Course Descriptions

Cloud Computing Security Knowledge- Foundation

There is a lot of hype and uncertainty around cloud security, but this class will slice through the hyperbole and provide students with the practical knowledge they need to understand the real cloud security issues and solutions. The Cloud Computing Security Knowledge- Foundation class provides students a comprehensive one day review of cloud security fundamentals and prepares them to take the Cloud Security Alliance CCSK certification exam. Starting with a detailed description of cloud computing, the course covers all major domains in the latest Guidance document from the Cloud Security Alliance, background on the CSA CCM and CAIQ tools, and the recommendations from the European Network and Information Security Agency (ENISA). This class is geared towards security professionals, but is also useful for anyone looking to expand their knowledge of cloud security. (We recommend attendees have at least a basic understanding of security fundamentals, such as firewalls, secure development, encryption, and identity management).

Course Outline:

This course is broken out into 6 modules that cover the 14 domains of the CSA Guidance and the ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security.

M**odule 1**: Introduction to Cloud Computing. This module covers the fundamentals of cloud computing, including definitions, architectures, and the role of virtualization. Key topics include cloud computing service models, delivery models, and fundamental characteristics. It also introduces the Shared Responsibilities Model and a framework for approaching cloud security.

Module 2: Infrastructure Security for Cloud Computing. This modules digs into the details of securing the core infrastructure for cloud computing- including cloud components, networks, management interfaces, and administrator credentials. It delves into virtual networking and workload security, including the basics of containers and serverless.

Module 3: Managing Cloud Security and Risk. This module covers important considerations for managing security for cloud computing. It begins with risk assessment and governance, then covers legal and compliance issues, such as discovery requirements in the cloud. It also covers important CSA risk tools including the CAIQ, CCM, and STAR registry.

Module 4: Data Security for Cloud Computing. One of the biggest issues in cloud security is protecting data. This module covers information lifecycle management for the cloud and how to apply security controls, with an emphasis on public cloud.

Topics include the Data Security Lifecycle, cloud storage models, data security issues with different delivery models, and managing encryption in and for the cloud, including customer managed keys (BYOK).

Module 5: Application Security and Identity Management for Cloud Computing. This module covers identity management and application security for cloud deployments. Topics include federated identity and different IAM applications, secure development, and managing application security in and for the cloud.

Module 6: Cloud Security Operations. This module covers key considerations when evaluating, selecting, and managing cloud computing providers. We also discuss the role of Security as a Service providers and the impact of cloud on Incident Response.

Cloud Computing Security Knowledge- Plus

The CCSK- Plus class builds upon the CCSK Basic class with expanded material and extensive hands-on activities integrated into the training. Students will learn to apply their knowledge as they perform a series of exercises as they complete a scenario bringing a fictional organization securely into the cloud.

This expanded material includes additional lecture, although student's will spend most of their time assessing, building, and securing a cloud infrastructure during the exercises.

Course Outline:

This is a two day class that integrates the CCSK- Foundation training with expanded lectures and hands-on labs. The Plus content extends the course with:

Exercise 1: Core Account Security. Students learn what to configure in the first 5 minutes of opening a new cloud account and enable security controls such as MFA, basic monitoring, and IAM.

Exercise 2: IAM and Monitoring In-Depth. Attendees expand their work on the first lab and implement more-complex identity management and monitoring. This includes expanding IAM with Attribute Based Access Controls, implementing security alerting, and understanding how to structure enterprise-scale IAM and monitoring.

Exercise 3: Network and Instance Security. Students create a virtual network (VPC) and implement a baseline security configuration. They also learn how to securely select and launch a virtual machine (instance), run a vulnerability assessment in the cloud, and connect to the instance.

Exercise 4: Encryption and Storage Security: Students expand their deployment by adding a storage volume encrypted with a customer managed key. They also learn how to secure snapshots and other data.

Exercise 5: Application Security and Federation. Students finish the technical labs by completely building out a 2-tier application and implementing federated identity using OpenID.

Exercise 6: Risk and Provider Assessment. Students use the CSA CCM and STAR registry to evaluate risk and select a cloud provider.