando el cliente que el fabricante es el único responsable de los mismos, ¿correcto?

Respuesta:

El contratista asumirá la total responsabilidad de la ejecución del contrato frente a la Administración.

15. Respecto a las auditorías basadas en políticas configurables. ¿Cuáles serían los frameworks de vuestro interés (por ejemplo, CIS)?

Respuesta:

El framework de referencia de seguridad para el sector público en España es el indicado en el Esquema Nacional de Seguridad, en su anexo II.

16. ¿Podríais indicarnos el número (aproximado) de dispositivos y usuarios en su red? Para el servicio NDR, ¿es suficiente basarnos en 126.000 endpoints y 7.000 servidores? Adicionalmente, ¿esto incluye también los ubicados en otros CPDs? ¿Sería posible obtener más información de dispositivos amparada por un NDA (si fuera necesario)?

Respuesta:

Para la realización de la oferta, es suficiente basarse en los datos de dimensionamiento indicados en el apartado 4.1.2.2.2 del PPT, por tanto, no es necesario ampliar dicha información. Este dimensionamiento incluye los dos CPD's de Madrid Digital, los dos CPD's de la Consejería de Sanidad y el CPD principal de EducaMadrid.

17. Respecto al histórico de incidentes de seguridad, ¿podrías proporcionarnos algún detalle (como, por ejemplo, los sistemas / plataformas afectadas)?

Respuesta:

Por motivos de confidencialidad y de ciberseguridad no es posible revelar este tipo de información.

18. Se mencionan diferentes consejerías, organismos y marcas, lo que implica un compendio de diferentes segmentos y bloques de control y supervisión, lo que afecta a la arquitectura y dimensionado de la plataforma.
¿Podríais proporcionarnos una estimación de las dimensiones del despliegue (número de assets y la tipología (Servidores, Virtual Appliances, Network devices, etc.) por cada diferente unidad o entorno de operación)?
Adicionalmente, sobre los activos TIC (8.000), nos gustaría conocer cuántos activos están en Cloud para la solución CSPM. Necesitaríamos saber el número de activos a cubrir por la solución CSPM (y si están incluidos en la cuenta de los 8.000 activos).

Respuesta:

Madrid Digital da servicio a todas las consejerías de la Comunidad de Madrid mediante CPDs centralizados.

El dimensionamiento de los mismos queda reflejado en el punto 4.1.2.2.2 del PPT, siendo éste el siguiente:

- 126.0000 endpoints (PC's de usuario de sobremesa y portátiles).
- 4.000 servidores, alojados en los dos CPD's de Madrid Digital.
- 3.000 servidores alojados en los dos CPD's de la Consejería de Sanidad – SERMAS y en el CPD principal de EducaMadrid.

Madrid Digital está en proceso de despliegue de plataformas en nube, lo que supone actualmente menos activos gestionados que los presentes en sus CPDs. La solución deberá ser escalable en previsión de que los activos en nube vayan en aumento.

19. Para cada uno de dichos entornos o unidades existe un responsable diferente de IT/Seguridad? Implica esto generar notificaciones independientes a cada unidad, crear informes individualizados, realizar un seguimiento y gestión del ciclo de vida de vulnerabilidades de forma independiente con un scope acotado a dicho grupo?

Respuesta:

Las notificaciones, informes y/o seguimiento y gestión del ciclo de vida de vulnerabilidades, su alcance y contenido debe ser conforme con lo solicitado por cada uno de los servicios de ciberseguridad detallados en el PPT.

20. El número de Webs a analizar es un factor relevante para determinar el licenciamiento de la plataforma, se podría obtener una cantidad de WebApps y urls esperadas para ser analizadas, y también alguna expectativa de crecimiento en el número de ésta?

Respuesta:

Para el servicio de análisis de vulnerabilidades de seguridad de aplicaciones, que se realiza de forma manual por parte de los analistas de seguridad, se consensuará con estos analistas los objetivos a cumplir para cada uno de los análisis. Con carácter estimativo, se viene realizando, de media, un análisis web por semana pudiendo incrementarse la demanda en función de las necesidades que tenga en ese momento Madrid Digital.

21. Tenemos acceso a informes previos e información del servicio existente, incluyendo informes personalizados, volumetrías, vulnerabilidades existentes no resueltas?

Respuesta:

Por motivos de confidencialidad y de ciberseguridad no es posible revelar este tipo de información.

22. Respecto a la vigilancia digital, ¿podráis facilitarnos volumetrías respecto a los activos (dominios, marcas, IPs...), así como el inventario de los mismos?

Respuesta:

La volumetría actual del servicio es la siguiente:

- Número de marcas: 2 marcas principales: Comunidad de Madrid y Madrid Digital, Agencia para la Administración Digital de la Comunidad de Madrid.
- Dominios y direcciones IP: 10
- Personas de interés: 0
- Número de CPEs: 5 (a nivel de “vendor” según la estructura de CPE del NIST)

23. Anexo I Precios: Página 78: Teniendo en cuenta que hay ítems de facturación de diferente naturaleza, ¿el descuento general indicado en este Anexo I se aplicará a las tarifas de servicios profesionales y a todas las partidas de precios unitarios de cuota fija (tanto SIEM, NDR, ... como a servicios profesionales, cuota fija y variable)?

Respuesta:

Sí, el porcentaje general de baja se aplica a todos los conceptos facturables.

24. En el punto 2.3 del Apartado 6 de la cláusula I (Página 13) se pide Compromiso de adscripción, ¿este compromiso solo es para el Lote 1 o es para todos los lotes?

Respuesta:

Este compromiso de adscripción a la ejecución del contrato de medios personales y/o materiales, es para todos los lotes, para los 4 lotes.

25. En la plataforma Licit@ se indica que la “Propuesta económica será en un único archivo, formato PDF, firmado digitalmente, sin estar adjuntado dentro de un .zip e incluirá los datos de todos los lotes a los que se vaya a licitar”, ¿Esto quiere decir que unimos los Anexos I de todos los lotes a los que nos presentamos en un único pdf?

Respuesta:

Se pueden unir el Anexo I de todos los lotes en un único archivo con formato PDF.

26. En el apartado 4.1.1.4 Ciberejercicios, ¿Cuántos usuarios de Madrid Digital estarían incluidos en las simulaciones de ataque?

Respuesta:

660 usuarios, en previsión de crecimiento hasta unos 700.

27. En el apartado 4.1.1.4 Ciberejercicios, ¿Se tiene un estimado de cuántas simulaciones anuales se precisan?

Respuesta:

Se establece en dicho apartado un mínimo de un ciberejercicio anual.

28. En el apartado 4.1.1.1 ¿Cuál es la cantidad aproximada de targets (dominios públicos, IP públicas, consejerías, marcas, etc.) que incluirá el servicio?

Respuesta:

La volumetría actual del servicio es la siguiente:

- Número de marcas: 2 marcas principales: Comunidad de Madrid y Madrid Digital, Agencia para la Administración Digital de la Comunidad de Madrid.
- Dominios y direcciones IP: 10
- Personas de interés: 0
- Número de CPEs: 5 (a nivel de “vendor” según la estructura de CPE del NIST)

29. En el apartado 4.1.1.1 ¿Cuántas aplicaciones en “store” están dentro del alcance de los servicios?

Respuesta:

Actualmente, se dispone de 20 aplicaciones en “store”. Tal y como se menciona en el PPT, al inicio de la ejecución del contrato, Madrid Digital definirá en colaboración con el adjudicatario, la relación completa de activos a vigilar, pudiendo incrementarse este número en dicho momento.

30. En el apartado 4.1.5 ¿Cuántas personas hay en el personal técnico de Madrid Digital?

Respuesta:

El personal técnico susceptible de recibir la formación indicada en dicho apartado es aproximadamente 20 personas.

31. Pag 23: “Punto 17 PCAP Plazo total: El plazo de ejecución del presente contrato será de, 24 meses comprendidos entre 1 de julio de 2024 a 30 de junio de 2026.”

Respuesta:

El plazo de ejecución es de veinticuatro (24) meses. Posteriormente en la adjudicación del contrato se reajustará fecha de inicio, y demás aspectos relacionados.

32. Pag 15: Criterio 04: Por favor aclarar a que refieren cuando mencionan “revisión de la explotabilidad de vulnerabilidades identificadas”

Respuesta:

Tal y como se menciona en el PPT, en este servicio se valorará la puesta a disposición de soluciones específicas de seguridad que revisen de forma automatizada la explotabilidad de las vulnerabilidades identificadas en los análisis realizados sobre los sistemas internos, emulando la perspectiva de un atacante y permitiendo el descarte de falsos positivos y la priorización de la remediación.

33. Pag 15. Criterio 03: Podrían indicarnos la cantidad de assest que tienen alojados en Cloud (keyvaults, storageaccounts, virtualmachines, networksecuritygroup, base de datos, entre otros)

Respuesta:

El entorno tecnológico definido en el punto 10.1 del PPT recoge los datos mínimos necesarios para dimensionar adecuadamente cada uno de los servicios y/o criterios requeridos. Madrid Digital está en proceso de despliegue de plataformas en nube, lo que supone actualmente menos activos gestionados que los presentes en sus CPDs. La solución deberá ser escalable en previsión de que los activos en nube vayan en aumento.

34. Pag 18 del PPT. En el punto “Todos los elementos de la plataforma (SIEM), incluidos los elementos a desplegar on-premise, contarán con medidas de redundancia ante fallos.” ¿Por redundancia requieren que se duplique el hardware y software?

Respuesta:

La propuesta de solución de garantice la redundancia ante fallos queda a criterio del licitador.

35. En relación a las instalaciones de HW en los CPDs, el cliente pondrá a disposición los espacios en rack y energía segura para los equipos a instalar?

Respuesta:

Sí, en los CPDs gestionados por Madrid Digital.

36. PPT Pag 24. Apartado 4.1.2.2.1 Mencionan que el objetivo de la solución NDR es reemplazar el actual análisis de tráfico mediante Sondas IDS. Por favor confirmar que todas las sondas IDS (a excepción de las sondas de análisis de tráfico SAT-INET y SAT-ICS) mencionadas en la pag. 83 quedaran en desuso en una vez implantada la nueva solución NDR e integrada al SIEM

Respuesta:

Sí, en el momento que el sistema NDR esté completamente instalado y preste el servicio de forma eficaz y eficiente, siendo innecesario disponer de la información que aporte las sondas IDS indicadas.

37. Para la ingesta del tráfico en el NDR, confirmar desde donde podemos tomar el tráfico en los 04 CPD, indicando el tipo de interfaz de medio a suministrar (1gbs, 10gps, fibra, cobre, etc.)

Respuesta:

Tal y como se menciona en el PPT, en el apartado relativo a la solución NDR:

- La solución analizará el tráfico este-oeste cursado tanto en los dos CPD's de Madrid Digital como en los dos CPD's de la Consejería de Sanidad.
- El dimensionamiento del equipamiento a instalar en los CPD's (sensores) será responsabilidad del adjudicatario, estimándose que el tráfico generado en cada CPD a analizar será como mínimo de 20 Gbit/seg.

De lo que se deriva que, bajo la supervisión, asesoramiento y validación de Madrid Digital, será responsabilidad del adjudicatario proponer una arquitectura que cumpla los objetivos establecidos en el contrato.

38. En el apartado 9 de la cláusula 1 del PCAP (página 22 del PCAP) se indica que la documentación técnica asociada a los criterios objetivos, así como los CVs deben ir en el Sobre N°2 de la oferta. Sin embargo, en la cláusula 12 del PCAP (páginas 53 y 54) se indica que la respuesta a esos criterios objetivos debe incluirse en el sobre 3, junto con la propuesta económica, reservándose el sobre 2 únicamente para la documentación técnica cuya valoración depende de un juicio de valor. Entendemos que esto último es lo correcto y que la respuesta a los criterios técnicos de valoración objetiva (anexo V del PCAP), así como los CVs anonimizados deben ir en el sobre N°3, junto con la propuesta económica. Por favor, confirmen si es así.

Respuesta:

Respondido en la publicación de resolución de corrección de errores del PCAP.

39. Con relación a la longitud máxima de la oferta técnica para el Lote 4, se indica que debe ser de 25 páginas, mientras que el resumen ejecutivo tiene una longitud máxima de 5 páginas. Por favor indiquen si las 5 páginas del resumen ejecutivo son independientes de las 25 de la oferta principal, o bien si el resumen ejecutivo debe considerarse también incluido dentro de las 25 páginas máximas.

Respuesta:

En el PPT en el punto 9.4. *CONTENIDO DE LAS OFERTAS PARA EL LOTE 4*, se indica que la oferta no debe exceder en ningún caso las 25 páginas, lo que incluye el resumen ejecutivo que debe tener un número máximo de 5 páginas.

40. También con relación al Lote 4, se indica que la oferta técnica debe incluir “ejemplos de cuadros de mando con los contenidos propuestos”. Dada la limitación de 25 páginas del documento, por favor indiquen si dichos ejemplos de cuadro de mando podrían incluirse en anexos y no ser considerados dentro del límite total de 25 páginas.

Respuesta:

No, el licitador debe respetar los límites establecidos.

41. Enunciado: Capacidad mínima de ingesta diaria total de 3 TeraBytes, ampliable bajo demanda (y reducible) de eventos, flujos y alertas de seguridad. Cada 6 meses se procederá a la revisión del número medio de TeraBytes diarios ingestados para decidir si procede su regularización al alza o a la baja. Pregunta: Respecto a la facturación de la ingesta total de 3 TeraBytes / día, rogamos nos confirmen cómo sería el modelo de facturación en caso de no llegar a ingestar los 3 TeraBytes / día mínimo exigidos en pliego

Respuesta:

La facturación de la plataforma de gestión de eventos de seguridad – SIEM está descrita en la *cláusula 1, Apartado 22. REGIMEN DE PAGOS*. El importe semestral consignado de suscripción de herramienta SIEM contempla el pago en el primer semestre de 3TeraBytes/día. Esta ingesta será revisada semestralmente, de forma que las ampliaciones/reducciones posteriores se realizarán en base al valor de referencia indicado de 500 GigaBytes/día; por tanto, el pago aumentará o decrecerá según la ingesta aumente o disminuya respecto al coste del valor de referencia de 500 Gigabytes/día. Todo ello, considerando que estos importes se verán decrementados por el porcentaje de baja que resulte de aplicación debido a la adjudicación del contrato.

42. Enunciado: En este apartado, se indica lo siguiente: los licitadores indicarán en su repuesta económica el coste unitario del servicio para una ingesta diaria de 500 GigaBytes, de forma que las ampliaciones/reducciones posteriores se realizarán en base a este valor. Este precio deberá tener prorrateado todos los costes asociados correspondientes, no admitiéndose ningún coste adicional por ampliación, mantenimiento, operación o gestión. Pregunta: En el documento de presentación de oferta económica (ANEXO I), salvo error por nuestra parte, únicamente podemos completar el descuento sobre el precio máximo de licitación. En base a ello, ¿el PVP de cada bloque de 500GB/día adicionales sería proporcional al PVP marcado en pliego para la partida "Plataforma de gestión de eventos de seguridad - SIEM/SOAR - 3 Terabytes/ día", es decir, licencia base de 3 TB/día dividido entre 6?

Respuesta:

El importe es proporcional al coste de los 3 TB/día consignados en el presupuesto, siempre considerando que estos importes se verán decrementados por el porcentaje de baja que resulte de aplicación debido a la adjudicación del contrato.

43. Enunciado: En este apartado, se indica lo siguiente: los licitadores indicarán en su repuesta económica el coste unitario del servicio para una ingesta diaria de 500 GigaBytes, de forma que las ampliaciones/reducciones posteriores se realizarán en base a este valor. Este precio deberá tener prorrateado todos los costes asociados correspondientes, no admitiéndose ningún coste adicional por ampliación, mantenimiento, operación o gestión. Pregunta: Respecto a la facturación de las ampliaciones, rogamos nos confirmen cómo sería el modelo de facturación cuando no se llegue a un bloque de 500GB/día, es decir, que el incremento día se encuentre entre ">1GB y <500GB"

Respuesta:

La facturación se revisará semestralmente considerando el valor de referencia de 500 GigaBytes/día. Si no se incrementa o decremента la ingesta en cantidades iguales o superiores a ese valor, la facturación no se verá afectada.

44. Enunciado: En el PCAP se indica lo siguiente: Se efectuará mediante certificaciones trimestrales, contra factura conformada, y previa aceptación por la Subdirección General encargada de la inspección del servicio, a excepción de las suscripciones de herramientas incluidas en el lote 1 que se efectuarán mediante certificaciones semestrales. Pregunta: ¿El primer pago semestral de las suscripciones de herramientas por parte de Madrid Digital se realizará en el mes 1 o en el mes 7?

Respuesta:

Todos los pagos son contra factura conformada y previa aceptación y certificación, de la subdirección general promotora del contrato.

45. Enunciado: En el pliego para el Lote 1 se indica la necesidad de disponer de una CMDB. Pregunta: Sobre esta necesidad, no se detalla ningún requisito en cuanto a formato documental, ni acceso de usuarios ni integraciones con otras herramientas, por lo que entendemos que podemos utilizar las capacidades de las herramientas propuestas para disponer de un inventariado actualizado con la información requerida. Es correcto?

Respuesta:

Se podrán utilizar las capacidades de las herramientas propuestas para disponer de dicho inventario, así como de otras que, actualmente, disponga Madrid Digital y a las que tendrá acceso el adjudicatario una vez comience el servicio.

46. Enunciado: La solución estará dimensionada para proteger como mínimo los siguientes activos: 126.0000 endpoints (PC's de usuario de sobremesa y portátiles), 4.000 servidores, alojados en los dos CPD's de Madrid Digital, 3.000 servidores alojados en los dos CPD's de la Consejería de Sanidad – SERMAS y en el CPD principal de EducaMadrid. Pregunta: ¿La solución de NDR también debe analizar el tráfico este-oeste del CPD de EducaMadrid?. Se menciona el CPD principal, ¿se debe aplicar en algún otro CPD?

Respuesta:

No, únicamente lo indicado en el pliego.

47. ¿Hay actualmente desplegado algún Network packet broker? En caso de que, ¿Se plantea disponer próximamente de un NPM sobre el que valorar el diseño de despliegue de sensores?

Respuesta:

Actualmente hay desplegado servicio NPB en los CPDs que gestiona Madrid Digital. Respecto a la segunda pregunta, si por NPM se refieren a *Network Performance Monitoring*, no se plantea disponer por parte de Madrid Digital. En todo caso, el licitador puede proponer los elementos y arquitectura que considere.

48. Enunciado: El Throughput mínimo para los sensores que se plantea por cada CPDs será siempre de 20gb. Pregunta: ¿Podrían proporcionar algunas métricas de referencia que permita evaluarlo en detalle network bandwidth, número de servidores por cada CPD?

Respuesta:

El throughput recogido en el PPT es una estimación basada en análisis previos realizados por una muestra de fabricantes de este tipo de soluciones; por tanto, no es un dato de medición real ya que gran parte del tráfico este-oeste está contenido en los hosts físicos que dan soporte a nuestra infraestructura de máquinas virtuales. En consecuencia, el ancho de banda estimado de 20 Gbit/seg incluye tráfico entre máquinas físicas y el tráfico interno en dichos hosts. El ancho de banda disponible para las máquinas en los CPD's supera con creces el dato facilitado. En todo caso, el dimensionamiento de la solución deberá realizarse como mínimo en base al ancho de banda especificado y número de activos a proteger.

49. ¿Se incluyen en el número de servidores los servidores virtuales en los CPDs? ¿Que proveedor de infraestructura virtual se utiliza?

Respuesta

El número de servidores recogido en el PPT incluye los servidores virtuales. En cuanto la infraestructura, dado el amplio volumen de servidores que se gestionan, se utilizan las principales, entre las que destacan VMware, Azure y AWS.

50. ¿Cuál es el throughput del tráfico entrada/salida internet de las sondas IDS ubicadas en los 27 centros hospitalarios y 22 centros sanitarios? ¿Hay infraestructura virtual que posibilite el despliegue de sondas virtuales o es siempre necesario que valoren appliances físicos? ¿En estos centros hay algún tipo de servicios locales o están todos alojados en los CPDs? ¿Cuántos endpoints hay en estos centros? ¿Existe la posibilidad de optimizar el número de sondas ingesting el tráfico desde un punto común, por ejemplo los CPD's de Sanidad o la arquitectura actual no permite optimizar este número de sondas?

Respuesta

El throughput estimado de los centros hospitalarios (cuyo número es de 37 y no 27 como recoge la pregunta) y los centros sanitarios, es de 1,5Gb/s. El despliegue actual es mediante appliance físicos, tanto en los propios centros como en los CPD's principales. Tal y como se menciona en el PPT, en el punto 4.1.2.2.1. Análisis de tráfico para detección de intrusiones – sondas IDS, en el caso específico de sondas IDS ubicadas en los centros hospitalarios, los licitadores deberán indicar en su propuesta técnica de sustitución, si consideran necesario instalar algún equipamiento adicional, en modo local como complemento a los equipamientos centrales a instalar en los CPD's, detallando ventajas e inconvenientes. Madrid Digital se reserva el derecho de aceptar o no la propuesta de equipos locales a instalar que realicen los licitadores.

Por último, en cuanto a los endpoints, existen aproximadamente 65.000 en el entorno sanitario.

51. ¿Hay alguna solución SASE/SSE desplegada actualmente?

Respuesta

Actualmente solo hay implementado un SWG (puerta de enlace web segura).

52. Al no disponer del detalle de la arquitectura de red global actual, podemos proponer una solución optimizada con 3 grandes sondas redundadas (1 para cada entorno de comunicaciones MD, Sanidad y Educación)? O debemos contemplar replicar la arquitectura actual de sondas?

Respuesta

La propuesta de solución queda a criterio del licitador.

53. En la página 55 del PCAP se indica lo siguiente: Si se identificase alguna proposición que pueda ser considerada anormalmente baja, de acuerdo, en su caso, con lo indicado en la Cláusula 1 Apartado 8, se realizará la tramitación prevista en el Artículo 149 de la LCSP. Sin embargo, en la Cláusula 1 Apartado 8 no se da ninguna indicación sobre proposiciones que pueden considerarse anormalmente bajas. ¿Debe entenderse que ninguna oferta será considerada anormalmente baja?

Respuesta

Respondido en la publicación de resolución de corrección de errores del PCAP.

54. Se valorará una solución para analizar la postura de seguridad de servicios en nube (soluciones CSPM - Cloud Security Posture Management) ¿Podrían indicar cuántos servicios tienen ya en la nube (el volumen de servicios), para dimensionar este CSPM?

Respuesta

El entorno tecnológico definido en el punto 10.1 del PPT recoge los datos mínimos necesarios para dimensionar adecuadamente cada uno de los servicios y/o criterios requeridos. Madrid Digital está en proceso de despliegue de plataformas en nube, lo que supone actualmente menos activos gestionados que los presentes en sus CPDs. La solución deberá ser escalable en previsión de que los activos en nube vayan en aumento.

55. ¿Hasta cuándo están vigentes las licencias actuales de Exabeam y de Elasticsearch para operar estas plataformas?

Respuesta

La gestión y mantenimiento operativo mínimo de la plataforma actual está recogido en la *cláusula 1, Apartado punto 17 PLAZO DE EJECUCIÓN del PCAP*, y más en concreto en el epígrafe de *FASE DE IMPLANTACIÓN DE LOS SERVICIOS*.

56. ¿Se podría conocer el número aproximado de tecnologías/activos a monitorizar sobre las que se obtenga información de vulnerabilidades de seguridad?

Respuesta

Por motivos de confidencialidad y de ciberseguridad no es posible revelar este tipo de información.

57. Atendiendo a las tareas de cierre técnico de dominios maliciosos, ¿qué estimación anual de dominios maliciosos a cerrar se tiene?

Respuesta

El número de dominios maliciosos a cerrar por cada periodo es un dato muy variable difícilmente estimable, depende en muchos casos de factores externos no controlables por la organización, como pueden ser entre otros, las campañas de ataques realizadas por actores maliciosos de todo tipo, y también depende de las medidas de detección que el adjudicatario implemente.

58. Al principio de cada año el adjudicatario hará una recomendación de los ejercicios a realizar. ¿Se podrán fijar las fechas de inicio de cada ejercicio?

Respuesta

Tal y como se menciona en el PPT, en el punto 6.1, una vez comience el servicio en la FASE 1 (Diseño del ejercicio), con el asesoramiento del adjudicatario, se fijarán los parámetros globales del mismo, lo que incluye las fechas de inicio de cada ejercicio.

59. ¿Cuál será la duración de cada ejercicio de Red Team?

Respuesta

Tal y como se menciona en el PPT, en el punto 6.1, una vez comience el servicio en la FASE 1 (Diseño del ejercicio), con el asesoramiento del adjudicatario, se fijarán los parámetros globales del mismo: autorizaciones, comunicaciones, miembros de los distintos equipos (White Team, Red Team), así como el alcance y duración de los mismos.

60. ¿Nos podrían facilitar la información del expediente anterior que han llevado a cabo con la herramienta Insight Rapid7?

Respuesta

Por motivos de confidencialidad y de ciberseguridad no es posible revelar este tipo de información.

Por considerar de interés las aclaraciones y en virtud de lo establecido en el *Pliego de Cláusulas Administrativas Particulares*, se remite para su publicación en el perfil de contratante del Portal de la Contratación Pública de la Comunidad de Madrid.

*La Subdirectora de la Subdirección General de Ciberseguridad,
Protección de Datos y Privacidad*

Firmado digitalmente por: MUÑOZ FUENTES ESTHER
Fecha: 2024 08 08 11:45

Fdo.: Esther Muñoz Fuentes