COMUNICADOS TECNIMAP 2010

CCN-CERT: SISTEMAS DE ALERTA TEMPRANA

8 de marzo de 2010

Titulo de la comunicación: CCN-CERT: SISTEMAS DE ALERTA TEMPRANA

Línea de trabajo a la que se adscribe: *Iniciativas legales y tecnológicas. Seguridad, conservación y normalización de la información, formatos, y aplicaciones.*

RESUMEN:

Para garantizar el nivel de seguridad adecuado en los sistemas de las administraciones públicas es necesario actuar antes de que se produzca un incidente o, por lo menos, detectarlo en un primer momento para reducir su impacto y alcance. Por este motivo, desde el año 2008 el CCN-CERT viene desarrollando un Sistema de Alerta Temprana para la detección rápida de incidentes y anomalías dentro del ámbito de la Administración, que permite realizar acciones preventivas, correctivas y de contención.

Este Sistema de Alerta Temprana cuenta con dos vertientes: por un lado, y en colaboración con el Ministerio de la Presidencia, la monitorización de la Red de intercomunicación de todos los organismos de la Administración Pública Española, SARA[1], y por otro, la monitorización del tráfico perimetral de los accesos a Internet de las distintas administraciones.

A través de ambos sistemas, el Centro Criptológico Nacional, en colaboración con el organismo adscrito, puede detectar todo tipo de ataques, evitando su expansión, respondiendo de forma rápida ante el incidente detectado y, de forma general, generar normas de actuación que eviten futuros incidentes. El Sistema de Alerta Temprana, a través de un portal web, ofrece, además, informes y estadísticas sobre el número de eventos e incidentes en cada área de conexión. Estas métricas se pueden utilizar para medir el estado general de la seguridad de un Organismo.

1. ANTECEDENTES

En el año 2006, y con el fin de contribuir a la mejora del nivel de seguridad de la información de las administraciones públicas españolas (general, autonómica y local), el Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, creó el servicio de Respuesta a Incidentes de Seguridad, **CCN-CERT[2].** Esta estructura (tal y como la define el Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad**) nació con el firme propósito de convertirse en el centro de alerta nacional que coopere y ayude a toda la Administración a responder de forma rápida y eficiente a los incidentes de seguridad que pudieran surgir y afrontar de forma activa las nuevas y crecientes amenazas a las que hoy en día están expuestos. Y es que, la implantación generalizada de las redes corporativas o Intranet, el uso generalizado de Internet y la interconexión de los sistemas han contribuido al incremento de los riesgos acentuados, en el caso de la administración pública, por la difícil tarea de conjugar la prestación de más y mejores servicios a través de las nuevas tecnologías (tal y como recoge la Ley 11/2007), con la generación de confianza en los medios electrónicos por parte de los ciudadanos, minimizando o eliminando los riesgos asociados a su utilización.

A lo largo de estos más de tres años, el CCN-CERT ha ido desarrollando diferentes servicios puestos a disposición de todas las administraciones públicas, con el fin de asesorar a todas ellas en la implantación de medidas que mitiguen el riesgo de sufrir cualquier ataque; colaborar en la resolución de incidentes; formar al personal responsable de seguridad de la Administración y proporcionar información sobre vulnerabilidades, alertas y avisos de amenazas a sus sistemas. No obstante, y dado el ritmo vertiginoso que alcanzan las nuevas tecnologías y los ataques recibidos por éstas, el CERT Gubernamental español está en la obligación de incrementar continuamente sus servicios, haciendo especial hincapié en las labores de prevención, protección

[1] S.A.R.A.: Sistema de Aplicaciones y Redes para las Administraciones.

[2] *Computer Emergency Response Team*. Nombre comúnmente aceptado para definir a aquellos Equipos o Centros de Seguridad en donde se centralizan las labores de prevención, reacción, coordinación y gestión de incidentes, ataques o anomalías que pueda sufrir los sistemas y las redes de una organización o un grupo objetivo (comunidad) a los que presta el servicio el CERT, en este caso la Administración Pública.

y detección. Sólo con esta actitud proactiva se pueden mejorar los procesos de infraestructura y seguridad de los sistemas de la Administración antes de que un incidente ocurra o sea detectado.

Así, a principios de 2008, y dentro de sus servicios proactivos, el CCN-CERT inició el desarrollo de su **Sistema de Alerta Temprana** de la **Red SARA**, en colaboración con el Ministerio de Administraciones Públicas (actual Ministerio de la Presidencia). Posteriormente, en 2009, comenzó la implantación de este servicio de detección rápida y eficaz de incidentes de seguridad a las plataformas públicas de la Administración, con el despliegue de IDS[3] en las salidas de Internet (**Sondas de Internet)** de los organismos públicos que firman el correspondiente convenio con el CCN.

2. IMPLEMENTACIÓN DEL PROYECTO

El Sistema de Alerta Temprana desarrollado por el CCN-CERT, tal y como se ha mencionado, tiene dos vertientes: Sistema de Alerta Temprana de la Red SARA y Sistema de Alerta Temprana de las Sondas de Internet. Ambos sistemas tienen un denominador común: la detección temprana de intrusiones, considerando como tal la acción o acciones que pueden comprometer la integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios de los sistemas de la Administración

2.1. Sistema de Alerta Temprana de la Red SARA

Este sistema está basado en la correlación de logs (registro de datos) sobre las áreas de conexión de la red SARA, que proporcionan de forma continua un índice de compromiso de la seguridad y emite alarmas ante cualquier incidente. El sistema permite detectar de manera proactiva las anomalías y ataques del **tráfico** que circula **entre los diferentes Ministerios** y Organismos conectados a la citada Red (nunca lo que ocurre en el interior) y ofrece una visión en tiempo de real del estado de la seguridad de la red, mediante diferentes sensores.

Dada la magnitud de la red SARA y de la gran cantidad de tráfico que circula por ella, el sistema cataloga las alertas con diferentes niveles de criticidad, pasando a niveles superiores las alertas que han sido procesadas y escaladas por el motor de correlación y convirtiéndose en incidentes de seguridad en función de la evaluación que se realiza de ellas a través de un equipo de expertos en seguridad.

[3] Siglas en inglés de *Intrusión Detection System* o Sistema de Detección de Intrusos (programas usados para detectar accesos no autorizados a un ordenador o a una red).

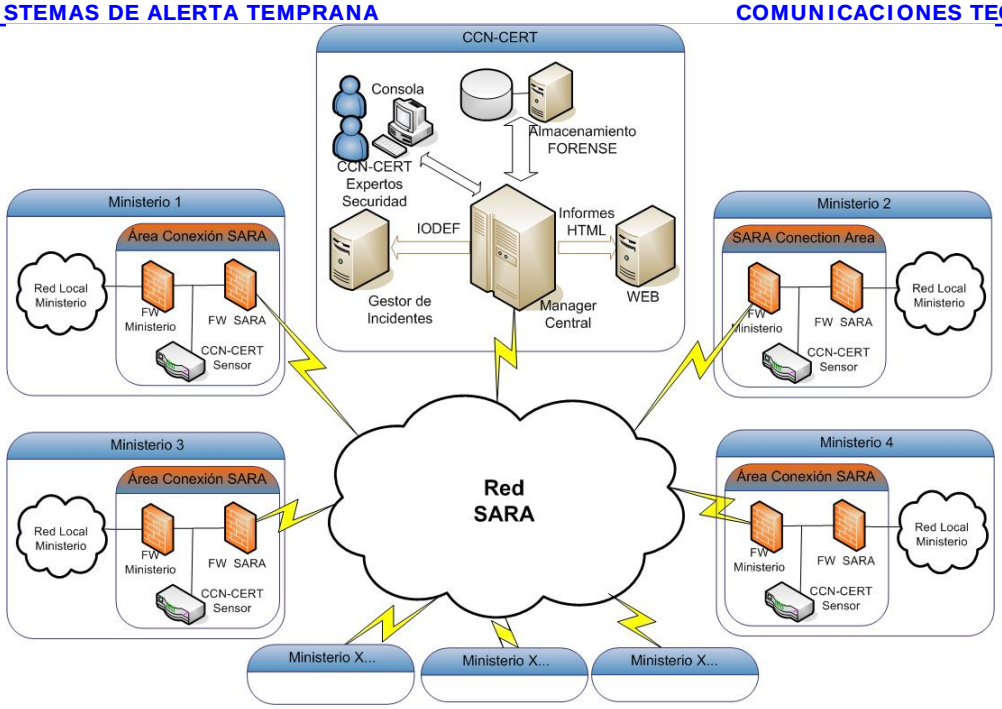

Figura 1. Arquitectura del Sistema

Desde el agente se puede recolectar información de diferentes tipos de fuentes, según el organismo al que se está accediendo. En la *Figura 2* se muestra un ejemplo de cómo se realiza la recolección y desde qué fuentes se puede recoger dicha información

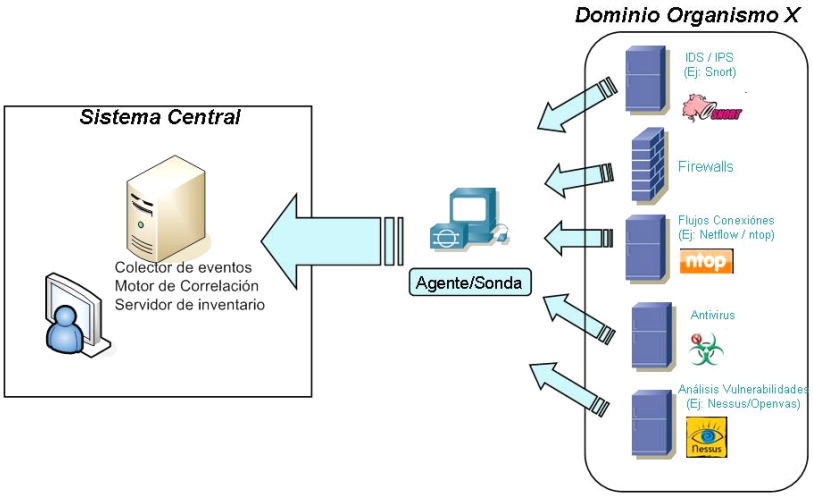

Figura 2. Recogida de información por un agente

El sistema ofrece información de gran valor a los distintos responsables de las administraciones públicas que pueden ver en tiempo real el estado de su red con respecto a la seguridad. En la *Figura 3* se aprecia el flujo del sistema, con la visión de la participación de los distintos elementos:

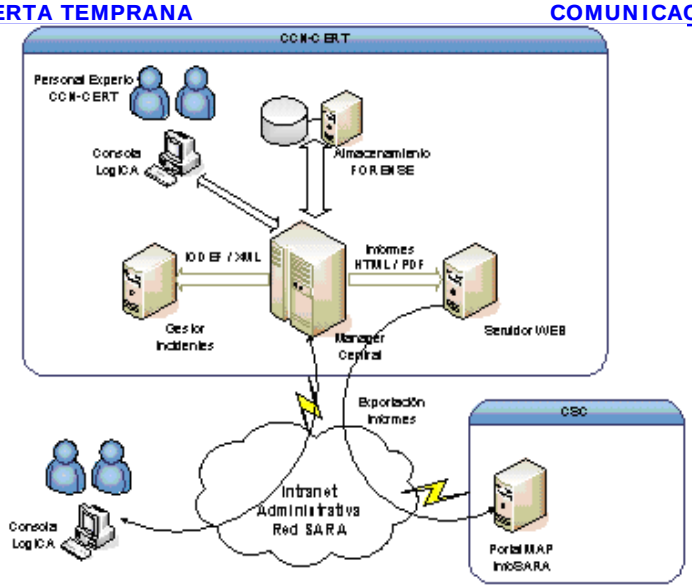

Figura 3. Flujo del Sistema

2.1.1. Actividades realizadas

Este sistema se puso en marcha a principios del año 2008 y desde entonces se han desarrollado las siguientes actividades:

- Despliegue de 23 sondas de recolección que incluyen todos los Ministerios y otros cinco organismos.
- Integración de distintas fuentes de datos (sistema de detección de intrusos, Cortafuegos perimetrales de la red SARA entre otras).
- Implantación de sistemas centrales de correlación.
- Adaptación de reglas al Sistema de Detección Intrusos (IDS).
- Generación de informes sobre incidentes detectados.
- Generación de informes estadísticos periódicos.
- Desarrollo del Portal web de acceso a informes.

En estos dos años se ha conseguido una gran estabilidad y maduración dentro del Sistema y de la propia red, lo que permite una detección mucho más fiable, eliminando los falsos positivos propios de cada red de organización y detectando rápidamente un incidente real. Así, durante el año 2009 este sistema ha recibido y analizado **más de un millón y medio de eventos** recogidos de las distintas fuentes y organismos.

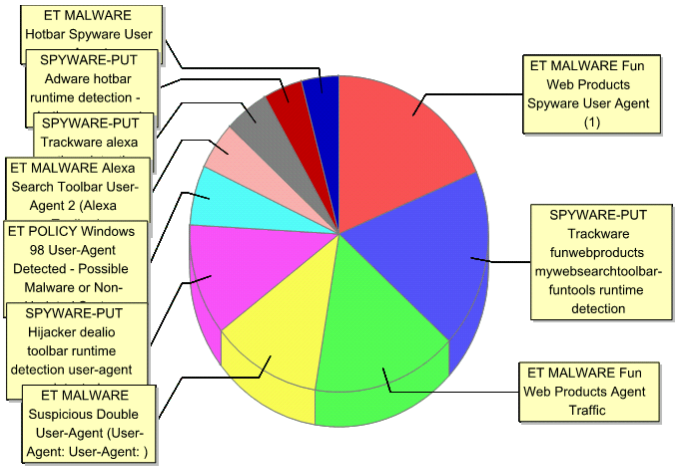

Figura 4. Eventos de seguridad más frecuentes en 2009

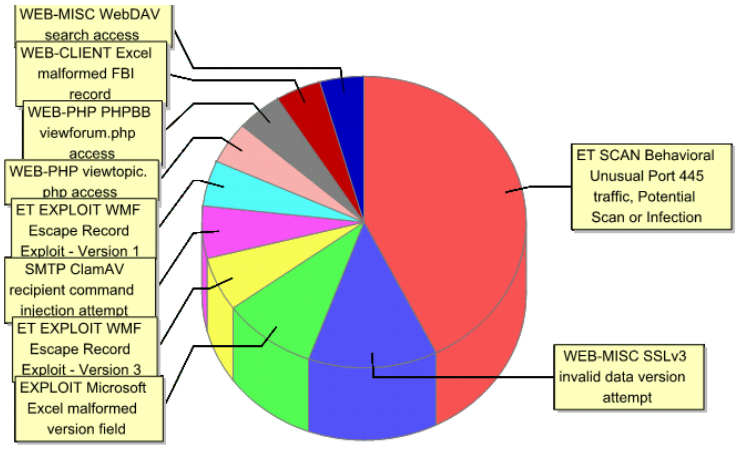

Figura 5. Malware más detectado en 2009

2.1.2. Procedimiento de actuación

- Detección del evento, análisis y clasificación. En el caso de ser un incidente se continua con el procedimiento.
- Comunicación con el organismo implicado, con remisión de informe de alerta con recomendaciones de actuación.
- Se alerta en la plataforma de Gestión de Incidentes del CCN-CERT.
- Seguimiento del incidente, con posibilidad de apoyo del CCN-CERT en actividades de parametrización del código dañino, análisis forense, etc.
- Cierre del incidente: propuesta de mejoras, elaboración de recomendaciones, ajuste o sintonía del sistema de alerta.

2.1.3. Acceso a información relevante

Todos los organismos incluidos en el sistema pueden acceder, en tiempo real, a la información del tráfico perimetral de su red (nunca a la de otros organismos), conociendo de forma inmediata el estado real de la seguridad en la misma. Para acceder a esta información puede realizarse a través de la consola de explotación (desde aquí se realiza la explotación de la información recibida, generando reglas de correlación y activando el seguimiento de un evento concreto) (ver *Figura 6*) o a través de un Portal de Informes (*Figura 7*), que ofrece estadísticas e informes, bajo demanda, sobre el estado general de la seguridad.

Figura 6. Consola de explotación

Figura 7. Portal de Informes de seguridad del Sistema

2.2. Sistema de Alerta Temprana de Internet (sondas individuales)

En este caso se trata de la implantación de una sonda individual en la red pública del Organismo adscrito al sistema (mediante convenio correspondiente con el CCN-CERT) que se encarga de recolectar la información de seguridad relevante que se detecte, y después de un primer filtrado, envía eventos de seguridad hacia el Sistema Central que realiza una correlación entre los distintos elementos y entre los distintos dominios.

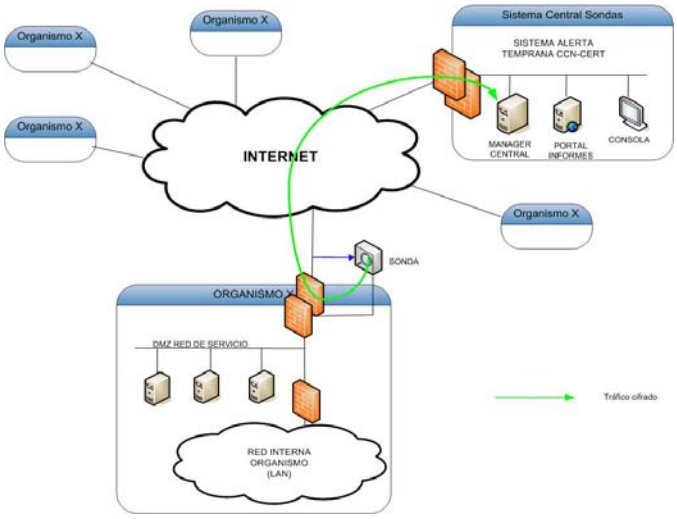

Figura 8. Arquitectura Sistema de Sondas de Internet

2.2.1. Procedimiento de actuación

Este sistema se implantó a mediados del año 2009, y desde entonces hasta la actualidad se ha desarrollado una mejora en la incorporación de fuentes en la propia sonda y la fiabilidad de la detección del sistema central. El despliegue se realiza del siguiente modo:

- Los eventos se transportan por la salida de Internet del Organismo.
- La sonda podría ser gestionada totalmente por el personal del Organismo que puede actualizar o incluir más fuentes y afinar las reglas de detección.

- Correlación exclusiva de los eventos de seguridad detectados en la propia DMZ.
- El sistema central realiza correlación avanzada de eventos, permitiendo la detección de ataques distribuidos hacia los distintos organismos adscritos al sistema.
- Transporte de los eventos por canales seguros (VPN, SSL, etc).
- La gestión, actualización y mantenimiento del sistema central está a cargo del CCN-CERT, que lleva a cabo tareas de administración, maduración de las reglas de detección e inclusión de posibles nuevas fuentes.

2.2.2. Acceso a información relevante

Al igual que en el Sistema de la Red SARA, el acceso a la información puede realizarse a través de la consola de explotación (en donde se ven los eventos en tiempo real que se están recibiendo) o a través de informes restringidos, en donde cada organismo puede ver exclusivamente los eventos e informes relacionados con su red monitorizada.

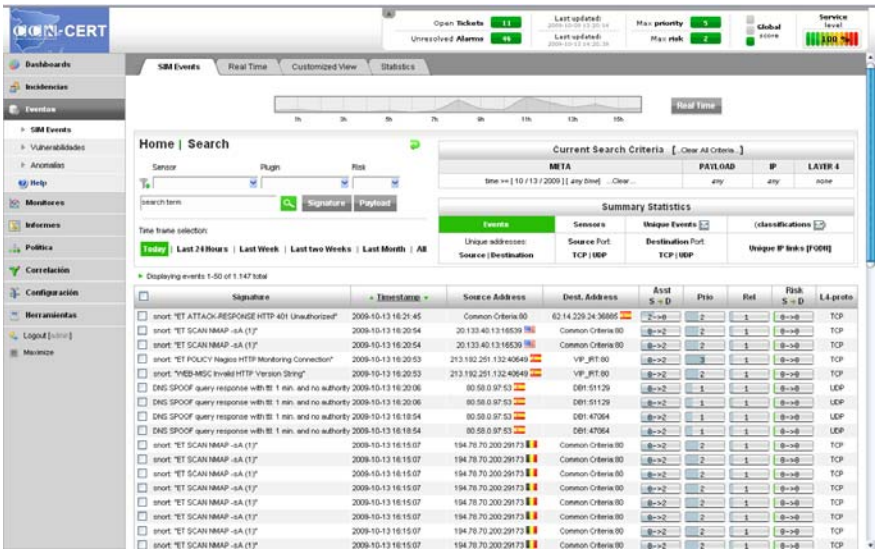

Figura 9. Consola de explotación

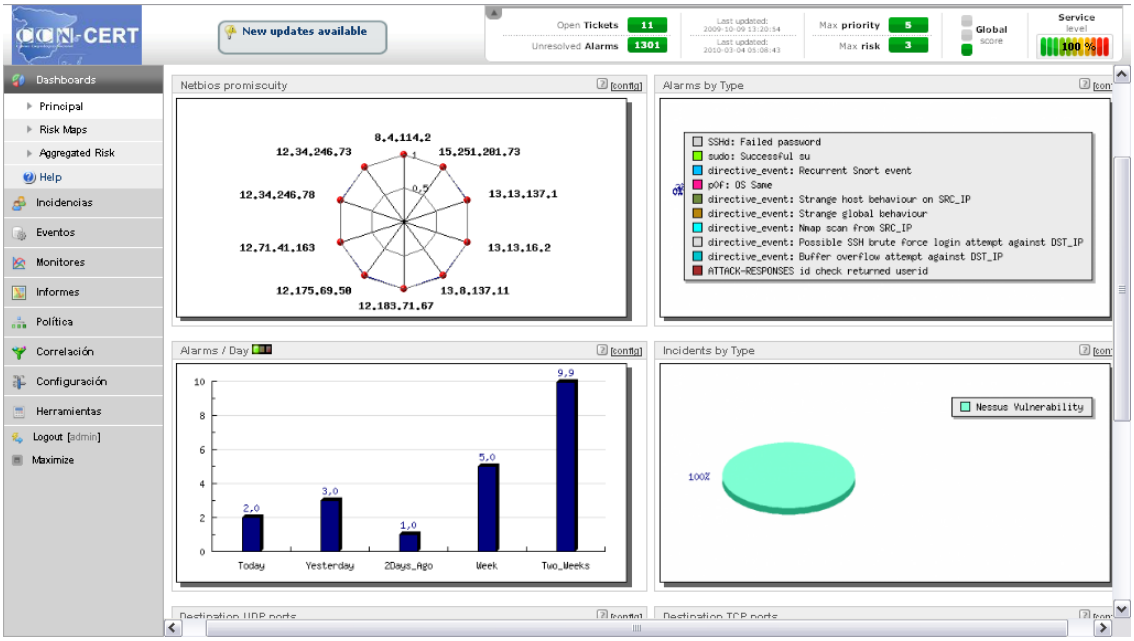

Figura 10. Gráficos estadísticos

3. BENEFICIOS APORTADOS A LAS AAPP

Los servicios de alerta temprana tienen como principal función la **protección proactiva** (aplicación de medidas antes de que se produzca un incidente o sea detectado) y **protección reactiva** (en el caso de producirse un incidente, la rápida detección del sistema permite la aplicación de medidas de contención y eliminación de la amenaza necesaria para evitar el incidente).

En el caso de los sistemas descritos, estas ventajas podrían resumirse en las siguientes:

- Mejora de los procesos de infraestructura y seguridad de los sistemas de la Administración antes de que un incidente ocurra o sea detectado.
- Detección avanzada interdominio, es decir, la detección de un incidente antes de que llegue a introducirse en un determinado dominio.
- Información de gran valor para los responsables TIC de las administraciones públicas, que pueden ver en tiempo real el estado de su red con respecto a la seguridad, así como acceder a informes estadísticos.
- Detección de todo tipo de ataques y, con ello, una respuesta rápida y eficaz a los incidentes.
- Detección de código malicioso o malware, evitando su expansión a través de toda la infraestructura interministerial.
- Protección adicional hacia los ciudadanos que acceden a los distintos servicios ofrecidos por los organismos públicos.
- Normalización de la información, unificando los eventos que se recogen de las distintas fuentes, su lenguaje y su tratamiento posterior, ofreciendo modelos para una lectura adecuada de la misma.
- Ajuste de herramienta de correlación (sintonía) y enriquecimiento de patrones de firma de los diferentes elementos de seguridad.
- Consolidación y centralización. Todos los eventos se consolidan y centralizan en un único sistema, realizando una revisión a través de una única consola.
- Correlación. Con la utilización de técnicas avanzadas de correlación, el sistema central no solo detecta incidentes importantes de forma individual, si no que se llega a la detección de eventos mucho más complejos que pueden involucrar a distintos organismos.