«Con LogICA NGSIEM y los servicios gestionados desde el CiberSOC de ICA SYS hemos conseguido aumentar nuestra eficiencia en el triage de alertas, la investigación y la respuesta ante incidentes».

Julián Hernández Vigliano

Subdirector Adjunto Subdirección General de Tecnologías y Servicios de Información

El Ministerio de la Presidencia refuerza su ciberseguridad

Acerca de Ministerio de la Presidencia

El Ministerio de la Presidencia (MPR) tiene como principales competencias la coordinación de los asuntos de relevancia constitucional, la preparación, desarrollo y seguimiento del programa legislativo, el apoyo inmediato a la Presidencia del Gobierno, la asistencia al Consejo de Ministros, a las Comisiones Delegadas del Gobierno, a la Comisión General de Secretarios de Estado y Subsecretarios y, en particular, al Gobierno en sus relaciones con las Cortes Generales, así como las relaciones con las Comunidades Autónomas y las Entidades que integran la Administración Local y las relativas a la organización territorial del Estado.

Un cambio de paradigma en la gestión de la seguridad

El Ministerio de la Presidencia, era consciente del cambio de paradigma que debía darse en la gestión de su seguridad para garantizar la disponibilidad de los servicios críticos que presta en la actualidad de cara a Internet, incluyendo páginas web, servicio de correo electrónico y accesos remotos. Para ello, el MPR y el CiberSOC de ICA Sistemas y Seguridad (ICA SYS) trazaron un nuevo escenario en la ciberseguridad del Ministerio, evolucionando el enfoque reactivo que su seguridad había tenido hasta entonces a uno proactivo y preventivo. Para ello, se puso en marcha un ambicioso proyecto que permitiera al Ministerio alcanzar unas altas cotas de protección mediante la combinación de servicios y plataformas de última generación.

Detección proactiva de incidentes de seguridad

Para ayudar al Ministerio en la transición hacia este nuevo escenario proactivo y preventivo, se colaboró conjuntamente en el análisis y diseño de una solución adaptada, flexible y escalable. Esta solución parte de la monitorización de la infraestructura tecnológica completa, que suministra logs y otros flujos de información a la plataforma LogICA NGSIEM.

También cuenta con un modelo de análisis de amenazas en tiempo real, capaz de detectar mediante la correlación de información proveniente de los sistemas internos del Ministerio y de la información extraída de la analítica de información de internet, deep web y dark web, entre otros, intentos de ataques por parte de grupos organizados, exfiltración de información, manejo de datos sensibles, análisis de información corporativa, analítica de vulnerabilidades y exploits asociados, seguimiento de actores así como mitigación de ataques en países extranjeros (bloqueo de IPs, dominios concretos, etc.).

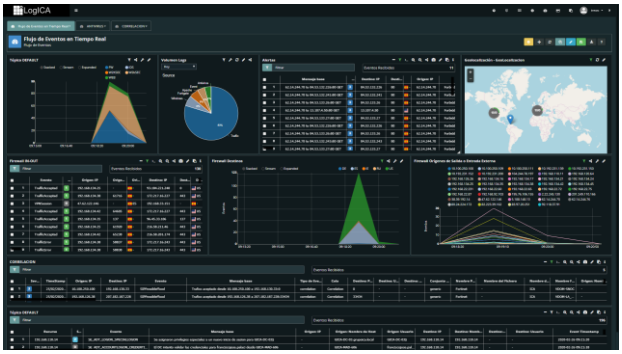
"La consola centralizada de LogICA nos permite tener una visión unificada y controlada de todos los datos de seguridad provenientes de las distintas fuentes de

información. Disponemos de un mayor contexto y conocimiento de las amenazas y actores involucrados."

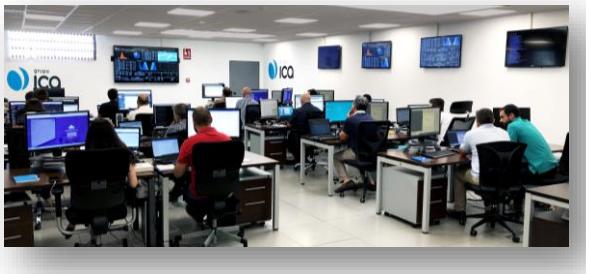
Adicionalmente y para completar el requisito de proactividad y reactividad, se implantó de un servicio de auditoría periódica, tanto externa como interna, confiando en los servicios del CiberSOC Atalaya y Achilles, que combinan las capacidades de plataformas con los conocimientos y experiencia del equipo Red Team del CiberSOC de ICA SYS. Estas auditorías están orientadas a la detección temprana de vulnerabilidades, errores de configuración o situaciones que puedan derivar en una degradación del servicio. Por ello, incorpora el análisis de vulnerabilidades y test de intrusión, con idea de identificar y subsanar posibles debilidades en la arquitectura de seguridad (incluyendo plataforma de sistemas, redes y aplicaciones), evitando su explotación malintencionada y procediendo a su reconfiguración y subsanación. Desde el punto de vista técnico, implicó la construcción de un servicio amparado en las tecnologías de ciberseguridad más avanzadas y sustentado en personal con una cualificación técnica capaz de desarrollar las actividades con los máximos requisitos de seguridad y calidad. Asimismo, y dada la criticidad de los activos y servicios a proteger, se trabaja en una modalidad mixta, con soporte in situ mediante un especialista en seguridad TI perteneciente al CiberSOC en modalidad 8x5 y el soporte remoto del personal completo de CiberSOC en modalidad 24x7. De manera adicional, para hacer frente a situaciones críticas puntuales, se plantea un soporte basado en guardias que requieren un soporte in situ mayor. El trabajo conjunto del Ministerio de la Presidencia e ICA Sistemas y Seguridad, ha aportado una base que permite afrontar las diferentes situaciones enfrentadas de manera proactiva.

Con estos requisitos, el nuevo planteamiento estaba basado en cuatro componentes esenciales:

- Servicio de monitorización de la plataforma TI.
- Servicio de operación y administración.
- Servicio de cibervigilancia.
- Servicio de análisis de vulnerabilidades y auditorías de seguridad.



"La complementación de LogICA NGSIEM con otros servicios de seguridad proporcionados por el CiberSOC de ICA SYS ha reforzado nuestra ciberseguridad. Es una tranquilidad contar con su respaldo en caso de crisis."



En sus propias palabras

SLAS CUMPLIDOS

«Desde nuestro primer contacto hasta el despliegue total del servicio, ICA SYS ha cumplido nuestras expectativas».

UN EQUIPO DE CONFIANZA

«Es una tranquilidad saber que juntos podemos hacer frente a las amenazas más graves».

LISTOS PARA RESPONDER

«Ahora somos capaces de detectar amenazas en tiempo real para reducir el impacto que pueden causar en los sistemas del Ministerio».

Julián Hernández Vigliano
Subdirector Adjunto Subdirección General de Tecnologías y Servicios de Información