Sistemas de gestión de información y eventos de seguridad (SIEM) del ecosistema CCN-CERT

Abstract: el CCN-CERT pone a disposición de las Administraciones Públicas dos (2) soluciones de gestión de información y eventos de seguridad (SIEM), GLORIA y MÓNICA conscientes de la necesidad de que dispongan de soluciones de ciberseguridad que permitan mejorar e incrementar la capacidad de identificación y gestión de amenazas, que presentan un mayor riesgo y requieren atención inmediata.

Contenido:

1 CONTEXTO

Los equipos de ciberseguridad deben hacer frente al creciente volumen y sofisticación de las amenazas. La falta de visibilidad de la red, el volumen de datos a analizar, la escasez de personal y la necesidad de filtrado y rápida respuesta en forma de alertas lleva consigo que para las organizaciones ya no es posible hacer este análisis en forma manual.

Con un sistema de gestión de información y eventos de seguridad (SIEM), los profesionales de la ciberseguridad cuentan con un método efectivo para automatizar sus procesos y centralizar la gestión de Seguridad de una forma que ayude a simplificar la difícil tarea de proteger la información que se maneja y el servicio que se presta.

Por este motivo, el CCN-CERT ofrece dos (2) soluciones SIEM, que permiten mejorar e incrementar la capacidad de identificación y gestión de amenazas, que presentan un mayor riesgo y requieren atención inmediata antes de que lleguen a causar incidentes con un impacto grave.

GLORIA y MÓNICA, cuyas características se describen a continuación, son soluciones nacionales que pueden ser utilizadas por la Administración Pública sin necesidad de requerir coste de licenciamiento.

2 GLORIA

GLORIA (Gestor de Logs para Respuesta ante Incidentes y Amenazas) es una solución que, desarrollada por el CCN-CERT y S2 Grupo, va más allá del SIEM para la operación integral de un Centro de Operaciones de Seguridad (CSIRT/CERT o SOC).

GLORIA es la solución española, adoptada por el CCN-CERT para la operación de sus servicios, entre ellos SAT-INET, SAT-SARA o SAT-ICS y está a disposición de la Administración Pública española, sin coste de licencias, como parte de la familia de soluciones del CCN-CERT.

GLORIA tiene capacidades de monitorización y recolección de eventos de seguridad tanto del mundo IT (*Information Technology*) como del mundo OT (*Operational Technology*), de centralización, normalización y análisis de eventos (*logs*), así como de inteligencia avanzada mediante técnicas de correlación compleja de eventos o análisis de patrones para la detección de amenazas y la identificación de anomalías.

En definitiva, el uso de GLORIA aumenta la eficiencia de los equipos de analistas de los Centros de Operaciones de Seguridad (SoC) mediante la aplicación de técnicas de automatización y orquestación de las tareas de detección y respuesta (análisis de eventos, identificación de incidentes, recolección de información de contexto, confirmación y notificación de incidentes).

2.1 Arquitectura y capacidades de GLORIA

GLORIA está compuesta por cuatro (4) módulos que asumen las distintas funciones de la solución.

- **ARGOS** es el módulo de monitorización y recolección de eventos de Seguridad dentro de la arquitectura de GLORIA. Su misión es la monitorización de seguridad del entorno tanto IT como OT, así como la recolección, modelado y centralización de los registros de actividad de los mismos para su posterior almacenamiento y análisis.
- **TRITÓN** es el módulo de inteligencia de GLORIA para la correlación y procesamiento de los eventos remitidos por el sistema de monitorización. Incluye un potente conjunto de reglas de correlación predefinidas para caracterizar un amplio abanico de situaciones de riesgo.
- **EMAS** es la consola para la gestión, análisis y detección de alertas e incidentes de seguridad que utiliza GLORIA. Recoge todas las incidencias o alertas automáticas generadas por el sistema de correlación o por los propios operadores, cuyo origen sea el proceso de soporte a usuarios o el propio equipo del SoC. Para la comunicación con el usuario final en la gestión del incidente, EMAS está integrado nativamente con LUCIA, solución de notificación de incidentes del CCN-CERT.

- **HERA** es el módulo de cuadro de mandos en tiempo real de GLORIA. Su objetivo es analizar la información en tiempo real para componer un cuadro de mando con los indicadores clave del funcionamiento de un SoC.

2.2 Integración con las soluciones CCN-CERT

GLORIA está integrada de forma nativa con las principales soluciones de detección, monitorización e intercambio de información del CCN-CERT.

La integración con **CARMEN, CLAUDIA y microCLAUDIA,** como parte natural de su arquitectura, y con **MARTA** dota al conjunto de capacidades de análisis de comportamiento (*behavioural analytics*) y potencia las actividades de búsqueda y detección de amenazas (*threat hunting*). La integración bidireccional con **LUCÍA** automatiza la comunicación y gestión de ciberincidentes conforme a las directrices del Esquema Nacional de Seguridad.

GLORIA también se comunica con **REYES** en los procesos de análisis, detección y respuesta, intercambiando inteligencia y automatizando la respuesta. Actualmente, GLORIA se encuentra en proceso de integración con **PILAR** con el objetivo de poder obtener un modelo de análisis de riesgos dinámico.

3 MÓNICA

MÓNICA es un desarrollo 100% español de la empresa ICA Sistemas y Seguridad, adoptada por el Centro Criptológico Nacional como una de las plataformas SIEM en la Administración Pública y organismos dependientes.

Como sistema automatizado de gestión de información y eventos de seguridad, recoge en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que sucedan.

3.1 Arquitectura y capacidades de MÓNICA

- **SEM (gestión y correlación de eventos en tiempo real)**
  - Detecta y resuelve amenazas en tiempo real mediante su motor de correlación PBR.
  - Prioriza e investiga incidentes relevantes mediante casos de uso (*playbooks*) personalizables.
  - Analiza el comportamiento del usuario (UEBA).
  - Ciberinteligencia de Amenazas mediante la integración con MISP/REYES.

- Responde de forma automática (*Security Orchestration and Automation Response*). Integración con The Hive/Cortex.

- **SIM (gestión y almacenamiento de registros)**
  - Punto único de control securizado y almacenamiento centralizado.
  - Securización de los registros para generación de evidencias digitales.
  - Tratamiento y almacenamiento ilimitado de eventos (*logs*) diarios (implantaciones diarias desde 5Gb a más de 1,5 Tb).

En definitiva, MONICA es tecnología española alineada con la Estrategia Nacional de Ciberseguridad. En este sentido, el acuerdo entre el Centro Criptológico Nacional e ICA SyS incluye la compartición de hoja de ruta y el desarrollo de funcionalidades específicas, así como la integración con las herramientas existentes del CCN-CERT.

3.2 Integración con soluciones CCN-CERT

MONICA tiene la posibilidad de integrarse con otras soluciones del CCN-CERT, con la herramienta LUCIA para la gestión de ciberincidentes en el ámbito de aplicación del Esquema Nacional de Seguridad y REYES para inteligencia de amenazas.

4 CONCLUSIONES

Dentro del ecosistema de herramientas del CCN-CERT surgen dos (2) soluciones para dar respuesta a la necesidad de gestión de información y eventos de seguridad: GLORIA y MONICA.

GLORIA es un gestor de eventos (*logs*) para responder ante incidentes y amenazas, permitiendo una centralización y recolección de *logs,* su consulta masiva y centralizada y la aplicación de inteligencia para la detección de amenazas mediante técnicas de correlación compleja de eventos.

GLORIA es la solución utilizada en los servicios de alerta temprana del CCN-CERT para la recogida de información de usos indebidos y anomalías en red, y está integrada junto a CARMEN/CLAUDIA, herramientas de detección de amenazas avanzadas (APT) basada en comportamientos anómalos, para orquestar la información de dichas herramientas en un punto único.

MONICA es un sistema automatizado de gestión de información y eventos de seguridad, que permite consumir información de *data lakes* existentes en su vertiente forense o aprovechar su capacidad forense propia y gestionar casos de uso mediante su motor de correlación en tiempo real, con capacidad de procesado en origen, lo que permite ser independiente de la disponibilidad o no del registro de eventos (*logs*) para dar una respuesta inmediata.

Ambas soluciones completan un escenario de seguridad 360, aportando capacidades de gestión de eventos, centralización de fuentes y correlación de eventos de seguridad mediante GLORIA, consumo de *data lakes* masivos de información con conexión a terceros y correlación (*Management, Detection and Response*) mediante MONICA y en conjunción de ambas la gestión de casos de uso y detección y respuesta automatizada integrada (*Security Orchestration and Automation Response*).

- **MÓNICA**

  Es un sistema automatizado de gestión de información y eventos de seguridad que recoge en una única plataforma toda la información existente sobre amenazas potenciales, permitiendo no solo reaccionar ante los ataques, sino adelantarse a ellos para remediarlos antes de que sucedan.

  Permite las siguientes funcionalidades:

  - Detecta y resuelve amenazas en tiempo real.
  - Prioriza e investiga incidentes relevantes.
  - Punto único de control y almacenamiento centralizado.
  - Tecnología española alineada con la Estrategia Nacional de Ciberseguridad.
  - Analiza el comportamiento del usuario (UEBA).
  - Ciberinteligencia de amenazas.
  - Responde de forma automática (*Security Orchestration and Automation Response*).
  - Capacidad de integración con herramientas del CCN-CERT.

- **GLORIA**

  Es una plataforma diseñada para servir de base para la operación integral de un Centro de Operaciones de Seguridad, dando apoyo en las actividades de recolección, análisis, detección y respuesta ante incidentes.

  Permite las siguientes funcionalidades:

  - Procesamiento centralizado de grandes volúmenes de información de eventos.
  - Capaz de analizar y correlar de forma homogénea, eventos del mundo IT y del mundo OT (sistemas de control industrial).
  - Aplica técnicas de automatización y orquestación (*Security Orchestration and Automation Response*) para mejorar la eficiencia del equipo de analistas y reducir la fatiga cuando se está expuesto a una gran cantidad de alarmas frecuentes y, en consecuencia, se vuelve insensible a ellas.

- No limita las capacidades de escalado aun si se monitoriza un número elevado de fuentes.
- Soporta un modelo de correlación distribuida, en el que los eventos pueden ser recolectados y correlados en origen.
- Utiliza solo alertas previamente correladas para identificar amenazas que afecten de forma coordinada a varias fuentes.
- Aporta capacidades avanzadas de búsqueda y detención de amenazas junto con análisis de comportamiento (*threat hunting, threat detection* y *Behavioural Analytics*).
- Integrado nativamente con gran parte de las soluciones del CCN-CERT.