MUSEO NACIONAL DEL PRADO: gestión avanzada continua y proactiva de las ciberamenazas

Si al aumento de ciberataques que hemos sufrido estos últimos años con el impulso de la digitalización que ha provocado la pandemia, le sumamos la presión extra que supone la inestabilidad geopolítica derivada del conflicto ucraniano, la situación en materia de ciberseguridad está más tensa que nunca. Y tanto pequeñas instituciones públicas como grandes ministerios han sufrido los devastadores efectos de los ciberataques causados por correos maliciosos, suplantaciones de identidad o ataques de *ransomware,* entre otros. Para gestionar las ciberamenazas, el Museo Nacional del Prado (MNP) ha optado por los servicios especializados de ICA Sistemas y Seguridad combinados con la plataforma MÓNICA NGSIEM de esta compañía española.

Alberto Cañadas

Los equipos de ciberseguridad deben hacer frente al creciente volumen y sofisticación de las amenazas, pero la falta de visibilidad de la red, los análisis manuales que consumen mucho tiempo y la falta de contexto, afectan negativamente a la eficiencia de los equipos. En el caso del **Museo Nacional del Prado** (**MNP**), su necesidad principal era potenciar la recogida de *logs* y la seguridad TIC de sus principales sistemas informáticos, comunicaciones y de seguridad perimetral. Esta institución tenía como objetivo mejorar los sistemas y procesos de información para corregir carencias y, para ello, buscaba un SIEM para correlacionar eventos potencialmente peligrosos para la seguridad de los sistemas de información del Museo.

Además, el MNP necesitaba una herramienta que le permitiera evidenciar digitalmente cualquier incidente de seguridad que se pudiera producir en sus instalaciones y responder a cualquier requerimiento de evidencia o respuesta a un incidente de seguridad TIC que pudiera tener lugar. Por otro lado, contaba con diferentes tecnologías tradicionales de seguridad que no estaban conectadas entre sí, por lo que el equipo de seguridad no podía tener una visión completa, ya que recibía muchos datos independientes que son difíciles de interpretar de forma individual. De esta manera, también surge la necesidad de contar con una herramienta que centralice toda la información y que pueda brindar visibilidad para detectar y proteger de ataques avanzados a este organismo.

Para abordar todos estos retos tecnológicos, el MNP determinó que la herramienta que mejor se adaptaba a sus necesidades era el NGSIEM que ofrece el CCN-CERT en su catálogo de soluciones, Mónica NGSIEM, ya que cumplía todas las características de interés buscadas. Desarrollado por el equipo de **ICA Sistemas y Seguridad**, se trata del único NGSIEM nacional y europeo certificado *Common Criteria* y producto cualificado y aprobado por el Centro Criptológico Nacional.

Mónica NGSIEM 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 prevenirlos. El NGSIEM del CCN-CERT triplica la productividad de un equipo tipo de ciberseguridad y permite alcanzar un retorno de la inversión completo en solo cuatro meses.

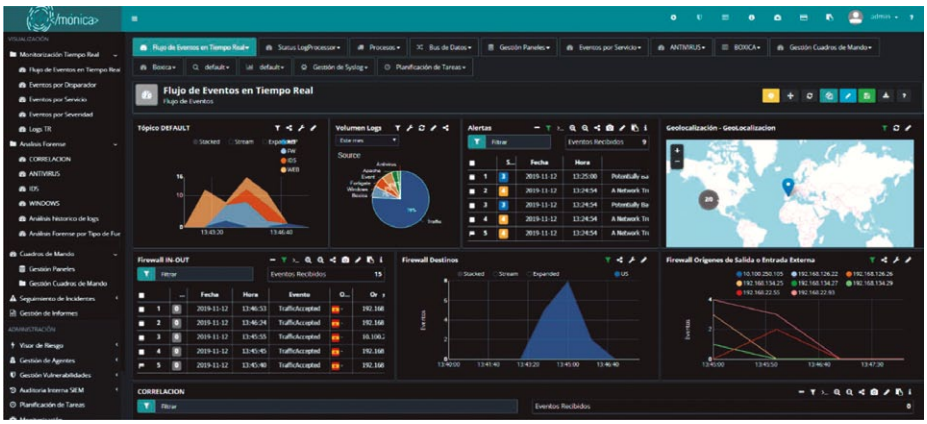
Una visión completa y real del ciberestado de la infraestructura tecnológica

Mónica NGSIEM consume cantidades masivas de datos que proceden de fuentes técnicas, investigaciones, fuentes abiertas, fuentes ocultas, redes sociales, fuentes internas y de terceros. Una vez recogida toda esta información, la agrega, analiza y contextualiza en un único lugar. Ayudado por el aprendizaje automático y la automatización, Mónica NGSIEM consigue analizar más de 100.000 eventos por segundo, frente a los 4.800 eventos que una persona es capaz de procesar en un día. Sus capacidades SOAR facilitan la orquestación entre múltiples fuentes, reducen los falsos positivos, permiten establecer un triaje y una priorización de incidentes y facilitan la respuesta automática ante amenazas conocidas.

La gestión de la seguridad de Mónica NGSIEM tiene en cuenta tres estadios temporales -el histórico de eventos, la acción en tiempo real y la acción preventiva- y permite la monitorización de eventos de cualquier dispositivo, sistema o aplicación. Entre los agentes intranet, se pueden encontrar dispositivos de seguridad lógica, de electrónica de red, servidores web, sistemas gestores de bases de datos, sistemas operativos y de seguridad de Host o aplicaciones propietarias. Por otro lado, los portales web de clientes y proveedores, aplicaciones *cloud-store* y aplicaciones no corporativas, se encuentran entre los agentes extranet, mientras que los agentes ambiente incluyen redes sociales, páginas web y blogs, sistemas de información no TIC y dispositivos de seguridad física.

La recopilación, análisis y entrega automatizada de datos proporcionan inteligencia en tiempo real a escala. Mónica NGSIEM emplea las técnicas más avanzadas de recopilación y análisis de datos, como el aprendizaje automático, la ciberinteligencia de amenazas y el análisis del comportamiento del usuario (UEBA).

De esta manera, el Museo del Prado pretende reducir el tiempo de trabajo que los equipos TIC internos dedican a la resolución de incidentes de seguridad y promover una gestión más eficaz de las alertas sobre ciberamenazas que afecten potencialmente a sus sistemas de información, además de dar una respuesta rápida a aquellas que lleguen a materializarse, permitiendo que sus esfuerzos se concentren en otras tareas.



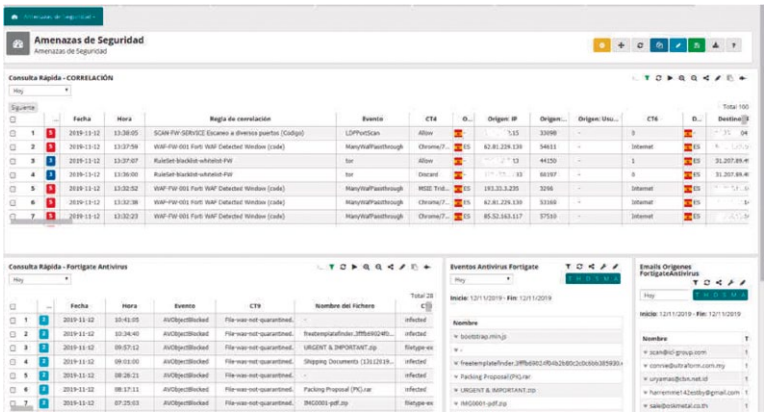
Uno de los objetivos del MNP es reducir el tiempo de trabajo que los equipos TIC internos dedican a la resolución de incidentes y promover una gestión más eficaz de las alertas sobre ciberamenazas que afecten potencialmente a sus sistemas de información, además de dar una respuesta rápida a aquellas que lleguen a materializarse, permitiendo que sus esfuerzos se concentren en otras tareas.

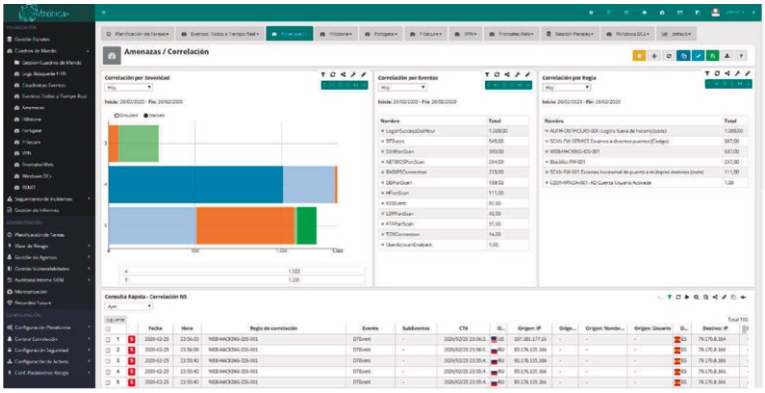
En virtud del uso de esta plataforma, el equipo de seguridad del MNP puede centrarse en lo que realmente importa y sus analistas pueden identificar amenazas a una velocidad 10 veces mayor, ayudando a resolver incidentes un 63% más rápido. Con Mónica NGSIEM, la eficiencia de los equipos de seguridad aumenta en un 32% y son capaces de identificar un 22% más de amenazas antes de lleguen a causar graves consecuencias.

MÓNICA, el NGSIEM de referencia de la Administración Pública

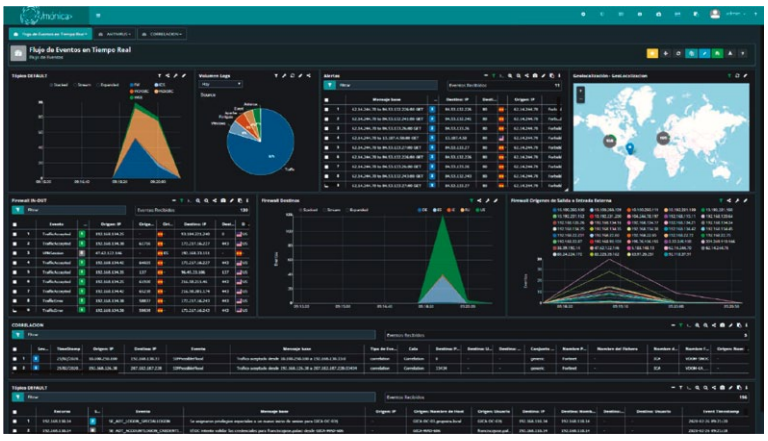
El Museo Nacional del Prado se une así a las diferentes instituciones públicas locales, autonómicas y estatales que ya confían en Mónica NGSIEM, como los ministerios de la Presidencia y Asuntos Económicos y Transformación Digital, las Diputaciones de Castellón y Barcelona o HAZI. En total, más de 50 organismos públicos ya disfrutan de esta plataforma y de los servicios de ciberseguridad de ICA Sistemas y Seguridad.

Mónica NGSIEM es un producto certificado en sus funcionalidades de seguridad, clasificado en el Esquema Nacional de Seguridad (ENS) con categoría Alta que lo habilita para ser empleado en sistemas afectados por el ENS en cualquiera de sus niveles: Alto, Medio y Básico. Además, está incluido en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) y permite la integración con otras soluciones del CCN-CERT como Carmen, Lucía, Pilar, Claudia, SAT-INET, Reyes e Inés.





Los expertos del CiberSOC de ICA Sistemas y Seguridad ofrecen al MNP el servicio de detección y respuesta en modalidad 24x7, a través del cual monitorizan eventos de seguridad mediante el uso de la plataforma MÓNICA NGSIEM, realizan correlación y análisis de eventos, se encargan de la operación y notificación de alertas de seguridad y participan en la coordinación de respuestas a incidentes.



Servicios de ciberseguridad avanzados con el CiberSOC de ICA SyS

Pero si disponer de una herramienta NGSIEM es casi imprescindible hoy en día, contar con personal experto lo es aún más para poder hacer un uso eficaz de ella. Además de confiar en la herramienta del CCN desarrollada por ICA, el Museo Nacional del Prado ha apostado por sus servicios del CiberSOC para la gestión de incidentes y ciberamenazas.

Los expertos del CiberSOC de ICA ofrecen al MNP el servicio de detección y respuesta en modalidad 24x7. A través de este servicio, monitorizan eventos de seguridad gracias a la plataforma Mónica NGSIEM, realizan correlación y análisis de eventos, se encargan de la operación y notificación de alertas de seguridad e incluso de la coordinación de respuestas e incidentes. En este sentido, el CiberSOC también gestiona los eventos e incidentes de seguridad del Museo. El equipo de ICA SyS ofrece respuesta ante incidentes que engloba la notificación de los detectados, así como su gestión completa, trabajando de forma alineada junto a los responsables de seguridad TIC, sistemas y redes del MNP y coordinando las actuaciones necesarias sobre los sistemas o redes que lo requieran.

Un CiberSOC altamente cualificado

Al margen de las certificaciones ISO 9000/27000/20000 y ENS categoría Alta con las que cuenta ICA, su CiberSOC es miembro de los foros y organizaciones más relevantes en el campo de la ciberseguridad a nivel nacional e internacional, FIRST, CSIRT, CERT y TF-CSIRT. Además, el equipo de ICA SyS trabaja activamente de la mano de los principales organismos gubernamentales encargados de la ciberseguridad nacional, como el INCIBE y CCN-CERT, para que las empresas nacionales y las organizaciones gubernamentales puedan operar de forma segura, minimizando el riesgo de ciberataques.

Así, Mónica NGSIEM y el CiberSOC de ICA Sistemas y Seguridad forman una robusta defensa para la lucha contra la ciberdelincuencia. Mónica NGSIEM es el ojo de halcón que permite ver el ecosistema completo de aplicaciones conectadas a la red en tiempo real de forma centralizada. Recopila y analiza eventos y datos contextuales y detecta más de 100.000 eventos por segundo. Además, proporciona al equipo de seguridad el contexto necesario para tomar decisiones eficientes ante amenazas desconocidas. Las ventajas de esta plataforma, junto al equipo de expertos que forman el CiberSOC, proporcionan al Museo del Prado una gestión avanzada continua y proactiva de su ciberseguridad. ■

Alberto Cañadas
Gerente de Ciberseguridad – Preventa y Desarrollo de Negocio
BU-Ciberseguridad
GRUPO ICA SISTEMAS Y CIBERSEGURIDAD