ENTE OPERADOR REGIONAL
DEL MERCADO ELÉCTRICO DE AMÉRICA CENTRAL

Términos de Referencia
"Implementación de SIEM"

Los presentes términos de referencia son requerimientos mínimos esperados, por consiguiente, no deberá entenderse que son absolutos y limitantes a los alcances y valores agregados que se puedan ofrecer.

Entidad contratante

El Ente Operador Regional (EOR) es una institución constituida por el "Tratado Marco del Mercado Eléctrico de América Central"; Acuerdo Ejecutivo N° 1292, del Ramo de Relaciones Exteriores, aprobándolo y Decreto Legislativo N° 207, ratificándolo; ha sido creado con personalidad jurídica propia y capacidad de derecho público internacional.

1. Objeto.

Realizar el monitoreo de ciberseguridad 24x7x365 de los sistemas informáticos de la institución por medio de un Centro de Operaciones de Seguridad (Security Operations Center) denominado SOC, empleando las herramientas especializadas en la gestión de eventos e información de seguridad (Security Information and Event Management) denominadas SIEM para mitigar, detectar, analizar y responder oportunamente a incidentes de ciberseguridad.

2. Alcance del servicio

Gestión de Eventos Informáticos y Registros de Auditoría (LOGS)

Software de gestión de eventos e información de seguridad, dicho software deberá ser líder en la industria de ciberseguridad como SIEM para respaldar la detección de amenazas, el cumplimiento y la gestión de incidentes de seguridad a través de la recopilación y el análisis, tanto en tiempo real como histórico, de eventos de seguridad, así como una amplia variedad de otros eventos y fuentes de datos contextuales.

Las funciones a desarrollar para la gestión de eventos son las siguientes:

- ✓ Instalación y configuración de herramienta en servidor recolector de información.
- ✓ Monitorear el estado de registro de todas las fuentes de registro de eventos de los sistemas informáticos (Logs).
- ✓ Tableros personalizados en tiempo real de cada fuente de información monitoreada.
- ✓ Recopilar, centralizar y normalizar los datos de registro de diversas fuentes de datos: puntos finales (endpoints), servidores y estaciones de trabajo con diversos sistemas operativos, red (firewalls, switches, routers, etc.), sitios web, servicios en la nube, base de datos, aplicaciones, gestores de identidad/perfiles digitales y bitácoras de escaneo de vulnerabilidades, entre otros.
- ✓ Configurar el sistema de registro de eventos según sea necesario y actualizarlo según cambios de política, regulaciones, cambios tecnológicos, casos de uso y otros factores.
- ✓ Verificar, adquirir, probar e implementar las actualizaciones y parches necesarios para mantener el SIEM de registro vigente y adecuado a las necesidades de detección, análisis y respuesta.
- ✓ Documentar y notificar las anomalías en los ajustes, configuraciones y procesos de registro.
- ✓ Correlacionar registros de diferentes fuentes para detección de anomalías de comportamiento, casos sospechosos, intentos de acceso no autorizado y movimientos laterales, entre otros.
- ✓ Integrarse con los sistemas y fuentes de registro existentes.
- ✓ Proveer, oportunamente, informes que incluyan las recomendaciones pertinentes y acciones sugeridas para mitigar los riesgos inherentes a los incidentes, anomalías y amenazas detectados, con la debida justificación y documentación de respaldo.

TIPOS	Sistema Operativo	CANTIDAD
HP PROLIANT DL20 -GEN 10	Alpha VMPRO	**1**
DELL PowerEdge E210	WINDOWS SERVER 2008	**1**
Servidor HP G10	ESXi 7.0	**1**
Servidor DL 380 G10	WINDOWS SERVER 2016	**1**
Servidor DL 380 G9	WINDOWS SERVER 2016	**1**
ServidorDL 380 G7	WINDOWS SERVER 2008	**1**
Servidor DL 380 G7	WINDOWS SERVER 2008	**1**
NAS-Storage 1650	WINDOWS SERVER 2012	**1**
Servidor DL 380 G10	WINDOWS SERVER 2019	**2**
Servidor DL 380 G10	Red Hat Linux Server	**1**
Servidor DL 380 G10	ESXi 6.0	**1**
HP Proliant DL 360 10	Windows Server 2016	**1**
HP Proliant DL 360 G9	Windows Server 2016	**1**

HP Proliant DL 160 G9	Windows Server 2016	**1**
HP Proliant DL 180 G9	Linux Centos 7.6	**1**
HP Proliant DL 160 G9	Windows Server 2012 R2	**3**
HP Proliant DL 160 G9	Linux Centos 7.9	**1**
HP Proliant DL 360 G9	Windows Server 2012 R2	**2**
HP Proliant DL 360 G9	Oracle Linux Server 7.6	**1**
HP Proliant DL 360 G9	Red Hat Enterprise Linux Server 7.6	**1**
HP ProLiant DL380 Gen10	Linux	**2**
MSA 2050 SAN	Linux	**1**
HP Proliant DL 160 G9	Windows Server 2012 R2	**1**
HP Proliant DL 180 G9	Windows Server 2012 R2	**2**
HP Proliant DL 380 G7	Linux Centos 6.7	**1**
DELL Poweredge R720	Windows Server 2008 R2	**1**
HP Proliant DL 360 G10	Oracle Linux Server 7.5	**1**
ORACLE SERVER X6-2	Solaris 11	**2**
SUN FIRE X4170	Solaris 10	**2**
SUN SERVER X4-2	Solaris 10	**2**
SUN Oracle Server X5-2	Solaris 10 / Oracle Linux 7.9	**2**
Oracle FS1	Solaris 10	**1**
Oracle STORAGETEK SL150	Unidad de cinta	**1**
HP Proliant DL 380 G10	Oracle Linux Server 7.9	**1**
DELL Poweredge R320	Windows 2012 Standard	**3**
DELL Poweredge R720	Windows 2012 Standard	**1**
DELL Poweredge R730	Windows 2012 Standard	**1**
Servidor DL 380 G10	WINDOWS SERVER 2019	**2**
Servidor DL 380 G10	WINDOWS SERVER 2019	**2**
Servidor DL 380 G9	WINDOWS SERVER 2016	**1**
Switches	Fortinet / Cisco	**8**
Firewalls	Fortinet	**12**
Planta Telefonica	AVAYA	**2**
Workstations	Windows 10	**2**
TOTAL		**78**

Servicios del Centro de operaciones de Seguridad (SOC)

Monitoreo 24x7x365 de los eventos de ciberseguridad, con personal calificado que ejecute los procedimientos de detección, análisis y respuesta necesarios, en función de la complejidad y severidad de los incidentes que se presenten

Detección:

- ✓ Monitoreo 24x7x365 de la disponibilidad de los activos de información, equipo y sistemas.
- ✓ Identificación de incidentes

- ✓ Detección y seguimiento de intentos de ataque de denegación de servicio
- ✓ Generación de alertas
- ✓ Descarte de falsos positivos
- ✓ Comunicación multicanal de alertas (e-mail, chat, SMS, teléfono móvil y consola WEB, entre otros)

Análisis:

- ✓ Correlación de eventos de ciberseguridad
- ✓ Manejo y priorización de incidentes
- ✓ Investigación y búsqueda de amenazas relacionadas con exploits, malware, ransomware, virus y ataques, entre otros
- ✓ Establecimiento de Reglas y casos de uso ajustables

Respuesta:

- ✓ Aplicación de reglas
- ✓ Tableros de control (dashboards) y reportes personalizados
- ✓ Informe de estado de salud de los equipos físicos semanales
- ✓ Reporte inmediato ante una incidencia critica de ciberseguridad, con las recomendaciones para mitigar la misma
- ✓ Reporte de seguimiento de incidencias de ciberseguridad quincenal

Condiciones Generales

- ✓ El proveedor de servicios de SOC debe de tener su centro de monitoreo 24x7x365.
- ✓ El ofertante deberá demostrar experiencia en la prestación de los servicios requeridos en este documento. (presentar al menos 2 referencias de clientes).
- ✓ Se deberá contar con personal con conocimiento comprobado y certificado como analista de SOC, mínimo dos ingenieros.
- ✓ Se deberá contar con personal con conocimiento comprobado y certificado para manejo de incidentes de SOC, mínimo un ingeniero.
- ✓ El oferente debe ser partner con el nivel más alto por el fabricante en la herramienta de SOC ofertada en el servicio. (Presentar acreditación del fabricante).
- ✓ El oferte debe estar habilitado por parte del fabricante como partner a nivel de MSSP (Proveedor de Servicios Gestionados de Seguridad) para El Salvador.
- ✓ El oferente debe presentar al menos una certificación de un ingeniero especialista que lo acredite por parte del fabricante con los conocimientos del uso de la herramienta de SOC ofertada en el servicio.
- ✓ La información de registros, logs, analítica, reportería deberá ser almacenada de forma local, en las instalaciones del centro de monitoreo SOC del oferente.

3. <u>Tiempo de entrega</u>

El tiempo requerido de entrega será de 4 semanas posterior a la firma de la orden de compra.

FIN TDR

Ing. Marlon Castillo - Gerente de IT