Advanced Cloud Security Practitioner (ACSP) Course Outline

Below is an outline of the topics covered on each day of training, and what you’ll be building in the labs.

Day 1

We begin on day one with an in-depth discussion of cloud platform technologies; giving you a look into how the services are built and managed, and the security implications. We will then quickly start building out a landing zone in Amazon Web Services and a multi-account sandbox environment and deploying security controls.

Some of the topics and techniques covered will include:

- Use of multi-account architectures for managing blast radius
- Creating a landing zone and building multi-account security architectures in AWS
- Principles for expanding security for multi-cloud deployments
- Building out advanced cloud virtual networks. Including transit networks
- Leveraging inherent cloud capabilities for network security
- Security using Infrastructure as Code with CloudFormation
- Diving deep into security monitoring, logging and alerting
- Use of auto scale groups, load balancers, and other technologies for immutable infrastructure
- Advanced Identity and Access management for cloud, including setting up SAML federation across providers, permission boundaries, multi-account federation, and preventing privilege escalation
- Privileged user management, MFA, and other access essentials
- Securing PaaS and mixed IaaS/PaaS architectures
Day 2

Day two shifts gears to focus on designing secure architectures, integrate with DevOps, and build your own DevSecOps toolkit for managing cloud security at scale:

- Fundamentals of DevSecOps
- Building secure deployment pipelines and fundamentals of Git and Jenkins security
- Leveraging multi path pipelines for secure production deployments
- Integrating automated security testing into deployment pipelines with pre and post build tests in Jenkins
- Basics of secrets management for DevOps
- Cloud security architectural patterns for major application types and serverless security, including AuthN/Z with API gateways
- Cloud data security and encryption
- Security automation through the console
- Use of Open Source security tools
- Fundamentals of security automation through code (predominantly Python/lambda)
- Advanced Cloud Security Practitioner
- AuthN/Z for security automation and credential management and role chaining
- Scaling your security operations to hundreds (or thousands) of accounts through automation
- Workload security, including principles for container and serverless functions.

Labs

All labs in this course reflect how processes actually happen. These are not merely academic exercises.

**Day 1:** We will configure a production-quality account with multiple virtual networks and core security controls.

**Day 2:** We will build a deployment pipeline, integrate it into our existing application stack, and implement a variety of security automation controls.

All labs will be in Amazon Web Services, with some demonstrations and integrations with Microsoft Azure. All labs can be completed outside of class for students unable to keep up with the rapid pace of the training.

Programming labs will utilize Python. Text snippets will be provided so students don’t need to code from scratch, but students without Python skills may be limited to using only the provided snippets.