SOW – Declaración de Trabajo
Servicio de Fortalecimiento de Seguridad

Preparado para:

BanCoppel

Noviembre 16, 2021

Confidencialidad

La información presentada en este documento es exclusivamente confidencial para Red Hat. Se ha puesto a disposición de BanCoppel para su consideración y revisión. En ningún caso, todo o parte de este documento se divulgará o difundirá sin el permiso expreso por escrito de Red Hat. El titular de este documento no podrá divulgar la información a ninguna persona fuera del grupo responsable por la evaluación del mismo, sin el consentimiento expreso de Red Hat.

Introducción

Este documento fue preparado para BanCoppel para cotizar y explicar el servicio de fortalecimiento de seguridad. Este documento se rige por los términos y condiciones comerciales que se mencionan a continuación.

Objetivos

El área de Desarrollo de Sistemas de BanCoppel enfrenta la necesidad de revisar y ajustar la configuración de 30 servidores RHEL v6.x o superior seleccionados, para realizar una serie de ajustes en la configuración que permitan fortalecer las defensas de estos contra posibles ataques de seguridad.

Se designará por parte de Red Hat un grupo de consultores que acompañarán al equipo designado por BanCoppel por un periodo de 2 meses.

Este equipo asistirá al personal de BanCoppel en la realización de acciones para el contexto de negocio del Cliente, con el fin de:

- Instalación de software Red Hat de autentificación y conectar a 30 servidores RHEL v6.x o superior para su autentificación.
- Revisión de configuración de 30 servidores RHEL v6.x o superior para validar el registro de Linux.
- Revisión de configuración de 30 servidores RHEL v6.x o superior para mejorar la protección del servicio OpenSSH.
- Revisión de configuración de 30 servidores RHEL v6.x o superior para limitar los puertos abiertos y los servicios.
- Revisión cuentas privilegiadas en 30 servidores RHEL v6.x o superior.
- Eliminación de los shells innecesarios o no utilizados en 30 servidores RHEL v6.x o superior.
- Limpieza y verificación del sistema operativo en 30 servidores RHEL v6.x o superior.

Actividades a realizar:

<u>Revisión del registro de Linux:</u>

- Configurar el sistema de syslog en 30 servidores RHEL v6.x o superior.
- Revisión de la configuración de iptables en 30 servidores RHEL v6.x o superior.

- Configuración del paquete sudoers en 30 servidores RHEL v6.x o superior.
- Limitar el uso del crontab únicamente para usuarios con privilegios en 30 servidores RHEL v6.x o superior.
- Configuración del cliente de Red Hat Insights en 30 servidores RHEL v6.x o superior.
- Verificar que las bitácoras de los 30 servidores de RHEL se archiven y reenvíen a un SIEM (Security Information and Event Manager) para su almacenamiento, procesamiento y análisis fuera de línea. Las bitácoras que se consideran son:
    - Bitácoras DHCP.
    - Bitácoras de eventos de seguridad (controladores de dominio, servidores y sistemas críticos).
    - Bitácoras de autenticación web (IIS, Apache) de sistemas y servicios críticos.
    - Bitácoras de la solución de administración de cuentas privilegiadas (PAM)
    - Bitácoras de tecnología de detección basada en antivirus/host.
    - NOTA: El cliente deberá contar con un sistema de SIEM y garantizar que este sea compatible con las versiones del sistema operativo RHEL en uso.
- Verificar que los 30 servidores de RHEL estén configurados para registrar y retener información según las siguientes recomendaciones:
    - Intentos de autenticación exitosos y fallidos, con prioridad en los servicios de red los cuales pueden proporcionar acceso administrativo (ej. SSH).
    - Uso de cualquier invocación de cuenta "root" o privilegiada, como el comando "su" (ej. Registro de "sudoers").
    - Conexiones entrantes denegadas (ej. aquellas bloqueadas por iptables)
    - Historial de comandos (ej. bitácoras del historial de bash shell), incluidos los registros de fechas.
    - Los registros de fechas se pueden incluir con el historial de bash modificando el archivo predeterminado "bashrc" o "/etc/profile.d".
- Entregar documentación a BanCoppel de los comandos y pasos que se utilizaron para la realización de las actividades descritas en esta sección.

<u>Revisión del servicio OpenSSH:</u>

- Revisión de la configuración de OpenSSH en 30 servidores RHEL v6.x o superior.
- Verificar que se cuenta con un acceso restringido para las cuentas y grupos accesibles por OpenSSH en 30 servidores RHEL v6.x o superior.
- Verificar que se cuenta con un acceso restringido para procesos automatizados y accesos remotos por OpenSSH en 30 servidores RHEL v6.x o superior.
- Verificar que se cuenta con un acceso restringido a usuarios autentificados por OpenSSH en 30 servidores RHEL v6.x o superior.
- Verificar cuando aplique, cual es el puerto al que escucha el demonio sshd y hacer ajustes de esta configuración en caso de ser necesario.
- Configurar el acceso con privilegios mínimos para todas las cuentas y grupos accesibles por OpenSSH, especialmente para procesos automatizados y acceso remoto.
- Limitar el acceso al servidor por medio de OpenSSH sólo a cuentas de usuarios autenticados ajenos a root. Verificar si se puede implementar la autenticación criptográfica basada en llaves públicas se puede configurar junto con la contraseña para habilitar la autenticación

multi factor y proteger el acceso al servicio OpenSSH configurado en el sistema.
- Entregar documentación a BanCoppel de los comandos y pasos que se utilizaron para la realización de las actividades descritas en esta sección

Revisión de puertos abiertos y servicios de red:

- Desactivar puertos de red que BanCoppel ha identificado como no necesarios, dentro de 30 servidores RHEL v6.x o superior.
- Desactivar servicios de red que BanCoppel ha identificado como no necesarios, dentro de 30 servidores RHEL v6.x o superior.
- Bloquear las direcciones IP, los puertos y los sinkholes de nombres de dominio que hayan sido identificados por BanCoppel para los 30 servidores RHEL.
- Verificar que las comunicaciones de salida de los 30 servidores y sus sistemas críticos se pueden denegar de forma predeterminada. Las restricciones de acceso a Internet deben configurarse idealmente para denegar todo, con cualquier excepción documentada y aprobada por el equipo de seguridad de la información, el cual debe implementar los controles para inhibir y detectar cualquier actividad sospechosa asociada con la excepción.
- Validar que todo el tráfico de salida de red aprobado bajo excepción debe registrarse, continuar enrutado por medio de un proxy web y restringirse a un conjunto específico de direcciones IP, puertos y protocolos. Si no se pueden bloquear eficazmente todas las comunicaciones de salida de los servidores, se considerará (como mínimo) restringir el acceso a sitios externos por medio de FTP, HTTP, HTTP y SSH. Además, BanCoppel debe considerar bloquear el acceso a sitios de almacenamiento en la nube externos (ej. OneDrive, Dropbox, SendSpace, ShareFile) para que no sean accesibles desde todos los servidores. Con un proxy web o un filtro de contenido web, denegar el acceso a los sitios de almacenamiento en la nube debería ser factible mediante la configuración de categorización del sitio (en lugar de tener que definir cada sitio por separado).
- Verificar que se está utilizando un firewall basado en host como iptables para restringir el acceso a servicios que no son necesarios como parte del negocio en RHEL v6.x y 7.x. En el caso de RHEL v8.x, validar que se está utilizando el marco nftables en lugar de iptables, como la función predeterminada de filtrado de paquetes.
- Deshabilitar el acceso fuera de BanCoppel de los protocolos FTP y Telnet en los 30 servidores RHEL.
- Entregar documentación a BanCoppel de los comandos y pasos que se utilizaron para la realización de las actividades descritas en esta sección.

Revisión y documentación de cuentas privilegiadas:

- Revisar y documentar las cuentas configuradas en 30 servidores RHEL v6.x o superior.
- Revisar y documentar las cuentas que tienen privilegios de root en 30 servidores RHEL v6.x o superior.
- Validar que la documentación de las cuentas privilegiadas incluye a los miembros de los grupos a los que se les haya delegado acceso privilegiado dentro del dominio y a los miembros de todos los grupos privilegiados integrados, incluidos: Operadores de

cuentas, Administradores, Operaciones de respaldo, Administradores de DNS Administradores de dominio, Administradores de esquemas, Bitácoras del cortafuegos/NetFlow y proxy web, Bitácoras de proxy inverso/WAF, Bitácoras del balanceador de carga (incluidos los encabezados HTTP X-Fordered-For), Bitácoras de autenticación de VPN, incluida la IP de origen y el nombre de host (todos los dispositivos VPN) y Operadores de servidor.

- Eliminar todos aquellos usuarios que no correspondan o estén autorizados de acuerdo a las recomendaciones de BanCoppel, relacionados con las aplicaciones que actualmente se ejecutan en 30 servidores RHEL v6.x o superior.
- Verificar que el único usuario configurado en un sistema con UID 0 sea la cuenta predeterminada de root.
- Habilitar las opciones "Password is Required" y “Sensitive account and cannot be delegated" en las cuentas ya existentes y que han sido identificadas por BanCoppel en los 30 servidores RHEL.
- Eliminar el atributo "Admin SDHolder" de todas las cuentas que no están en grupos privilegiados en los 30 servidores RHEL.
- Imponer la caducidad de las contraseñas en las cuentas privilegiadas de los 30 servidores RHEL.
- Entregar documentación a BanCoppel de los comandos y pasos que se utilizaron para la realización de las actividades descritas en esta sección.

Eliminación de los Shells innecesarios o no utilizados:

- Eliminar todos aquellos Shells que no se utilicen o no estén autorizados de acuerdo a las recomendaciones de BanCoppel, que se ejecutan en 30 servidores RHEL v6.x o superior.
- Verificar si el shell predeterminado de la cuenta root no ha sido reemplazado por otro binario de shell en 30 servidores RHEL v6.x o superior.
- Verificar los shells de inicio en 30 servidores RHEL v6.x o superior.
- Entregar documentación a BanCoppel de los comandos y pasos que se utilizaron para la realización de las actividades descritas en esta sección.

Limpieza y verificación del sistema operativo:

- Verificar que el sistema operativo tenga los parches requeridos en 30 servidores RHEL v6.x o superior.
- Verificar que el sistema opera haya actualizado el antivirus (firmas) y se haya completado un análisis total del disco en 30 servidores RHEL v6.x o superior.
- Verificar que se hayan restablecido todas las contraseñas de las cuentas locales del sistema en 30 servidores RHEL v6.x o superior. Este servicio incluye las cuentas de nivel de sistema operativo (SO) y las cuentas específicas de la aplicación (ej. SQL, Oracle, aplicación web) que están presentes en los servidores revisados.
- Entregar documentación a BanCoppel de los comandos y pasos que se utilizaron para la realización de las actividades descritas en esta sección.

- Los precios están expresados en dólares americanos y no incluyen el IVA correspondiente.
- Esta cotización no incluye viáticos fuera de la Ciudad de México.
- La vigencia de la cotización es hasta el 26 de Noviembre del 2021.
- El 100% de las horas de servicio se llevará a cabo de forma remota.
- El pago del servicio se realizará al terminar cada entregable.
- El pago de la bolsa de horas se llevará a cabo de forma mensual.
- Los Servicios Profesionales de Red Hat se considerarán concluidos cuando se realice la aceptación de los entregables.
- La bolsa de horas se considerará concluida cuando se consuma el total de horas contratadas.
- El cliente debe de solicitar el inicio de las actividades del servicio con 3 (tres) semanas de anticipación a la fecha solicitada. En caso de requerirse los recursos antes de este periodo de tiempo, se harán los esfuerzos comercialmente razonablemente para acelerar el inicio de actividades.
- El cliente debe programar las actividades de la bolsa de horas con 2 (dos) semanas de anticipación a la fecha solicitada. En caso de requerirse los recursos antes de este periodo de tiempo, se harán los esfuerzos comercialmente razonablemente para acelerar el inicio de actividades.
- La presente cotización invalida las propuestas presentadas previamente para los mismos servicios.
- Este esquema de servicio no reemplaza el soporte técnico de Red Hat, el cual no está incluido.
- Si cualquier supuesto establecido en la sección de responsabilidades del Cliente, demuestra no ser válido o resulta imposible para el Cliente cumplir, Red Hat tendrá derecho a ajustes equitativos para los Servicios Profesionales o sus Tarifas. Incluso cobrarle al Cliente según el tiempo y materiales empleados utilizando las tasas estándar aplicables en ese momento de Red Hat para el trabajo adicional a ejecutarse como consecuencia o tiempo de espera. Esto también se aplica en el caso de demoras y trabajo adicional requerido que no sea responsabilidad de Red Hat.
- Los componentes a instalar (en caso de aplicar) serán validados utilizando criterios de aceptación previamente acordados. Los criterios de aceptación deberán aprobarse (firmados) antes de iniciar el servicio.
- Cualquier alteración de los supuestos enumerados anteriormente se deberá manejar a través de la Solicitud de Cambio y esto podrá producir un cambio en los plazos del proyecto.
- El conocimiento y entendimiento de los supuestos mencionados anteriormente son importantes para establecer el marco del proyecto. Previo a iniciar el proyecto estos supuestos deben ser confirmados y aceptados por ambas partes.
- La estimación de esfuerzo requerido para la ejecución de este SoW se basa en los supuestos mencionados anteriormente. De no cumplirse estos, los esfuerzos requeridos pueden variar de forma considerable.

- Queda fuera de alcance cualquier requerimiento que no se encuentre explícitamente citado en este documento.

Ubicaciones

Lugar	Dirección	Teléfono
Oficinas Red Hat México	Torre Diana Río Lerma 232 – Piso 22 | Colonia Cuauhtémoc | Delegación Cuauhtémoc | C.P. 06500 | Ciudad de México	(55) 8851-6400

Administración del Proyecto

BanCoppel designará a un Administrador de Proyecto calificado para el seguimiento a los asuntos relacionados con el cumplimiento de este SOW. El Administrador de Proyecto de Red Hat será el punto de contacto con el Administrador de Proyecto del cliente.

Proceso de Cambio

Cualquiera de las partes podrá solicitar un cambio sujetos a los términos establecidos en el contrato mediante la presentación de una Solicitud de Cambio escrita al Administrador de Proyecto, representando a la otra parte. Todas las solicitudes de cambio se realizarán completando el formato proporcionado en el Apéndice 1, "Formato de Solicitud de Cambio". Los Formatos de Solicitud de Cambio aprobados y debidamente firmados por el cliente serán evaluados por Red Hat para determinar si el cambio implica una evaluación económica. En dicho caso el área comercial de Red Hat realizará la propuesta de servicios adicionales.

Apéndice 1 – Formato para Solicitud de Cambio

ANEXO 1 – Formato para Solicitud de Cambio

Proyecto/Oportunidad:	

Número Solicitud de Cambio:		**Fecha de Solicitud:**	

Descripción del Cambio:

Más Detalles Descriptivos / Documentos Anexos al Formato de Solicitud:		**Si**		**No**

Razones para el Cambio Propuesto: (X)

	Problema/Error/No-conformidad (cambio correctivo)
	Mejora (cambio perfecto)
	Cambio en Ambiente (cambio adaptativo)
	Otros

Documentos/Entregables que requieran Actualización: (X)

	Orden de Compra		**SOW**	
	Plan de Proyecto		**Anexo PM**	
	Otros			

Estimación de Impacto

Grado del Impacto: (X)		**Mínimo**		**Moderado**		**Mayor**

Costo de Impacto del Cambio Solicitado	
Tiempo/Anexo: (Si/No) (Detalle Abajo)	**Dólares: (Si/No) (Detalle Abajo)**

Resolución Inmediata: (X)		**Si**		**No – Proceso Inicial Formal del Control de Cambio**

Evaluación Completa Requerida: (X)		**No**		**Si – (Ingresar aquí estimados)**
Estimación de costo /	**Horas:**		**Dólares:**	

Evaluación				

Nombre /Evaluador Recomendado:		**Cargo:**

Aprobaciones Para Evaluación Completa:

Cliente: _____ Cargo: _____

Resultados de la Evaluación	**Fecha de Revisión:**

Decisión: (X)

	Aprobado		**Rechazado**		**Diferido Hasta:**

Acordado:

Proveedor: _____ Fecha: _____

Cliente: _____ Fecha: _____