



CORSO AWSSE: Security Engineering on AWS

CEGEKA Education
corsi di formazione professionale

Security Engineering on AWS

Cegeka e beSharp propongono il corso Security Engineering on AWS che illustra come utilizzare i servizi di sicurezza di AWS per garantire la protezione e la conformità nel cloud AWS in modo efficiente. Questo corso si concentra sulle best practice di sicurezza consigliate da AWS che aiutano a migliorare la protezione dei dati e dei sistemi nel cloud. Il corso descrive le caratteristiche di sicurezza dei più importanti servizi di AWS, tra cui i servizi di elaborazione, di storage, di rete e di database. Il corso illustrerà infine come sfruttare i servizi e gli strumenti di AWS per creare automazioni e monitorare i carichi in modo continuo, e rispondendo agli incidenti nella sicurezza.

Durata del corso 3 giorni

Destinatari / Audience

- Tecnici della sicurezza
- Progettisti che si occupano della sicurezza dell'architettura
- Operazioni di sicurezza
- Sicurezza informatica

Obiettivi / Goals

- Assimilare e sfruttare il modello di responsabilità condivisa della sicurezza di AWS
- Progetta e realizza infrastrutture di applicazioni AWS che sono protetti dalle minacce di sicurezza più diffuse
- Proteggi i dati inattivi e i dati in movimenti con la crittografia
- Applica i controlli e le analisi di sicurezza in modo automatico e riproducibile
- Configura l'autenticazione per risorse e applicazioni nel Cloud AWS
- Informazioni dettagliate sugli eventi tramite l'acquisizione, il monitoraggio, l'elaborazione e l'analisi dei log
- Identifica e controlla le minacce in entrata contro applicazioni e dati
- Esegui valutazioni sulla sicurezza per assicurare che siano riparate le vulnerabilità comuni e siano applicate le best practice di sicurezza

Requisiti / Requirements

- AWS Cloud Practitioner Essentials
- AWS Security Fundamentals
- Architecting on AWS (AWSA)
- Conoscenza di lavoro delle procedure di sicurezza IT e dei concetti relativi all'infrastruttura
- Familiarità con i concetti di cloud computing

Certificazione

Questo corso è parte della seguente certificazione: AWS Certified Security - Specialty (ACSS)

Moduli / Modules

Introduction

- Welcome and introductions
- Introduction to Security on AWS

Identifying entry points on AWS

- Ways to access the platform
- IAM policies
- Securing entry points
- Incident response

Security Considerations - Web Applications

- Security points in an AWS web application environment
- Analyse a three-tier application model and identify common threats
- Assess environments to improve security

Application Security

- Securing EC2 instances
- Assess vulnerabilities with Inspector
- Apply security in an automated way using Systems Manager
- Isolate a compromised instance

Securing Networking Communications - Part 1

- Apply security best practices to VPC
- Implement an ELB device as a protection point
- Protect data in transit using certificates

Data Security

- Protect data at rest using encryption and access controls
- AWS services used to replicate data
- Protect archived data

Security Considerations: Hybrid Environments

- Security points outside of a VPC
- Common DoS threats

Monitoring and Collecting Logs on AWS

- Monitor events and collect logs with CloudWatch
- Use Config to monitor resources
- AWS-native services that generate and collect logs

Processing Logs on AWS

- Stream and process logs for further analysis
- AWS services used to process logs from S3 buckets

Securing Networking Communications - Part 2

- Identify AWS services used to connect on-premise to AWS
- Data protection between on-premise and AWS

- Securely access VPC resources in other accounts

Out-Of-Region Protection

- Use Route 53 to isolate attacks
- Implement WAF to protect applications
- Use CloudFront to deliver content securely
- Protect applications using Shield

Account Management on AWS

- Manage multiple accounts
- Use identity providers / brokers to acquire access to AWS services

Security Considerations: Serverless Environments

- How to secure data in a serverless environment
- Use Cognito to authorize users
- Control API access with API Gateway
- Use AWS messaging services securely
- Secure Lambda functions

Secrets Management on AWS

- Manage key and data encryption with KMS
- Describe how CloudHSM is used to generate and secure keys
- Use Secrets Manager to authenticate applications

Security Automation on AWS

- Deploy security-oriented AWS environments in a reproducible manner
- Provide management and control of IT services to end-users in a self-serve manner

Threat Detection and Sensitive Data Monitoring

- Threat detection and monitoring for malicious or unauthorized behaviour
- Leverage machine learning to gain visibility into how sensitive data is being managed in the AWS Cloud

CEGEKA Education

corsi di formazione professionale

La formazione di qualità, su misura per te



Flessibile

I corsi possono essere organizzati negli orari e nelle modalità più adatte alle tue esigenze, in modo che abbiano il minor impatto possibile sulle tue attività quotidiane.



Training on the job

Docenti altamente qualificati ti affiancheranno durante una giornata di lavoro e ti aiuteranno ad utilizzare le tecnologie per risolvere problemi reali.



Two-steps

Teoria e pratica vanno a braccetto. Il nostro percorso formativo, suddiviso in due fasi, ti permette di acquisire la conoscenza e di testarne subito l'efficacia.



Sharing Course

Corsi in aula di gruppo, con teoria e laboratori, questi ultimi proposti da ogni singolo partecipante su aspetti reali tratti dalla pratica quotidiana



On-Site

I corsi possono svolgersi presso una delle sedi CEGEKA o presso la vostra sede sia sul territorio nazionale che internazionale.



One-to-One

Corsi progettati e realizzati su misura, sia di gruppo che individuali con docente interamente dedicato

www.cegeka.it/education/
learning@cegeka.it

Milano

Via Alessandro Volta, 16
20093 Cologno Monzese, MI
Tel: +39 02 254427 255

Roma

Via Casilina 3T, Palazzina D
00182 Roma
Tel: +39 06 72910119

Padova

Corso Stati Uniti 18/B
35127 Padova
Tel. +39 049 8976800