

## **PLIEGO COMPRAS DIRECTAS**

### **CAPITULO I**

#### **Objeto:**

Objeto: Adquisición e instalación de un SIEM (Security Information and Event Management), estos eventos serán generados por hardware y software generado por equipos instalados en la infraestructura de la unidad. Con la misma se gestionaran los eventos generados.

Ordenamiento de Ítems:

Las ofertas comprenderán el suministro de los siguientes ítems:

ITEM	ARTICULO (descripción)	CANTIDAD (UN)
1	Adquisición e instalación de SIEM.	1

## CAPITULO II – CONDICIONES GENERALES

### **Forma de cotizar**

Solo se aceptarán cotizaciones:

- En condiciones plaza  
Cotización por la totalidad del objeto:

### **Antecedentes del oferente**

El oferente deberá demostrar la capacidad técnica necesaria para llevar adelante este proyecto.

En cuanto a sus antecedentes comerciales, el oferente deberá presentar una relación de comercialización y/o implementación del producto ofrecido, que se encuentre implantada en al menos dos empresas de Uruguay de porte similar al de UTE, y con resultados satisfactorios verificables.

El no cumplimiento de estos requisitos será motivo de rechazo de la oferta.

El oferente deberá fundamentar su experiencia en la prestación de servicios de Similares características. En dicha documentación se podrá incluir: Nombre de la empresa, fecha de entrega de los servicios, descripción de los mismos y Responsable de recepción de los servicios de dicha empresa, incluyendo número telefónico para contactarlo.

El oferente deberá adjuntar documentación que acredite que es representante oficial o distribuidor en Uruguay de la marca ofertada, con una antigüedad de por lo menos 5 años. La no presentación de dicha documentación será motivo de rechazo de la oferta, a sólo juicio de U.T.E

### **Condiciones de rechazo de la oferta**

- 1) No cumplir el plazo de mantenimiento de oferta (30 días) solicitado en el punto 7 de las Condiciones Generales para Compra Directa.- (esta causal de rechazo es para todos los casos)

### **Comparación de ofertas**

- La comparación de ofertas se realizara por la totalidad de los Ítems
- El cumplimiento de las especificaciones técnicas

### **Adjudicación**

La adjudicación se realizara por la totalidad de los Ítems solicitados a un único proveedor

### **Condiciones de entrega**

El suministro deberá ser entregado e instalado en Sede Norte, Aparicio Saravia 4292.

### **Forma de Pago**

El pago se realizará de acuerdo al Punto 13 de las Condiciones Generales para Compras Directas, previa conformidad del área usuaria

## **CAPITULO III – CONDICIONES TECNICAS**

### **Especificaciones Técnicas**

#### **ITEM 1 – Adquisición e instalación de SIEM.**

##### **REQUISITOS GENERALES**

La solución de SIEM deberá:

- El software se deberá instalar en servidores virtuales instalados en las instalaciones de PAC.
- Contar con soporte y licencias por 1 año,
- Permitir la integración con nuevas soluciones de terceras partes,

Se valorará que la solución ofrecida se encuentre en el cuadrante mágico de Gartner.

##### **CAPACIDAD OPERATIVA**

La solución de SIEM deberá:

- Ser escalable para permitir crecer en la cantidad de fuentes de origen de eventos y en volumen de datos almacenados.
- Ser capaz de coleccionar eventos provenientes de dispositivos y aplicaciones que componen las soluciones tecnológicas existentes en PAC. Se priorizará el no requerir la instalación de agentes en los componentes de generación de eventos.
- Tener capacidad de descubrir nuevas fuentes de eventos una vez que empiece a recibir tráfico de las mismas.
- Centralizar los eventos a correlacionar y emitir de alertas basadas en reglas de análisis en tiempo real.
- Tener la capacidad de correlacionar eventos de un mismo y/o distinto origen, y de diferentes aplicaciones y plataformas.
- Permitir hacer drill down en un determinado evento cuando esto se requiera para obtener más información.
- Tener la capacidad de generar una alerta en base a un conjunto de eventos correlacionados, aunque los mismos en forma individual no generen una alerta.
- Proporcionar alertas basadas en anomalías y cambios de comportamiento observados en los datos de la actividad de la red.
- Monitorear y alertar en caso de que se interrumpa el flujo de logs desde un dispositivo por una cantidad de minutos que se podrá configurar en el sistema.

- Tener capacidad de brindar información de contexto de los eventos detectados.
- Proveer una interfaz para la gestión de las alertas y la minimización de los falsos positivos de modo de poder proveer resultados más precisos.
- Permitir generar reglas de correlación personalizadas entre diferentes dispositivos según los criterios y necesidades de PAC.
- Incluir una librería de reglas (filtros) predefinidos para cada una de las plataformas/aplicaciones, permitiendo su rápida implantación sobre el sistema.
- Permitir la configuración de las reglas de correlación en forma sencilla a través de asistentes y definiciones de alto nivel.
- Permitir ejecución de un script a partir de un incidente.
- Disponer de un mecanismo de archivado a largo plazo de todos los eventos de seguridad.
- Permitir analizar los eventos de un periodo determinado, aunque los mismos ya hayan sido archivados.
- Soportar la detección de la ubicación geográfica del origen de la comunicación en tiempo real.
- Proveer mecanismos para realizar el seguimiento de los incidentes de seguridad a través de un amplio rango de atributos (por ej: direcciones IP, usuarios, direcciones MAC, orígenes de logs, reglas de correlación, atributos definidos por el usuario, etc). Se debe poder filtrar los incidentes por estos atributos definidos.
- Tener la capacidad de enmascarar datos sobre la interfaz gráfica,
- Permitir categorizar eventos en función de su importancia y/o reglas definidas por UTE,
- Procesar eventos enviados via syslog, SNMP, SNMP traps y acceder a tablas de auditoría propias en bases de datos,
- Permitir que se definan campos nuevos que no forman parte de los predefinidos en el producto,
- Almacenar los paquetes de los eventos en su formato original con fines forenses además de en su formato procesado/parseado,
- Permitir la recolección, análisis y clasificación de paquetes de red, para realizar análisis forense,

En caso que la solución incluya la instalación de agentes en los dispositivos monitoreados deben especificarse:

- Patrones y valores de referencia sobre la carga de procesamiento extra generada por el producto sobre los equipos.
- Patrones y valores de referencia sobre el tráfico generado en la red.
- Se valorará que la solución presentada permita:
  - i. Una cantidad ilimitada de orígenes de eventos que se pueda procesar.

ii. vincular la información de cada evento que se centraliza, con la vulnerabilidad de cada activo que se haya encontrado y aportar información a las reglas de correlación.

iii. supervisar las configuraciones de topología de red, switches, routers, firewalls y sistemas de prevención de intrusiones (IPS) y detecte condiciones que generen riesgos de seguridad. Por ejemplo La solución deberá simular ataques de red y modelar cambios de configuraciones para evaluar su impacto sobre la seguridad.

#### **ADMINISTRACIÓN**

La solución de SIEM deberá:

- Tener una consola única de administración con una interfaz gráfica intuitiva.
- Permitir la administración remota vía HTTPS y SSH.
- Proporcionar autenticación de usuarios vía LDAP/Radius/AD, permitir la definición de usuarios y perfiles con diferentes privilegios y/o niveles de ejecución.
- Proveer un tablero de control restringido por perfiles de usuarios.
- Proveer una interfaz de consulta sobre todos los eventos consolidados o sobre un
- Subconjunto de los mismos. Las consultas deben poder predefinirse para determinados
- perfiles.
- Tener sincronización horaria automática vía NTP.
- Permitir la configuración de alarmas ante determinados eventos, mediante diferentes.
- Mecanismos de notificación (correo, SMS, etc.).
- Proveer capacidades de workflow.
- Permitir la gestión de respaldos, restores e históricos.

#### **REPORTES**

La solución de SIEM deberá:

- Permitir la creación y personalización de dashboards, reportes en HTML y PDFs y reglas.
- Adecuadas a los provistos por la solución en forma nativa para la captura y visualización de eventos.
- Permitir la generación y visualización de reportes por diferentes usuarios del sistema según su perfil.
- Generar reportes de forma automática y periódica.
- Permitir la edición de reportes predefinidos y guardar los cambios para utilizarlos en otro momento.

- Se valorará la existencia de reportes predefinidos que la solución incluya en forma nativa, como por ejemplo aquellos que colaboren en el cumplimiento de normas de seguridad. Ej: ISO 27001, COBIT, etc.

#### LICENCIAS Y ACTUALIZACIONES

La solución ofrecida debe incluir:

- Licenciamiento para hasta 1100 eventos por segundo sin limitar por orígenes.
- La licencia de software debe ser perpetua y permitir cambios y crecimiento de arquitectura.
- Reutilizando lo adquirido por UTE en esta instancia.
- Actualización de firmas online en forma automática.
- Actualización automática y de forma programada de parsers y parches de la plataforma, no se aceptarán soluciones cuyas actualizaciones se realicen únicamente de forma manual.
- Actualizaciones de firmware vía HTTPS, FTP, etc,
- Las actualizaciones deberán incluir también las liberadas por el fabricante respecto a
- Corrección de bugs y vulnerabilidades del propio sistema,
- Integración con sistemas de reportes de amenazas globales que permiten identificar, detectar y reportar potenciales incidentes de seguridad El funcionamiento del sistema no debe quedar atado a una renovación de mantenimiento, suscripción, etc. En caso de no realizarse esta renovación, el sistema debe continuar operativo en toda su funcionalidad (solo se perderán los derechos a contar con nuevas versiones del software y actualizaciones, respuesta contra amenazas globales, así como el soporte técnico del fabricante).

#### INSTALACIÓN, IMPLEMENTACIÓN.

El oferente será responsable por la instalación e implementación del producto.

El producto se adquiere en la modalidad “llave en mano”. Los servicios de relevamiento, implementación y puesta en marcha son parte de la propuesta, se deberán realizar junto con los Analistas de Seguridad y Monitoreo de PAC, y deben incluir:

- Relevamiento, recolección de datos y documentación de requerimientos
- Armado, control y seguimiento del plan del proyecto
- Recomendaciones relacionadas a las mejores prácticas y procesos para implementar la herramienta.
- Diseño de la solución.
- Instalación de los módulos del producto.
- Documentación de la instalación realizada.

- Configuración de los módulos de acuerdo a los requerimientos.
- Carga inicial de datos.
- Ajustes de la implementación hasta quedar operativo.
- Se pedirá la Implementación de 3 (tres) orígenes nativos del SIEM que serán elegidos por UTE.