SIEM

La infraestructura informática actual de una empresa es un mecanismo complejo que incluye una multitud de sistemas corporativos. Técnicamente, cualquier evento en esos sistemas es registrado (protocolizado). Pero es imposible rastrear, analizar y reaccionar oportunamente a todos los eventos sin un sistema automatizado.

SearchInform SIEM (Gestión de Eventos e Información de Seguridad) puede recopilar, analizar, correlacionar y procesar información sobre eventos de muchas distintas fuentes:

- Estaciones de trabajo y servidores
- Sistemas operativos
- Servidores de correo electrónico
- Servidores de archivos
- Sistemas de gestión de bases de datos
- Sistemas de DLP
- Equipos de la red y otro hardware
- Dispositivos de seguridad de red integrados
- Controladores de dominios
- Active Directory
- Firewalls
- Antivirus
- Entornos de virtualización
- Aplicaciones
- Otras fuentes del syslog
- Equipos/aplicaciones propios desarrollados por el cliente (gracias al conector customizable basado en PowerShell)

SearchInform SIEM revela (entre otros eventos):

- Epidemias de virus
- Intentos de obtener acceso a los datos
- Intentos de adivinar la contraseña
- Cuentas activas de los ex-empleados
- Errores de configuración del hardware
- Rango de temperatura permitida
- Eliminación de datos de recursos críticos
- Uso de sistemas fuera de horario
- Eliminación de máquinas virtuales
- Conexión de nuevos equipos
- Cambios en la política del grupo
- Uso de TeamViewer, acceso remoto
- Eventos críticos en los sistemas de protección
- Errores y fallas en los sistemas de información

Ventajas competitivas de SearchInform SIEM:

- **Solución innovadora y facil de usar:** no es necesario ser un especialista de TI ni saber programar para operar la herramienta o crear las reglas de correlación
- **Más de 300 reglas preestablecidas:** el sistema cuenta con 30 conectores distintos, permitiendo a los usuarios editar y personalizar las reglas existentes y crear propias
- **Instale e implemente en 2 horas:** rápida implementación sin una configuración preliminar intensiva, el software comienza a funcionar el mismo día de la instalación
- **Licenciamiento por usuarios:** la solución no dejará de procesar los eventos si su número se multiplica por un ataque externo en curso

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT