¿CÓMO IMPLANTAR UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)?

CÉSAR GÓMEZ LÓPEZ

SOBRE MÍ....

César Gómez López

Director Comercial & Marketing

IMAGAR SOLUTIONS COMPANY

Director Comercial y Key Account Manager con 20 años de experiencia profesional en los sectores de Servicios IT y Marketing Digital.

Apasionado del uso y aplicación de las nuevas tecnologías, así como de la innovación multidepartamental.

Consultor especializado en Tecnología, Transformación Digital y Social Selling.

INTRODUCCIÓN

ESTA GUÍA TE AYUDARÁ A CONOCER LAS VENTAJAS QUE OFRECE Y LA HOJA DE RUTA NECESARIA PARA IMPLANTAR UN SISTEMA DE GESTIÓN DE LA INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM).

La ciberseguridad se ha convertido, con el auge del teletrabajo, en una prioridad dentro de los procesos de Transformación Digital.

Los **SISTEMAS DE GESTIÓN DE DE LA INFORMACIÓN Y EVENTOS DE SEGURIDAD**, también conocidos como **SIEM**, son la herramienta que utilizan las empresas para dotar de estrategia a la seguridad, convirtiéndose en la hoja de ruta a seguir para prevenir ciberataques.

¿QUÉ ES UN SISTEMA DE GESTIÓN DE LA INFORMACIÓN Y EVENTOS DE LA SEGURIDAD (SIEM)?

Un sistema **SIEM** es un conjunto de herramientas software que mediante su interconexión ayudan a recopilar, a través de una consola central, todo lo relativo a posibles amenazas que se vayan produciendo en una infraestructura IT.

¿POR QUÉ DOTAR DE ESTRATEGIA A LA CIBERSEGURIDAD?

Nos encontramos en la era en la que, además de la operativa y continuidad del negocio, lo más importante es el dato, y por ello protegerlo se ha convertido en prioridad absoluta para los departamentos IT de las compañías. Los sistemas SIEM constituyen una herramienta imprescindible para conseguirlo, ya que centralizan y recopilan toda la información relativa a las amenazas que se van produciendo.

BENEFICIOS DE IMPLANTAR UN SISTEMA SIEM

- **Proactividad:** Un sistema SIEM consigue no tener que esperar a que se produzca un ataque malicioso, ya que dispone de un conjunto de alertas que permiten su detección y por lo tanto reaccionar previamente impidiéndo que se produzca.

- **Procedimentación:** Está compuesto internamente por grandes cantidades de información archivada respecto a vulnerabilidades y ataques, lo cual disminuye los tiempos de respuesta y de exposición. La *inteligencia artificial* y el *machine learning* son la base de este tipo de sistemas.

- **Retroalimentación:** Gracias a la potencia de la analítica de la que disponen las herramientas del sistema, los administradores pueden aplicar reglas y/o políticas preventivas para el futuro.

- **Monitorización en tiempo real:** La alta disponibilidad de este tipo de sistemas provoca que cualquier indicio de ataque o acción maliciosa sea rápidamente identificada, ya que disponen en todo momento de toda la información relativa a usuarios, dispositivos y sus respectivas acciones e interacciones dentro de la infraestructura en cuestión.

¿QUÉ NOS APORTAN LOS SISTEMAS SIEM DESDE EL PUNTO DE VISTA DE COMPLIANCE?

- El cumplimiento de la actual **normativa GDPR** se simplifica en gran medida al implantar una solución SIEM.

- Un sistema de gestión de la información y eventos de seguridad ayuda a la creación de directivas de auditoría y responsabilidad como parte de los procedimientos estándar de los Sistemas de Gestión de la Seguridad de la Información **(SGSI - ISO 2700X)**.

- Disminuye esfuerzos y costes a la hora de realizar posibles **análisis forenses** si fueran necesarios.

REQUISITOS PARA LA IMPLANTACIÓN DE UN SISTEMA SIEM

- Definición de activos que van a ser objetos de monitorización.
- Análisis de vulnerabilidades sobre dichos activos y establecimiento de niveles de criticidad.
- Definición del plan de acción sobre las vulnerabilidades identificadas.
- Dispositivos de seguridad perimetral con los que cuenta la infraestructura.
- Definición del modelo de gestión de eventos y logs.

¿CÓMO FUNCIONA UN SISTEMA SIEM?

- IDENTIFICACIÓN DE LA INFORMACIÓN
- ANÁLISIS Y UNIFICACIÓN DE EVENTOS
- APLICACIÓN DE REGLAS
- IDENTIFICACIÓN DE INCIDENCIAS

La identificación de la información se realiza a través de algoritmos que, en tiempo real, recogen toda la información procedente de los SSOO, elementos de red, software, antivirús, etc.

"EL OBJETIVO ES CENTRALIZAR LA RECOGIDA DE INFORMACIÓN Y PREPARARLA PARA LOS ANÁLISIS POSTERIORES POR PARTE DEL SISTEMA".

IDENTIFICACIÓN DE INFORMACIÓN

El análisis y unificación de eventos se encarga de centralizar toda la información proveniente de la fase de identificación, normalmente a través de los logs.

"MEDIANTE EL ANÁLISIS Y UNIFICACIÓN DE EVENTOS CONSEGUIMOS LA CENTRALIZACIÓN Y ALMACENAMIENTO DE LOS LOGS DEL SISTEMA, SIRVIENDO DE INTERFAZ DE MONITORIZACIÓN AL EQUIPO RESPONSABLE DE LA SEGURIDAD IT ".

ANÁLISIS Y UNIFICACIÓN DE EVENTOS

Disciplinas como la inteligencia artificial y el machine learning contribuyen en los sistemas SIEM a establecer y a aplicar relaciones a la información recogida y analizada, con el objetivo de generar alertas que identifican los diferentes ataques.

"PARA IDENTIFICAR EL NIVEL DE CRITICIDAD DE LOS INCIDENTES Y LA FORMA DE RESPONDER ANTE ELLOS, ES NECESARIO APLICAR REGLAS AL ANÁLISIS DE DATOS ".

APLICACIÓN DE REGLAS

En esta fase se alcanzan las conclusiones necesarias para declarar la incidencia de seguridad, fruto del resultado de las condiciones que han surgido como resultado de la aplicación de las reglas de la fase anterior.

"LA DECLARACIÓN DE LA INCIDENCIA ES EL RESULTADO DE LA APLICACIÓN DE ANÁLISIS HEURÍSTICOS Y FORENSES, REGISTROS IDENTIFICADOS DE ATAQUES, INFORMACIÓN RELATIVA A COMPORTAMIENTOS, ETC, A TODA LA INFORMACIÓN RECOPILADA Y ANALIZADA EN TIEMPO REAL ".

DECLARACIÓN DE INCIDENCIAS

¿CÓMO IMPLANTAR UN SISTEMA SIEM?

- Establecer una planificación a corto, medio y largo plazo, identificando alcances, dispositivos y magnitud de infraestructura a monitorizar, ya que estos sistemas cuentan con la característica de la escalabilidad.

- Es imprescindible para comenzar, identificar qué activos de la compañía tienen mayor nivel de criticidad, con el objetivo de que queden en el alcance inicial del sistema.

FASES EN LA IMPLANTACIÓN DE UN SISTEMA SIEM

1. Identificar elementos del sistema: En esta fase tendrá lugar el dimensionamiento del sistema, identificará todos aquellos componentes y dispositivos de la infraestructura que van a ser objeto de la gestión .

2. Definición de reglas: Se debe proceder a definir todas la reglas y políticas que indicaran los eventos que se van a controlar a través del sistema .

FASES EN LA IMPLANTACIÓN DE UN SISTEMA SIEM

3. Pulir las políticas de actuación del sistema : Con el objetivo de que todos los eventos del sistema sean lo más reales posibles, minimizando los falsos positivos.

4. Establecer los eventos de seguridad: Se definirán en esta fase aquellos eventos que han surgido fruto de las fases anteriores, con el objetivo de declarar las incidencias o ataques producidos.

Un sistema SIEM va mas allá de la administración y centralización de logs, ya que su misión es predecir ataques o incidentes de seguridad, permitiendo reaccionar para evitarlos.

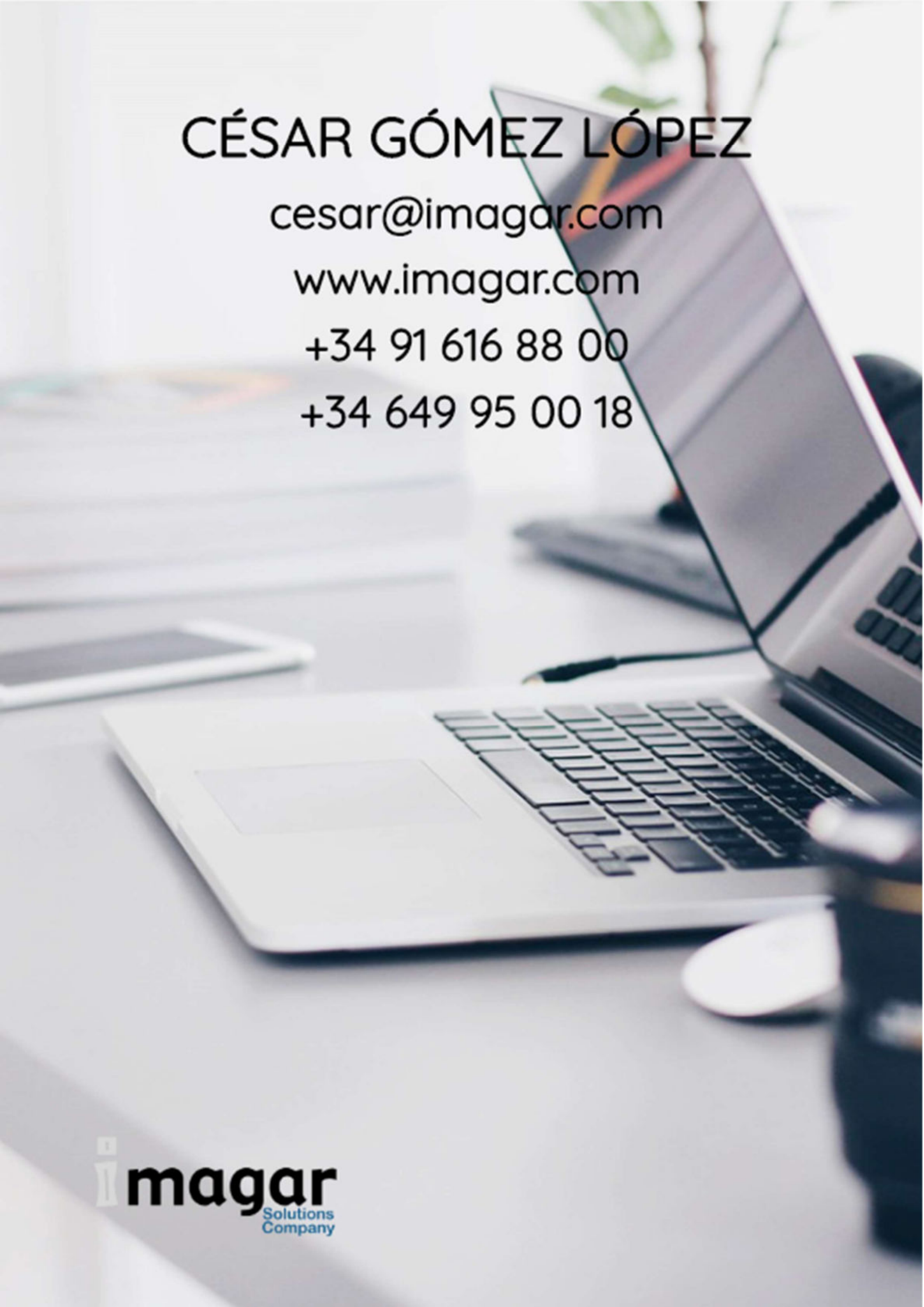
SISTEMAS SIEM Y SERVICIOS DE SOC

Los SOC (Security Operations Center) abarcan los procesos y profesionales que se encargan de dar respuesta a las incidencias recopiladas a través de los sistemas SIEM.

IMAGAR Y LOS SISTEMAS SIEM

• La transformación digital es un reto para todas las empresas y la ciberseguridad se ha convertido en un aspecto clave dentro de ella.

• Desde Imagar, empresa especialista en soluciones tecnológicas y estrategias de digitalización, ayudamos a nuestros clientes desde nuestro área de ciberseguridad con diferentes proyectos y servicios de auditoría y consultoría (tests de intrusión, consultoría y compliance ISO 2700X, plan de director de seguridad IT, etc). Y por supuesto también con servicios de seguridad gestionada, como pueden ser los sistemas SIEM y servicios de SOC.



CÉSAR GÓMEZ LÓPEZ

cesar@imagar.com

www.imagar.com

+34 91 616 88 00

+34 649 95 00 18

imagar
Solutions Company