**Day 5 - Integration & Application (16.6)**

**1. Mini Project: Design & Deploy a Secure AWS Environment (AWS Focus)**

**Topics**

Integration of IAM, VPC, Subnets, Logging & Monitoring

Project-based learning: End-to-end secure architecture deployment

Automation basics with AWS CLI and CloudFormation (optional)

Secure development lifecycle & DevSecOps considerations

**Required Infrastructure & Components**

One AWS account per participant/team

Custom VPC with:

Public and private subnets

Route tables, IGW & NAT Gateway

IAM setup (users, roles, policies with MFA)

Logging services (CloudTrail, Config, CloudWatch)

GuardDuty and Security Hub enabled

EC2 instances (web + database tier)

**To-Dos & Steps**

Plan & diagram the target architecture

Create VPC with subnets and proper routing

Configure IAM roles and enforce MFA

Deploy EC2 instances into subnets (web tier → public, DB tier → private)

Apply Security Groups & NACLs based on best practices

Enable all monitoring and compliance tools:

CloudTrail, Config rules, GuardDuty, Security Hub

Demonstrate encrypted data storage with KMS

Perform basic penetration test (e.g., Nmap from bastion host)

Document and present architecture + controls implemented

**Webinars**:

[AWS – Security by Design: Building Secure Architectures](https://docs.aws.amazon.com/prescriptive-guidance/latest/security-reference-architecture/welcome.html)

AWS Webinar: Infrastructure as Code with AWS CloudFormation - <https://awsforengineers.com/blog/aws-engineering-blog-mastering-infrastructure-as-code/>

[AWS – DevSecOps Best Practices](https://codefresh.io/learn/devsecops/devsecops-on-aws/)

**YouTube**:

[How to Design a Secure AWS Architecture](https://www.youtube.com/watch?v=repMqla4OfU) – 00:04

[AWS CLI Tutorial](https://www.youtube.com/watch?v=21-t7Rkokmo) -00:11

[AWS CloudFormation Full Course](https://www.youtube.com/watch?v=0Sh9OySCyb4&t=301s) – 00:16

[What is DevSecOps? (AWS Security)](https://www.youtube.com/watch?v=045UQXAPUbQ) – 00:47

**Reading Material**:

[AWS Well-Architected Framework – Security Pillar](https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html)

[AWS CloudFormation User Guide](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html)

Introduction to DevSecOps on AWS - <https://aws.amazon.com/what-is/devsecops/>

[AWS KMS Developer Guide (Encryption)](https://docs.aws.amazon.com/kms/latest/developerguide/overview.html)

[AWS CLI Command Reference](https://docs.aws.amazon.com/cli/latest/index.html)

[Security Best Practices for AWS EC2 Instances](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-best-practices.html)

**2. Audit Scenario: Compliance Simulation (Compliance Focus)**

**Topics**

Cross-mapping of deployed infrastructure to compliance frameworks (GDPR, SOC 2, ISO 27001)

Gap analysis and control validation

Incident response simulation (e.g., access anomaly, GuardDuty finding)

Writing compliance evidence and audit documentation

**Required Infrastructure & Components**

AWS Config with compliance conformance packs

Audit logging and log storage (CloudTrail, S3)

IAM & KMS policy documentation

GuardDuty alerts for incident simulation

Predefined audit checklist templates

**To-Dos & Steps**

Map deployed architecture to selected compliance frameworks

Use AWS Security Hub and Config to identify non-compliant resources

Run audit scenario: Simulate access misuse or misconfiguration

Analyze logs and document root cause

Complete audit checklist and generate evidence package

Discuss mitigation and long-term recommendations

**Webinars**:

AWS Compliance and Governance on AWS Webinar - <https://www.youtube.com/watch?v=41_RycHftdw> – 00:50

[AWS re:Inforce – Compliance Automation with AWS Config and Security Hub](https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-setup-prereqs.html)

**YouTube**:

[Compliance Frameworks Explained: GDPR, ISO 27001, SOC 2](https://www.youtube.com/watch?v=Pqdr6WTgZx8) – 01:01

[AWS Config Rules and Conformance Packs Tutorial](https://www.youtube.com/watch?v=tT8LXTztKjE) – 00:05

[AWS Security Hub Tutorial](https://www.youtube.com/watch?v=f17l2v5v9g4) – 00:08

[AWS GuardDuty Hands-on Simulation](https://www.youtube.com/watch?v=WXl4gW0znVc) – 00:25

**Reading Material**:

[AWS Compliance Center Overview](https://aws.amazon.com/compliance/)

[AWS Config Conformance Packs Documentation](https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html)

[AWS Artifact: Access Compliance Reports](https://docs.aws.amazon.com/artifact/latest/ug/what-is-aws-artifact.html)

AWS Security Incident Response Guide - <https://elhacker.info/manuales/Cybersecurity%20Books/AWS%20Security%20Incident%20Response%20Guide.pdf> – S. 1-37

[AWS Well-Architected Framework: Operational Excellence Pillar](https://docs.aws.amazon.com/wellarchitected/latest/operational-excellence-pillar/welcome.html)

AWS Security Best Practices - <https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf> - S. 1-20

**🎯End-of-Day Goal / Outcomes**

Participants should be able to:

Integrate all learned AWS security components into a working secure environment

Perform an end-to-end compliance mapping and simulate an audit scenario

Analyze monitoring data, interpret findings, and take action

Produce documentation suitable for audit readiness

Present their solution with justification of design decisions and security controls