Course duration

- 3 days

Course Benefits

- Assimilate and leverage the AWS shared security responsibility model
- Architect and build AWS application infrastructures that are protected against the most common security threats
- Protect data at rest and in transit with encryption
- Apply security checks and analyses in an automated and reproducible manner
- Configure authentication for resources and applications in the AWS Cloud
- Gain insight into events by capturing, monitoring, processing, and analyzing logs
- Identify and mitigate incoming threats against applications and data
- Perform security assessments to ensure that common vulnerabilities are patched and security best practices are applied

Authorized AWS Training

Webucator has partnered with an Authorized AWS training delivery partner to offer official AWS courses utilizing Amazon Authorized Instructors.

Course Outline

1. Identifying Entry Points on AWS
2. Security Considerations: Web Application Environments
3. Application Security
4. Securing Networking Communications – Part 1
5. Data Security
6. Security Considerations: Hybrid Environments
7. Monitoring and Collecting Logs on AWS
8. Processing Logs on AWS
9. Securing Networking Communications – Part 2
10. Out-Of-Region Protection
11. Account Management on AWS
12. Security Considerations: Serverless Environments
13. Secrets Management on AWS
14. Automating Security on AWS
15. Threat Detection and Sensitive Data Monitoring

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.