Tracston

Cloud Security Essentials

Introduction

Cloud Security is one of the most discussed topics among IT professionals today. And not too long into any conversation about the most highly touted cloud models software as a service (SaaS), infrastructure as a service (IaaS) or platform as a service (PaaS) the talk often turns to cloud security.

The growing adoption of cloud services will increase the demand for security professionals who can apply the proper controls to public, private, community and hybrid cloud models. Also, cloud service providers, organizations adopting cloud services and professional service firms assisting with cloud management and implementation will all need qualified cloud professionals. As organizations replace traditional IT architectures with cloud models, cloud expertise will move from a "nice to have" capability to a "must have."

This Course provides employers with a reliable source of information of overall competency in cloud security; thereby ensuring they put the right people in place who can leverage the 3 benefits of cloud computing and possess the knowledge, skills and abilities needed to address the security and business issues associated with the complexities of cloud computing.

This course also address financial malware operates and how different scenarios are treated and handled by financial institutions using cloud security technology. Financial gain is still one of the major motivations behind most cybercriminal activities and there is little chance of this changing in the near future.

Tracston

Objectives

This course is designed to introduce you to fundamental cloud computing and security concepts including access control and management, governance, logging, and encryption methods. It also covers security-related compliance protocols and risk management strategies, as well as procedures related to auditing your security infrastructure.

In this course we will:

- Learn about cloud computing
- Cloud security best practices
- Cloud security monitoring and protection
- Cloud Users and Keys management
- Effectively working with multiple cloud providers

Duration: 8 hours

Target Audience

- All levels of IT Security and Networking Professionals
- All new students who are looking transition into cloud security
- Anyone who wants to learn vulnerability management, computer networking and cloud security

Prerequisites

- Students should have a basic understanding of network and web based security.
- Basic understanding of security architecture is recommended

Tracston

Contents

- Cloud Security Monitoring, Cloud Protection
- Azure Active Directory – Access and Identity management
    - Security Services
    - Management Azure Role-Based Access Control (RBAC)
    - Microsoft Azure security attributes
- AWS Identity and Access Management (IAM)
    - Security Services
    - Amazon Virtual Private Cloud (VPC)
    - CIA and AAA models, ingress vs. egress filtering, and which AWS services and features fit
    - AWS security attributes (customer workloads down to physical layer)
- Cloud encryption key management best practices
- Cloud SSO Solutions
    - User Management
    - Single Sign-On
    - Password & Encryption keys
    - Remote Access
- Cloud Security and Financial Malware relationship
- Managing incident response
- Summary