

CONSULTAS LICITACIÓN 90005775
“SERVICIO DE ADMINISTRACIÓN Y SOPORTE QRADAR”

De acuerdo al calendario del proceso de Licitación 90005775, a continuación se presentan las consultas recibidas con sus respectivas respuestas.

1. Favor aclarar opciones para demostrar cumplimiento del requerimiento (3). “El proveedor no ha tenido un evento de seguridad en el último año en su infraestructura”

Respuesta: Una declaración jurada simple firmada por los representantes.

2. Favor aclarar opciones para demostrar cumplimiento del requerimiento (4). “El proveedor debe contar con al menos 3 años ofreciendo estos servicios” en Chile.

Respuesta: Una declaración jurada simple firmada por los representantes.

3. ¿Cuál es el promedio de ticket por concepto de administración de plataforma?

Respuesta: 15 a 20 ticket por mes aproximadamente.

4. ¿Cuántos casos de uso mensuales se generan aproximadamente?

Respuesta: 5 aproximadamente.

5. ¿Cuántos Data Sources promedio mensual son integrados al ambiente?

Respuesta: 10 a 15 aproximadamente.

6. De los SLA de servicio, ¿aplica tanto para administración como para las bolsas de soporte fuera de horario?

Respuesta: Sí.

7. ¿Cómo está distribuido el ambiente, esta implementado en on-premise, nube o híbrido?

Respuesta: Esta información será entregada a la empresa adjudicataria.

8. ¿Cuentan con soporte activo del producto?

Respuesta: Sí.

9. ¿Se puede entregar información del diseño del ambiente, distribución, Event Processor, Event Collector, etc.?

Respuesta: Esta información será entregada a la empresa adjudicataria.

10. ¿Qué tipo de licenciamiento poseen a la plataforma instalada, es sólo el de SIEM?

Respuesta: SIEM Y UBA.

11. ¿Qué módulos posee desplegados el ambiente?

Respuesta: Esta información será entregada a la empresa adjudicataria.

12. ¿En qué versión esta hoy la plataforma?

Respuesta: Esta información será entregada a la empresa adjudicataria.

13. ¿Poseen un control interno de la cantidad de EPS activos y el total de los licenciados? ¿qué sucede si no quedan disponibles y se pide integrar data Source nuevos? ¿existe un responsable de eso o somos nosotros quienes informamos?

Respuesta: La empresa adjudicataria deberá entregar recomendaciones y mejoras del servicio, con el fin de poder evaluar las posibles mejoras en la infraestructura y plataforma.

14. ¿Se debe ocupar su plataforma de ticket para la generación y control de los apoyos o podemos usar la nuestra o bien se debe integrar?

Respuesta: Se puede usar la plataforma de la empresa.

15. Solicitamos confirmar que en el caso de empresas con presencia regional, se acepta que la oferta sea presentada en conjunto entre la filial chilena y la casa matriz.

Respuesta: No, debe tener Centro de operaciones en Chile.

16. Solicitamos confirmar que se acepta que los servicios sean brindados en forma remota en caso que el Centro de Operaciones de la empresa adjudicada se encuentre fuera de Chile.

Respuesta: No, debe tener Centro de operaciones en Chile.

17. Solicitamos aportar información que permita dimensionar el servicio y la asignación de recursos.

Respuesta: En el Anexo A de las Bases de Licitación se indican los servicios requeridos.

18. Solicitamos informar versión de Qradar que estará dentro del alcance del servicio.

Respuesta: Esta información será entregada a la empresa adjudicataria.

19. Solicitamos informar cantidad de servidores de Qradar que estarán dentro del alcance del servicio (colectores, datanodes, etc.).

Respuesta: Esta información será entregada a la empresa adjudicataria.

20. Solicitamos informar si la plataforma se encuentra implementada en HA.

Respuesta: Esta información será entregada a la empresa adjudicataria.

21. Solicitamos informar si la plataforma implementada es multitenant.

Respuesta: Esta información será entregada a la empresa adjudicataria.

22. Solicitamos informar cantidad y tipo de fuentes integradas al SIEM.

Respuesta: Esta información será entregada a la empresa adjudicataria.

23. Solicitamos informar cantidad de casos de uso implementados / activados.
Respuesta: Esta información será entregada a la empresa adjudicataria.
24. Solicitamos informar cantidad de usuarios de Qradar.
Respuesta: Esta información será entregada a la empresa adjudicataria.
25. Solicitamos informar cantidad de reportes definidos en la plataforma. Y un estimado de complejidad de los mismos.
Respuesta: Esta información será entregada a la empresa adjudicataria.
26. Solicitamos informar si los informes incluyen correlación (o no) de distintas fuentes.
Respuesta: Esta información será entregada a la empresa adjudicataria.
27. Solicitamos informar la cantidad de incidentes gestionados por período (día, mes, año)
Respuesta: Esta información será entregada a la empresa adjudicataria.
28. Solicitamos informar la carga diaria / mensual relacionada con la extracción de información / reportes.
Respuesta: Esta información será entregada a la empresa adjudicataria.
29. Solicitamos informar la frecuencia de solicitudes para restauración de logs.
Respuesta: 5 mensuales aproximadamente.
30. Solicitamos informar frecuencia y cantidad de creación de nuevos casos de uso.
Respuesta: 5 mensuales aproximadamente.
31. Solicitamos informar cual es la expectativa de crecimiento futuro (en %).
Respuesta: Esta información será entregada a la empresa adjudicataria
32. Solicitamos confirmar que la plataforma (hardware, software) que está dentro del alcance del servicio está bajo soporte y mantención del fabricante.
Respuesta: SI está con contratos vigentes.
33. Solicitamos informar si las actividades de actualización y upgrade de plataforma se deben ejecutar consumiendo de la bolsa de 10 horas o se cotizarán de forma adicional como horas fuera de horario.
Respuesta: Si deben estar incluidas.
34. En relación a los SLA; solicitamos indicar ejemplos de requerimiento simple / complejo.
Respuesta: Un caso complejo puede ser crear casos de uso que unan actividades de múltiples log sources, versus uno simple que busque solo un evento particular.

35. En relación a los SLA; solicitamos indicar ejemplos de revisión simple / compleja.

Respuesta: Un caso complejo puede ser crear casos de uso que unan actividades de múltiples log sources, versus uno simple que busque solo un evento particular.

36. Favor indicar cual es la arquitectura actual de Qradar, ¿cuántos event processor, app host, collectors, si la arquitectura está en HA?

Respuesta: Esta información será entregada a la empresa adjudicataria.

37. ¿Cuántos data source están integrados actualmente?

Respuesta: Esta información será entregada a la empresa adjudicataria.

38. ¿Qué tipo de data source o tecnologías están actualmente integradas?

Respuesta: Esta información será entregada a la empresa adjudicataria.

39. ¿mensualmente cuantas nuevas integraciones se realizan?

Respuesta: 10 a 15 aproximadamente.

40. ¿cuántos casos de usos personalizados cuentan actualmente?

Respuesta: Esta información será entregada a la empresa adjudicataria.

41. ¿cuál es el criterio de Banco para identificar un requerimiento siempre de uno complejo?

Respuesta: Un caso complejo puede ser crear casos de uso que unan actividades de múltiples log sources, versus uno simple que busque solo un evento particular.

42. ¿cuántos requerimientos se genera mensualmente?

Respuesta: 15 a 20 ticket por mes aproximadamente.

43. ¿Cuántos incidentes con afectación de continuidad operativa han tenido los últimos 3 años?

Respuesta: Esta información será entregada a la empresa adjudicataria.

44. ¿La plataforma actual esta virtualizada o son hardware físico?

Respuesta: Esta información será entregada a la empresa adjudicataria.

45. ¿Cuántos agentes tienen integrados a la plataforma?

Respuesta: Esta información será entregada a la empresa adjudicataria.

46. Compartir la ubicación de los Datacenters donde se encuentran los componentes de QRadar.

Respuesta: Esta información será entregada a la empresa adjudicataria.

47. Bolsa de 10 horas mensuales acumulables por hasta tres meses, para casos de soporte o incidentes fuera de horario en caso de ser requerido. ¿Cuál es el alcance de este servicio?

Respuesta: Atender incidentes en los que se necesite hacer análisis de logs, búsquedas de actividad anómala, etcétera. Atención de soporte por falla en la plataforma o de cualquier equipo que pertenezca a la infraestructura de QRadar.

48. ¿Se necesita renovar licenciamiento del SIEM QRadar?

Respuesta: No.

15 de noviembre de 2023
Departamento de Adquisiciones