Seguridad en la Nube Avanzado

Código: ARC-408

Propuesta de Valor: ARCITURA

Duración: 10 Horas

Este curso avanzado cubre los mecanismos de seguridad en la nube y los patrones de diseño arquitectónico que abordan la seguridad de los datos y el control de acceso para las máquinas virtuales, así como los límites de confianza, geoetiquetado y seguridad BIOS.
El curso también explica los métodos habituales que utilizan los atacantes para infringir recursos y proporciona una metodología para contrarrestar dichos ataques. El curso concluye demostrando la relación entre amenazas, ataques y riesgos a través del modelado de amenazas.

AUDIENCIA

- Recién graduados.

PRE REQUISITOS

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

OBJETIVOS

Adquirir conocimientos en los siguientes temas principales:

- Patrones de seguridad del servicio en la nube y mecanismos de soporte.
- Patrones de protección de plataforma de máquina virtual.
- Consideraciones para configurar perímetros efímeros seguros.
- Grupos confiables de recursos en la nube y control de acceso a los recursos en la nube.
- Protección permanente contra pérdida de acceso a datos.
- Protección contra violaciones de datos en la nube.
- Límites de confianza aislados.
- El ciclo de vida de los ataques y el ciclo de vida de la seguridad.
- Mitigación proactiva frente a respuesta ante incidentes.
- Amenazas, vulnerabilidades, impactos de la explotación.

- Modelado de amenazas, amenazas y mitigaciones.

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.

CONTENIDO

1. PATRONES DE DISEÑO DE SEGURIDAD EN LA NUBE

1.1. PROTECCIÓN DE PLATAFORMA VM
1.2. ORIENTADO A DATOS
1.3. CONTROL DE ACCESO
1.4. 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

3. MECANISMOS

3.1. MÓDULO DE SEGURIDAD DE HARDWARE (HSM)
3.2. GEOETIQUETA
3.3. POLÍTICA DE CONFIANZA DE LA PLATAFORMA
3.4. IMAGEN DE SERVIDOR VIRTUAL REFORZADA
3.5. SISTEMA DE SEGURIDAD BASADO EN HOST (HBSS)
3.6. HIPERVISOR
3.7. SUPERVISOR DE AUDITORÍA
3.8. PROGRAMADOR DE CARGAS DE TRABAJO EN LA NUBE
3.9. SISTEMA DE DESCUBRIMIENTO DE VM BASADO EN HARDWARE
3.10. ADMINISTRADOR DE INFRAESTRUCTURA VIRTUAL (VIM)
3.11. SISTEMA DE GESTIÓN DE MOVILIDAD EMPRESARIAL (EMM)
3.12. AUTORIDAD DE ATRIBUTO
3.13. SERVICIO DE TOKEN SEGURO (STS)
3.14. SISTEMA DE CONTROL DE ACCESO BASADO EN ATRIBUTOS (ABAC)
3.15. INICIO DE SESIÓN ÚNICO (SSO)

BENEFICIOS

- Al finalizar el curso, tendrás conocimientos en patrones de seguridad del servicio en la nube y mecanismos de soporte.