FICHA DE ASIGNATURA

Título: Monitorización de acontecimientos de seguridad

Descripción: En esta asignatura vamos a profundizar en el concepto de “gestión de riesgos” y, en particular, de los riesgos asociados al uso de las tecnologías por parte de las organizaciones.

Carácter: Básica

Créditos ECTS: 4

Contextualización: La inteligencia operacional se refiere a una categoría de métodos y tecnologías que permiten dar visibilidad al negocio y descubrimiento de conocimientos para las TI en toda la organización. La inteligencia operacional no es una consecuencia de la inteligencia empresarial (BI), sino un nuevo enfoque basado en fuentes de información no típicamente en el ámbito de las soluciones de BI. Detrás de cada infraestructura de TI, detrás de los sistemas que ejecutan su negocio, se están generando masivamente flujos de datos generados por las máquinas. Las principales organizaciones se dan cuenta de que estos datos pueden ser increíblemente valiosos para mejorar la eficiencia no solo de TI, sino también de otras partes del negocio. La inteligencia operacional está diseñada específicamente para abordar esta oportunidad.

Modalidad: Online

Temario:

Semana 1. Introducción y registros propios del sistema
Temario:

- Introducción y registros propios del sistema
- Filtrado de eventos en Windows
- Auditoría de borrado de documentos
- Alarma "para pobres" (tareas + datos de evento + script)
- Búsqueda en otros registros de eventos
- Configuración de Syslog para aceptar logs de SSH
- Centralización de logs mediante Syslog remoto
- Envío de eventos de Windows a Syslog
- Herramientas:
- Visor de Eventos, Editor de directivas, Programador de tareas
- Editor del registro, Firewall de Windows
- EventCreate, EventToSyslog
- Logrotate, Syslog (Rsyslog), Logger, OpenSSH

Semana 2. Sistemas de detección y monitorización
Temario:

- Sistemas de detección y monitorización
- Jugando con Snort (instalación, sniffer, NIDS, contenido)
- Jugando con OSSEC (instalación, WebUI, agentes, integridad)
- Herramientas:
- Snort, PulledPork

- OSSEC (OSSEC, OSSEC WUI, agentes Linux/Windows)

Semana 3: Fuentes heterogéneas de datos y correlación de logs
Temario:

- Fuentes heterogéneas de datos
- Acceso a la Deep Web mediante TorBrowser
- Uso de Maltego (instalación, Twitter, Shodan)
- Correlación de logs
- Jugando con OSSIM (configuración, activos, vulnerabilidades, OSSEC)
- Jugando con Splunk (instalación, datos locales y remotos, búsquedas)
- Herramientas:
- Tor Browser, Maltego, Deep Web, Pastebin, Twitter, CVE
- OSSIM (OSSIM, Collectors, nmap, Nagios, OpenVAS, OSSEC)
- Splunk (Splunk, Forwarders, Apps)

Competencias

CB1. Que los estudiantes posean y comprendan conocimientos los conceptos generales en los que se fundamenta la Monitorización de acontecimientos de seguridad,.

Actividades Formativas

Actividad Formativa	Horas	Presencialidad
Sesiones síncronas	3	
Videos con teoría	6	
Caso práctico	5	
Estudio autónomo	TBD	
Tutoría	TBD	

Metodologías docentes

- Clases síncronas

- Vídeos con píldoras de conceptos teóricos

- Caso práctico

- Soporte a consultas

-

Sistema de Evaluación

Sistemas de evaluación	Ponderación mínima	Ponderación máxima
Examen	55%	55%
Trabajo individual	45%	45%