Malwarebytes

ES CONSULTING

SECURITY SUMMARY

https://es.consulting info@es.consulting +502 2375-7765

Revisión de Buenas Prácticas Consola Malwarebytes

CENDIS

1. Actualizar el agente de Malwarebytes

Endpoints
DESKTOP-CR5IUNS.cendis.centrodistribuidor.com
GT_FSAL_TELE_05.cendis.centrodistribuidor.com
GT_FSAL_COOR_12.cendis.centrodistribuidor.com
GR_RETA_TELE_01.cendis.centrodistribuidor.com
GT_CUIN_AUXI_.cendis.centrodistribuidor.com

Recomendación

Actualice el agente ya que es la parte del software que se encarga de comunicarse con el servidor de Malwarebytes y obtener las actualizaciones de definiciones de virus y otras actualizaciones importantes. Asegúrese que el software tenga la versión disponible más reciente para garantizar la protección optima contra las amenazas de malware y para que este software funcione correctamente en el sistema.

2. Evaluar Endpoints Inactivos

Validar inactividad de los endpoints

Endpoints inactivos +2 semanas
DESKTOP-CR5IUNS.cendis.centrodistribuidor.com
GT_FSAL_TELE_05.cendis.centrodistribuidor.com
GT_FSAL_COOR_12.cendis.centrodistribuidor.com
GR_RETA_TELE_01.cendis.centrodistribuidor.com
GT_CUIN_AUXI_.cendis.centrodistribuidor.com

Recomendación

Verificar que el endpoint cuente con conexión a internet, y que el servicio de malwarebytes se encuentre corriendo, esto para mejorar la conexión entre endpoint y consola, esto para contar con el registro de detecciones en tiempo real.

3. Realizar escaneos

Endpoints
DESKTOP-CR5IUNS.cendis.centrodistribuidor.com
GT_FSAL_TELE_05.cendis.centrodistribuidor.com
GT_FSAL_COOR_12.cendis.centrodistribuidor.com
GR_RETA_TELE_01.cendis.centrodistribuidor.com
GT_CUIN_AUXI_.cendis.centrodistribuidor.com

Recomendación

Realizar escaneos regulares en Malwarebytes para detectar y eliminar cualquier amenaza de malware que pueda haber infectado su computadora. Estos escaneos pueden ayudar a identificar y eliminar cualquier programa malicioso que pueda estar afectando el rendimiento de su computadora o comprometiendo su privacidad y seguridad.

4. Eliminar amenazas que se encuentran en cuarentena

Threat name	Category	Type	Endpoint	Location	Date
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...
PUP.Optio...	PUP	Registry V...	GT_Dige_L...	HK\S-1	05/03/202...

Recomendación

Elimine los archivos que se encuentran en cuarentena una vez que haya confirmado que se trata de amenazas de malware y ya no necesita conservarlos. Esto ayuda a liberar espacio en su disco duro y reduce el riesgo de que los archivos vuelvan a infectar su computadora. Para más información verificar la plataforma.

5. Tiene instalado otro antivirus o anti-malware

Recomendación

Desactivar o eliminar programa antivirus adicional a Malwarebytes ya que tener activos estos al mismo tiempo en un endpoint pueden entra en conflicto ya que estos trabajan constantemente en detectar y eliminar malware y lo estarían haciendo al mismo tiempo, un antivirus puede detectar un archivo como malicioso mientras que el otro programa lo marca como seguro. Esto puede llevar a un menor rendimiento del sistema, bloqueo de archivos y otros problemas.

Si en dado caso desea dejar el antivirus adicional:

Desactive la función de análisis en tiempo real de Windows Defender porque Malwarebytes funciona como programa antivirus principal en la computadora.

Adjunto se encuentra como crear exclusiones en windows para McAfee: https://service.malwarebytes.com/hc/en-us/articles/4413789721235

6. Realizar reinicios requeridos por Malwarebytes

Recomendación

Malwarebytes puede requerir un reinicio del sistema para instalar actualizaciones de software importantes y también después de un escaneo para completar la eliminación de cualquier archivo de malware restante y limpiar completamente su computadora.

Recomendaciones generales

Coordinar con los usuarios que es necesario realizar estos procedimientos para que la protección de Malwarebytes pueda cubrir el endpoint y así mismo estará resguardando los activos de información que manejen dentro de la empresa.

Eliminar el agente en los endpoints que no se estén utilizando y añadir el agente a el endpoint que estén usando, recordando que se debe hacer configuraciones de antivirus adicionales y en dispositivos mac dar acceso completo al disco.

*las recomendaciones generales dependen del cliente

CONFIDENCIAL

https://es.consulting info@es.consulting +502 2375-7765