**Cloud Security for Application**

**Duration: 5 days**

**Day 1: Introduction to Cloud Security**

*Cloud Platform Overview*

* Understanding the chosen cloud platform (e.g., AWS) and its key components.
* Common security concerns across different cloud platforms.
* Introduction to shared responsibility model in cloud security.

*Overview of Security Domains*

* Container Security: Understanding the importance of securing containers, runtime security, and container image security.
* Data Security: Encryption protocols, data protection strategies, and securing sensitive information in the cloud.
* PKI on Cloud: Introduction to Public Key Infrastructure and its role in cloud security.

*Labs: Setting up an AWS environment, configuring IAM, and understanding basic container security.*

**Day 2: Identity and Access Management (IAM) in the Cloud**

*IAM Fundamentals*

* IAM concepts and best practices.
* Implementing least privilege principles.
* Secure session management and robust user authentication.

*Advanced IAM and API Security*

* Using OAuth or OpenID Connect for third-party authentication.
* API Security: API Gateways, validating input/output API calls.
* Overview of common API security threats (OWASP Top 10).

*Labs: Configuring IAM roles, setting up API Gateway with security features.*

**Day 3: Data Security and DevSecOps Integration**

*Data Security in the Cloud*

* Encryption and data protection strategies.
* Best practices for secure data storage and transmission.
* PII Analyzers and handling sensitive information.

*DevSecOps Integration*

* Integrating security checks in the CI/CD pipeline.
* Automating security testing, static and dynamic analysis.
* Dependency scanning: Identifying and updating third-party dependencies.

*Labs: Implementing data encryption, integrating security checks in CI/CD pipeline.*

**Day 4: Application Security and Error Handling**

*Secure Coding Practices*

* Mitigating common vulnerabilities (SQL injection, XSS, security misconfigurations).
* Implementing secure coding practices in cloud applications.

*Error Handling and Session Management*

* Secure error handling to avoid exposing sensitive information.
* Session management best practices: rotating session tokens, timeouts, secure storage.

*Labs: Implementing secure coding practices, configuring secure error handling.*

**Day 5: Container and Network Security**

*Container and Orchestration Security*

* Runtime security for containers.
* Security of container images and scanning for vulnerabilities.
* Best practices for container orchestration (e.g., Kubernetes).

*Network Security and Wrap-up*

* Overview of cloud network security.
* CVE, SPBD, and the importance of staying updated.
* Cloud security tools and scanners.

*Labs: Implementing container security measures, configuring network security settings.*

***Note****: Each day's lab sessions should include practical exercises and real-world scenarios to reinforce theoretical concepts. The training should be interactive, allowing participants to apply learned skills in a hands-on environment.*