Spidernext - SOAR

Spidernext SOAR es una solución avanzada de Respuesta, Automatización y Orquestación de la Seguridad (SOAR).
Permite la captura y análisis de eventos e IOCs de seguridad, así como establecer la automatización de la respuesta, interconectándose si es necesario con otras soluciones y herramientas, con las que puede intercambiar información o solicitar la ejecución de acciones para hacer frente a eventos o incidentes de seguridad.

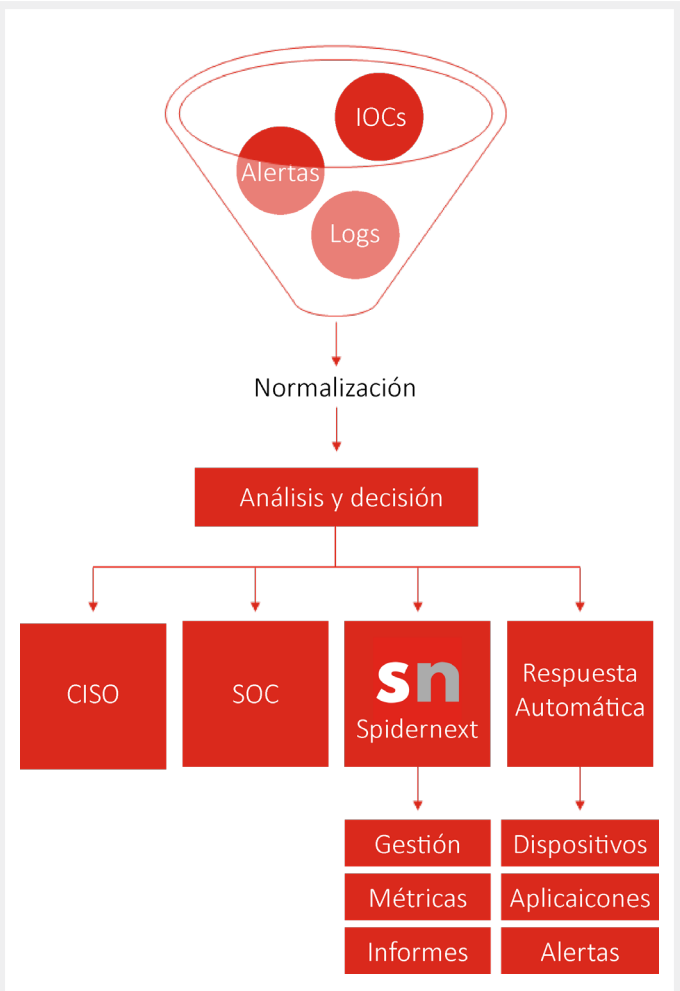
Capacidades

Respuesta a incidentes de seguridad: Respuesta inmediata y automatizada a los eventos e incidentes de seguridad, limitando el posible impacto de estos sobre la organización.

Automatización de operaciones de seguridad: Mediante la definición de flujos de trabajo, permite la automatización de operaciones de seguridad, como análisis, auditorías, verificaciones y otros procesos recurrentes, que influirán en una mejora de la protección.

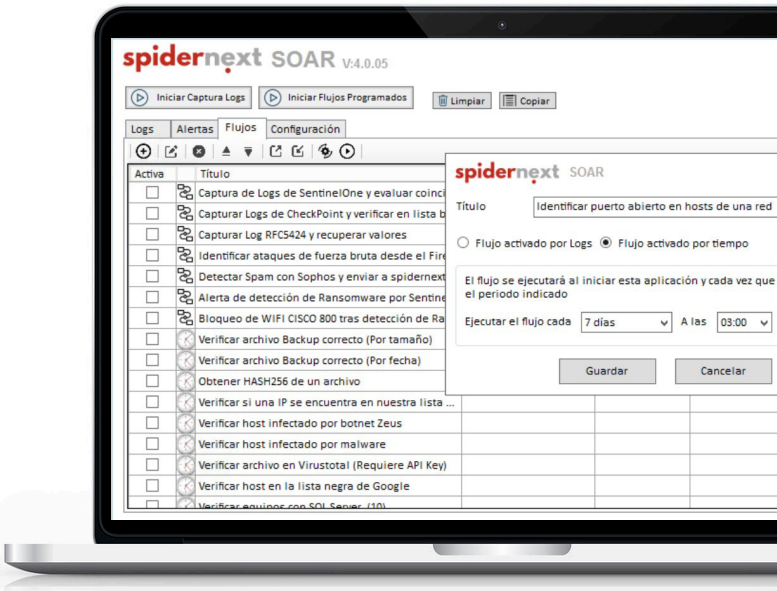
Identificación y gestión de amenazas y vulnerabilidades: Las capacidades de centralización y correlación, permiten la simple identificación de vulnerabilidades y eventos.

Mayor rendimiento y productividad: La automatización de procesos permite liberar recursos y hacer que funcionen de forma más eficiente lo equipos de IT, SOC y SecOps.



Trabaje de forma más inteligente, acelere las auditorías y respuesta a incidentes con la automatización de proceso

Organice flujos de trabajo de seguridad y automatice tareas en segundos para agilizar y potenciar su SOC.



Características y funcionalidades

Obtención de información e IOCs

- Logs UDP (RFC 5424, RFC 3164, DSF y otros).
- Información de la infraestructura de Red.
- Información de los Sistemas Operativos y usuarios.
- Información de las aplicaciones implementadas.
- Información y eventos de otras soluciones.

Operaciones

- Realización de operaciones con valores recibidos.
- Asignación, agrupación, clasificación y evaluación de datos e información.
- Operaciones con la información de administración de equipos de la red.
- Envío de alertas a la plataforma centralizada.
- Envío de notificaciones por correo electrónico.
- Mostrar mensajes y alertas.

Normalización

- Normalización de los datos recibidos por las fuentes de información.
- Normalización del formato de los Logs.

Interconexiones

- Consultar y enviar instrucciones a la electrónica de la red (SSH, SNMP y otros).
- Interconexión directa con la herramienta NMAP y uso de sus más de 600 scripts NSE.
- Integración bidireccional con EMMA del CCN-CERT.
- Interconexión con soluciones de seguridad (SIEMs, PAMs, DLPs y otras).
- Interconexión con aplicaciones de terceros.
- Consumo de servicios y APIs de terceros.

Verificaciones

- Comparación de datos y valores obtenidos.
- Verificación por patrones y expresiones regulares.
- Verificación según información de archivos.
- Verificación de disponibilidad de activos.
- Verificación de IOCs.

Exportación

- Envío de datos e información a otras soluciones, APIs o archivos.