BANCO CENTRAL DE RESERVA DEL PERÚ

INFORME Nº 0147-2020-GTI230-N

ASUNTO : Informe técnico previo de evaluación de software - Renovación de servicios de la solución de gestión de información y eventos de seguridad informática (Mcafee SIEM)

---

1. NOMBRE DEL ÁREA:

Dpto. de Redes, Telecomunicaciones y Bases de Datos

2. RESPONSABLE DE LA EVALUACIÓN:

Alexander Gamboa Inga

3. CARGO:

Especialista en Redes, Telecomunicaciones y Bases de Datos

4. JUSTIFICACIÓN:

Una vez que se han implementado los puntos de detección y control en una red corporativa, se presenta el desafío de lograr una gestión coherente a partir de una multitud de vistas de productos individuales para, de este modo, resolver posibles problemas de seguridad en forma eficiente.

Firewalls, IPS, VPNs, son elementos críticos de una arquitectura de defensa a profundidad, asimismo también es necesario aplicar protección a ruteadores, switches y otros elementos de la red. De allí que el objetivo sea conseguir la capacidad de ver, analizar y responder a información a través de la infraestructura completa, dado que la suma de todos esos productos y equipos proporcionarán un significado más útil que la vista de componentes individuales.

Por otra parte, con la necesaria proliferación de puntos de detección y control en la red, los operadores tienen disponible una gran cantidad de información producida por todos esos productos con capacidades de registro. Eventos y alertas constituyen la evidencia crítica para entender cómo se propagan amenazas a través de la red, pero el problema está en encontrar el modo de recolectar, analizar y priorizar en forma efectiva esta evidencia, cuando cientos de miles (y hasta millones) de registros de eventos son originados diariamente desde estos dispositivos. La información sobre amenazas y alarmas viene desde muchas fuentes tales como archivos de registro de servidores y estaciones, firewalls, IPS, switches, datos de flujo de red, registros de VPN o alertas. Esto crea un enorme desafío para el personal de TI que debe analizar datos desde una multitud de fuentes para entender las amenazas que están enfrentando y determinar qué acciones tomar.

Frente a esta problemática, en el grupo de sistemas de gestión de seguridad, se desarrollaron dos categorías de producto complementarias:

- ✓ Gestión de eventos de seguridad (Security Event Management - SEM)
  Proporciona monitoreo en tiempo real de eventos de seguridad. SEM está orientado a identificar amenazas y alertar al personal de soporte técnico, que es responsable de su atención.

- ✓ Gestión de información de seguridad (Security Information Management – SIM)
  Proporciona administración de logs y reportes referentes a eventos de seguridad. SIM está orientado a mantener registros históricos, necesarios para generar reportes sobre el estado de cumplimiento de normativas, investigación forense y análisis de las amenazas presentadas.

Posteriormente las necesidades de la industria llevaron a la aparición de una nueva categoría de producto, que combina funcionalidades SEM y SIM, y que ha sido denominada Gestión de Información y Eventos de Seguridad (SIEM – Security Information and Event Management).

Next Generation SIEM

La primera generación de soluciones SIEM se enfrentó a la siguiente problemática

- ✓ El incremento en la frecuencia y complejidad de las amenazas de seguridad
  Cada día se incrementa el número de amenazas, las mismas que se hacen cada vez más sofisticadas en sus estrategias, con lo cual la detección de las mismas es cada vez más compleja.

- ✓ Nuevos dispositivos y aplicaciones
  El uso de dispositivos móviles en el entorno laboral ha complicado enormemente la seguridad. Hoy en día se realizan transacciones y acceso a información sensitiva a través de teléfonos móviles y tabletas con acceso a Internet, por lo que se requiere entregar servicios seguros a través de dichos dispositivos.

- ✓ Creciente complejidad del ambiente regulatorio
  Empresas tanto del sector público como privado tienen que adecuarse a nuevas regulaciones y requerimientos de cumplimiento, lo que obliga a que luego de pocos años, las soluciones sean reevaluadas, actualizadas o incluso reemplazadas.

- ✓ Inadecuada recolección de datos
  Uno de los aspectos más importantes de encontrar un correcto balance de elementos en recolección de datos, almacenamiento y análisis. La respuesta más simple a la pregunta ¿qué datos se debería recolectar? es “todo”, pero es imposible de cumplir en la mayoría de los casos. Puede suceder que no se recolecte la información necesaria, o que esta por tanto no esté disponible cuando se necesite.

- ✓ Gestión de datos de gran volumen
  Aún si una empresa recolecta todos los datos relevantes a sus necesidades de seguridad, administrar esa información es otra historia. La gran mayoría de organizaciones tienen una cantidad limitada de recursos en planta física, hardware de almacenamiento, personal y costos de operación. El volumen de datos a ser recolectados y administrados puede llegar a ser asombrosamente

alto – en algunos casos hasta petabytes al año – especialmente cuando las regulaciones requieren retención de datos por un año o más.

- ✓ Análisis de datos de gran volumen
  Incluso si una organización puede contar con toda la data relevante que necesita, aún enfrentará obstáculos en la tarea de extraer la información necesaria para conducir una investigación. Esto incluye la necesidad de realizar un análisis inicial para detectar un problema, ejecutar consultas complejas sobre grandes volúmenes de datos de los datos, en búsqueda de tendencias significativas o patrones sospechosos.

- ✓ Sobre-normalización
  La solución más común a la sobrecarga de datos es la normalización, la cual permite destacar los eventos más significativos. Pero la normalización a menudo puede despojar a la información de su significado, por ejemplo eliminando registros específicos que podrían ser necesarios como elementos probatorios.

Ante la problemática mencionada surgió una nueva generación de soluciones SIEM (Next Generation SIEM), enfocados en los siguientes procesos clave:

- ✓ Uso de fuentes de información adicionales
  Se agregan nuevas fuentes de información más allá de los logs, tales como servicios de reputación, detección de anomalías y monitoreo de la actividad de red (análisis de flujos y en algunos casos captura de paquetes).

- ✓ Cumplimiento de normativas y regulaciones
  Pueden incluirse métricas de alineamiento a normativas y regulaciones tales como ISO, PCI, SOX, entre otras.

- ✓ Detección de amenazas en tiempo real
  Mayores capacidades de correlación de eventos para detección de amenazas, a través de motores de detección inteligentes.

- ✓ Respuesta a incidentes
  Se proporciona estrecha integración con los dispositivos de seguridad, permitiendo automatizar respuestas ante comportamientos anómalos. Por ejemplo detectar un atacante y generar automáticamente el bloqueo de este a través de reglas del firewall o el IPS.

- ✓ Análisis de datos e investigación forense.
  Se incluye la capacidad de análisis de datos de gran volumen (big data analytics).

NTP-ISO/IEC 27001 : 2014 y SIEM

Las soluciones SIEM nos permiten implementar controles requeridos en el Anexo A de la norma NTP-ISO/IEC 27001 : 2014, entre ellos:

Dominio	Objetivos de control	
Seguridad de las operaciones	12.4.1	Registro de eventos

Seguridad de las comunicaciones	13.1.1	Controles de la red
Gestión de incidentes de seguridad de la información	16.1.2	Reporte de eventos de seguridad de la información
	16.1.4	Evaluación y decisión sobre eventos de seguridad de la información
	16.1.5	Respuesta a incidentes de seguridad de la información
	16.1.6	Aprendizaje de los incidentes de seguridad de la información
	16.1.7	Recolección de evidencia

5. ALTERNATIVAS:

El BCRP cuenta con la solución de gestión de información y eventos de seguridad informática (SIEM) de la marca Mcafee, adquirida el año 2016.

6. ANÁLISIS COMPARATIVO TÉCNICO:

Debido a que es una solución con la cual ya cuenta el BCRP desde el año 2016, y el cual ha sido solicitado sea estandarizado, lo que se desea es contratar la renovación de servicios.

7. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

Beneficios:

- Correlación de eventos registrados por múltiples soluciones de seguridad informática, permitiendo mejorar la detección de amenazas.

- Análisis de grandes volúmenes de datos recopilados, permitiendo visibilidad de amenazas en tiempo real, así como investigación forense de incidentes de seguridad.

Costos:

Las prestaciones requeridas corresponden al periodo de un (01) año de servicio:

Prestación principal

- ✓ Renovación de servicios de soporte, incluyendo las actualizaciones de software y soporte técnico (escalamiento) del fabricante Mcafee.
- ✓ Renovación de la suscripción Mcafee Global Threat Intelligence (GTI).

Prestación accesoria

- ✓ Servicio de mesa de ayuda y soporte técnico local 24 x 7.
- ✓ Servicio de mantenimiento técnico preventivo.
- ✓ Capacitación.

En lo que respecta a los costos asociados, la solución fue adquirida por S/ 559 338,00 incluido IGV (AS 0090-2016-BCRPLIM). Se obtuvo una cotización referencial para la renovación de servicios por el periodo de un (01) año, por un

monto de S/ 207 820,00 incluido IGV, lo que representa el 37,15% del monto de adquisición.

8. CONCLUSIONES:

Por lo expuesto anteriormente, se considera conveniente la contratación de la renovación de servicios de la solución de gestión de información y eventos de seguridad informática (Mcafee SIEM) por el periodo de un (01) año.

Lima, 4 de agosto de 2020

cc.

BANCO CENTRAL DE RESERVA DEL PERÚ

FIRMADO POR:

Alexander John Anthony GAMBOA INGA
Especialista en Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

Leandro Manuel ALVAREZ FIGUEROA
Jefe de Departamento de Redes, Telecomunicaciones y Bases de Datos
Departamento de Redes, Telecomunicaciones y Bases de Datos

VISADO POR:

Miguel Angel TEJADA MALASPINA
Subgerente de Servicios de Tecnologías de Información
Subgerencia de Servicios de Tecnologías de Información

Felipe Ernesto ROEL MONTELLANOS
Gerente de Tecnologías de Información
Gerencia de Tecnologías de Información

Javier Ernesto OLIVERA VEGA
Gerente Central de Administración
Gerencia Central de Administración