PROGRAMAS IMPLEMTADOS PARA EVALUAR SOC - NOC – ANTIVIRUS DENTRO DE PAGRAME

KASPERSKY

Kaspersky Internet Security detecta y neutraliza virus y otras amenazas de seguridad informática a petición en la cobertura del análisis especificada. Puede configurar las acciones que la aplicación debe realizar con archivos infectados. Por defecto, Kaspersky Internet Security desinfecta o elimina objetos maliciosos.

VELOCIRAPTOR

Velociraptor es un monitoreo de punto final de código abierto único y avanzado, Plataforma forense digital y de respuesta cibernética.

Velociraptor le proporciona la capacidad de responder de manera más efectiva a una amplia gama de Investigaciones forenses y de respuesta a incidentes cibernéticos y violaciones de datos:

- Reconstruir las actividades de los atacantes a través del análisis forense digital
- Busca evidencia de adversarios sofisticados
- Investigar brotes de malware y otras actividades sospechosas de la red
- Supervisar continuamente las actividades sospechosas de los usuarios, como archivos copiado a dispositivos USB
- Descubrir si la divulgación de información confidencial se produjo fuera de la red

NETWORK PERFORMANCE MONITOR (NPM) DE SOLARWINDS

No importa el tamaño de tu red ni la escala que deba alcanzar el análisis de datos y el monitoreo de recursos, te permitirá tener siempre una idea detallada del estado de tu red, en tiempo real y te funcionara como una de tus herramientas de monitoreo de red.

Monitorear disponibilidad de red.

- Reducir los tiempos durante los cuales la red permanece caída.
- Detectar fallos y generar alertas y reportes de disponibilidad.
- Resolver problemas de conectividad en tiempo récord.
- Identificar y aislar el problema de manera oportuna.

Visualizar rutas críticas.

- Detectar problemas en redes de todo tipo.
- Observar rutas en la red.
- Analizar el paso de paquetes de datos, a través de routers, entre los diferentes segmentos (hop).
- Tener claro el impacto de cada hop en el desempeño.

Mapear la estructura de la red.

- Construir el atlas de su propia red para ubicar cada elemento de manera geográfica.
- Automatizar el mapeo de la infraestructura.
- Crear mapas de calor inalámbricos.
- Asignar tareas de forma eficiente según capacidades y niveles de tráfico.

Analizar desempeño

- Correlacionar múltiples elementos en líneas de tiempo.
- Comparar entre sí todo tipo de datos.
- Aumentar la colaboración entre equipos de trabajo funcionales.