REPÚBLICA DOMINICANA
JUNTA CENTRAL ELECTORAL
COMITE DE COMPRAS Y CONTRATACIONES

JUNTA CENTRAL ELECTORAL • Comité de Compras y Contrataciones •

CCC-005/2024

Santo Domingo, D.N.,
4 de enero, 2024.

A los	:	Inscritos en la Licitación Pública Nacional Referencia: JCE-CCC-LPN-2023-0018, destinada a la adquisición e implementación de Herramientas de Ciberseguridad Asset Management (CSAM).
Asunto	:	Respuestas.

Actuando en nombre y representación del Comité de Compras y Contrataciones, en atención a lo dispuesto en el Pliego de Condiciones sobre respuestas, aclaraciones y enmiendas, tenemos a bien comunicarles lo siguiente:

1) La solución debe estar en la capacidad de dar respuesta automatizada frente a amenazas, análisis de riesgo y vulnerabilidad, así como monitorización de cambios en los activos IoT,OT, IT, entre otros. **¿Pueden detallar cuales, y cuantos son los activos IoT, OT, IT con los que cuentan?**

   Respuesta: *Uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es reducir la superficie de ataque de cualquier activo (IoT, OT, IT), mejorar la postura de seguridad de los mismos y obtener un inventario completo de cualquier tipo de dispositivo, por lo tanto, ejemplos, impresoras, switches, routers, UPS, aires acondicionados, sistema de gestión de edificios (BMS), celulares, racks inteligentes, sistema de control de incendios, cámaras de videovigilancia, dispositivos de control de accesos por biometría y NFC, sistemas de SmartTV para Videos Conferencias entre muchos otros.*

2) La solución deberá soportar la interfaz de programación de aplicaciones API REST con la finalidad de habilitar integraciones (DevOps) con las herramientas existentes y facilitar los requerimientos de automatización. **¿Qué tipo de integraciones DevOps requieren hacer y contra qué tipo de aplicaciones, soluciones, servicios?**

   Respuesta: *La JCE, es un órgano que se encuentra en constante evolución y desarrollo tecnológico de aplicaciones con una visión innovadora, por lo tanto, es un requerimiento indispensable que la herramienta solicitadas en la presente licitación esté preparada desde el inicio del contrato para integrarse con las herramientas existentes y futuras para facilitar cualquier requerimiento de automatización durante la vigencia del contrato.*

3) La solución deberá tener la capacidad de integrarse de forma nativa con las siguientes categorías de soluciones con la finalidad de enriquecer los datos, ejecutar una acción o alertar:

- Herramientas de control de acceso. **¿Qué herramienta de control de accesos?**

Respuesta: *Por razones de confidencialidad, esta información se proporcionará al licitante ganador y es una de las razones indispensables de solicitar una herramienta de seguridad con interfaz de programación de aplicaciones API REST, agnóstica a cualquier marca. Pero son dispositivos de control de accesos por biometría y NFC.*

- Switches.

Respuesta: *Por razones de confidencialidad, esta información se proporcionará al licitante ganador y es una de las razones indispensables de solicitar una herramienta de seguridad con interfaz de programación de aplicaciones API REST, agnóstica a cualquier marca.*

- Herramientas de vulnerabilidades (Obligatorio Tenable, otros). **Tenable es una solución similar en capacidades a la solicitada, que se pretende realizar con esta integración?**

Respuesta: *Se requiere para complementar el rango de direcciones IPs escaneados actualmente por Tenable, sobre todo para aquellos activos que no soportan este tipo de escaneos activos o agentes, ya que ponen en riesgo su funcionamiento, adicionalmente, de acuerdo a las mejores prácticas de seguridad de la JCE, se requiere utilizar otra fuente de información de riesgos, amenazas y vulnerabilidades, así como el análisis y monitoreo en tiempo real de manera continua y consolidar la información de las distintas herramientas actuales a través de las integraciones (APIs) en un solo dashboard o tablero.*

- Herramientas de administración de parches. **¿Qué herramienta de control de parches?**

Respuesta: *Por razones de confidencialidad, esta información se proporcionará al licitante ganador y es una de las razones indispensables de solicitar una herramienta de seguridad con interfaz de programación de aplicaciones API REST nativa, agnóstica a cualquier marca.*

- Herramientas de protección de dispositivos finales. **¿Qué herramienta de protección de dispositivo final?**

Respuesta: *Por razones de confidencialidad, esta información se proporcionará al licitante ganador y es una de las razones indispensables de solicitar una herramienta de seguridad con interfaz de programación de aplicaciones API REST nativa, agnóstica a cualquier marca.*

84

- Bases de datos de inventarios de activos o CMDB.
- Ambientes virtuales (Vmware vCenter).
- Entornos de nubes públicas (AWS, Azure, GCP) a través de APIs.e APIs. **¿Qué tipo de integración y a cuantos dispositivos, por agentes instalados en los equipos o sensores de escaneo?**

Respuesta: *Por razones de confidencialidad, esta información se proporcionará al licitante ganador y es una de las razones indispensables de solicitar una herramienta de seguridad con interfaz de programación de aplicaciones API REST nativa, agnóstica a cualquier servicio de nube.*

- SIEM. **¿Qué marca de SIEM?**

Respuesta: *Por razones de confidencialidad, esta información se proporcionará al licitante ganador y es una de las razones indispensables de solicitar una herramienta de seguridad con interfaz de programación de aplicaciones API REST nativa, agnóstica a cualquier marca.*

4) La solución deberá tener la capacidad de mostrar e identificar el inventario, conexiones de red de manera gráfica (Topología), alertas, actividades, factores de riesgos, acción (enforce), aplicaciones de cualquier dispositivo (IT, IoT, OT, BMS) que se encuentre conectado en la red con la misma plataforma y consola de administración. **¿La conexión entre los segmentos IT / OT / BMS esta segmentada? ¿De qué forma? ¿Por hardware o software?**

Respuesta: *Uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es que la herramienta de seguridad solicitada permita realizar una segmentación lógica, por categoría o tipo de dispositivo o la combinación de las mismas para cualquier tipo de ambiente aunque si tengamos segmentada los dispositivos.*

5) La solución debe detectar amenazas y anomalías mediante el monitoreo continuo de comunicaciones y protocolos del dispositivo (tanto externos como internos), sin necesidad de programar o realizar algún tipo de escaneo. **La detección de amenazas es una capacidad adicional a lo solicitado (CSAM), ¿están de acuerdo en agregar esta solución adicional del mismo fabricante?**

Respuesta: *Uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es reducir la superficie de ataque de cualquier activo, mejorar la postura de seguridad de los mismos y obtener un inventario completo de cualquier tipo de dispositivo, por lo tanto, es obligatorio que la herramienta de seguridad lo cumpla cabalmente conforme a lo solicitado requerimientos funcionales.*

6) Para los dispositivos ICS que se encuentran en las instalaciones, edificios y centros de datos, la solución deberá identificar las actividades de lectura y escritura cuando los controladores han sido accesados por estaciones de Ingeniería y/o SCADA servers. **La detección de vulnerabilidades en redes SCADA es una capacidad adicional a lo solicitado (CSAM), ¿están de acuerdo en agregar esta solución adicional del mismo fabricante?**

Respuesta: *Uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es reducir la superficie de ataque de cualquier activo, mejorar la postura de seguridad de los mismos y obtener un inventario completo de cualquier tipo de dispositivo, por lo tanto, es obligatorio que la herramienta de seguridad lo cumpla cabalmente conforme a lo solicitado requerimientos funcionales.*

7) La solución deberá de poder llevar a cabo las acciones de documentación y disparo de actividades a través de API's las acciones de remediación tales como:

- Desinstalar el producto afectado del activo.
- Cambio en la configuración del activo.
- Programación de la aplicación del parche (una vez disponible).
- Actualización del producto/Software afectado en el activo evaluado. **El manejo de parches es una capacidad adicional a lo solicitado (CSAM), ¿están de acuerdo en agregar esta solución adicional del mismo fabricante?**

Respuesta: *Uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es reducir la superficie de ataque de cualquier activo, mejorar la postura de seguridad de los mismos y obtener un inventario completo de cualquier tipo de dispositivo, así como la herramienta de seguridad tenga la capacidad de integrarse a través de API, agnóstica a cualquier marca, por lo tanto, es obligatorio que la herramienta de seguridad lo cumpla cabalmente conforme a lo solicitado requerimientos funcionales.*

8) La solución deberá ser basada 100% en nube, con la finalidad que el proveedor de la solución se encargue de las actividades administrativas asociadas al diseño, seguridad, soporte y actualización de la infraestructura requerida para la solución, tales como, una da para la solución, tales como, una arquitectura en alta disponibilidad, respaldo, restauración, escalabilidad y la supervisión del sistema, entre otros. **¿Cuándo se refiere a 100% nube, podría detallar? ¿Solo la gestión? Más a delante en este mismo documento (puntos detallados a continuación) se habla de un colector virtual, un colector físico y requerimientos de hardware. ¿Aceptarían una arquitectura hibrida?**

Respuesta: *No se acepta una arquitectura híbrida, la solución debe estar basada en nube, el colector es un sensor o elemento que forma parte de la solución.*

9) El colector virtual de la solución deberá soportar los siguientes hipervisores:

- VMware ESXi v5.5 y posteriores.
- Microsoft Hyper--V 2012 y posteriores.V 2012 y posteriores.

10) El colector físico la solución deberá ser de propósito específico, basado en un sistema propósito específico, basado en un sistema operativo Unix Hardenizado.

11) Los servidores o appliance serán proporcionados por el oferente o fabricante. **¿Están contemplando un proyecto llave en mano?**

Respuesta: *El colector es parte del servicio de la herramienta de seguridad solicitada y si es un proyecto llave en mano.*

Presentar documento con las configuraciones de los servidores o appliance a entregar:

- Procesador.
- Memoria.
- Almacenamiento.
- Tarjetas de Red.
- Puertos.
- Sistemas Operativos.
- Otros.

12) La solución deberá contar con una base de conocimientos de al menos 2,000 millones de dispositivos rastreados, además de tener acceso a la lista de los puntos vulnerables y las exposiciones comunes (CVE).

Consulta: Qualys hace uso de la fuente global de búsqueda conocida como Shodan, con inteligencia en tiempo real que alimenta nuestro CSAM/EASM indexando billones de IPs y atributos junto con CVEs asociados. Esto como una de las fuentes principales, **¿se acepta el cumplimiento de esta manera?**

Respuesta: *No se acepta, ya que la herramienta de seguridad solicitada no debe estar limitada solamente a las funcionalidades tradicionales CSAM/EASM e indexación de IPs, ya que se puede omitir dispositivos que no soportan escaneos activos o agentes y en consecuencia, pueden presentar una posible superficie de ataque, así como la herramienta de seguridad debe considerar otros tipos de atributos, tales como el perfil de riesgos basado en comportamientos, detección de amenazas en tiempo real, monitoreo constante, entre otros, conforme a lo solicitado en requerimientos funcionales.*

13) La solución deberá tener la capacidad de integrarse de forma nativa con las siguientes categorías de soluciones con la finalidad de enriquecer los datos, ejecutar una acción o alertar:

Consulta: Considerando que los requerimientos solicitados por la institución en el presente pliego, la integración con Tenable resultaría en la duplicidad de funciones. **¿podría considerarse esta integración como integración opcional?**

Respuesta: *No se acepta, no existe tal duplicidad, debido a lo comentado en la respuesta a la pregunta 3.*

14) La solución deberá promover la higiene de TI a través de la detección de la deuda técnica de los dispositivos basados en Windows, Linux y otros sistemas operativos.

Consulta: ¿Podría la institución aclarar a qué se refiere con que la solución debe promover deuda técnica de los dispositivos?

Respuesta: *La deuda técnica es la capacidad de identificar los dispositivos, sistemas operativos, versiones de software y hardware (firmware), permitiendo la creación de reportes y tableros estandarizados que proveén, entre otros, el fin de vida (EoL), fin de soporte (EoS) y los dispositivos obsoletos por parte de los fabricantes.*

15) La solución deberá proporcionar un inventario de los activos pasivamente con los siguientes atributos:

a) Nombre del Dispositivo.
b) Marca.
c) Modelo.
d) Tipo de dispositivos, (Computadora, Servidor, Gateway, Máquina Virtual, Firewalls, etc.).
e) Categoría del dispositivo, (Equipos de automatización, redes y seguridad, Computadoras, dispositivos móviles, etc.).
f) Sitios.
g) Sistema Operativo y/o versiones.
h) Número de serie, (si existe).
i) Dirección IP (V4 y V6).
j) Dirección MAC.
k) Factores de riesgo y clasificación.
l) Lista de vulnerabilidades asociadas.

m) Aplicaciones instaladas.
n) Conexiones hacia a otros servicios, sistemas y/o dispositivos.
o) Actividades observadas por cada dispositivo.

Consulta: Los mecanismos de escaneo o análisis pasivos no entregan una lista de vulnerabilidades confiable al no lograr un método de análisis profundo a nivel de puertos, servicios y sistema operativo que sean los más óptimos. Considerando lo dicho, ¿podría la institución considerar la opción de usar escaneos a nivel de red por medio de un scanner virtual sin uso de agentes para dicho propósito?

Respuesta: *No se acepta, ya que uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es reducir la superficie de ataque de cualquier activo, , mejorar la postura de seguridad de los mismos y obtener un inventario completo de cualquier tipo de dispositivo (IT, IoT o OT), así como la herramienta de seguridad solicitada tenga la capacidad de integrarse a través de API, agnóstica a cualquier marca o herramienta actual de seguridad y TI, para prevenir o complementar la visibilidad, por lo tanto, es obligatorio que la herramienta de seguridad cumpla cabalmente conforme a lo solicitado requerimientos funcionales.*

16) La solución debe proporcionar un mapa de activos interactivo que muestra la topología de red, los patrones de comunicación, los protocolos utilizados y las conversaciones, consumo de ancho de banda. Además, deberá permitir agrupar por diferentes criterios, tales como tipo de activo, riesgo, vulnerabilidad y filtrar por múltiples criterios como fabricante, tipo, nivel de riesgo y fecha de descubrimiento.

Consulta: Considerando que de acuerdo a lo que se observa en el requerimiento, la funcionalidad de la solución solicitada tiene un propósito de análisis de seguridad del tráfico en términos de: tráfico malicioso, análisis e identificación de conexiones y servicios como en general temas asociados al uso de recursos.

Respuesta: *No se entiende su pregunta, la herramienta de seguridad deberá cumplir cabalmente conforme a lo solicitado requerimientos funcionales tales como un mapa de activos interactivo que muestra la topología de red, los patrones de comunicación, los protocolos utilizados y las conversaciones, consumo de ancho de banda, etc.*

17) ¿Podría la institución considerar como opcional el análisis de conversaciones que va más asociado al contenido de comunicación donde la solución se orienta más hacia el manejo de conmutación y señalización de protocolos de voz (SIP, H.323, etc.)?

Respuesta: *No se acepta, ya que uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es reducir la superficie de ataque de cualquier activo, mejorar la postura de seguridad de los mismos y obtener un inventario completo de cualquier tipo de dispositivo, es por eso, que es indispensable que la herramienta de seguridad solicitada deberá contar con una base de conocimientos de al menos 2,000 millones de dispositivos rastreados, para evitar limitar cualquier tipo de análisis.*

18) La plataforma deberá de poder catalogar los activos basado en al menos 20 categorías B130.

Consulta: ¿Sería la institución tan amable de especificar la necesidad de cubrir este requerimiento y algunas de las categorías que serían importantes para el cumplimiento de este punto?

Respuesta: *La necesidad de contar con al menos 20 categorías tiene como objetivo obtener un inventario completo y preciso de dispositivos, con la finalidad de reducir la superficie de ataque de cualquier activo y mejorar la postura de seguridad de los mismos.*

19) Además de los protocolos tradicionales de TI, la solución debe soportar los protocolos industriales más comunes que se encuentran las instalaciones, edificios y centros de datos, tales como: CIP, EtherNet/IP, PCCC, S7Comm, S7Comm-Plus, Modbus, Tristation, GE Fanuc, GE Mark VIe, DeltaV, FTE, VNET, MMS, RNRP, CNCP, HSMS, OPC-DA, OPC- HDA, OPC-AE, OPC-UA, BACnet, KNX, Fox entre otros.

Consulta: Considerando que los alcances de la institución van más asociados a temas administrativos en términos electorales, y con la finalidad de entender y no encarecer la complejidad de la arquitectura a entregar, ¿Sería la institución e tan amable de ejemplificar casos de uso donde aplicaría el análisis de vulnerabilidades industriales?

Respuesta: *La razón es que uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es obtener un inventario completo de cualquier tipo de dispositivo e identificar cualquier protocolo asociado a los mismos, con el fin de reducir la superficie de ataque de cualquier activo (IoT, OT, IT) y mejorar la postura de seguridad de los mismos, por ejemplo, sistemas de gestión de edificios (BMS), alarmas, sistemas de control de incendio (HVAC), en el centro de datos, entre otros, por eso la herramienta de seguridad debe estar preparada para cualquier tipo de ambiente o dispositivo.*

20) La solución debe ser capaz de identificar vulnerabilidades conocidas para todos los dispositivos TI/IoT/OT/IoMT/BMS, obteniendo las mismas de forma segura, es decir, sin la necesidad de ejecutar escaneos de vulnerabilidades.

Consulta: Considerando que los alcances de la institución van más asociados a temas administrativos en términos electorales, y con la finalidad de entender y no encarecer la complejidad de la arquitectura a entregar, ¿Sería la institución tan amable de ejemplificar casos de uso donde aplicaría el análisis de en IoMT?

Respuesta: *La razón es que uno de los objetivos de la licitación, de manera enunciativa, más no limitativa, es obtener un inventario completo de cualquier tipo de dispositivo e identificar cualquier protocolo asociado a los mismos, con el fin de reducir la superficie de ataque de cualquier activo y mejorar la postura de seguridad de los mismos, aunque actualmente no se usan dispositivos IoMT, la JCE cuenta con dispensarios médicos en algunas regiones, lo que es importante que la herramienta de seguridad debe estar preparada para cualquier tipo de ambiente o dispositivo que es posible que hoy no se encuentra inventariada ni en uso.*

21) La solución deberá soportar una arquitectura distribuida con una administración centralizada, completamente nativa en la nube y alojada en alguno de los tres principales proveedores de nube (AWS, GCP, Azure), con la finalidad de beneficiarse de la agilidad, elasticidad, la analítica y las capacidades de cálculo computacional que provee la nube.

Consulta: Nuestra solución es 100% nativa en la nube, certificada SOC2 Type 2, con disponibilidad 24x7x365 consistente en el 99%. Cuenta con múltiples puntos de presencia con la arquitectura distribuida solicitada y que anuncia públicamente todos los mantenimientos, actualizaciones con su programación calendarizada. No se encuentra alojada en los proveedores mencionados, pero todos los sensores y mecanismos de detección están certificados y listos

para desplegar sin costo en los mercados de cada uno de los proveedores solicitados (AWS, GCP y Azure) de manera que se incrementa aún más la presencia de la marca.

Dicho lo anterior, **¿acepta la institución nuestra oferta con las garantías que se ofrecen?**

Respuesta: *Se acepta, si y sólo si: se indique cuál es su proveedor de nube donde se encuentre alojado y además de la certificación SOC2 Type 2, cumpla con las certificaciones ISO/IEC 27001:2013 y ISO/IEC 27018:2014.*

22) La solución deberá de permitir agregar, eliminar o modificar las funciones (Dashlets) según la operación de los usuarios y administradores.

Consulta: Para este punto, **¿Podría la institución e aclarar si esto se cumple mediante la modificación de las funciones de los usuarios por medio de roles y privilegios?**

Respuesta: *Se refiere a la creación de tableros de control personalizables donde muestran los datos de diferentes maneras y que pueden ser consultados por usuarios específicos. La funcionalidad de control de acceso basado en roles (RBAC) o múltiples roles de usuario es un concepto distinto y solicitado.*

23) Capacidad de adaptación a políticas de confianza cero.

Consulta: Para este punto, donde las soluciones confianza cero "Zero Trust" están asociadas tecnologías de control de acceso desde redes externas, donde usualmente vemos Firewalls, SDWAN, accesos de nube como CASB, o Analizadores / Balanceadores de tráfico, **¿Podría la institución detallar si se busca que se puedan crear integraciones hacia este tipo de soluciones y no ejecutar dichas funciones?**

Respuesta: *Es correcto, La herramienta de seguridad se deberá conectar/integrar a través de APIs con las soluciones de seguridad y gestión de TI existentes, a la infraestructura de red y realizar el análisis pasivo de la red a través de sensores o colectores para descubrir, clasificar, evaluar y monitorear continuamente todos los dispositivos en de cualquier ambiente (IoT, IoT, OT), en una red cableada y la red inalámbrica (WLC).*

NOTA:
Les recordamos que el plazo para preguntas venció en fecha 22/12/2023.

Atentamente,

LICDA. ELIZABETH AMARO CAMILO
Coordinadora

EAC/vd.-

JUNTA CENTRAL ELECTORAL
Comité de Compras y Contrataciones