INFORME DE EVALUACIÓN DE OFERTAS TECNICAS - PROCESO DE LICITACIÓN PÚBLICA NACIONAL

INDOTEL-CCC-LPN-2023-0009

DIRECCIÓN DE CIBERSEGURIDAD, COMERCIO ELECTRÓNICO Y FIRMA DIGITAL

DEPARTAMENTO DE CIBERSEGURIDAD

INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES

7 DE DICIEMBRE 2023

DCCEF-I-000041-23

INDICE

Equipo de Peritos

Cesar Moliné Rodríguez
Nidson Polanco

Introducción

En fecha 5 de diciembre 2023 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 "Licitación Pública Nacional INDOTEL-CCC-LPN-2023-0009" sobre la adquisición e implementación de un gestor de seguridad de información y eventos (SIEM).

Base de los resultados

La evaluación se realiza en base al "PLIEGO DE CONDICIONES ESPECÍFICAS PARA COMPRA DE BIENES Y SERVICIOS CONEXOS – ADQUISICIÓN E IMPLEMENTACIÓN DE UN GESTOR DE SEGURIDAD DE INFORMACIÓN Y EVENTOS (SIEM)", cubriendo los aspectos técnicos establecidos en el punto 2.7 Especificaciones Técnicas.

Evaluación de Requerimiento vs Cumplimiento

NO.	**REQUERIMIENTOS**		
	Oferentes	**ASYSTEC**	**SOLVEX**
	OBJETIVOS ESPECIFICOS	CUMPLE	CUMPLE
	1. Implementación e integración con la red del INDOTEL.	CUMPLE	CUMPLE
	2. Integración con Sophos Central	CUMPLE	NO CUMPLE
	3. Solución Cloud, 35 GB de almacenamiento diario	CUMPLE	CUMPLE
	4. Integración Microsoft 365	CUMPLE	CUMPLE
	5. Asesoría para implementación de controles y casos de usos.	CUMPLE	CUMPLE
	6. Soporte 24/7 por el proveedor.	CUMPLE	CUMPLE
	7. Capacitación full de administración para 4 colaboradores.	CUMPLE	CUMPLE

NO.	REQUERIMIENTOS TECNICOS		
	Oferentes	**ASYSTEC**	**SOLVEX**
	PLATAFORMA SIEM INTEGRADA		
1	Arquitectura de la solución debe ser vendor flexible con capacidad de ingestar fuentes multi-nube, hibrido y local.	CUMPLE	NO CUMPLE
2	La solución debe permitir la ingesta de datos sin la necesidad de conectores de clientes o soporte de proveedores.	CUMPLE	NO CUMPLE
3	La solución debe tener capacidad de modelos de aprendizajes automáticos usando Machine Learning.	CUMPLE	NO CUMPLE
4	La solución debe permitir fácil integración con Sophos Central.	CUMPLE	NO CUMPLE
5	La solución debe abordar la gestión de registros y la generación de informes la cual incluya investigaciones de incidentes, análisis forense, capacidad para correlacionar cualquier dato de la máquina, perfil de comportamiento y detección de anomalías, monitoreo de aplicaciones, integración con soluciones de automatización.	CUMPLE	NO CUMPLE
6	La solución debe tener la capacidad de integración con soluciones de UBA.	CUMPLE	NO CUMPLE
7	La solución debe ser un producto único e integrado para casos de uso de registro y SIEM.	CUMPLE	NO CUMPLE
8	La solución debe poseer una arquitectura altamente escalable y que pueda indexar grandes cantidades de datos por día.	CUMPLE	NO CUMPLE
9	La solución debe tener la capacidad de indexar todos los datos originales sin modificar y hacer que se puedan buscar sin normalización o reducción de datos.	CUMPLE	NO CUMPLE
10	La solución debe ofrecer múltiples opciones para el almacenamiento a largo plazo.	CUMPLE	NO CUMPLE
11	La solución debe ser una opción de nube totalmente administrada.	CUMPLE	NO CUMPLE
12	El proveedor de la nube de cumplir con certificaciones SOC 2 Type II y ISO 27001.	CUMPLE	NO CUMPLE
13	La solución debe incluir búsquedas de correlación predefinidas, informes, paneles y visualizaciones para respaldar los casos de uso de seguridad.	CUMPLE	NO CUMPLE
14	La solución debe proporcionar contenido para ayudar en la corrección y educación del panorama de amenazas, y este contenido debe actualizarse regularmente.	CUMPLE	NO CUMPLE

15	La solución debe asignar el contenido disponible a mandatos de cumplimiento comunes, marcos de detección o modelos adversarios como CIS20, NIST 800-53, NERC-CIP, PCI, Mitre ATT & CK, Cyber Kill Chain y otros.	CUMPLE	NO CUMPLE
16	La solución debe respaldar la capacidad de los equipos de seguridad para investigar de manera colaborativa incidentes, problemas y brechas de seguridad.	CUMPLE	NO CUMPLE
17	La solución debe cumplir con los requisitos reglamentarios en torno a la administración, retención, revisión y monitoreo continuo de registros.	CUMPLE	NO CUMPLE
18	La solución debe admitir la creación de cuadros de mando e informes para medir el cumplimiento de algún control técnico rastreable en los datos de la máquina.	CUMPLE	NO CUMPLE
19	La solución debe poder generar hashes criptográficos para los datos ingeridos para demostrar que no se ha producido ninguna manipulación después de la ingesta.	CUMPLE	NO CUMPLE
20	La solución debe proporcionar cifrado de datos de eventos antes de la ingesta.	CUMPLE	NO CUMPLE
21	La solución debe admitir diversas fuentes de datos de forma inmediata.	CUMPLE	NO CUMPLE
22	La solución debe admitir de forma nativa la recopilación de todos los tipos de fuentes de datos multi-nube. Proveedores de nube comunes, como Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).	CUMPLE	NO CUMPLE
23	La solución debe tener la capacidad de indexar todos los datos originales no modificados y hacerlos disponibles tanto para búsquedas como para informes.	CUMPLE	NO CUMPLE
24	La solución debe ofrecer una tecnología de agente ligera y segura para recopilar datos de hosts * NIX, MacOS o Windows.	CUMPLE	NO CUMPLE
25	La solución debe poder configurarse para capturar datos detallados de terminales para detectar ejecuciones de procesos comunes y poco comunes.	CUMPLE	NO CUMPLE
26	La solución debe admitir tipos comunes de ingestión de datos por cable, como Netflow, IPFIX, Bro y Cisco NVM, ya sea de forma nativa desde fuentes o desde taps como Gigamon.	CUMPLE	NO CUMPLE
27	La solución debe tener la capacidad de conectarse directamente a cualquier tabla (s) de base de datos SQL y extraer el contenido para indexarlo.	CUMPLE	NO CUMPLE
28	La solución debe tener la capacidad de consultar cualquier base de datos SQL y traer los resultados para verlos ad-hoc.	CUMPLE	NO CUMPLE

29	La solución debe tener la capacidad de realizar búsquedas de texto completo en cualquier campo de los datos indexados basándose en palabras clave, rangos de tiempo, lógica booleana, expresiones regulares, sintaxis de comodines y análisis estadístico.	CUMPLE	NO CUMPLE
30	La solución debe tener la capacidad de realizar líneas de base y luego aplicar la lógica de búsqueda para encontrar valores atípicos / anomalías desde la línea de base que pueden ser amenazas avanzadas no basadas en firmas.	CUMPLE	NO CUMPLE
31	La solución debe tener la capacidad de ejecutar múltiples búsquedas simultáneas.	CUMPLE	NO CUMPLE
32	La solución debe poder extraer nuevos campos de cualquier fuente de datos sobre la marcha, sin tener que volver a ingerir los datos.	CUMPLE	NO CUMPLE
33	La solución debe permitir crear comandos personalizados para buscar en sus datos de nuevas formas.	CUMPLE	NO CUMPLE
34	La solución debe utilizar varias técnicas para acelerar la devolución de datos a los analistas.	CUMPLE	NO CUMPLE
35	La solución debe permitir crear fácilmente visualizaciones personalizadas y actualizar esas visualizaciones en tiempo real.	CUMPLE	NO CUMPLE
36	La solución debe incluir una interfaz de usuario de arrastrar y soltar para permitir a los usuarios no técnicos crear informes complejos sin tener que usar comandos de búsqueda o comprender el formato de los datos sin procesar subyacentes.	CUMPLE	NO CUMPLE
37	La solución debe proporcionar una interfaz compatible con dispositivos móviles.	CUMPLE	NO CUMPLE
38	La solución debe ser compatible con el control de acceso basado en roles (RBAC) flexible para el acceso controlado de usuarios y API. Debe poder restringir el acceso a fuentes de datos, tipos de datos, períodos de tiempo, vistas específicas, informes o paneles de control específicos.	CUMPLE	NO CUMPLE
39	La solución debe admitir la integración de autenticación y autorización con Active Directory, eDirectory y otras implementaciones compatibles con LDAP.	CUMPLE	NO CUMPLE
40	La solución debe integrarse con las soluciones empresariales de inicio de sesión único para permitir la autenticación de paso a través de credenciales de terceros.	CUMPLE	NO CUMPLE
41	La solución debe permitir la indexación remota de datos en tiempo real para minimizar la oportunidad de alteración de pistas de auditoría en hosts comprometidos.	CUMPLE	NO CUMPLE
42	La solución debe proporcionar acceso seguro al flujo de datos y funcionalidad distribuida a través de SSL / TCP.	CUMPLE	NO CUMPLE
43	La solución debe admitir eventos de signos de bloqueo con una firma digital para demostrar la integridad de los datos indexados.	CUMPLE	NO CUMPLE

44	La solución debe monitorear sus propias configuraciones y uso para mantener una pista de auditoría completa y firmada digitalmente de quién está accediendo al sistema, qué búsquedas están ejecutando, qué informes están viendo y qué cambios de configuración están haciendo.	CUMPLE	NO CUMPLE
45	La solución debe ofrecer una API REST para exponer todos los datos indexados, los comandos de búsqueda y la funcionalidad a sistemas, aplicaciones y paneles externos.	CUMPLE	NO CUMPLE
46	La solución debe tener varios SDK escritos en la parte superior de la API. De ser así, se deben especificar los nombres de los SDK.	CUMPLE	NO CUMPLE
47	La solución debe incluir aplicaciones públicas y gratuitas para productos puntuales o casos de uso para crear más valor.	CUMPLE	NO CUMPLE
48	La solución debe permitir que las configuraciones del sistema se configuren a través de la interfaz de usuario, la CLI o los archivos del sistema de archivos para permitir cambios granulares y personalización.	CUMPLE	NO CUMPLE
49	La solución debe permitir que los informes y paneles se editen a través de la interfaz de usuario o archivos XML subyacentes.	CUMPLE	NO CUMPLE
50	La solución debe permitir que los datos se reenvíen fácilmente a sistemas externos o herramientas de registro.	CUMPLE	NO CUMPLE
51	La solución debe admitir algún método seguro basado en estándares (p. Ej., HTTPS) de ingesta de datos de aplicaciones personalizadas.	CUMPLE	NO CUMPLE
52	La solución debe proporcionar actualizaciones públicas periódicas sobre nuevas técnicas de seguridad que se deben lograr con su sistema.	CUMPLE	NO CUMPLE
53	La solución debe tener la capacidad de minimizar o consolidar la cantidad de conexiones hacia la nube entorno a controlar el tráfico en el ancho de banda.	CUMPLE	NO CUMPLE
54	El proveedor debe ser un partner autorizado de la solución a ofertada.	CUMPLE	CUMPLE
55	El proveedor deberá tener la capacidad de realizar la implementación de la solución.	CUMPLE	CUMPLE
56	El proveedor debe realizar la integración con nuestras diferentes fuentes de datos.	CUMPLE	NO CUMPLE
57	El proveedor debe realizar la integración de los componentes necesarios para la colección eventos de nuestras fuentes con la nube.	CUMPLE	NO CUMPLE
58	El proveedor deberá implementar paneles de Postura de Seguridad, los cuales indiquen: • Alertas de intrusión por gravedad clasificada. • Alertas de intrusión por gravedad. • Alertas de intrusión. • • Alertas con vistas de 24 horas de Las 10 principales alertas de intrusión de gravedad indicando su nivel de gravedad.	CUMPLE	NO CUMPLE

59	El proveedor deberá implementar paneles de monitoreo continuo de: • Cambios de Windows para ver eventos en Windows. • Tablero de todas las autenticaciones para ver todas las acciones de autenticación. • Panel de malware para ver soluciones antivirus. • Panel de control de detección de intrusos (IDS/IPS) para ver los sistemas de prevención y detección de intrusos. • Tablero de firewalls para ver eventos de firewall. • Tablero de tráfico de red para ver los datos del firewall en su red. • Tablero de acceso VPN para ver los datos de la sesión VPN. • Cuentas bloqueadas. • Escaladas de privilegios. • Cambiar métricas. • • Métricas de autenticación.	CUMPLE	NO CUMPLE
60	El proveedor deberá implementar paneles para amenazas avanzadas que incluyan los siguientes parámetros: • Panel de Anomalías para identificar riesgos de seguridad • Paneles de anomalías de red para identificar anomalías de red • Panales de casos de uso personalizado para incorporar búsquedas y tableros personalizados.	CUMPLE	NO CUMPLE
61	El proveedor deberá implementar paneles Investigar las actividades de comportamiento del usuario tales como: • Información del usuario. • Acceso de usuarios por fuente. • Acceso en el tiempo por acción. • Acceso por fuente. • Mapa de autenticación que muestra hasta 250 destinos de autenticación. • Los 100 eventos más recientes • Comportamiento para investigar la actividad del host utilizando la siguiente información: • Comunicaciones de red • Mapa de comunicaciones de la red • Autenticaciones y cambios. • • Malware e intrusión	CUMPLE	NO CUMPLE
62	El proveedor deberá implementar paneles e informes. Ejemplos: • Administración activamente el ciclo de vida de las cuentas de aplicaciones y sistemas, incluida su creación, uso, inactividad y eliminación, para minimizar las oportunidades para los atacantes. • Detección, prevención y corrección de flujo de información de seguridad en redes de diferentes niveles de confianza • Controle la instalación, propagación e implementación de código malicioso en varios puntos de la plataforma. • • Optimización y automatización de actualizaciones de contra medidas y las acciones correctivas	CUMPLE	NO CUMPLE

63	El proveedor deberá implementar vistas ejecutivas que incluya paneles, que muestre la siguiente información para informar sobre el estado del entorno a: • Ataques detenidos • Malware bloqueado • Usuarios protegidos • Dispositivos protegidos • Tendencias de usuario • • Orígenes del ataque	CUMPLE	NO CUMPLE
64	Proveedor deberá entregar la arquitectura propuesta para la solución.	CUMPLE	NO CUMPLE
65	El proveedor deberá entregar un cronograma de la implementación	CUMPLE	CUMPLE

Conclusión

Luego de agotar los procesos sobre las evaluaciones de la información documentada recibida, se puede concluir que en la oferta presentada por **SOLVEX**, se evidencia la no presentación de informaciones documentadas requeridas para determinar el cumplimiento de múltiples requisitos técnicos establecidos en el "PLIEGO DE CONDICIONES ESPECÍFICAS PARA COMPRA DE BIENES Y SERVICIOS CONEXOS – ADQUISICIÓN E IMPLEMENTACIÓN DE UN GESTOR DE SEGURIDAD DE INFORMACIÓN Y EVENTOS (SIEM)", por lo que entendemos que su oferta se considera **NO HABILITADO** para la apertura del sobre B del proceso de Licitación Pública Nacional INDOTEL-CCC-LPN-2023-0009.

En cuanto a la oferta de **ASYSTEC** se evidencia su conformidad en todos los requisitos técnicos establecidos en el "PLIEGO DE CONDICIONES ESPECÍFICAS PARA COMPRA DE BIENES Y SERVICIOS CONEXOS – ADQUISICIÓN E IMPLEMENTACIÓN DE UN GESTOR DE SEGURIDAD DE INFORMACIÓN Y EVENTOS (SIEM)". En consecuencia, de conformidad con el numeral **3.5 Fase de Evaluación**, para que una oferta pueda ser considerada CONFORME, deberá cumplir con todas y cada una de las características contenidas en las referidas Fichas Técnicas. Es decir que, **ASYSTEC** se considera CONFORME de lo ofertado, quedando el oferente **HABILITADO** para la apertura del sobre B del proceso de Licitación Pública Nacional INDOTEL-CCC-LPN-2023-0009.