CONSULTAS LICITACIÓN 90008918
"SERVICIOS DE CIBERINTELIGENCIA Y OPENCTI"

De acuerdo al calendario del proceso de Licitación 90008918, a continuación se presentan las consultas recibidas con sus respectivas respuestas.

1. Respecto a la implementación de OpenCTI.
   a. ¿Cuál es el plazo esperado para la implementación y puesta en marcha de la plataforma?
   b. ¿Existe una infraestructura actual o plataforma de SIEM/SOC con la que se deba integrar OpenCTI?
   c. ¿Cuántas personas componen el equipo de Ciberdefensa que recibirá el entrenamiento?

Respuesta:
   a. El plazo esperado para la implementación es máximo 3 meses desde la adjudicación.
   b. No es requisito integrarla con SIEM/SOC.
   c. Alrededor de 10 personas.

2. Sobre los feeds de ciberinteligencia.
   a. ¿Qué tipos de actores de amenaza son considerados de mayor relevancia para la infraestructura crítica del sistema financiero que opera el Banco Central?
   b. ¿Qué tipo de indicadores de compromiso (IOCs) son más valiosos para su operativa actual: dominios, IPs, hashes, URLs, o requieren un balance específico?

Respuesta:
   a. Eso es parte del servicio que debiese conocer y ser entregado por los oferentes.
   b. Eso es parte del servicio que debiese conocer y ser entregado por los oferentes.

3. Acerca de la protección de marca.
   a. ¿Cuántas credenciales de usuarios (aproximadamente) deberían monitorearse?
   b. ¿Cuáles son los 3 dominios específicos a monitorear?
   c. ¿Existe algún límite de takedowns esperado por año?
   d. ¿Cuántos proveedores aproximadamente se incluirían en el monitoreo de cadena de suministro?

Respuesta:
   a. 800 aproximadamente.
   b. Se acordará con la empresa adjudicataria.
   c. 100 aproximadamente.
   d. Se estima un número de proveedores entre 10 y 20.

4. Sobre las investigaciones bajo demanda.
   a. ¿Cuál es el tiempo máximo de respuesta esperado para estas investigaciones?
   b. ¿Existe algún procedimiento específico para la solicitud y aprobación de estas investigaciones?
   c. ¿Se ha estimado una distribución de las 50 horas a lo largo del año o serán según demanda?

Respuesta:
   a. Dependerá de la criticidad, pero serán acordadas con la empresa adjudicataria.
   b. Eso es parte del servicio que debiese conocer y ser entregado por los oferentes.
   c. Según demanda.

5. Consideraciones técnicas generales.
   a. ¿El Banco tiene requisitos específicos sobre la ubicación de los servidores donde se alojaría la solución SaaS?
   b. ¿Existen restricciones regulatorias específicas que debamos considerar para el manejo de los datos?
   c. ¿Con qué herramientas de seguridad actuales se requiere integración? (SIEM, EDR, etc.)

Respuesta:
   a. Debe estar de acuerdo a las especificaciones de Filigran OpenCTI.
   b. Debe estar acorde a la ley de protección de datos chilena y al manejo de confidencialidad que se firma con el Banco.
   c. No se especifica ninguna integración.

6. Aspectos comerciales:
   a. ¿Hay algún requerimiento específico sobre la forma de facturación de los servicios?
   b. ¿Se valorarán propuestas que incluyan servicios adicionales no especificados en la RFP?

Respuesta:
   a. Favor revisar bases.
   b. No.

7. Valoración de elementos diferenciadores.
   a. ¿Qué aspectos específicos serán valorados positivamente más allá del cumplimiento básico de los requerimientos?
   b. ¿Cómo evaluarán específicamente las certificaciones en inteligencia de amenazas? ¿Reconocerán certificaciones que incluyan módulos de threat intelligence aunque no lleven ese nombre específicamente, como eJPT, C|CISO, Magister en Ciberseguridad, ISO 27032, ISO 27001, OSCP, OPST, OPSA o IRCP?

Respuesta:
   a. Favor revisar Bases.
   b. Se Aceptan solo las de Inteligencia de amenazas como Certified Threat Intelligence Analyst (CTIA) ó CREST Practitioner Threat Intelligence Analyst (CPTIA).

8. ¿Se puede presentar un servicio de CTI basado en otra solución que NO sea OpenCTI?
Respuesta: Favor revisar Bases.

9. ¿Es excluyente no tener referencias de éxito en Chile sobre servicios de CTI?
Respuesta: Favor revisar Bases.

10. ¿Es excluyente que la Empresa debe contar con ingenieros certificados en Inteligencia de amenazas y analistas calificados en manejo de plataforma OPEN CTI?
Respuesta: Es excluyente como se indica en las Bases, Anexo A, numeral 4.

15 de mayo de 2025
(Actualizado el 19 de mayo de 2025)
Departamento de Adquisiciones