Funcionalidades obligatorias de la solución SIEM

1. La solución SIEM debe proporcionar una arquitectura distribuida a escala con las siguientes características:

a. Todos los componentes de la Colección, de aquí en adelante referidos como Colectores, se proporcionan como un dispositivo virtual.

b. Los recolectores envían datos de eventos al nivel de almacenamiento y correlación

c. Los recolectores pueden almacenar datos en caché en caso de que el recolector pierda comunicación con el motor de correlación principal, luego que la comunicación se reestablezca el recolector deberá de enviar los datos almacenados en caché en caso de una implementación distribuida.

d. Los recolectores comprimen los datos antes de enviarlos al nivel de almacenamiento y de correlación.

e. Los recopiladores se comunican con el nivel de almacenamiento y correlación a través de HTTPS. La dirección de comunicación es DESDE los recopiladores al nivel de almacenamiento y correlación.

f. Si falla un colector, se puede implementar un colector de reemplazo simplemente volviendo a registrar el colector con el nivel de almacenamiento y correlación. Los recopiladores no se configuran individualmente, sino que se administran centralmente y no debe haber ninguna configuración específica, aparte de la información de la dirección IP para volver a implementar un recopilador. Nota: no debe existir ningún licenciamiento adicional para el despliegue de n recolectores.

g. Los recolectores deben ser capaces de procesar 10K EPS.

h. Los recolectores deberían poder procesar la información de NetFlow.

i. Los recopiladores también deberían actualizar automáticamente los nuevos analizadores cuando se actualicen nuevos analizadores en el sistema de gestión central de SIEM

2. El nivel de almacenamiento y correlación de SIEM al que ahora se hace referencia como SIEM Cluster debería:

Utilizar dispositivos virtuales (VA) en lugar de físicos segundo.

Los VA debe proporcionarse para:

Vmware,

Hyper-V

KVM iv.

Imagen de AWS disponible

c. El SIEM Clúster puede escalar agregando VA adicional al clúster. Esta capacidad de escalamiento debe:

i. Proporcione correlación de reglas distribuidas en tiempo real en memoria en todos los componentes del clúster.

ii. Proporcione reportes distribuidos y reportes analíticos a través del Clúster SIEM. Esto debe ser automático y el usuario no debería necesitar especificar qué componente necesita ejecutar una búsqueda En el sistema de gestión central de SIEM

d. El Clúster de SIEM no debe limitar la cantidad de datos de eventos que se almacenan. Este límite solo debería ser la cantidad de almacenamiento que se proporciona.
e. El SIEM Clúster debería ser capaz de escalar, esto significa que el SIEM Clúster puede comenzar con un solo VA y escalar agregando más VA. Los datos de eventos se pueden almacenar en un disco virtual cuando se trabaja con un solo VA y también en NFS cuando se trabaja con el SIEM Clúster (VA múltiples). Nota: no debe existir ningún licenciamiento adicional para el despliegue nuevos VA.
f. El SIEM Clúster debe poder escalar a más de 500K EPS
g. El SIEM Clúster debe poder almacenar tanto el registro de eventos brutos como el registro de eventos analizados / datos normalizados.
h. No debería haber ningún requisito para un nivel de "almacenamiento" separado que filtre o envíe un subconjunto de eventos reenviados por los recopiladores a un nivel de correlación. El SIEM Clúster debe poder procesar cada evento reenviado por el nivel de colección.
i. Los datos del evento deben almacenarse en un modo comprimido.
j. El SIEM Clúster no debe usar una base de datos relacional (MS SQL, Postgresql, MySQL, Oracle) para almacenar los datos del evento. Se debe usar una base de datos moderna para almacenar datos de eventos como una base de datos no SQL.
k. Una base de datos relacional se puede usar para almacenar plantillas, incidentes y otra información estructurada.
l. Él VA debe ejecutarse en Linux y tener la capacidad de actualizar los paquetes del sistema operativo.

3. El SIEM debe ser capaz de recopilar contexto adicional más allá de los datos de registro de los dispositivos y esto debe lograrse mediante:
Descubrir activamente los dispositivos dentro de la red sin un agente y usar protocolos estándar tales como:

SNMP
WMI
VM SDK
OPSEC
JDBC
Telnet
SSH
JMX

b. Capacidad para controlar el estado y la capacidad de respuesta de los servicios, incluidos DNS, FTP / SCP, TCP / UDP genérico, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH y Web - HTTP, HTTPS (paso único y paso múltiple)

i. Los resultados de este monitor de disponibilidad se pueden usar para calcular la capacidad del servicio, como la disponibilidad de un servicio que está disponible al 99%.
c. Una vez descubierta, la inmersión debe presentarse en una Base de Datos de Gestión de Configuración (CMDB) dentro de la solución SIEM y mostrarse como mínimo.
i. Versión / Firmware / OS instalado en el dispositivo
ii. Número de serie del dispositivo
iii. Interfaces configuradas en el dispositivo junto con
1. Nombre de la interfaz
2. IP y subred
3. Estado de la interfaz (habilitado, deshabilitado)
4. Cualquier nivel de seguridad configurado en el dispositivo
5. La velocidad de la interfaz
6. La velocidad y el nombre de la interfaz deben ser editables
iv. Procesos que se ejecutan en el dispositivo o sistema operativo
v. Alertar cuando hay un cambio en el estado del proceso al monitorear activamente usando protocolos como se describe en los protocolos 3.a. Por ejemplo, alerta cuando un proceso o servicio se detiene.
d. Los dispositivos se deben llenar automáticamente dentro de Grupos en la CMDB, por ejemplo, Grupo de servidores de Windows, Grupo de cortafuegos.
e. Las aplicaciones que se ejecutan en dispositivos deben descubrirse automáticamente y la CMDB debe tener un grupo de aplicaciones que llene automáticamente los dispositivos del grupo. Por ejemplo, el grupo de aplicaciones "Servidores IIS" debe enumerar todos los dispositivos que ejecutan Microsoft IIS.
f. Ser capaz de informar sobre toda la información dentro de la CMDB:
i. Informe sobre el firmware de los dispositivos o el número de versión
ii. Proporcione un informe de auditoría con aprobación / falla, ya sea que el dispositivo tenga la versión apropiada de Versión / Firmware / SO instalada en el dispositivo.
g. Una vez que se complete el descubrimiento activo de los dispositivos, el SIEM debe tener una plantilla incorporada que definirá automáticamente qué métricas se recopilarán para los dispositivos y los intervalos de recolección. Las métricas se deben recopilar usando protocolos que se muestran en la sección 3.a.
Las métricas de rendimiento recopiladas deben incluir:
i. Uso de la interfaz, errores, bytes enviados y recibidos
ii. UPC
iii. Memoria
iv. Disco
v. Utilización del proceso

4. El SIEM debe proporcionar una interfaz de análisis unificada que permita que el mismo lenguaje de consulta analice tanto los datos de registro como los datos de rendimiento.
5. El sistema debería poder incluir eventos en los recopiladores que no son relevantes o que no son necesarios. Esto no debería afectar ninguna licencia.
6. Tanto los datos brutos, analizados y enriquecidos se deben pasar al clúster SIEM desde los recopiladores.

7. El procesamiento de datos de eventos debe ser realizado por analizadores sintácticos en el sistema.
8. Todos los analizadores deberían poder ser modificados y personalizados.
9. Los analizadores personalizados deberían poder crearse y definirse en la GUI sin acceso CLI.
10. Se pueden agregar nuevos atributos (variables analizadas), dispositivos y tipos de eventos a través de la GUI sin acceso CLI.
11. Los analizadores deben definirse en un marco XML con las siguientes capacidades:
a. Capacidad de definir patrones que se repiten como variables.
b. Posibilidad de definir funciones para identificar pares clave de valores
c. Capacidad para realizar pruebas y funciones de casos
d. Capacidad de realizar transformaciones en los datos en la etapa de análisis sintáctico.

12. Los dispositivos se pueden monitorear sin agentes a través de SSH, telnet WMI, JMX y PowerShell.
13. Capacidad de recopilar eventos de Windows a través de WMI y agente
14. El SIEM debe proporcionar un Agente de Windows que tenga las siguientes capacidades:
a. Agentes administrados centralmente
b. Capaz de recoger registros de archivos de texto en dispositivos con Windows
c. Capaz de recopilar registros de eventos que no sean Seguridad, Sistema y Aplicación
d. Realizar la supervisión de integridad de archivos
e. Realizar el seguimiento del registro
f. Monitor para dispositivos extraíbles
g. Ejecute los comandos de PowerShell y envíe de vuelta la salida como registros
h. Ejecutar comandos WMI y enviar de vuelta la salida como registros
i. El agente de Windows debe enviar datos de eventos a los componentes de SIEM cifrados mediante HTTPS
15. El SIEM debe proporcionar acceso basado en roles para restringir el acceso a los datos y también restringir el acceso a la GUI.
16. El SIEM debería ser capaz de descubrir Active Directory y LDAP y mostrar el directorio en la GUI.
17. El directorio se puede usar en condiciones de filtro dentro de informes y análisis.
18. Los métodos de autenticación externa deben ser compatibles e incluyen:
a. Directorio Activo
b. LDAP
c. RADIUS

19. Posibilidad de integrar feeds de Threat Intelligence (TI):
a. integración de archivos CSV se puede realizar a través de la GUI
b. Soporte para
i. Direcciones IP
ii. Dominios
iii. Hashes
iv. URLs
c. Cada TI puede admitir hasta 200.000 entradas

d. Se deben proporcionar varias integraciones a TI comerciales y del fabricante de la solución de SIEM.
e. Se debe proporcionar una cantidad de integraciones a Open Source TI en la caja
f. Posibilidad de correlacionar datos de TI en tiempo real, en memoria contra datos de eventos.
g. Posibilidad de correlacionar datos de TI con datos de eventos históricos.

20. Capacidad de consultar eventos en una vista analítica en un modo de transmisión, de modo que se informe sobre eventos antes de almacenarlos en el disco.

21. Proporcione informes listos para usar, sin costo adicional, para:
a. PCI-DSS
b. HIPAA
c. SOX
d. NERC
e. FISMA
f. ISO
g. GLBA
h. GPG13
i. Controles críticos SANS

22. Capacidad para exportar e importar paneles, informes y reglas a través de XML.
23. Capacidad para recopilar la configuración del dispositivo de red, identificar cambios y proporcionar una comparación lado a lado.
24. Los paneles se pueden presentar en una vista de diapositivas.
25. Las visualizaciones del tablero deben admitir tipos de gráfico de:
a. Bar
b. Tarta
c. Línea
d. Mesa
e. Combinación (línea y vista de tabla)
f. Treemap
g. Gráfico de dispersión
h. Valores individuales
i. Calibradores
j. Mapa Geográfico
k. Los umbrales rojos, ámbar y verde se pueden definir en los cuadros, según corresponda.

26. Notificación y gestión de incidentes
a. Marco de notificación de incidentes basado en políticas
b. Posibilidad de activar un script de corrección cuando ocurre un incidente especificado
c. Integración basada en API a sistemas de tickets externos: ServiceNow, ConnectWise y Remedy
d. Posibilidad de ampliar la integración del sistema de tickets a través de API.
e. Sistema integrado de emisión de boletos

27. Analítica potente y escalable
a. Busque eventos en tiempo real, sin la necesidad de indexar y usar operadores lógicos como AND, OR, NOT y paréntesis.
b. Búsquedas basadas en palabras clave y búsquedas por atributos de eventos analizados contra datos.
c. Buscar eventos históricos: consultas similares a SQL con condiciones de filtro booleanas, grupos por agregaciones relevantes, filtros de hora del día, coincidencias de expresiones regulares, expresiones calculadas, GUI y API.
d. Los operadores para la búsqueda deben incluir =,! =, <,>, IS NULL, IS NOT NULL, contiene, no contiene, contiene regex, no contiene regex.
e. Dispara en patrones de eventos complejos en tiempo real utilizando el motor de reglas.
i. Las reglas deben poder variar desde umbrales simples como el número X de eventos con una cantidad de tiempo Y de Z Distinct Values.
ii. Patrones completos que admiten la lógica booleana completa y permiten:
1. Sub patrones conectados en la dimensión de tiempo por operadores como AND, OR, FOLLOWED BY, AND NOT, y NOT FOLLOWED_BY
2. Cada subpatrón puede filtrar y aplicar operadores de agregación como AVG, MAX, MIN, COUNT y COUNT DISTINCT
3. Los umbrales pueden ser estáticos o estadísticamente derivados de datos pro.
a. El perfil estadístico y las alertas de eventos deberían incluir
i. Promedios móviles
ii. Desviaciones estándar
b. Si se excede un umbral estadístico, se generará una alerta casi en tiempo real.
f. Usar objetos CMDB descubiertos y datos de usuario / identidad y ubicación en búsquedas y reglas

g. Programar informes y entregar resultados por correo electrónico
i. Posibilidad de exportar informes en CSV y PDF
h. Buscar eventos en toda la organización o en un dominio de informes físicos o lógicos
J Listas dinámicas de vigilancia para realizar un seguimiento de los infractores críticos: con la posibilidad de utilizar listas de vigilancia en cualquier informe o norma
i. Escale las fuentes analíticas añadiendo nodos VA sin tiempo de inactividad en el clúster SIEM
k. La priorización de informes de incidentes se puede implementar a través del servicio comercial crítico. Los servicios empresariales permiten modelar, dentro del SIEM, los dispositivos y aplicaciones que conforman un servicio.
l. Capaz de correlacionar automáticamente al usuario con la ubicación y la dirección IP:
i. Proporcionar la capacidad de informar y buscar en el usuario a la dirección IP a la ubicación. La ubicación puede ser el puerto del conmutador físico, la dirección MAC o VPN.
ii. Enriquezca eventos en los que no se proporcione un contexto de usuario basado en la dirección IP.
28. Posibilidad de reenviar cualquier información de evento recopilada a través de KAFKA.
29. Archivo de datos basado en políticas a otra ubicación, como un montaje NFS. Los datos deben poder restaurarse a través de la GUI para búsquedas analíticas.

30. La integridad de los datos del evento se puede verificar a través de la GUI recalculando el hash de los datos del evento con un hash almacenado dentro del SIEM en el momento de escribir los eventos en el disco.

Requerimientos técnicos de implementación

1- Empresa con técnico certificado en: solución ofertados y CEH, ITIL Foundation y 10 años de experiencia en implementaciones de la solución, Unico ingeniero. (No se permiten certificaciones individuales)
2- Certificación del fabricante de distribución autorizado
3- Servicios técnicos basados en la migración de los equipos actuales y nuevos requerimientos
4- Logística de distribución de equipos en todo el país
5- Precio final debe de incluir viáticos de implementación.