ComWare

Nos conecta, Nos transforma

Administración de la infraestructura de seguridad

ComWare ofrece a sus clientes el servicio de administración de equipos de seguridad, el cual es posible llevar a cabo de manera remota, a través de un canal dedicado con el cliente o directamente en las instalaciones del mismo.

A continuación se describen algunas tareas de administración que se realizan sobre las plataformas administradas:

- Administración y gestión de Firewall.
- Monitoreo y creación de politicas de seguridad.
- Instalación y actualización de versiones de seguridad sobre equipos administrados.
- Administración de Firewall de bases de datos.
- Administración de WAF.
- Gestión de Amenazas Avanzadas Persistentes.
- Monitoreo de equipos de seguridad.
- Análisis de Incidentes de seguridad.
- Gestión de Consolas de Antivirus.
- Implementación de buenas practicas a nivel deseguridad informática.

01 - Firewall de Nueva Generación: Los firewalls de nueva generación, a diferencia de los firewalls tradicionales, tienen la capacidad de analizar todo el tráfico que circula a través de la red, identificando los tipos de aplicaciones que utilizan los usuarios, vinculando dichos usuarios a las aplicaciones y mitigando al máximo las amenazas relacionadas con las aplicaciones y el tráfico no deseado.

Actividades de administración sobre los Firewall de Próxima Generación (NGF):

- El equipo de especialistas de ComWare brinda prevención de amenazas mediante la eliminación de aplicaciones no deseadas y aplicación de políticas de seguridad dirigidas, para bloquear exploit de vulnerabilidades, virus, spyware, botnets y malware desconocido (APTs).

- Con nuestros servicios de administración y configuración de Firewall, es posible evitar los ataques que aprovechan la web como vector, incluyendo enlaces de phishing en correos electrónicos, sitios de phishing, comandos y control basados en HTTP, sitios de malware y páginas que llevan kits de exploit.

- Nuestros especialistas realizan descifrado SSL con políticas granulares que equilibran la inspección de contenido potencialmente dañino, al tiempo que permiten que los sitios con información confidencial y personal permanezcan cifrados.

- ComWare lleva a cabo el control granular de directivas para la actividad de navegación web, como una extensión de las políticas basadas en aplicaciones.

- Contamos con tecnologías de prevención de amenazas, con la capacidad de identificar la presencia de amenazas avanzadas, a través de la supervisión y correlación del tráfico de la red y registros de amenazas para que nuestros especialistas puedan identificar rápidamente a los usuarios infectados y analizar patrones de comportamiento anómalos.

- A través de nuestros servicios, es posible identificar quién está utilizando cada una de las aplicaciones en su red y quién puede haber transmitido una amenaza o está transfiriendo archivos.

- Nuestros especialistas de seguridad cuentan con múltiples técnicas de identificación para determinar la identidad exacta de las aplicaciones que atraviesan su red, independientemente del puerto, protocolo y táctica evasiva.

- Los firewalls de nueva generación utilizados por el grupo de seguridad de ComWare bloquean la transferencia no autorizada de archivos y datos confidenciales, como números de tarjeta de crédito o de Seguro Social, tanto en el contenido de la aplicación, como en los archivos adjuntos.

- ComWare lo ayuda a alinear el uso de las aplicaciones con sus requisitos empresariales y si es necesario y el cliente lo requiere, informa a los usuarios que están infringiendo las políticas, o incluso bloquea el uso de la aplicación de forma directa.

- Brindamos una clasificación de aplicaciones por categorías, sub-categorías, tipo de tecnología y riesgo asociado.

- ComWare le brinda detección altamente eficaz de malware y vulnerabilidades que intentan evadir el análisis dinámico, así como la identificación instantánea de variantes del malware existente.

- Nos encargamos de la implementación de Políticas Corporativas de forma centralizada o distribuida, dependiendo de la solicitud del cliente.

- Establecemos roles de acceso administrativo para brindar disponibilidad de datos.

- Realizamos la gestión centralizada de actualizaciones de software, firmas antivirus, firmas de amenazas, base de datos de filtrado de URL, licencias y demás actualizaciones que la plataforma de protección perimetral requiera.

- Los administradores encargados generan políticas relacionadas con el filtrado WEB, prevención de fuga de información perimetral, control de aplicaciones y detección de intrusos a través del IPS incorporado a la herramienta.

- Los especialistas de ComWare realizan la configuración, modificación y/o eliminación de enrutamiento de datos, independiente del tipo de protocolo, ya sean dinámicos o estáticos.

- El grupo de administradores lleva a cabo la configuración y administración de VPN Site to Site y Client to Site.

- A nivel de mantenimiento de soluciones de firewall, los operadores de seguridad realizan depuración de políticas, configuración de alertas a nivel de logs, así como el mantenimiento preventivo de hardware y software.

- Respecto al monitoreo, los operadores de SOC se encargan de vigilar todo lo relacionado con el flujo de sesiones, monitoreo de VPN´s, análisis de tráfico, seguimiento a los paquetes rechazados y validación de las aplicaciones categorizadas con riesgo alto y medio.

Reportes relacionados con el servicio de firewall de nueva generación:

- El grupo de operadores del SOC crea y envía informes personalizados para ver el tráfico de aplicaciones, amenazas y el comportamiento de los usuarios en todo lo referente a la utilización de software y aplicativos.

- El grupo de especialistas de ComWare presenta reportes de actividad de usuario en los cuales se muestran las aplicaciones utilizadas, las categorías de URL visitadas y todo lo referente a navegación web durante el período de tiempo solicitado por el cliente.

- Realizamos informes de uso y amenazas de Software como Servicio (SaaS) a través del cual se proporciona una visibilidad detallada de toda la actividad.

- El grupo de expertos de seguridad de ComWare realiza el análisis, investigación y reportes centralizados del tráfico de red, incidentes de seguridad y modificaciones administrativas.

- Los analistas de seguridad del SOC generan un informe de comportamiento de botnets: los datos relativos a aplicaciones desconocidas, tráfico IRC, sitios de malware, DNS dinámicos identificados y generan una lista con hosts potencialmente infectados.

- Dentro de los informes presentados mensualmente los administradores de la plataforma generan un mapa de amenazas en el cual se muestra una vista geográfica, incluyendo la severidad de los ataques identificados.

- Informe de supervisión de la red: este tipo de reporte es muy útil para los administradores de red ya que muestra el ancho de banda dedicado a diversas funciones de la red.

02 - Administración del servicio de protección de correo:

ComWare ofrece a sus clientes protección de los correos en la nube o en Sitio. A través de este servicio se analizan los mensajes de correo electrónico en búsqueda de archivos con comportamientos maliciosos.

A continuación se listan las actividades relacionadas con este servicio, las cuales son monitoreadas desde el SOC de ComWare:

- El grupo de especialistas de seguridad realiza la identificación de comportamientos anómalos sobre los archivos adjuntos que ingresan a través de correo.

- Los especialistas determinan la posible identidad y los motivos de un autor de amenazas para controlar cuál será su actividad en los sistemas, antes de que ingrese a la infraestructura.

- El grupo de monitoreo identifica mensajes de phishing selectivo.

- El monitoreo ejecutado sobre los correos permite localizar copias del correo electrónico maliciosos; así mismo los operadores buscan determinar si el mensaje se reenvía a nuevos objetivos de forma automática.

- El grupo de operadores identifica si las URL´s adjuntas se relacionan con direcciones maliciosas.

- A través del servicio ofrecido, se protegen los entornos de office 365 y arquitecturas de Exchange en Sitio.

Reportes relacionados con el servicio de Protección de Correo:

Los informes mensuales que se entregan asociados con el monitoreo del correo son:

- Estadística de correo maliciosos detectados.
- Cantidad de correo enviados
- Frecuencia de aparición de Malware
- Reporte ejecutivo de amenazas detectadas y controladas.
- Reporte de detonación de las muestras que
- fueron identificadas.
- Reporte de periodicidad relacionado con las amenazas.

03 - Administración de Web Applications Firewall (WAF):

Las aplicaciones WEB son uno de los principales objetivos de ataque a los cuales apuntan los ciberdelicuentes.

A continuación se describen las actividades de administración y gestión realizadas sobre el servicio de WAF:

- De manera automática se configura la herramienta para que realice un escaneo de las aplicaciones web. Con base en la información arrojada, los especialistas analizan los comportamientos normales y anormales identificados por el dispositivo de protección.

- Creación de reglas básicas: a través de esta actividad se generan reglas de bloqueo, de acuerdo con los comportamientos anómalos identificados. Así mismo los especialistas realizan ajustes y configuraciones.

- Los especialistas realizan análisis de variables de llegada GET y POST. Con esta actividad, se lleva a cabo la verificación de los métodos y encabezados sobre las páginas que están siendo protegidas.

- El grupo de analistas y administradores realiza el afinamiento de sufijos de las URL para poder filtrar los tipos de dominio y analizarlos por agrupamiento.

- Afinamiento de caracteres especiales y longitudes de enunciado: a través de esta tarea, los analistas validan las aplicaciones web en cuanto a su longitud y acceso. Así mismo, verifican el ingreso de información para caracteres alfanuméricos o especiales.

- Los operadores SOC monitorean las respuestas del servidor web y verifican los paquetes de datos relacionados con las aplicaciones publicadas.

- El grupo de operadores SOC realiza el monitoreo y análisis del tráfico web en el WAF. Lo anterior para identificar y analizar alertas críticas. Así mismo llevan a cabo las siguientes tareas:

  - Elaboración de reglas de bloqueo.
  - Afinamiento de políticas
  - Instalación de certificados web en el WAF, para poder vigilar los ingresos a través del protocolo https.
  - Administración de Listas Blancas, lo cual hace referencia a la gestión de accesos permitidos a nivel de aplicación.
  - Administración de Listas Negras, lo cual hace referencia a la gestión de accesos bloqueados.

Los analistas de SOC, posterior a la identificación de vulnerabilidades, realizan la configuración de parches virtuales.
Esta funcionalidad permite que los ciberdelincuentes no aprovechen las vulnerabilidades conocidas a nivel de motores y plataformas de desarrollo.

- **Reportes Vinculados a la administración y gestión de WAF:** El siguiente listado describe algunos de los reportes que se le entregan al cliente en el informe mensual, este Informe hace referencia a los clientes que tienen un appliance como WAF.

  - OWASP top-10 attacks: hace referencia a los reportes basados en complimiento y desviaciones según OWASP (Open Web Application Security Project).

  - Reporte de ataques de SQL Injection: el grupo de especialistas describen los ataques en donde se ha intentado inyectar sentencias SQL.

  - Reporte de ataques tipo Cross Site Scripting: se describen los ataques en donde los ciberdelicuentes han intentado inyectar sentencias código de programación.

Los siguientes reportes se relacionan con diferentes ataques, los cuales están incluidos en el informe mensual:

  - Reporte Cookie Poisoning y Reporte de inteligencia de amenazas profunda.

A continuación se mencionan los reportes que se incluyen en el informe mensual, referentes al servicio de WAF en la nube:

  - Reporte de performance, en el cual se detalla el ancho banda utilizado
  - Reporte de tráfico bloqueado.
  - Reporte relacionado con el tráfico humano y el tráfico generado por robots.
  - OWASP top-10 attacks, hace referencia a los reportes basados en complimiento y desviaciones según OWASP (Open Web Application Security Project).
  - Geolocalización, explica los sitios desde donde están atacando el portal.
  - Cantidad de ataques y la clasificación de los ataques. IP, origen de los ataques
  - Tipo de ataque (boot reputation, Cross Site Scripting, SQL entre otros)

04 - Administración de Data Loss Prevention (DLP) local o perimetral:

El DLP es un dispositivo que mitiga la fuga de información, de acuerdo con la clasificación de la misma, con que cuente la compañía. Este software de protección se instala de manera local en los equipos de los usuarios o de manera perimetral como una funcionalidad adicional que ofrecen los Firewall de nueva generación.

Los especialistas de seguridad implementan políticas de filtrado de datos que reducen los riesgos asociados con la transferencia de archivos no autorizados. Este servicio se ofrece realizando una configuración de manera local en los equipos de escritorio del cliente y de manea perimetral, habilitando la funcionalidad en el firewall de nueva generación. En ambos escenarios es necesario que el cliente tenga clasificada la información que desea proteger.

A continuación se describen las actividades de administración del DLP:

Bloqueo de archivos por tipo: el grupo de especialistas controla el flujo de una amplia gama de tipos de archivos utilizando tecnologías que inspeccionan la meta data y el contenido para identificar el tipo de archivo.
Filtrado de datos: los administradores de la herramienta controlan la transferencia de archivos que contienen datos sensibles como, números de tarjetas de crédito, número de cédula, o demás información que el cliente considere como confidencial.
Control de transferencia de archivos: los administradores del SOC controlan la transferencia de archivos dentro de una aplicación individual, permitiendo el uso de la aplicación y evitando las transferencias de datos entrantes o salientes no deseadas.

Reportes Vinculados a la administración del DLP.: Con respecto a la prevención de fuga de información se generarán los siguientes reportes:

- Archivos clasificados como confidenciales, los cuales usuarios finales han intentado copiar o enviar a través de correo.
- Desde el SOC se generará un documento con la cantidad de archivos filtrados en el mes.
- Verificación de agentes instalados en equipos y su estado a nivel de actualización y actividad.
- Impresoras rechazadas por no encontrase en las
- Listas Blancas.
- Listado de archivos protegidos
- Generación de listados asociados con eventos según gravedad.

05 - Administración de Prevención de Intrusos (IPS):

Los sistemas de prevención de intrusos son equipos que toman decisiones de control de acceso basados en los contenidos del tráfico.

A diferencia de los Firewall tradicionales, no solamente validan los puertos y direcciones IP, sino que también verifican el volumen de datos y las actividades de tráfico que ingresan a la compañía.

Estos dispositivos son ofrecidos por ComWare de manera dedicada o integrados, a través de los firewalls de nueva generación.

A continuación, se enuncian las actividades de administración del servicio IPS:

- Los administradores de la herramienta configuran los dispositivos IPS de tal manera que protejan las redes de todo tipo de explotaciones de vulnerabilidades, desbordamientos de búferes, ataques D.O.S y exploraciones de puertos que llevan a comprometer y dañar los recursos de información de la empresa.

- De igual manera, ComWare utiliza tecnologías que permiten realizar la decodificación de los protocolos, efectuar la detección de anomalías, comparar patrones de estado, detectar anomalías estadísticas y hacer un análisis basado en heurística.

- Nuestros especialistas se encargan de normalizar el tráfico para eliminar paquetes inválidos y malformados, además de realizar el re-ensamblaje TCP y desfragmentación IP de los paquetes, para asegurar la máxima precisión y protección a pesar de cualquier técnica de evasión a nivel de paquetes que se esté generando en la Red.

- El grupo de operadores SOC analizan los llamados de Malware denominados detección de Callback, de tal manera que se evite la devolución de llamados denominados.

- **Informes generados mensualmente asociados con la administración de IPS:** A continuación, se describen algunos reportes relacionados con la administración de IPS:

  - Detección heurística de bots.
  - Correlación de múltiples ataques.
  - Reporte general relacionado con la prevención de intrusiones avanzadas.
  - Resumen de informe, en donde se describen los equipos que están en cuarentena y las limitaciones de flujos de tráfico.
  - Limitación de conexiones basadas en hosts.
  - Informe resumido, en donde se describe el autoaprendizaje y la detección basada en perfiles.

06 - Administración de Firewall de File Server: Actualmente los enfoques convencionales para auditar la actividad de archivos y para administrar los permisos son bastante restringidos a nivel de funcionalidad. Las herramientas administrativas de terceros y otras soluciones de amplio uso, como los grupos de servicios de directorio y la auditoría de archivos incorporada a los sistemas operativos, se quedan atrás respecto a los cambios organizacionales y el crecimiento de la información no estructurada.
Con base en lo anterior, ComWare ofrece en modalidad de servicio o venta, un firewall para proteger el File Server, proporcionando la monitorización, la auditoría, la protección y la administración de los derechos de usuario en tiempo real, sobre los documentos almacenados en servidores y en dispositivos NAS.

Así mismo este producto permite auditar y bloquear, si se requiere, en tiempo real todas las actividades que se estén llevando a cabo sobre los documentos compartidos publicados en el servidor de archivos de cualquier compañía. De igual manera el Firewall de File Server permite proteger y enviar alertas generadas por accesos no autorizados, Dichas alertas son originadas en tiempo real, en el instante en el cual se están realizando actividades sobre las carpetas configuradas para ser monitoreadas.

A continuación se describen las actividades relacionadas a la administración con Firewall de File Server:

- Administración e identificación de usuarios con acceso a información restringida: esta actividad es posible realizarla a través de la creación de políticas y generación de alertas.
- Monitoreo para validar e identificar usuarios con derechos excesivos de acceso.
- Detección de usuarios con intentos de acceso a carpetas o archivos a los cuales no tienen permisos para ingresar.
- Los operadores del SOC configuran alertas y bloqueos en tiempo real, para identificar actividades anormales sobre archivos clasificados como confidenciales.
- Los analistas realizan investigación y respuesta ante los incidentes relacionados con el borrado o movimiento de archivos alojados en el File Server.
- El grupo de especialistas realiza la identificación de los archivos a los que no se haya tenido acceso recientemente.
- Los administradores de la herramienta apoyan con información que permita simplificar los análisis de los derechos de usuario durante los proyectos de migración y de consolidación.

- **Reportes:** A continuación se describen algunos de los reportes que pueden ser originados sobre la herramienta de protección de File Server.

  - Los operadores SOC realizan la generación de informes relacionados con los archivos creados, borrados o movidos durante el mes sobre el Servidor de Archivos.
  - Reporte de carpetas con mayor antigüedad de haber sido creadas.
  - Listado de usuarios y carpetas a las cuales tienen acceso dichos usuarios.

Adicional a los anteriores reportes y según las políticas acordadas con el cliente, se generará la información que con base en auditorías de archivos el área de tecnología considere necesaria.

07 - Administración del Firewall de Base de Datos: ComWare ofrece a sus clientes un Firewall de base de datos, con el cual es posible automatizar las auditorías de las bases de datos e identificar en tiempo real los ataques, las actividades malintencionadas y el fraude que se pueda realizar sobre las diferentes bases de datos que se estén auditando.

A continuación se describen las diferentes actividades de administración que se realizan en este producto:

- El grupo de especialistas del SOC realiza auditoría de todos los accesos a información restringida sobre tablas y en general las bases de datos.
- Los operadores SOC configuran alertas y bloqueos de ataques a las bases de datos y las actividades no autorizadas, de esta manera los movimientos anómalos son reportados en tiempo real.
- Con Base en el monitoreo configurado desde el SOC, es posible detectar y aplicar parches virtuales a las vulnerabilidades de las bases de datos que no puedan ser remediadas, en ocasiones por obsolescencia. Esta actividad es llevada a cabo por los administradores especialistas de la herramienta.
- A través de tareas programadas, los administradores identifican los derechos excesivos de usuario.
- De acuerdo con la información identificada por los administradores durante la gestión de la herramienta, es posible entregar información que permita agilizar la respuesta ante incidentes.

Así mismo, a través de la herramienta es posible aportar información que en determinado momento apoye las investigaciones forenses que el cliente esté llevando a cabo.

Reportes

- Los especialistas generan informes relacionados con la auditoría continua del uso de la información restringida.
- Elaboración de reporte relacionado con la detección de accesos no autorizados y de actividades fraudulentas durante el período.
- Los administradores generan informes en los cuales describen el bloqueo en tiempo real de las inyecciones SQL, de los ataques D.O.S, entre otros.
- Si el cliente lo requiere, se entrega un reporte de cumplimiento según las normas SOX, PCI DSS e HIPAA.
- Mensualmente se diagnostica y se genera un listado basado en la evaluación de parches virtuales para las vulnerabilidades de las bases de datos.
- Dentro de los listados que se le entregan mensualmente al cliente, se incluye una descripción de los derechos de usuario en todas las bases de datos.

08 - Administración Anti APT – Vector WEB: A continuación se detallan actividades relacionadas con la administración de estos equipos:

- El grupo de operadores SOC monitorea 7x24, buscando identificar amenazas avanzadas de acuerdo con los movimientos laterales de archivos sospechosos que se puedan verificar en el dash board de la herramienta.

- Al existir algún tipo de hallazgos asociado con APT, los analistas nivel 1 investigan para determinar la posible identidad y los motivos de un autor de amenazas.

- El grupo de operadores realiza una identificación y documentación de las nuevas amenazas, con lo cual se alimenta la base de datos de conocimiento interna del SOC.

Reportes – Anti APT WEB: Los principales reportes que se generan a nivel de APT son:

- Detalle mensual de los intentos de llamado hacia direcciones web maliciosas. (callback).
- Descripción de los servidores de comando y control externos que han sido bloqueados.
- Detalle de los Host con posibles infecciones según comportamiento.
- Identificación de las alertas asociadas con actividad de malware.
- Detonación de las muestras de malware en la nube del proveedor y resultado de las mismas.

Bogotá
Cra. 13 No. 97 - 98
Tel: (57) 1 6382100
Fax: (57) 1 6382107

Cali
Calle 13A No 100 - 35 Oficina 709
Torre Empresarial Ciudad Jardín
Tel: (57) 2 4898434 - (57) 2 4898432

Medellín
Cra 43A # 1-50 Torre 1, Piso 6 - Oficina 618
Centro Empresarial San Fernando Plaza
Teléfono: 57 4 6044799
Línea de Fax: 57 4 6044731

www.ComWare.com.co **e-Mail:** mercadeo@comware.com.co