

Seguridad Avanzada para Servicios, Microservicios y SOA

Código: ARC-319

Propuesta de Valor: ARCITURA

Duración: 10 Horas



Este curso cubre una serie de temas técnicos y de seguridad complejos relacionados con el diseño contemporáneo de soluciones orientadas a servicios, infraestructura, microservicios, gateways para APIs y tecnologías de servicios modernas.



AUDIENCIA

- Perfiles técnicos que tienen conocimientos de programación y desarrollo de software.
- Recién graduados.



PRE REQUISITOS

- Se recomienda realizar el curso: Fundamentos de Seguridad para Servicios, Microservicios y SOA.



OBJETIVOS

Adquirir conocimientos en:

- STRIDE (suplantación de identidad, manipulación, repudio, divulgación de información, denegación de servicio, elevación de privilegios).
- Patrones de seguridad SOA para la arquitectura de servicios internos (protección de excepciones, filtrado de mensajes, subsistema de confianza, protección del perímetro del servicio).
- Estructuras y emisión de tokens de seguridad (JWT, nombre de usuario, X.509, SAML).
- Sesiones de autenticación y conversaciones seguras.
- Federación y seguridad de intermediación de confianza.

- Diseño de políticas y gobernanza.
- Controles y diseños de seguridad REST.
- Especificación de API abierta (OAS v 3.0), Open ID Connect.
- Diseños y controles de seguridad de servicios web.
- WS-Policy, WS-SecurityPolicy, WS-Trust y WS-Secure Conversation con SAML.
- Consideraciones de seguridad de microservicios y contenedores.
- Extensiones y controles de seguridad para puertas de enlace API y ESB.
- Riesgos de seguridad y consideraciones para servicios basados ??en la nube y composiciones de servicios.
- Preparación para amenazas de seguridad SOA comunes.

CERTIFICACIÓN DISPONIBLE

- La ruta de Especialista en Seguridad de Servicios se compone de los Módulos 1, 2, 18, 19 y 20 de SOACP.

CONTENIDO

1. PASO

- 1.1. SPOOFING
- 1.2. MANIPULACIÓN
- 1.3. REPUDIO
- 1.4. DIVULGACIÓN DE INFORMACIÓN
- 1.5. NEGACIÓN DE SERVICIO
- 1.6. PRIVILEGIO DE ELEVACIÓN

2. MECANISMOS DE SEGURIDAD

- 2.1. ACCIONES DE TOKEN DE SEGURIDAD
- 2.2. INTERMEDIACIÓN DE CONFIANZA
- 2.3. SESIONES DE SEGURIDAD
- 2.4. POLITICAS DE SEGURIDAD

3. DEFENSA EN PROFUNDIDAD DE LOS ESTÁNDARES AVANZADOS DE LA INDUSTRIA

- 3.1. SERVICIOS WEB
- 3.2. SERVICIOS REST

4. MIDDLEWARE SOA

- 4.1. TAREAS DE SEGURIDAD
- 4.2. TEMAS DE SEGURIDAD
- 4.3. PATRONES

5. AMENAZAS ESPECÍFICAS DE LA NUBE

- 5.1. AGENTES DE AMENAZA
- 5.2. ORIENTADO A DATOS

6. PATRONES DE SEGURIDAD DEL SERVICIO

6.1. BLINDAJE DE EXCEPCIONES

6.2. PANTALLA DE MENSAJES

6.3. SUBSISTEMA DE CONFIANZA

6.4. GUARDIA PERIMETRAL DE SERVICIO

7. SEGURIDAD DEL CONTENEDOR

7.1. PRINCIPIO DE PRIVILEGIO MÍNIMO

7.2. DEFENSA EN PROFUNDIDAD

8. AMENAZAS DE SEGURIDAD

8.1. AMENAZAS ORIENTADAS A DATOS

8.2. AMENAZAS ORIENTADAS AL ACCESO

BENEFICIOS

- Al finalizar el curso, tendrás comprensión de las amenazas a la seguridad SOA.