

ARQUITECTURA DE SOC-COLOMBIA

Este es el planteamiento de lo que sería un proceso cíclico de la gestión en la seguridad informática para las organizaciones a través de un SOC, teniendo como base el sistema OSSIM. Se realiza mediante la experiencia obtenida durante el desarrollo del proyecto S.O.C-Colombia, donde hemos clasificado 8 etapas importantes.

- Dimensionamiento
- Métricas y afinamiento
- Recolección
- Detección
- Análisis
- Acción
- Respuesta
- Mantenimiento

El dimensionamiento

Tienen como principal objetivo establecer unos límites de las zonas a proteger y definir estrategias para captura del tráfico a utilizar. Se tienen en cuenta los diferentes procesos, personas y aspectos de tipo físico, siendo este el tema primordial en la elaboración de un presupuesto.

Métricas y afinamiento, se realiza durante esta etapa, las valoraciones de manera selectiva y cualitativa de los activos, que involucra la monitorización a través de un S.O.C.

Recolección

Es un análisis de despliegue de las sondas para lograr la máxima captura de datos relevantes en las redes. Así mismo se instalan mecanismos de almacenamiento que faciliten el cumplimiento del control de evidencia, y la clasificación de los mismos mediante los plugins instalados en la implementación, primer filtro de la colección de eventos.

Detección

Se hace de acuerdo a un estudio de valoración de activos previo y clasificación de vulnerabilidades en los mismos, ajusta los valores que involucran un mayor índice de riesgo para una organización, interviniendo todas las directivas que se instalan por defecto en el sistema OSSIM.

Análisis;

Intervienen todas las correlaciones cruzadas de las directivas existentes, incluyendo las mejoras logradas durante el proyecto para la sugerencia de

directivas en el motor de correlación de Ossim. Cubre las intervenciones humanas de detección y ajustes, siendo una detección de mayor nivel.

Acción;

Bajo intervención humana o automatizada, tiene el objetivo de direccionar las incidencias. Se puede lograr acciones de primer nivel que cubran los dos primeros aspectos de una acción, y comunicar oportunamente para mitigación del impacto.

Respuesta;

Tiene como principal objetivo la toma de decisiones para la reducción del riesgo. En algunos casos esta respuesta puede ser drástica para mitigar la amenaza o permisiva de acuerdo al gobierno asumido por una organización ante determinados riesgos.

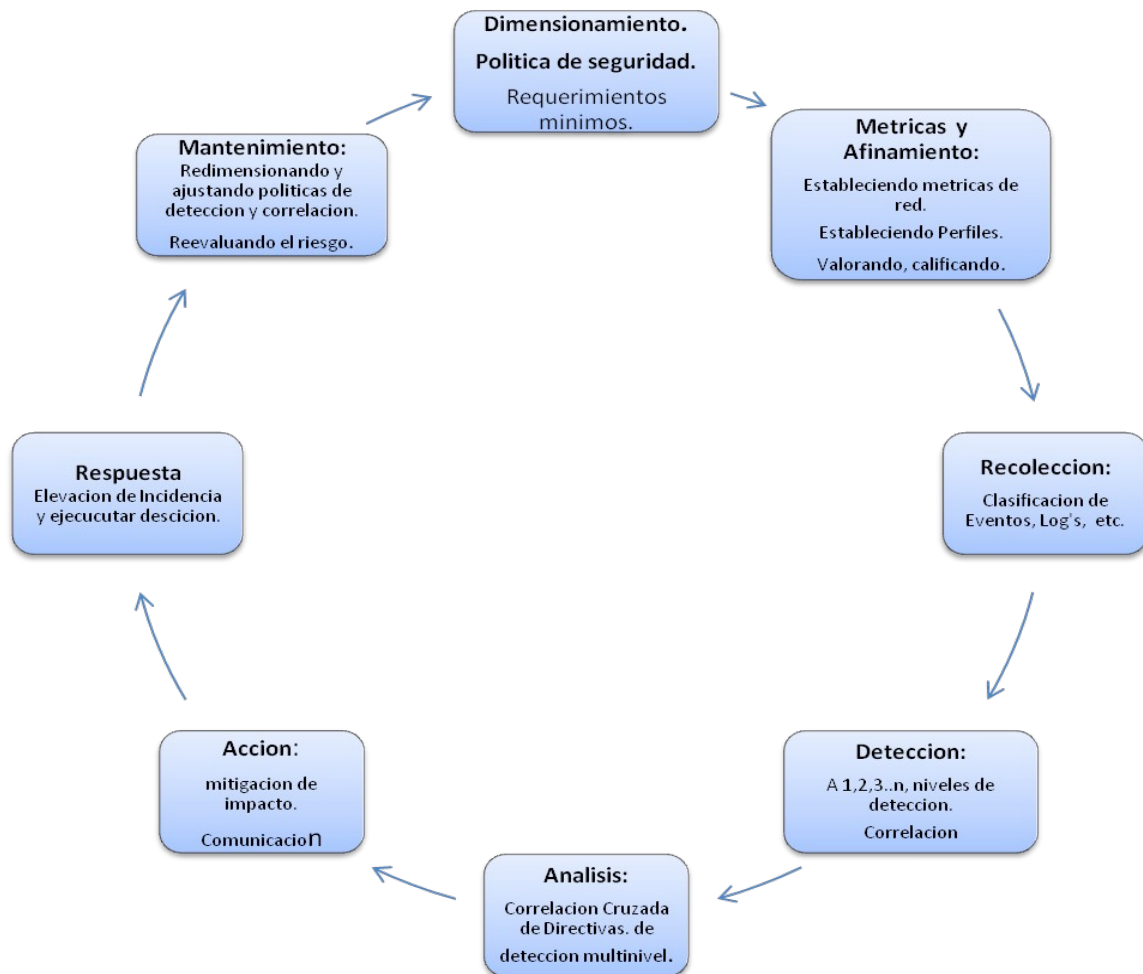


FIGURA 1. Arquitectura del S.O.C.