



VISITA RECOMENDADA

<http://sans.org>



ordenados por su campo de acción, pista muy útil para aquellos lectores que necesiten realizar un estudio de mercado en una tecnología de seguridad en concreto. Las referencias no proceden de los propios vendedores, sino de usuarios de esos productos. Toda esta información también se ofrece condensada en unos *posters* descargables en formato pdf.

El instituto SANS es de sobra conocido en el mundo de la formación en seguridad en tecnologías de la información por sus cursos de gran calidad, tanto presenciales en diversas partes del globo, como en línea. Me gustaría detenerme en algunos productos gratuitos en inglés que ofrece su web. Se encuentran en tres de las secciones del menú horizontal que presenta su portada:

- Recursos (“resources”) - sección a la que dedicaré mayor atención)
- Centro de Incidencias (“storm center”)
- Desarrolladores (“developer”)

La sección de recursos es la más prominente. De ella destacaría las listas de éxitos, como la de los 25 errores de programación más peligrosos (publicada en enero de 2009, en la que han participado organizaciones tan diferentes y representativas como OWASP o Microsoft), los 20 riesgos de seguridad más importantes (de momento con información de 2007), los 5 informes esenciales de datos históricos—logs—(con la participación de Chris Benton y Marcus Ranum) o las 10 tendencias dentro de la seguridad (publicada en 2006).

Sin salir de la sección de recursos, la “sala de lectura” (en inglés, “reading room”) es toda una biblioteca gratuita de documentos elaborados por estudiantes y corregidos por correctores y/o profesores de SANS. Un lugar muy adecuado para recabar referencias útiles si el lector tiene como tarea elaborar una política de seguridad, un procedimiento o investigar un caso técnico concreto de seguridad. Todos los documentos incluyen su autor y la fecha de creación.

En esta misma sección, el apartado titulado “qué funciona” (“what works”) proporciona nombres de productos de seguridad

Para terminar con la sección de recursos, me gustaría señalar los “webcasts” y los boletines semanales a los que el visitante puede suscribirse, p.e. sobre incidentes de seguridad actuales o las últimas vulnerabilidades encontradas en diversos productos.

El centro de incidencias (literalmente, el centro [de seguimiento] de tormentas, “storm center”) es uno de los enclaves más veteranos de este sitio. Cada día, el lector puede comprobar el estado global de Internet en relación con posibles amenazas en el diario del centro de incidencias. La tarea de mantener el diario rota entre los expertos más conocidos relacionados con SANS (p.e. Tom Liston, todo un nombre en seguridad en máquinas virtuales, y Raúl Siles, ídem en seguridad en redes inalámbricas, entre otros).

En la sección de desarrolladores (“developers”), me gustaría destacar los planes de acción de los exámenes para programación segura de aplicaciones (“secure programming exam blueprints”): interesante referencia para construir un perfil de experto de seguridad en desarrollo de aplicaciones.

Finalmente, no quisiera concluir sin mencionar una dirección de SANS exclusivamente dedicada a la forensia elaborada por Rob Lee: forensics.sans.org. Una visita recomendada especialmente si el lector se dedica a la investigación forense.

Como anécdota, cabe recordar que el 13 de julio de 2001, el grupo de *hackers* Fluffy Bunny colocó en la web de SANS el eslogan “¿Confiarías en estos tipos para que te enseñen seguridad?” (aún visible en <http://mirror.ainex.net/fluffy/sans.org/>). Ya ha pasado mucho tiempo de esto, pero en SANS aún lo recuerdan vivamente.

Alberto Partida Rodríguez
Especialista en Seguridad TI
Securityandrisk.blogspot.com



Sugerencias y comentarios:
apartidar@gmail.com