

**RESPUESTAS A CONSULTAS FORMULADAS
EN LA CONSULTA AL MERCADO
90007426
ESCANER DE VULNERABILIDADES WEB**

De acuerdo con lo establecido en el Calendario de Actividades de esta Consulta al Mercado, a continuación, el Banco Central de Chile da respuesta a las consultas efectuadas por las Empresas participantes.

I.- RESPUESTAS A LAS CONSULTAS FORMULADAS

Pregunta N°1: ¿Cuántos objetivos están intentando escanear?

Respuesta: Aproximadamente, 10 sitios web.

Pregunta N°2: ¿Son internos o para clientes?

Respuesta: Son los sitios web del Banco que están expuestos a Internet. Los usuarios externos acceden a dichos sitios desde internet, no desde la red local.

Pregunta N°3: ¿Quieren alojar la herramienta localmente o en la nube?

Respuesta: En la nube, fuera de la red local del Banco.

Pregunta N°4: ¿Necesitan algún informe de cumplimiento?

Respuesta: El proveedor debe proporcionar puntos de referencia como OWAPS, CIS Controls u otros.

Pregunta N°5: ¿Necesitan alguna integración?

Respuesta: Lo ideal sería que incluyera integración con Azure Active Directory para que el login de los usuarios autorizados sea validado por el Active Directory del Banco. De forma alternativa autenticación multifactor podría ser una opción.

Pregunta N°6: ¿Están utilizando actualmente otra herramienta de escaneo?

Respuesta: El Departamento de TI tiene sus propias herramientas de escaneo. Somos la tercera línea de defensa del Banco y queremos realizar evaluaciones independientes.

Pregunta N°7: ¿Son revendedores?

Respuesta: No.

Pregunta N°8: ¿Que certificaciones de seguridad buscan que estén asociadas a la herramienta?

Respuesta: Certificaciones de la empresa que proporciona el servicio relacionadas con seguridad de la información, entre las que se podrían incluir por ejemplo ISO 27.001 para la empresa u OSCP para sus consultores.

Pregunta N°9: Solicitamos mayores detalles del requerimiento: "La plataforma debe ser accesible y utilizable exclusivamente a través de un navegador web desde la red interna del Banco." ¿Se refiere a que la solución debe estar implementada on prem o en una nube privada del Banco?

Respuesta: Se refiere a que el acceso a la plataforma para ajustar configuraciones; ver reportes con los resultados de los escaneos; descargar reportes; entre otros, solo se pueda materializar desde una o varias direcciones IP predefinidas o validando login, usando integración con Azure Active Directory. La solución debe ser implementada en la nube fuera de la red del Banco.

“El Banco cuenta con una serie de sitios web públicos incluyendo el sitio web institucional, base de datos estadísticos, repositorios digitales, entre otros”

Pregunta N°10: ¿Cuántas direcciones IP se deben escanear en total?

Respuesta: Favor, ver respuesta 1.

Pregunta N°11: ¿La solución presentada debe ser con IP Fijas o puede ser con IP concurrentes?

Respuesta: Desconocemos a que se refieren con IP concurrentes. Lo que queremos prevenir es que en caso de ser bloqueada la dirección IP origen desde donde se realizan los escaneos de vulnerabilidades, no sea impedimento para continuar realizando las pruebas desde otra dirección IP.

La plataforma debe ser accesible y utilizable exclusivamente a través de un navegador web desde la red interna del Banco.

Pregunta N°12: ¿Este punto se refiere a que la solución propuesta debe ser Software as a Service, SaaS?

Respuesta: Ver respuesta 9.

Pregunta N°13: ¿Puede nuestra propuesta ser un appliance o software virtual que se instale, dentro de la red del Banco? En este caso un appliance o software virtual permite escaneo de aplicaciones con IP internas.

Respuesta: En esta etapa apuntamos a escanear solo recursos tecnológicos expuestos a Internet, no buscamos realizar instalaciones dentro de la red del Banco.

Contar con capacidades de analítica y reportería, permitiendo generar informes detallados y personalizados sobre las vulnerabilidades obtenidas en el último escaneo como en los anteriores.”

Pregunta N°14: ¿Los reportes deben ser en español o pueden ser en idioma inglés?

Respuesta: Preferentemente en español, sin embargo, aceptamos reportes en ambos idiomas.

¿Qué tipo de soporte técnico ofrece la empresa?

Pregunta N°15: ¿Esta pregunta se refiere al soporte de la empresa o también al soporte del fabricante?

Respuesta: Ambos.

Pregunta N°16: ¿En el caso de soporte de la empresa, de que tipo sería, administración, soporte ante fallas, dudas en general o capacitaciones?

Respuesta: Todas las indicadas.

Pregunta N°17: ¿Se requiere ambos tipos de soporte? ¿En el caso de soporte del fabricante de que tipo?

Respuesta: Si, en el caso de soporte ante fallas del servicio y ajustes en configuraciones específicas.

Pregunta N°18: ¿El soporte del fabricante puede ser en idioma inglés?

Respuesta: Si

Santiago, 27 de septiembre de 2024

Banco Central de Chile