Cloud Computing Security Course Overview

Table of Contents

Notice

Cloud Computing Security – Course Overview

**002 This cloud security Course explores guidance from the Cloud Security Alliance.

Cloud Computing Security -1

- Cloud Security Alliance (CSA)
- National Institute of Standards and Technology (NIST)
- Cloud Service Providers (e.g., Google, Amazon, Microsoft)

**003 The National Institute of Standards and Technology, and several cloud service providers, including Google, Amazon, and Microsoft.

Cloud Computing Security -2

- Basic cloud operations and concepts
- Security risks and threats
- Incident response
- Application security
- Data security
- Resource security

**004 We'll touch upon basic cloud operations and concepts and compare those to traditional on-premise solutions. Doing this also serves as an introduction or review to these key concepts that guide solution design and implementation of security controls.

Since this is intended to be a cybersecurity focus course, we will also touch upon cloud-related security risks and threats. These would be new concerns when using cloud-computing platforms, or perhaps a slight twist on old threats.

We'll cover incident response in the cloud; specifically, we will discuss several important things you should monitor and we'll use demonstrations with various cloud platforms to highlight some really neat

capabilities. We will also review best practices for application, data, and resource security, and how these can be achieved; and again, we'll use demonstrations of cloud provider tools and capabilities to reinforce key points.

Cloud Computing Security -3

**005 You should have some familiarity with cybersecurity and infrastructure technology concepts, lexicon, tools, controls, and other best practices. We will try to map numerous cloud services and capabilities back to more traditional implementation methods to help reinforce understanding.

This course is not a deep-dive into any one standard architecture or provider; instead it'll cover terminology and concepts that broadly apply to cloud computing.

However, specific sources and providers along with their tools will be referenced, and here are links to Microsoft Azure, Amazon Web Services, and Google's cloud platform. These include documentation, videos, and tutorials for their various services. There are also numerous YouTube videos, guidance from industry vendors, and dedicated courses for these platforms, or even specific services within those platforms.

As stated earlier, we will instead highlight core cloud concepts and how to securely deploy and monitor those basic services.

Learning Objectives

**006 So onto those learning objectives. We will define cloud models and components. We'll have numerous demonstrations on how to

apply security guidance from the Cloud Security Alliance and others. The Shared Responsibility Model is a key concept of cloud security, and this is where we'll take a deeper dive into identifying what controls you and your organization are responsible for versus the cloud service provider. We will also examine how this changes based on each cloud service model.

We will touch upon various provider tools that can help with governance and compliance within the cloud. We will compare cloud and traditional information technologies, such as routers, access control lists, network firewalls, web application firewalls, and more. We will review some common cloud computing threats and discuss specific things you can do to minimize your exposure to those.

And finally, we will introduce a number of tools that can be used to best plan for, deploy, and protect your cloud environment. For example, the Cloud Security Alliance maintains a Cloud Controls Matrix, which at the time of this recording has over 130 best practices listed that include documentation, policy, and service-level agreement recommendations.


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY