Fundamentos de Seguridad en la Nube

Código: ARC-407

Propuesta de Valor: ARCITURA

Duración: 10 Horas

Este curso básico proporciona una presentación completa y completa de conceptos esenciales técnicas, mecanismos, patrones y tecnologías industriales para establecer sistemas basados ??en la nube, controles de seguridad y arquitecturas de seguridad. Los fundamentos de la seguridad en la nube cubiertos en el módulo 2 continúan con la introducción de categorizaciones de amenazas y nuevos mecanismos de seguridad en la nube. Luego, el curso profundiza en una serie de mecanismos de seguridad en la nube y arquitectura asociada, patrones que exploran una variedad de temas, incluida la seguridad, la identidad y el acceso de la red en la nube, gestión y garantía de confianza.

Más información: AQUÍ

Reserve su plaza: AQUÍ

AUDIENCIA

- Recién graduados.

PRE REQUISITOS

- Se recomienda realizar el curso: Conceptos de Tecnología en la Nube.

OBJETIVOS

Adquirir conocimientos en los siguientes temas principales:

- Conceptos básicos de seguridad en la nube.
- Mecanismos comunes de seguridad en la nube.
- Amenazas de seguridad en la nube.
- Metodología de categorización de amenazas de seguridad en la nube.
- Identificación y tratamiento de amenazas comunes.
- Patrones de seguridad de la red en la nube y mecanismos de soporte.
- Asegurar las conexiones de red y las puertas de enlace de autenticación en la nube.
- Monitoreo y registro colaborativos.
- Auditoría independiente en la nube.
- Patrones de gestión de acceso e identidad en la nube y mecanismos de apoyo.

- Patrones de garantía de confianza y mecanismos de apoyo.
- Atestación de confianza y establecimiento de confiabilidad.

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. PASO

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

2. MECANISMOS

2.1. CONTROLADOR DE ENTREGA DE APLICACIONES (ADC)
2.2. SERVICIO DE NOMBRE DE DOMINIO (DNS)
2.3. SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDPS)
2.4. CERTIFICADO
2.5. RED PRIVADA VIRTUAL (VPN)
2.6. PUERTA DE ENLACE DEL CONSUMIDOR EN LA NUBE (CCG)
2.7. NUBE PRIVADA VIRTUAL (VPC)
2.8. CONCENTRADOR DE VPN EN LA NUBE
2.9. MIGRACIÓN DE VM EN VIVO
2.10. CORTAFUEGOS VIRTUAL
2.11. MONITOR DE TRÁFICO
2.12. FILTRO DE TRÁFICO
2.13. CONTROLADOR DE PERÍMETRO DEFINIDO AUTOMÁTICAMENTE (ADP)
2.14. GESTIÓN DE IDENTIDAD Y ACCESO (IAM)
2.15. AUTORIDAD CERTIFICADORA (CA)
2.16. LISTA DE REVOCACIÓN DE CERTIFICADOS (CRL)
2.17. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)
2.18. SERVICIO DE PUERTA DE ENLACE DE AUTENTICACIÓN (AGS)
2.19. SERVICIO DE VALIDACIÓN DE CERTIFICADOS (CVS)
2.20. SISTEMA DE GESTIÓN DE CLAVES CRIPTOGRÁFICAS (CKMS)
2.21. MÓDULO DE PLATAFORMA CONFIABLE (TPM)
2.22. SERVICIO DE ATESTACIÓN
2.23. MOTOR DE ORQUESTACIÓN

2.25. DETECCIÓN Y RESPUESTA DE AMENAZAS DE PUNTO FINAL (ETDR)
2.26. TARRO DE MIEL
2.27. MONITOR FORENSE DE RED
2.28. HASH DE MALWARE
2.29. SALVADERA
2.30. SISTEMA DE INTELIGENCIA DE AMENAZAS

3. CIMIENTOS

3.1. CRIPTOGRAFÍA
3.2. GARANTÍA DE CONFIANZA
3.3. GESTIÓN DE IDENTIDAD Y ACCESO (IAM)
3.4. TRÍADA AIC

4. AGENTES DE AMENAZAS

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

5. AMENAZAS

5.1. ORIENTADO A DATOS
5.2. ORIENTADO AL ACCESO

6. PROTECCIÓN DE RED

6.1. PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO EN LA NUBE
6.2. PROTECCIÓN CONTRA EL SECUESTRO DE TRÁFICO EN LA NUBE
6.3. PERÍMETRO DEFINIDO AUTOMÁTICAMENTE

7. CONEXIÓN DE RED SEGURA

7.1. ACCESO SEGURO A INTERNET EN LAS INSTALACIONES
7.2. CONEXIÓN SEGURA A LA NUBE EXTERNA
7.3. CONEXIÓN SEGURA PARA MÁQUINAS VIRTUALES ESCALADAS

8. GESTIÓN DE IDENTIDADES Y ACCESOS EN LA NUBE

8.1. AUTENTICACIÓN EN LA NUBE (COMPUESTA)
8.2. PUERTA DE ENLACE DE AUTENTICACIÓN EN LA NUBE
8.3. AUTENTICACIÓN EN LA NUBE FEDERADA

9. GARANTÍA DE CONFIANZA

9.2. SERVICIO DE ATESTACIÓN DE CONFIANZA
9.3. MONITOREO Y REGISTRO COLABORATIVOS
9.4. AUDITORÍA INDEPENDIENTE EN LA NUBE
9.5. PROCESAMIENTO DE INTELIGENCIA DE AMENAZAS

BENEFICIOS

- Al finalizar el curso, tendrás conocimientos de mecanismos para establecer sistemas basados ??en la nube, controles de seguridad y arquitecturas de seguridad.