sedian

Seguridad Digital
de Andalucía

Ficha técnica

Gestión y correlación de logs

Curso presencial. 10 horas

JUNTA DE ANDALUCIA
CONSEJERÍA DE ECONOMÍA, CONOCIMIENTO, EMPRESAS Y UNIVERSIDAD

ÍNDICE

1. Datos generales

Título:
Gestión y correlacion de logs.

Modalidad:
Presencial.

Fecha:
23 y 24 de abril en Sevilla.

Lugar de celebración:
Sevilla: Instalaciones Sandetel. Pabellón de Francia. PCT Cartuja. Camino de los descubrimientos, 11. Planta baja.

Duración:
10 horas.

Horario:
09:00 a 14:00.

Dirigido a:
Responsables de seguridad TIC y profesionales TIC de la Junta de Andalucía.

2. Ponente

Pedro Candel

Actualmente en CS3 Group Security Services donde es co-fundador.

Ha sido docente en varios Máster de Seguridad en diferentes Universidades como La Salle, UCJC, UCAV, EIG, Ilumno, etc. Especializado en Seguridad Ofensiva, Reversing, Malware, Desarrollo Seguro y Forense.

Ponente habitual en congresos, conferencias, eventos y otras instituciones nacionales e internacionales en materia de ciberseguridad presentando trabajos de investigación en todo el mundo.

Ha trabajado en Deloitte CyberSOC Academy, Buguroo Offensive Security, para el Servicio de Formación y Empleo de la Junta de Comunidades de Castilla-La Mancha y varias consultoras privadas de Telecomunicaciones y Seguridad TIC formando a cientos de grandes empresas de todo de sectores entre los que destaca el financiero, logístico, farmacéutico, TIC, etc. y formación a Fuerzas y Cuerpos de Seguridad.

También, como auditor de seguridad especializado, ha realizado auditorías de hacking ético para clientes del IBEX35, NASDAQ y todo tipo de empresas privadas.

Miembro del claustro de docentes de IMF. Business School. Andalucía, en el máster semipresencial en ciberseguridad y del claustro de docentes de IMF para el programa Servicio de Formación y Sensibilización. Confianza Digital de Sandetel.

3. Calendario y lugar de celebración

Sevilla: días **23 y 24 de abril** de 2018 de 09:00 a 14:00h.

Instalaciones IMF Business School Sevilla. PCT Cartuja. Camino de los descubrimientos, 11. Planta baja.

4. Objetivos

Alcanzar un conocimiento detallado sobre la administración, gestión y correlación de eventos, logs o flujos de información generados a partir de cualquiera de los dispositivos activos, así como las claves para la implantación de un SIEM, prácticas OSSIM y generación de informes. Conocimiento detallado sobre la nueva herramienta de gestión y correlación de los GLORIA.

5. Contenido

1.- Introducción a la monitorización, análisis, correlación y gestión de logs

1.2.- Herramientas fundamentales

2.- IDS basados en cliente (HIDS)

3.- IDS de red o Network IDS

3.1.- Snort

3.2.- Suricata

3.3.- Bro IDS

3.4.- Frameworks de análisis: XPLICO y Moloch

6. Material necesario.

Para poder realizar correctamente las prácticas y ejercicios necesarios para este curso, es necesarios que los alumnos dispongan de las siguientes herramientas:

1.- La VM SELKS (http://dl.stamus-networks.com/selks/SELKS-4.0-desktop.iso)

2.- Ls requisitos mínimos serían al menos 2 núcleos de CPU y 4 GB de RAM disponibles para poder ejecutarla.