INFORME DE EVALUACIÓN DE OFERTAS TECNICAS - PROCESO DE COMPARACIÓN DE PRECIOS INDOTEL-CCC-CP-2024-0007

Adquisición de Licencias MTR (Managed Threat)

INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES (INDOTEL)
01 DE AGOSTO DEL 2024
DCCEF-I-000028-24

INDICE

Equipo de Peritos

Cesar Moliné
Nidson Polanco

Introducción

En fecha 29 de julio del 2024 fue recibida, mediante correo electrónico desde la cuenta comprasycontrataciones@indotel.gob.do, la solicitud para realizar los procesos de evaluación y peritaje sobre las ofertas técnicas del proceso "Comparación de Precios INDOTEL-CCC-CP-2024-0007" sobre la Adquisición de Licencias MTR (Managed Threat).

Base de los resultados

La evaluación se realiza en base al "PLIEGO DE CONDICIONES ESPECÍFICAS adquisición de licencias MTR (Managed Threat)", cubriendo **los objetivos específicos de la contratación, los aspectos técnicos y la experiencia profesional requerida**, establecidos en el pliego de condiciones bajo la modalidad de "cumple/no cumple".

Evaluación de Requerimiento vs Cumplimiento

ID		REQUERIMIENTOS	SS-DOMINICANA, S.R.L.	XBYTE, SRL
		2.5.2 Objetivos Específicos de la Contratación		
1		Implementación e integración con la red del INDOTEL	CUMPLE	CUMPLE
2		Integración con firewall Sophos	CUMPLE	CUMPLE
3		Búsqueda de amenazas.	CUMPLE	CUMPLE
4		Telemetría optimizada	CUMPLE	CUMPLE
5		Descubrimiento de activos	CUMPLE	CUMPLE
6		Módulo XDR	CUMPLE	CUMPLE
7		Módulo de EDR	CUMPLE	CUMPLE
8		Licencias para 650 endpoints para pc finales y 40 para servidores con	CUMPLE	CUMPLE

		sistemas operativos mixtos		
9		Integración Microsoft 365 con capacidad para 632 buzones.	CUMPLE	CUMPLE
11		Soporte 24/7 por el proveedor por un año.	CUMPLE	CUMPLE
		2.5.4 Aspectos Técnicos y Logísticos		
13	Protección web	La herramienta deberá proteger la infraestructura frente a amenazas web y ayudar a regular el contenido no deseado.	CUMPLE	CUMPLE
14	Reputación de descargas	La herramienta deberá verificar que las descargas se realizan desde sitios webs con alta reputación (Confiable), de no ser así deberá bloquear las descargas.	CUMPLE	CUMPLE
15	Control de periféricos	La herramienta deberá permitir controlar el acceso a periféricos y medios extraíbles (Bloquear puertos).	CUMPLE	CUMPLE
16	Control de aplicaciones	La solución deberá permitir detectar y bloquear aplicaciones que no suponen una amenaza para la seguridad, pero cuyo uso no se considere adecuado en el entorno empresarial.	CUMPLE	CUMPLE
17	Detección de malware con Deep Learning	La solución deberá detectar malware de una manera rápida y efectiva e identificar elementos sospechosos de códigos potencialmente maliciosos y prevenir ataques de malware desconocido.	CUMPLE	CUMPLE
18	Escaneado de archivos anti-malware	La herramienta debe realizar escaneos en busca de archivos maliciosos, analizando y revisando todos los archivos.	CUMPLE	CUMPLE

19	Protección en vivo	La herramienta debe decidir instantáneamente si un archivo sospechoso es una amenaza y tomar las medidas especificadas en la política antivirus y HIPS.	CUMPLE	CUMPLE
20	Análisis de comportamiento previo a la ejecución (HIPS)	La herramienta debe realizar un análisis de comportamiento del tráfico de la red y los archivos, en busca de comportamientos sospechosos.	CUMPLE	CUMPLE
21	Bloqueo de aplicaciones no deseadas	La solución debe bloquear aplicaciones que no sean deseadas en la infraestructura.	CUMPLE	CUMPLE
22	Sistema de prevención de intrusiones	La solución ofertada deberá bloquear el tráfico peligroso, tanto entrante como saliente, y permitir que los usuarios autorizados accedan de forma segura para proteger la red.	CUMPLE	CUMPLE
23	Interfaz de análisis antimalware (AMSI)	La solución debe proteger contra ataques de secuencias de comandos que se ocultan a través de la ofuscación, el cifrado o la ejecución directa en la memoria.	CUMPLE	CUMPLE
24	Detección de tráfico malicioso (MTD)	La solución debe detectar las comunicaciones entre ordenadores y servidores de comando y control utilizados en un ataque de bots u otros ataques maliciosos.	CUMPLE	CUMPLE
25	Prevención de exploits	La solución debe detectar código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración.	CUMPLE	CUMPLE

26	Mitigaciones de adversarios activos	La solución debe evitar la persistencia en los equipos, proteger del robo de credenciales y detectar el tráfico malicioso.	CUMPLE	CUMPLE
27	Protección contra archivos de ransomware	La solución debe detectar y detener el cifrado espontáneo de datos por ransomware en cuestión de segundos.	CUMPLE	CUMPLE
28	Protección del registro de arranque y disco	La solución debe evitar variantes de ransomware o código malicioso que se dirigen al Master Boot-Record.	CUMPLE	CUMPLE
29	Protección contra navegación segura	La solución debe detectar y bloquear las intercepciones del navegador web, para prevenir robo de información inyección de código malicioso.	CUMPLE	CUMPLE
30	Bloqueo de aplicaciones mejorado	La solución debe permitir bloquear aplicaciones no deseadas	CUMPLE	CUMPLE
31	Live Discover	La solución debe permitir consultas SQL en toda la infraestructura para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI.	CUMPLE	CUMPLE
32	Biblioteca de consultas SQL	La solución debe contar con consultas ya escritas totalmente personalizables.	CUMPLE	CUMPLE
33	Detección y priorización de eventos sospechosos	La solución debe detectar en tiempo real eventos sospechosos y priorizarlos de acuerdo con la criticidad.	CUMPLE	CUMPLE
34	Fuentes de datos entre productos, p. ej. Firewall, correo electrónico	La solución debe permitir el intercambio de datos entre los distintos dispositivos de la infraestructura (Firewall, XDR, etc) para una efectiva respuesta ante amenazas.	CUMPLE	CUMPLE
35	Casos de amenazas (Análisis de causa raíz)	La solución debe investigar los casos de amenazas hasta llegar a la causa raíz de dicha amenaza.	CUMPLE	CUMPLE

36	Información sobre amenazas avanzada a demanda	La solución debe ofrecer información sobre nuevas amenazas siempre que sea necesario y demandado por parte del INDOTEL.	CUMPLE	CUMPLE
37	Exportación de datos forenses	La solución debe permitir extraer y exportar los datos forenses de las amenazas, para su posterior análisis y comprensión.	CUMPLE	CUMPLE
38	Eliminación de malware automatizada	La solución debe eliminar los archivos maliciosos de manera automática y sin intervención de personas.	CUMPLE	CUMPLE
39	Seguridad sincronizada	La solución debe incluir respuesta automatizada a incidentes y minimiza la exposición a las amenazas de seguridad, mientras que el intercambio de datos entre productos revela riesgos previamente ocultos.	CUMPLE	CUMPLE
40	Aislamiento de endpoints a demanda	La solución debe permitir aislar de la red a endpoints sospechosos o que el administrador considere para su posterior análisis.	CUMPLE	CUMPLE
41	Limpieza endpoints	La solución debe contar con fácil mecanismo de limpieza y bloqueo de endpoints en la red, debe contar con una interfaz sencilla para los usuarios.	CUMPLE	CUMPLE
42	Búsqueda de amenazas a partir de pistas 24/7	La plataforma de buscar amenazas según patrones sospechosos o pistas 24 horas al día 7 días a la semana.	CUMPLE	CUMPLE
43	Comprobaciones del estado de seguridad	La solución debe comprobar siempre el estado de seguridad de la infraestructura, actuar y alertar en caso de amenazas.	CUMPLE	CUMPLE
44	Retención de datos	La solución debe permitir retener datos como registros, logs, etc según considere el administrador.	CUMPLE	CUMPLE
45	Informes de actividades	La solución debe incorporar reportería o	CUMPLE	CUMPLE

		informes de todos los eventos de seguridad en la infraestructura.		
46	Neutralización y remediación de amenazas	La herramienta debe neutralizar las amenazas de seguridad detectadas en la infraestructura y remediar los daños causados por dicha amenaza.	CUMPLE	CUMPLE
47	Soporte telefónico directo	La solución debe incluir soporte telefónico directo disponible en caso de mal funcionamiento de la herramienta o en caso de que se necesite cualquier otro tipo de soporte relacionado con la solución.	CUMPLE	CUMPLE
48	Seguridad de Correos electrónicos	La solución debe incluir: reglas de flujo de correo de Microsoft 365, escaneado de malware y antispam, detección de URL maliciosas, reescritura de direcciones URL en el momento del clic, SPF, DKIM, DMARC, comprobaciones de dominios de imitación, cifrado TLS impuesto, cifrado basado en imposición.	CUMPLE	CUMPLE
		2.5.10 Experiencia Profesional Requerida **La empresa deberá cumplir con los siguientes requisitos:**		
49		Contar con personal de apoyo en el país.	CUMPLE	CUMPLE
50		Debe de ser socio o asociado (partner) del producto	CUMPLE	CUMPLE
51		Debe incluir el costo de emigrar la plataforma tecnológica, en caso de ser necesario.	CUMPLE	CUMPLE
52		El personal que trabaja en la implementación debe mostrar experiencia y certificaciones en ciberseguridad.	CUMPLE	CUMPLE

53		Asociado certificado del proveedor directo de la solución.	CUMPLE	CUMPLE
54		Experiencia en por lo menos dos (2) de proyectos relativos a implementación de XDR.	CUMPLE	CUMPLE
		La empresa deberá justificar lo anterior mediante la presentación de la siguiente documentación:		
55		Contratos de trabajo.	CUMPLE	CUMPLE
56		Currículums vitae (CV) del personal.	CUMPLE	CUMPLE
57		Certificaciones de formación del personal.	CUMPLE	CUMPLE
58		Certificado de partnership o asociado.	CUMPLE	CUMPLE
59		Acuerdo de partnership o asociado firmado por ambas partes.	CUMPLE	CUMPLE
60		Casos de éxito de proyectos anteriores.	CUMPLE	CUMPLE
61		Referencias de clientes satisfechos.	CUMPLE	CUMPLE

Conclusión

Luego de agotar el proceso de evaluación de la información documentada recibida, se evidenció conformidad por las dos oferentes **(SS-DOMINICANA S.R.L y XBYTE S.R.L)**, ya que cumple con todos los requisitos técnicos de pliego de condiciones. En consecuencia, Ambos oferentes quedan **HABILITADOS** para la apertura del sobre B.