RESPUESTAS SIC

Barcelona: 22 de junio de 2010
(Hotel Rey Juan Carlos I)

Madrid: 24 de junio de 2010
(Hotel NH Eurobuilding)

El uso inteligente de la información

La correlación de eventos con fines de seguridad

Inscripciones:

- Acceso gratuito previa solicitud de inscripción
- Solicitud: www.revistasic.com/respuestassic

> AFORO LIMITADO

Organiza:

Revista SIC seguridad en informática y comunicaciones

Copatrocinan:

ArcSight · IBM · ICA · Novell · RSA The Security Division of EMC

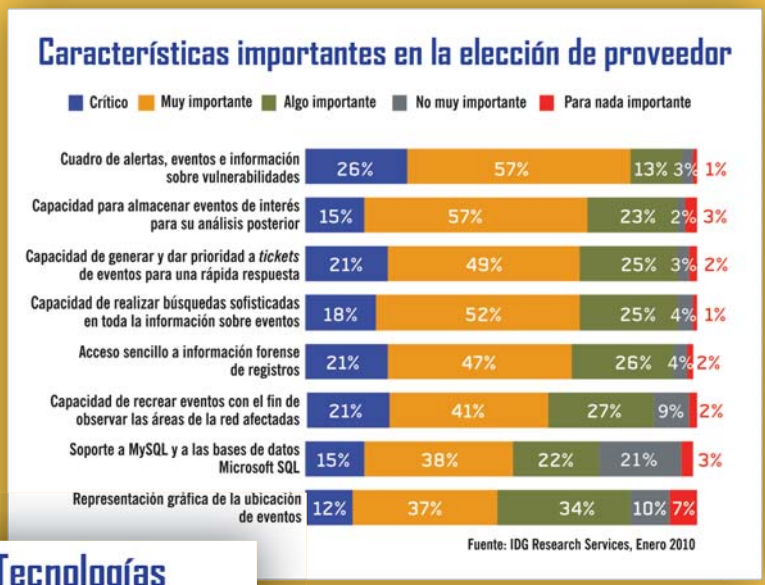
La correlación de eventos: qué

Uno de los pilares en los que se basa la gestión de riesgos de seguridad de la información es, sin duda, el análisis y la gestión de *logs* y la correlación de eventos, lo que se entiende por SIEM. La confluencia de este pilar de la seguridad con el de la gestión de identidades y accesos a sistemas, redes y aplicaciones, la gestión de documentos y la gestión de evidencias, permitiría al responsable de seguridad TIC alcanzar su objetivo específico en la cadena de protección: saber en tiempo real qué está pasando en los sistemas tecnológicos que pueda ser relevante para su seguridad, para la de la información que tratan, y, en definitiva, para el negocio y actividades de su entidad.

Las plataformas SIEM han tenido un desarrollo rápido en los últimos seis años, y constituyen hoy la base de proyectos de obligado emprendimiento para cualquier organización de cierta complejidad y bien gobernada. Sin embargo, la multicanalidad de las acciones fraudulentas y de los comportamientos no acordes con las políticas de seguridad, y el enfoque de la protección como un proceso integrado que afecta a la seguridad TIC y a la seguridad física, obliga a analizar con trazo fino –cuando no a replantearse– qué se quiere y puede monitorizar, a qué nivel, con qué reglas de correlación y para qué fines. Y tal reflexión obliga a la industria y a los desarrolladores a refinar sus herramientas para que se ajusten en lo posible a las necesidades crecientes de los usuarios y a los requisitos legales.

Conviene tener en cuenta, al respecto, que nos dirigimos hacia un escenario marcado por la centralización de procesos esenciales de seguridad en SOC y CERT, y hacia servicios con base en TIC fundamentados en el uso de técnicas de virtualización y en XaaS. Si a ello se suma el uso intensivo de las tecnologías de la información en la vigilancia tradicional

El reto del conocimiento



Índice de adopción de Tecnologías de Seguridad según el F1000

(Indica la urgencia sobre las necesidades de los usuarios y el gasto planeado para cada tecnología)

Posición	Tecnología	Puntuación
1	Acceso a la Red (NAC)	100
2	Seguridad en Redes LAN Inalámbricas	74
3	Sistema de Gestión de Eventos	69
4	Soluciones de Prevención de Pérdida de Datos	64
5	Gestión de Identidades - Provisión de Usuarios	61
6	Gestión de Eventos de Seguridad (SIEM)	60
7	Prevención de Intrusiones en Red (NIPS)	58
8	Gestión de Identidades - Autoservicio de Usuario	57
9	Cortafuegos de Aplicación	56
10	Correo Electrónico Seguro	56

Fuente: XI oleada "Estudio de Seguridad de la Información" de TheInfoPro. 2009.

Vulnerabilidades

Recolectar

Correlacionar

Gestionar

quiero y qué puedo saber

y en la prevención de fraude, y si se toma conciencia de la dependencia que tienen de las TIC los sistemas de gestión y control de procesos industriales (scada), puede vislumbrarse con la debida amplitud la nueva dimensión de la correlación de eventos con fines de seguridad. ¿Están preparadas las herramientas tecnológicas para apoyar este enfoque global? ¿Lo están las corporaciones?

Contenido

Este Respuestas SIC se estructurará en base a sus tres bloques tradicionales. En el primero, un experto en la materia, en este caso de **Hewlett-Packard,** enfocará el asunto propuesto con una perspectiva de consultoría, prescripción e integración, a fin de aportar claves para abordar proyectos de correlación o evolucionar los existentes.

El segundo bloque ofrecerá la posibilidad de conocer y contrastar el grado de adaptación actual de las herramientas que soportan este tipo de frentes de seguridad a las necesidades presentes y previsibles de los usuarios. Para ello, las compañías **ArcSight**, **IBM**, **ICA**, **Novell** y **RSA** mostrarán sus propuestas tecnológicas.

En el tercer y último bloque, tres expertos en seguridad de entidades usuarias y prestadores de servicios –en esta ocasión de **Bankinter**, **CESICAT** y **Telefónica**– darán su visión sobre este asunto que, como se ha dicho, es uno de los pilares fundamentales del control de los riesgos de seguridad con apoyo de TI.

Programa

09:00h. Acreditación y entrega de documentación.

CLAVES PARA DECIDIR

09:30h. **Cómo abordar proyectos de correlación o evolucionar los existentes**

Jorge Laredo de la Iglesia,
Senior Security Project Manager.
HP TS Security & Risk Mgmt. Services.
Hewlett-Packard.

10:20h. Coloquio.

APROXIMACIONES DE LA INDUSTRIA

10:25h. **ArcSight**.

Jordi Garasa Sibis,
Responsable de Ventas para el sur de Europa.

10:45h. **IBM**.

Vicente Gozalbo Moragrega,
Responsable de Ventas de productos de Seguridad Tivoli.

11:05h. **Informática y Comunicaciones Avanzadas-ICA**.

Alberto Cañadas Álvarez,
Gerente de Preventa del Departamento de Seguridad.

11:25h. Pausa-café.

11:55h. **Novell**.

Javier López Pedroche,
Responsable de Desarrollo de Negocio de Seguridad e Identidades.

12:15h. **RSA**.

Fidel Pérez Capón,
Director Comercial para España y Portugal.

12:35h. Coloquio general.

MESA REDONDA

13:00h. **La visión de los usuarios. Escenarios actuales, limitaciones y necesidades.**

Participantes:

Jesús Milán Lobo,
Director de Riesgos Tecnológicos y Seguridad Informática.
Bankinter.

Joan Manel Gómez Sanz,
Responsable de Operaciones del Centro de Seguridad de la Información de Cataluña.
CESICAT.

Juan Miguel Velasco López-Urda,
Director Asociado de Servicios y Proyectos de Seguridad.
Telefónica España.

14:30h. Almuerzo para todos los asistentes.

* Revista SIC se reserva el derecho a modificar el contenido o los ponentes de este programa si las circunstancias así lo requieren.

El uso inteligente de la información

El grado actual de dependencia que los negocios y actividades tienen de las TIC está forzando la integración de todos los procesos de seguridad. Las propias TIC son, además, el instrumento de apoyo necesario para detectar y registrar eventos, correlacionarlos, lanzar alarmas, prevenir, permitir la actividad forense y, en definitiva, crear inteligencia con fines de protección respetuosos con las leyes.

- ¿Qué orientación y alcance pueden tener hoy los proyectos de gestión de eventos y correlación con fines de seguridad?
- ¿Qué limitaciones funcionales tienen las herramientas orientadas al análisis y gestión de *logs*?
- ¿Aportan las plataformas SIEM inteligencia para detectar de forma temprana actividades fraudulentas o maliciosas?
- ¿Están preparadas las herramientas SIEM para ser la base de proyectos de integración de información de seguridad física y "lógica"?
- ¿Es costosa la adquisición y el despliegue SIEM? ¿En función de qué objetivos?

El camino hacia la protección

Saber en tiempo real qué está pasando en los sistemas que pueda ser relevante para la seguridad de la información de las organizaciones, y, en consecuencia, poder tomar decisiones de prevención y defensa, sigue constituyendo hoy el objetivo principal de los Responsables de Seguridad de la Información y, obviamente, de la Dirección de Sistemas de Información de cualquier entidad, pública o privada.

Pero crear procesos altamente automatizados tendentes a disponer de información sobre eventos completa, útil y de calidad en el momento justo, y que, además, permitan la implantación de mecanismos para la extracción, preservación y conservación de evidencias no es tarea fácil, ya que obliga de modo rotundo a considerar [illegible] información en su globalidad [illegible] sistemas de protección TI [illegible] definir a efectos corporativos [illegible] criticidad, clasificarlos y [illegible] actuación.

- ¿Han optimizado las actuales plataformas SIEM sus capacidades para trabajar en modo servicio hacia terceros desde SOC?
- ¿Están equilibradas en las herramientas SIEM las funciones de monitorización en tiempo real de eventos de seguridad y las capacidades forenses?
- ¿Qué retos de concepción y tecnológicos hay que afrontar en el frente de la correlación de eventos con fines de seguridad?
- ¿Existen limitaciones de enfoque en las soluciones tecnológicas SIEM que dificulten su integración con los sistemas de gestión de identidades y accesos?
- ¿Qué impacto tiene en los sistemas de análisis y gestión de *logs* y correlación de eventos el uso en los sistemas de técnicas de virtualización y de servicios Xaas?
- ¿Pueden las herramientas SIEM tratar evidencias?

RESPUESTAS SIC

La correlación de eventos con fines de seguridad

LUGAR Y FECHAS

- **BARCELONA: 22 de junio de 2010**
  Hotel Rey Juan Carlos I.
  Avda. Diagonal, 661-671. 08028 Barcelona
- **MADRID: 24 de junio de 2010**
  Hotel NH Eurobuilding.
  C/ Padre Damián, 23. 28036 Madrid

ORGANIZA

Revista SIC. Ediciones CODA.
C/ Goya, 39. 28001 Madrid
Tel.: 91 575 83 24
info@revistasic.com www.revistasic.com

SOLICITUD DE INSCRIPCIÓN GRATUITA

El procedimiento para la solicitud de la inscripción es vía web mediante la cumplimentación de un formulario. Al ser el aforo limitado, la inscripción se cursará por riguroso orden de fecha de entrada de solicitud.

Sitio web: www.revistasic.com/respuestassic

- Una vez realizada la solicitud, la organización le informará –por razones de limitación del aforo– si ha quedado inscrito o no.
- En ningún caso se admitirán más de dos inscripciones de profesionales de una misma compañía.
- La sesión incluye documentación, café y almuerzo.