Course ID
CLOUD-SEC
Course Duration
3-5 days

Course Title
Cloud Computing Security

Related Courses

- Cloud Computing Business and Technology Briefing™ (CLOUD-BRIEF, 1 day)
- Cloud Computing Market Briefing (CLOUD-MKT, 1 day)
- Cloud Computing Application Case Studies (CLOUD-APP, 1 or more days)
- Cloud Computing Architecture and Implementation (CLOUD-AI, 3-4 days)
- Cloud Computing Standards and Protocols (CLOUD-STND, 3-5 days)
- Cloud Computing End-to-End (CLOUD-E2E, 1 day)
- Principles of Network Security: CompTIA Security+ and US DoD Directive 8570.1 (NETSEC, 3-4 days)
- Security, Privacy and Information Integrity for Managers Executives, and Policy Makers (SECURITY-EXEC, 2-3 days)
- IP Security (IPSec) Architecture and Protocols (IPSEC, 2-3 days)
- IEEE 802.11 (WiFi) Wireless LAN Security (WIFISEC, 3 days)

Aimed At

Persons responsible for the security of cloud computing systems and information, working with cloud consumers, cloud providers, and/or third party consulting and security organizations, will find the greatest value in this course.

Group Size

5-25

Prerequisites

Prior experience in network security and information assurance is a pre-requisite.

Course in a Nutshell

Cloud computing has many dimensions but security considerations overall can be grouped into three meta-categories, which are covered in this course, including security policies, technologies and compliance, and governance. There are also a wide array of security concerns about systems that support cloud computing, such as client, transport, and server issues, that are not specifically addressed here but which are covered in other Eogogics courses as listed in the Related Courses section above.

Customize It!

This briefing can be scheduled as one three to five day standalone course or part of a larger curriculum. Any single module or selected modules may also be scheduled for web delivery.

Learn How To

- Identify the dependencies of cloud-only security mechanisms on non-cloud security mechanisms
- Separate the various functional components of "Cloud Security" and how to assign responsibilities for each to the proper area within an organization
- Perform liaison and coordination of security with carriers, service providers and cloud application providers
- Audit your Cloud Computing Security to assure compliance with the full range of governance and security requirements
- Identify and mitigate the Top Threats to cloud-based application delivery

Course Outline

Security Introduction

A high level overview of the topic and the briefing.

Security and Privacy

- Data Protection
- Identity management
- Physical and Personnel
- Availability
- Application Security
- Privacy

Lower Layer Security

Cloud Security Alliance (CSA)

Security Guidance for Critical Areas of Focus in Cloud Computing

- **Cloud Architecture**
  - Domain 1: Cloud Computing Architectural Framework Governing in the Cloud
  - Domain 2: Governance and Enterprise Risk Management
  - Domain 3: Legal and Electronic Discovery
  - Domain 4: Compliance and Audit
  - Domain 5: Information Lifecycle Management
  - Domain 6: Portability and Interoperability Operating in the Cloud
  - Domain 7: Traditional Security, Business Continuity, and

Disaster Recovery
  - Domain 8: Data Center Operations
  - Domain 9: Incident Response, Notification, and Remediation
  - Domain 10: Application Security
  - Domain 11: Encryption and Key Management
  - Domain 12: Identity and Access Management
  - Domain 13: Virtualization Cloud Controls Matrix
- **Compliance**
  - Data Governance
  - Facility Security
  - Human Resources Security
  - Information Security
  - Legal
  - Operations Management
  - Risk Management
  - Release Management
  - Resiliency
  - Security Architecture
  - Logs and Audit Trails
  - Unique Industry Compliance Requirements
- CloudAudit and Automated Audit, Assertion, Assessment, and Assurance API (A6)

Top Threats to Cloud Computing

- Threat #1: Abuse and Nefarious Use of Cloud Computing
- Threat #2: Insecure Interfaces and APIs
- Threat #3: Malicious Insiders
- Threat #4: Shared Technology Issues
- Threat #5: Data Loss or Leakage
- Threat #6: Account or Service Hijacking
- Threat #7: Unknown Risk Profile

Legal and Contractual Issues

- Public Record
- Disclosure
- FOIA / Open Records Laws

Security Review and Summary

A review of the briefing topics and summary of the program.

How You Will Learn

- A seasoned instructor will present this course in interactive lecture format.
- Along with the lecture, we will use group activities and exercises to enrich the instruction and drive home the major points. The course can be optionally taught as a hands-on workshop at no added cost.
- If you already know something about the technology, we will build on that. We'll compare and contrast what's familiar with what's new, making the new ideas easier to learn as well as more job-relevant.
- If your background is less technical, we will employ meaningful examples and analogies to minimize the subject matter complexity.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *November 2f, 2011*