Seguridad en la Nube Laboratorio

Código: ARC-409

Propuesta de Valor: ARCITURA

Duración: 10 Horas

Este curso presenta a los participantes una serie de ejercicios y problemas que diseñado para poner a prueba su capacidad para aplicar su conocimiento de los temas tratados anteriormente en los cursos ARC-407 y ARC-408. Completar esta práctica de laboratorio ayudará a resaltar las áreas que requieren mayor atención y demostrará además su competencia práctica en las prácticas, los mecanismos y los mecanismos de seguridad de la computación en la nube, patrones arquitectónicos a medida que se aplican y combinan para resolver problemas del mundo real.

Como laboratorio práctico, este curso proporciona un conjunto de ejercicios detallados que requieren que los participantes resuelvan una serie de problemas interrelacionados, con el objetivo final de evaluar, diseñar y corregir arquitecturas de tecnología de seguridad en la nube para cumplir con conjuntos específicos de soluciones y negocios requisitos de automatización.

AUDIENCIA

- Recién graduados.

PRE REQUISITOS

- Se recomienda realizar el curso: Seguridad en la Nube Avanzado.

OBJETIVOS

- Evaluar, diseñar y corregir arquitecturas de tecnología de seguridad en la nube.
- Adquirir conocimientos en mecanismos de seguridad de la computación en la nube.

CERTIFICACIÓN DISPONIBLE

- La ruta de Especialista en Seguridad en la Nube se compone de los Módulos 1, 2, 7, 8 y 9 de CCP. Realice el Examen C90.CSP, un único examen combinado para toda la ruta de certificación de Especialista en Seguridad en la Nube. Recomendado para quienes sólo quieren presentar un único examen que abarque todos los módulos de esta ruta.

Cognos tiene un único cronograma virtual para todos los países de habla Hispana. Los cursos presenciales están disponibles a través de los centros franquiciados.
Copyright © Cognos 2020 Todos los derechos reservados.

CONTENIDO

1. PATRONES DE DISEÑO DE SEGURIDAD EN LA NUBE

1.1. GARANTÍA DE CONFIANZA
1.2. GESTIÓN DE IDENTIDADES Y ACCESOS EN LA NUBE (IAM)
1.3. CONEXIÓN DE RED SEGURA
1.4. PROTECCIÓN DE PLATAFORMA VM
1.5. ORIENTADO A DATOS
1.6. CONTROL DE ACCESO
1.7. COMPUESTO

2. CIMIENTOS

2.1. CICLO DE VIDA DEL ATAQUE
2.2. MODELADO DE AMENAZAS
2.3. RIESGO
2.4. CICLO DE VIDA DE SEGURIDAD
2.5. CRIPTOGRAFÍA
2.6. GARANTÍA DE CONFIANZA
2.7. GESTIÓN DE IDENTIDAD Y ACCESO (IAM)
2.8. TRÍADA AIC

3. AMENAZAS

3.1. ORIENTADO A DATOS
3.2. ORIENTADO AL ACCESO

4. AGENTES DE AMENAZAS

4.1. ATACANTE EXTERNO
4.2. AGENTE DE SERVICIO MALINTENCIONADO
4.3. INQUILINO MALICIOSO
4.4. INFORMACIÓN PRIVILEGIADA MALICIOSA

5. PROTECCIÓN DE RED

5.1. PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO EN LA NUBE
5.2. PROTECCIÓN CONTRA EL SECUESTRO DE TRÁFICO EN LA NUBE
5.3. PERÍMETRO DEFINIDO AUTOMÁTICAMENTE

6. PASO

6.1. SPOOFING
6.2. MANIPULACIÓN
6.3. REPUDIO
6.4. DIVULGACIÓN DE INFORMACIÓN
6.5. NEGACIÓN DE SERVICIO

Cognos tiene un único cronograma virtual para todos los países de habla Hispana. Los cursos presenciales están disponibles a través de los centros franquiciados.
Copyright © Cognos 2020 Todos los derechos reservados.

BENEFICIOS

- Al finalizar el curso, usted tendrá conocimientos para evaluar, diseñar y corregir arquitecturas de tecnología de seguridad en la nube.

Cognos tiene un único cronograma virtual para todos los países de habla Hispana. Los cursos presenciales están disponibles a través de los centros franquiciados.
Copyright © Cognos 2020 Todos los derechos reservados.