UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

POSGRADO

Extracción de conocimiento a partir de fuentes de datos procedentes de la monitorización de eventos de seguridad

Andrés Caro Lindo
Universidad de Extremadura

Facultad de Informática
Sala de Grados - miércoles 24 de abril de 2019 - 18:00
Entrada libre hasta completar el aforo

Resumen:

La Gestión de Eventos e Información de Seguridad (Security Information and Event Management - SIEM) está cada vez más implantada en las organizaciones, debido a la importancia que en los últimos años está adquiriendo la seguridad en los Sistemas Informáticos. Estos sistemas proporcionan información muy útil sobre eventos relacionados con la seguridad y con potenciales amenazas de riesgos y vulnerabilidades, ayudando en la detección de conductas inusuales, generando alertas, y siendo capaces de monitorizar e incluso predecir comportamientos futuros. La Gestión de Eventos de Seguridad (SEM) tiene que ver con la monitorización y correlación de eventos de seguridad en tiempo real, mientras que la Gestión de Información de Seguridad (SIM) procesa esos datos, almacena, analiza y genera informes. Cuando los datos provienen de múltiples fuentes es fundamental gestionar adecuadamente el proceso de extracción, transformación y carga (ETL). Este proceso es crítico, ya que es muy posible que se utilicen varias soluciones, desde diferentes perspectivas de seguridad.

Sobre Andrés Caro Lindo:

Andrés Caro, Doctor e Ingeniero en Informática, es Profesor Titular de Universidad en el Departamento de Ingeniería de Sistemas Informáticos y Telemáticos de la Universidad de Extremadura (Área de Lenguajes y Sistemas Informáticos). Es el Investigador Principal del Grupo de Ingeniería de Medios (GIM) de la UEx, grupo formado por 16 investigadores (11 de los cuales son doctores). Desde el año 2000 imparte docencia en la Escuela Politécnica (Cáceres), siempre en las titulaciones de Ingeniería e Ingeniería Técnica en Informática. En la actualidad, su docencia se desarrolla en los Grados de Ingeniería Informática (Ingeniería del Software / Ingeniería de Computadores) y en el Máster de Ingeniería Informática, en asignaturas de programación de bases de datos, calidad de procesos y de productos software, auditoría y legislación informática, protección de datos, análisis forense y peritaje informático, hacking ético, etc. Es Investigador Principal en proyectos europeos y regionales, y autor de diversos artículos, ponencias e informes periciales.