La "conciencia situacional" en la Ciberdefensa

Una vez que se ha alcanzado suficiente nivel de madurez en las técnicas y medios de ciberdefensa, es necesario continuar mejorando y ser capaces de conocer, dinámicamente, el nivel de seguridad de los sistemas a nuestro cargo para que se posibilite una utilización adecuada de los recursos y la aplicación de los principios de la gestión de riesgos mediante información de las amenazas y modelos probabilísticos obtenidos del análisis de los datos de seguridad. Dado que la situación cambia de manera muy rápida y se requiere una respuesta inmediata a las amenazas de las que se recibe información y a los daños derivados de los incidentes de seguridad, es necesario apoyarse en técnicas de visualización de datos complejos para poder tomar las decisiones adecuadas en el menor tiempo posible. En el presente artículo se expone la situación actual de los sistemas de conciencia situacional para ciberdefensa y se esboza el concepto de visualización de la información como elemento esencial de la conciencia situacional. Por último, se presentan las principales conclusiones.

José Ramón Coz Fernández / Vicente José Pastor Pérez

La conciencia situacional (del término inglés *situational awareness*) se define de manera simple como el conocimiento de aquello que nos rodea eliminando todo lo que pueda considerarse "ruido" y centrándonos en lo que sea realmente importante para la tarea que se esté ejecutando. De acuerdo con la psicología cognitiva, nos referimos al modelo mental de un ser humano en la toma de decisiones o a un esquema de la evolución de la situación respecto de las tareas que tiene que realizar.

La mejora de la conciencia situacional ha sido uno de los principales objetivos de diseño para el desarrollo de las interfaces de operador, los conceptos de automatización y los programas de entrenamiento en una amplia variedad de campos que incluyen la aviación, el control del tráfico aéreo, las plantas energéticas, los sistemas avanzados de manufactura y, cómo no, ahora más que nunca, en el campo de la ciberseguridad. En situaciones complejas en las que los cambios suceden rápidamente, la toma de decisiones requiere un acceso constante a la información en el momento oportuno y de manera precisa y exhaustiva. En esos casos la sobrecarga de información es nuestro peor enemigo, ya que nos esconde la información realmente relevante bajo grandes cantidades de datos que no nos son de interés.

A los efectos de mejorar nuestra capacidad de ciberdefensa, es importante tener en cuenta que esta conciencia situacional del ciberespacio (o de la parte de él que nos interese en cada momento concreto) puede ser expresada en diferentes niveles de detalle dependiendo del receptor de la información y su poder de decisión en particular; así, encontraremos aplicaciones en las que estos receptores son analistas de seguridad y su poder de decisión se restringe a concluir si, con la información que se les muestra con diferentes técnicas de visualización, está o no ocurriendo en ese momento un incidente de seguridad más o menos complejo. En otros casos, se va un paso más allá y quien recibe la información son los gestores de incidentes que deben tomar decisiones respecto a las acciones a tomar para mitigar los efectos de un ataque, detener el mismo y restaurar los sistemas a su estado operacional.

Finalmente, en la cumbre, tenemos a los que han de tomar decisiones de carácter global, incluso en ámbitos fuera del propio ciberespacio, y relacionados con misiones y objetivos que reciben soporte más o menos directo de los sistemas de información y telecomunicaciones a los que se refiere el conocimiento de la situación de las amenazas, vulnerabilidades, debilidades y ataques que afecten al nivel de ciberseguridad y, por ende, al éxito de la misión.

Estado del arte

El "quién, qué, cuándo y cómo" de un ataque cibernético solo puede responderse, con garantías, cuando la conciencia situacional de la organización que lo sufre tiene un alto nivel de madurez. De acuerdo con las mejores prácticas internacionales implantadas en los países y las organizaciones más evolucionadas en el campo de la seguridad de la información, la principal prioridad es la protección contra filtración y manipulación de datos; un segundo objetivo está en la capacidad de recuperación; y un tercer objetivo son la protección contra ataques de denegación de servicio, virus, gusanos, etc. En el caso de la protección contra filtración y manipulación de datos las organizaciones requieren de una sólida defensa, con un gran conocimiento de lo que está sucediendo internamente y externamente en la organización. Este conocimiento va mucho más allá que el mero control de los enlaces, *routers*, *switches* y servidores, e incluye un amplio conocimiento técnico de la organización, de las amenazas emergentes, de la arquitectura tecnológica, de la actividad dentro y fuera de la organización y de las identidades que interactúan en la red.

Algunas grandes organizaciones han abordado la ciberseguridad como un problema conjunto e incluyen iniciativas para dar soporte

El Departamento de Defensa de Estados Unidos, que mantiene unos 10.000 sistemas de información –de lo cuales casi un 20% se consideran muy críticos–, 800 centros de procesamiento de datos y más de siete millones de ordenadores y dispositivos, está llevando a cabo iniciativas como la mejora del control de la evolución de su arquitectura empresarial; la capacitación y control sobre la conciencia situacional para operadores y usuarios; la evaluación y las pruebas de seguridad; la gestión de identidades, la acreditación y la certificación de sistemas; el gran proyecto de capacidades de recuperación ante desastres; la gestión de riesgos; el cibercomando 24x7, y el Centro de ciberoperaciones.

a la conciencia situacional que abarcan desde actividades como la monitorización de redes, la detección de incidentes y la gestión de identidades hasta la gestión dinámica de riesgos, la gestión de ciberincidentes e, incluso, la ciberformación o la ciberinnovación. Por ejemplo, en el caso del Departamento de Defensa de Estados Unidos, que mantiene unos 10.000 sistemas de información –de los cuales casi un 20% se consideran muy críticos–, 800 centros de procesamiento de datos y más de siete millones de ordenadores y dispositivos (según datos de la Secretaría de Defensa), se están llevando a cabo iniciativas como;

• La mejora del control de la evolución de su arquitectura empresarial, la capacitación y control sobre la conciencia situacional para operadores y usuarios, la evaluación y las pruebas de seguridad,

• La gestión de identidades, la acreditación y la certificación de sistemas,

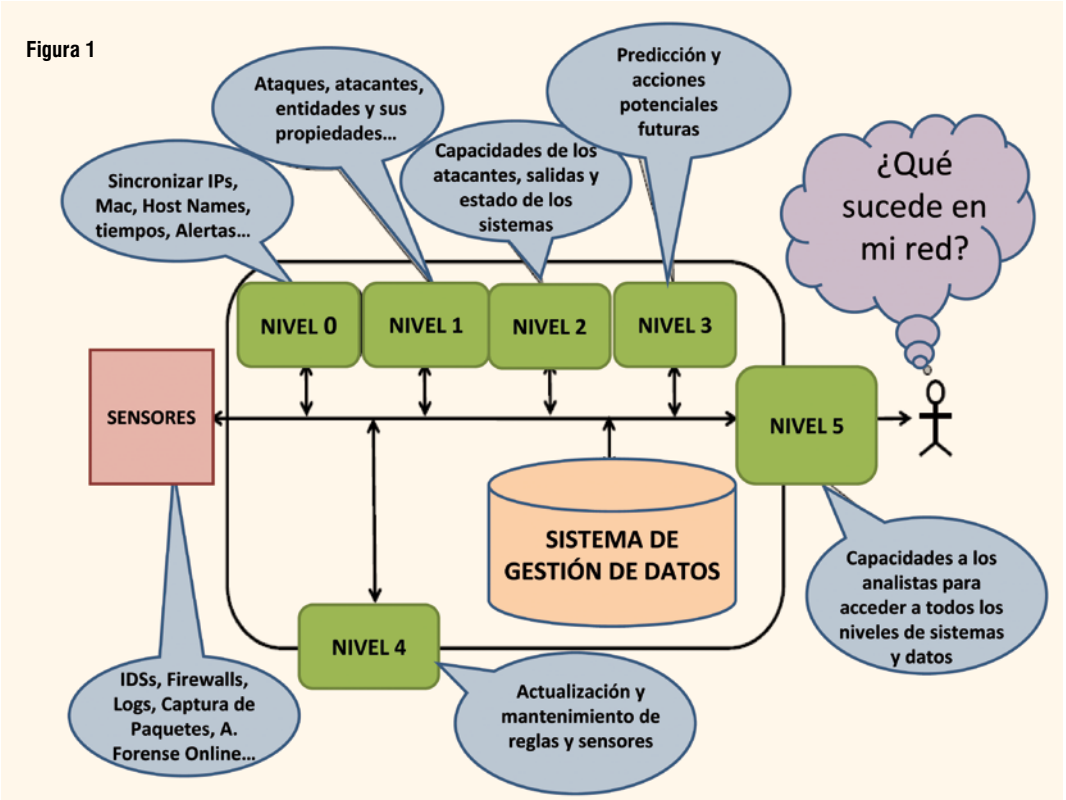
• El gran proyecto de capacidades de recuperación ante desastres,

• La gestión de riesgos, el cibercomando 24x7 o el Centro de ciberoperaciones.

Para llevar a cabo proyectos relacionados con la conciencia situacional, las organizaciones más avanzadas hacen uso de modelos extendidos, desde el modelo inicial propuesto por Endsleyy Jones, que incluye tres niveles de gestión: **Percepción**, **Comprensión** y **Proyección**. Estos niveles se refieren, respectivamente, a ser consciente de los datos actuales, a tener un entendimiento necesario que permita obtener conclusiones sobre la situación en la que nos encontramos en relación con esos datos y, finalmente, a intentar predecir la situación futura en la que nos encontraremos en base a esa información. Uno de los modelos extendidos más referenciados es el Modelo JDL del Joint Director of Laboratories, que permite relacionar las capas de la conciencia situacional con los niveles del proceso de fusión de datos en términos de seguridad cibernética (ver **Figura 1**).

Los sensores son dispositivos en el sistema que proporcionan información sobre la seguridad del sistema. Ejemplos de estos sensores son los sistemas de detección de intrusos (IDS) y, en general, todos los *logs* de

Figura 1



las diferentes capas software. En el nivel cero del modelo se integrarían con el proceso de fusión de datos procedentes de diversas fuentes, abordando los problemas de adaptación (por ejemplo, del nombre de host a una dirección IP) o las diferencias en la presentación de formatos de salida. El nivel uno del proceso de fusión combina estos datos para identificar individuos y eventos de seguridad, ya que se pueden observar desde varios sensores. A nivel dos se combinarían varias entidades para proporcionar una perspectiva actual del estado de los sistemas de información.

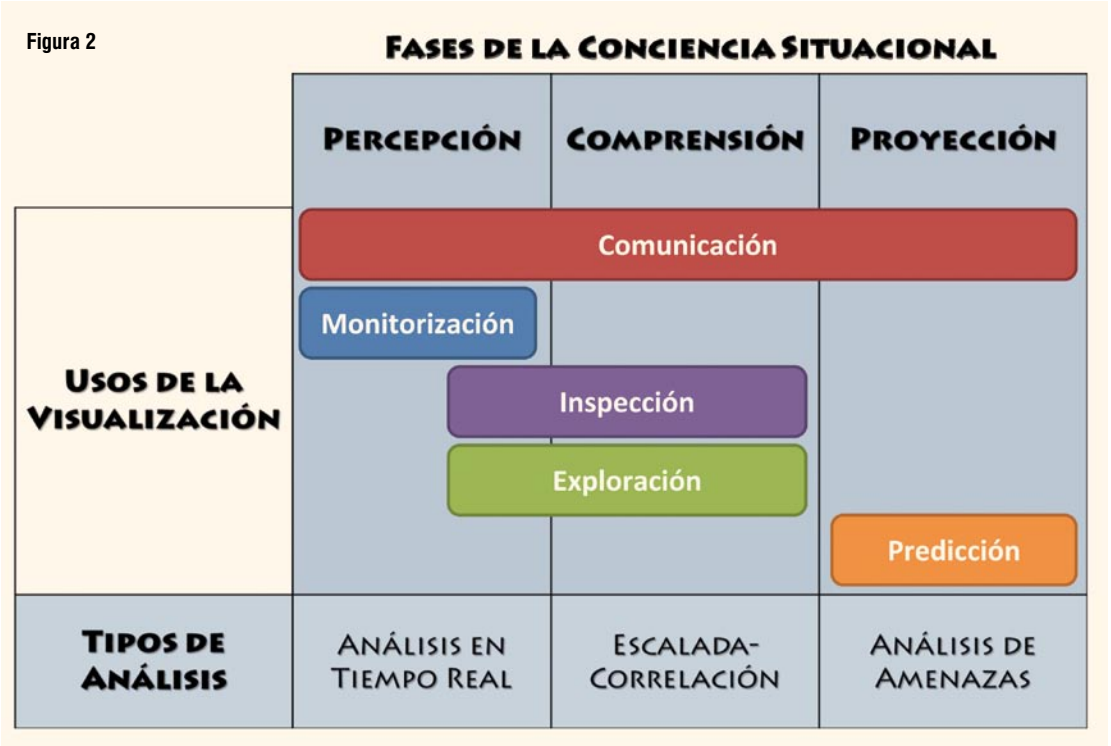
A nivel tres, el proceso proporciona una capacidad de predecir los estados futuros de los sistemas (por ejemplo, ¿el sistema se va a ver comprometido por un ataque específico?), o acciones futuras de un atacante. El nivel cuatro aborda la capacidad del sistema para el mantenimiento de reglas y sensores. Por ejemplo, la actualización de firmas del IDS sería un ejemplo de capacidad básica del nivel cuatro. Por último, el nivel cinco es la interfaz entre el analista de seguridad y el sistema de fusión de datos.

En la actualidad se están produciendo grandes avances en el desarrollo de sensores, monitorización de paquetes, analizadores y controladores de *logs*, y existen numerosos productos y herramientas disponibles para su uso, pero asimismo evolucionan los algoritmos y los interfaces gráficos de usuario en todos los niveles del modelo JDL. A modo de ejemplo podemos citar algunas herramientas *open source* del Software Engineering Institute, como SiLK (*System for Internet-Level Knowledge*), que facilita el análisis de seguridad en redes de gran tamaño y permite a los analistas consultar rápidamente grandes conjuntos de volúmenes de tráfico de datos; IPA (*IP Annota-*

La OTAN está desarrollando, mediante un sistema en espiral, dentro de la Capacidad Final Operativa de su Centro de Respuesta a Incidentes de Seguridad Informática (NCIRC FOC) un Sistema de Apoyo a la Decisión de Ciberdefensa (CDDSS) compuesto por una Imagen Consolidada de Aseguramiento de la Información (CIAP), un Repositorio Consolidado de Información de Seguridad (CSIR), un módulo de Evaluación Dinámica de Riesgos (DRA), así como un módulo de Gestión Dinámica de Riesgos (DRM).

tion system), una biblioteca que proporciona estructuras de datos eficientes para la manipulación de etiquetados de direcciones IP; o RAVE (*Retrospective Analysis and Visualization Engine*), una plataforma *middleware* extensible basada en Python, que simplifica la tarea de construir entornos de análisis para una supervisión de la red y la infraestructura tecnológica. En lo que se refiere al aspecto de visualización de la información, profundizaremos más en el siguiente apartado.

Figura 2



La visualización de la información en la conciencia situacional

La visualización es un componente esencial en la transmisión de la conciencia situacional y permite una mayor rapidez en la toma de decisiones. Las representaciones gráficas de los datos se realizan utilizando el color, la forma, la posición, el tamaño o cualquier otra propiedad gráfica que pueda codificar la información. Ha de ser posible, partiendo de unos datos de un alto nivel de abstracción, moverse de manera interactiva hacia los datos de menor nivel, en caso de que fuera necesario para poder comprender lo que se nos muestra u obtener más detalles sobre la información presentada. Las técnicas de visualización deben ser diseñadas o seleccionadas para alinearse con uno o más de las fases o niveles de la conciencia situacional de Endsley mencionados anteriormente.

Además, existen cinco usos estandarizados principales de la visualización: **Monitorización**, en la que se observa un fenómeno en curso en el que los datos pueden estar en continuo cambio; **Inspección**, en la que el analista busca detalles específicos, solicita aclaraciones y encuentra datos que le permiten comprobar hipótesis; **Exploración**, donde se realiza un estudio concienzudo y libre de los datos, se investiga sin tener pistas previas, se combinan los datos de forma novedosa y se experimenta interactivamente con las vistas de los datos, encontrando regiones de interés para su análisis y se generan nuevas hipótesis; **Predicción**, en la que, o bien intentamos encontrar el estado futuro más probable suponiendo que la progresión actual continuará si no se interviene, o determinamos un estado futuro particular basado en planes de acción potenciales; y **Comunicación**, en la que se presentan todos los datos a terceros, se realizan informes, o se presentan las actividades realizadas.

Son numerosos los esfuerzos de grandes organizaciones en diferentes países para promover la investigación de soluciones relacionadas con el tema que nos ocupa. Por ejemplo, el Ministerio de Defensa del Reino Unido, y no es el único, ha publicado recientemente una petición de iniciativas de investigación relacionadas con la conciencia situacional para la ciberdefensa por un valor de 400.000 libras.

La OTAN, por su parte, está desarrollando, mediante un sistema en espiral y dentro de la Capacidad Final Operativa de su Centro de Respuesta a Incidentes de Seguridad Informática (NCIRC FOC), un Sistema de Apoyo a la Decisión de Ciberdefensa (CDDSS) compuesto por una Imagen Consolidada de Aseguramiento de la Información (CIAP), un Repositorio Consolidado de Información de Seguridad (CSIR), un módulo de Evaluación Dinámica de Riesgos (DRA), y un módulo de Gestión Dinámica de Riesgos (DRM). Además, en otra fase del proyecto, se completará el equipamiento de la Célula de Evaluación de Amenazas Cibernéticas (NCIRC CTAC).

Más recientemente, se están dando los pasos para completar la Infraestructura de Colaboración e Intercambio de Datos de Ciberdefensa (CDXI). En un entorno más general mencionaremos VizSec, el Simposio sobre Visualización para la Ciberseguridad, que acaba de celebrar su novena edición y donde se presentan los avances científicos en el área cada año.

Conclusiones

En este artículo hemos introducido algunas consideraciones sobre el concepto de *situational awareness* o conciencia situacional, destacando su gran importancia en el campo de la ciberseguridad. En la actualidad, las organizaciones más avanzadas utilizan modelos como el JDL para gestionar la conciencia situacional y permitir que los analistas de seguridad y los responsables de la toma de decisiones puedan garantizar un control adecuado sobre la ciberseguridad. Se han expuesto algunos avances en este campo y se ha destacado el componente de la visualización de la información como elemento clave de la conciencia situacional. ■

Dr. José Ramón Coz Fernández
Auditor del proyecto de Ciberseguridad (NCIRC FOC). Bi-SC AIS Programme Management Integration Capability (PMIC). NATO Communications and Information Agency (NCIA)
ISDEFE
JoseRamon.Coz@ncia.nato.int

Vicente José Pastor Pérez
Jefe de Datos y Aplicaciones Especializadas Capacidad de Respuesta a Incidentes de Seguridad Informática de la OTAN (NCIRC)
OTAN
Vicente.pastor@ncirc.nato.int