Curso AWS Cloud Infrastructure Security

Alcance os benefícios do cloud computing com segurança

TENCHI
down-to-earth cloud security

A tecnologia de nuvem traz um estilo mais eficiente de operações de TI, com maior automação, escalabilidade e enormes ganhos na alocação de capital. Mas, mudanças de paradigmas em TI, sempre revelam às organizações grandes desafios de adequação.

O aproveitamento de todo o potencial de *cloud computing* requer entendimento de que arquitetura, operações e segurança neste novo tipo de ambiente são competências altamente especializadas. Porém profissionais com estas competências são extremamente escassos no mercado.

Tudo isso pode resultar em projetos que não atingem seus prazos, benefícios, projeções de custo ou, até mesmo, incidentes de segurança e violações de requisitos regulatórios como LGPD e GDPR. Estas são as principais conseqüências da falta de qualificação das equipes.

A Tenchi Security acredita que a segurança de sua organização tem como base fundamental o investimento em pessoas. Por isso, oferecemos o curso AWS Cloud Infrastructure Security - treinamento que cobre o conhecimento fundamental necessário para se utilizar serviços de Infraestrutura como Serviço (IaaS) da Amazon Web Services de forma segura.

Até 2025, 99% das falhas de segurança na nuvem serão de responsabilidade do cliente.

Fonte: Gartner, "Is the Cloud Secure?"

Sobre o Curso

AWS Cloud Infrastructure Security

Benefícios

- Reduza atrasos e acelere o ROI de seus projetos.
- Reduza o risco de vazamentos de dados causados por uso incorreto da infraestrutura de nuvem.
- Automatize ou elimine atividades repetitivas de segurança para maior agilidade e menor custo.
- Prepare seu ambiente para minimizar o impacto e reduzir o tempo de resposta a incidentes.
- Simplifique o atendimento de requisitos legais e regulatórios, e melhores práticas.
- Motive e retenha sua equipe.

Público-alvo

Esse é um treinamento fundamental que é recomendado a todos os profissionais da organização que terão responsabilidades operacionais, de segurança ou de conformidade com ambientes de nuvem pública AWS, tais como:

- Profissionais de administração, operação, SRE ou DevOps de rede ou TI;
- Arquitetos ou desenvolvedores de software;
- Profissionais ou gestores de segurança da informação;
- Auditores ou profissionais de controles internos ou conformidade de tecnologia da informação.

Metodologia

A metodologia de ensino conta com uma combinação de conteúdo teórico sobre conceitos básicos e serviços fundamentais, bem como laboratórios práticos em que os alunos poderão ganhar a confiança para aplicá-los em seu trabalho.

Material do curso

O material do curso foi escolhido para cobrir as razões mais frequentes pelas quais organizações se vêem vítimas de vazamentos e outros tipos de incidentes em seus ambientes de nuvem, como a muito frequente publicação acidental de dados confidenciais em buckets S3 ou a configuração de privilégios excessivos no control plane do provedor de nuvem.

Agenda | Módulo I: (24h)

1. Conceitos Gerais de Segurança da Informação
a. Proteção de Endpoint
b. Proteção de Rede
c. Proteção de Aplicações
d. Superfície de ataque
e. Modelagem de ameaças
f. Análise de eventos
g. Resposta a incidentes
h. Risco

2. Frameworks de Segurança e Modelagem de Ameaças para Nuvem
a. CIS Controls i. IaaS, PaaS, Saas, FaaS
b. MITRE ATT&CK
  i. Enterprise, Cloud
c. Modelo de responsabilidade compartilhada
  i. AWS
  ii. Empresa
d. Novos vetores de ataque

3. IAM
a.Visão Geral
b. Autenticação Multiplo Fator (MFA)
c. Usuários, Roles e Grupos
d. Permissões
e. Políticas
f. Laboratório Prático

4. EC2
a. Entendendo EC2
b. Tipos de instâncias
c. Proteções de endpoint
d. Metadados
e. Hardening f. Auto Scaling e Load Balancer
g. Laboratório Prático

5. EC2
a. Entendendo EC2
b. Tipos de instâncias
c. Proteções de endpoint
d. Metadados
e. Hardening
f. Auto Scaling e Load Balancer
g. Laboratório Prático

6. S3
a. Entendendo S3
b. Modos de uso
c. Monitoramento de acessos
d. Laboratório Prático

7. Criptografia e PKI
a. Certificate Manager
b. KMS
c. Laboratório Prático

8. Revisão do Módulo

Agenda | Módulo II: (16h)

1. Revisão do Módulo I
a. Console Gerenciamento / AWS CLI
b. IAM
c. EC2
d. S3

2. VPC
a. Entendendo VPC
b. Estudo de diagramas
c. Peering
d. VPC endpoints
e. Monitoramento de tráfego
f. Casos de uso
g. Laboratório Prático

3.Gerenciamento e Operação Segura de Infraestrutura
a. CloudWatch, CloudWatch Events e CloudWatch Logs
b. Systems Manager
c. Inspector d. Cloudtrail
e. Config
f. Laboratório Prático

4. Integração com Ambiente On-Premises
a. Conceitos de Integração e Compartimentalização Segura
b. Client VPN
c. Site-to-Site VPN e CloudHub
d. Organizations e Single Sign-on
e. Laboratório Prático

5. Introdução a Serviços de Segurança
a. CloudTrail
b. GuardDuty
c. WAF
d. Shield
e. Single Sign On
f. Security Hub

6. Estudo de Caso - Projeto de consultorias aplicando melhores práticas para a "ThunderBit Corporation"

Pré-Requisitos

- Laptop para uso durante o curso com permissão para instalar software e acessar a Internet sem filtragem a sites de documentação ou console de gerenciamento da AWS;
- Conta AWS nova criada com 48h de antecedência.

Este treinamento é voltado para profissionais ligados a tecnologia. De forma a tirar o máximo proveito do conteúdo teórico e principalmente dos laboratórios, o seguinte conhecimento prático é fortemente recomendado:

- Acesso remoto e uso de linha de comando de sistemas operacionais Linux ou Windows;
- Leitura de logs;
- Funcionamento de redes TCP/IP e protocolos HTTP / HTTPS.

Entre em contato para
treinamentos in company!

Av. das Nações Unidas, 12901 - Brooklin, São Paulo - SP
04578-910
contato@tenchisecurity.com.br
tenchisecurity.com.br

TENCHI
down-to-earth cloud security

/company/tenchisecurity/
@TenchiSecurity