Temario del curso:

Metodología de trabajo en Seguridad para redes móviles.

Duración: 24 horas.
Público: administradores de sistemas, operadores y usuarios de entornos móviles.
Objetivo: Crear conciencia de seguridad en entornos móviles, y ofrecer una fuerte base de conocimientos sobre el empleo seguro de estas infraestructuras.

Temario

1. FASE PRELIMINAR:
   a. Estudio del sistema a implantar.
   b. Análisis de riesgo.
   c. Determinación de requisitos de seguridad.
   d. Definición de sistemas de autenticación y control de accesos.
   e. Definición de tráfico tunelizado y no tunelizado.
   f. Determinación del empleo de criptografía para la transmisión de información
   g. Confección de una política de seguridad preliminar.

2. DESPLIEGUE DEL SISTEMA:
   a. Planificación de la red.
   b. Segmentación de la misma.
   c. Instalación del Hardware y Software.
   d. Bastionado de equipos.
   e. Instalación de sondas para captura de tráfico.
   f. Análisis de rutas y metodología de difusión de las mismas.
   g. Confección de reglas en FWs.
   h. Confección de ACL en Routers y Nodos.
   i. Creación de contextos y túneles.

3. TRABAJO COTIDIANO EN SEGURIDAD:
   a. Análisis de tráfico.
   b. Determinación de flujos.
   c. Control de túneles.
   d. Confección de scripts para la detección de tráfico tunelizado no permitido.
   e. Análisis de eventos.

f. Centralización, clasificación y evaluación de eventos.
g. Determinación de falsos positivos.
h. Ajuste de sensores.
i. Confección de estadísticas
j. Generación de informes periódicos y aperiódicos.
k. Actualización de los sistemas.
l. Realimentación de la política de seguridad

4. CAPACITACIÓN DE SEGURIDAD:

a. Empleo de política y planes de seguridad.
b. Procedimientos operativos normales.
c. Formación de administradores y usuarios.
d. Formación de personal de soporte técnico.
e. Preparación ante incidentes.
f. Análisis forense.
g. Simulaciones de incidencias.
h. LOPD.

5. DOCUMENTACIÓN DE SEGURIDAD:

a. Política de seguridad.
b. Procedimientos:
   - Test de procedimientos.
   - Procedimiento de Actividades agendadas.
   - Procedimientos ante incidentes.
   - Procedimientos post incidentes.
   - Procedimientos para evaluación de vulnerabilidades.
   - Procedimientos de autenticación y control de accesos.
   - Procedimientos de backup y restauración.
   - Procedimientos de bastionado.
   - Procedimientos de puesta en servicio.
   - Procedimientos para la administración de nombres y direcciones.
   - Procedimientos para la administración de cuentas.
   - Procedimientos para la administración de contraseñas y claves.
   - Procedimientos para la creación y administración de túneles.
   - Procedimientos para el empleo de criptografía.
   - Procedimientos para auditoría de seguridad.
c. Plan contra incidentes.
d. Metodología de trabajo con Roaming.
e. Metodología de trabajo con usuarios particulares y empresas.

f. Metodología de Autenticación y Control de accesos.
g. Metodología para la confección y presentación de informes de seguridad.