**Day 4 - Monitoring & Auditing (13.6.)**

**1. Logging & Monitoring (AWS Focus)**

**Topics**

Cloud-native monitoring stack:

**CloudTrail**: Event logging for AWS account activity

**AWS Config**: Resource configuration tracking and compliance auditing

**Amazon CloudWatch**: Logs, metrics, alarms, dashboards

**GuardDuty**: Threat detection & intelligent alerting

Integration with AWS Security Hub and Trusted Advisor

Best practices: centralized logging, alerting thresholds, retention policies

**Required Infrastructure & Components**

CloudTrail trails enabled across all regions

Config rules for compliance checks (custom + managed)

CloudWatch Log Groups and Metrics

Alarms and dashboards in CloudWatch

GuardDuty enabled and integrated with findings

Optional: S3 bucket for central log storage with lifecycle policies

**To-Dos & Steps**

Enable CloudTrail with multi-region and log file validation

Configure AWS Config with rules (e.g., "S3 bucket should not be public")

Set up CloudWatch metric filters (e.g., failed login attempts)

Create alarms and dashboards for key metrics (e.g., root user usage)

Enable GuardDuty and review generated findings

Forward all logs to a central S3 bucket and enable encryption with KMS

**Webinars**:

[AWS – Building Effective Logging and Monitoring Strategies](https://docs.aws.amazon.com/prescriptive-guidance/latest/implementing-logging-monitoring-cloudwatch/welcome.html)

AWS Webinar: Introduction to CloudTrail, GuardDuty, and Security Hub - [https://pages.awscloud.com/Introduction-to-CloudTrail-GuardDuty-SecurityHub.html](https://www.youtube.com/watch?v=Rg2ZzAAi1nY) - 00:21

**YouTube**:

[AWS CloudTrail Deep Dive](https://www.youtube.com/watch?v=-a3EX758Mq8) – 00:26

[AWS Config Tutorial](https://www.youtube.com/watch?v=qHdFoYSrUvk) – 00:09

[Amazon CloudWatch Logs and Metrics Overview](https://www.youtube.com/watch?v=Yxl7e88cTAQ) – 00:11

[AWS GuardDuty Hands-on Tutorial](https://www.youtube.com/watch?v=eq3_H-aiHhk) – 00:16

[AWS Security Hub Overview](https://www.youtube.com/watch?v=oBac-GAoZJ8) – 00:10

**Reading Material**:

[AWS CloudTrail User Guide](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

[AWS Config Developer Guide](https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html)

[Amazon CloudWatch User Guide](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/WhatIsCloudWatch.html)

[Amazon GuardDuty Documentation](https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html)

[AWS Security Hub Documentation](https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html)

[Best Practices for Securing Your AWS Log Data](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html)

[AWS Trusted Advisor Best Practices](https://docs.aws.amazon.com/awssupport/latest/user/what-is-trusted-advisor.html)

**2. ISO 27001 Deep Dive (Compliance Focus)**

**Topics**

Information Security Management Systems (ISMS) overview

ISO 27001 control domains and objectives

Deep dive: **Annex A Controls** related to:

Logging & monitoring (A.12.4)

Information security incident management (A.16)

Access control (A.9)

Evidence collection and audit readiness

Mapping AWS services to ISO 27001 requirements

**Required Infrastructure & Components**

AWS Config with conformance packs (ISO 27001)

GuardDuty, CloudTrail, Config, and CloudWatch dashboards

Centralized log storage (S3) and access review mechanisms

IAM controls to enforce log access separation of duties

**To-Dos & Steps**

Review ISO 27001 Annex A logging and incident response controls

Configure AWS services to align with specific controls (e.g., log retention, access review)

Implement encryption and access audit on log data in S3

Enable AWS Security Hub to aggregate findings and compliance status

Demonstrate an incident detection-to-response flow (e.g., GuardDuty finding triggers alert)

Download ISO 27001 documentation and reports via AWS Artifact

**Webinars**:

AWS ISO 27001 Compliance Webinar - <https://pages.awscloud.com/ISO-27001-Compliance-Webinar.html>

Achieving ISO 27001 certification with AWS - <https://www.youtube.com/watch?v=cFhddOcIGNU> – 00:49

**YouTube**:

[What is ISO 27001? Compliance Explained](https://advisera.com/27001academy/what-is-iso-27001/)

[AWS Artifact and ISO Certifications Walkthrough](https://www.datacamp.com/tutorial/aws-artifact)

**Reading Material**:

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

[ISO 27001 on AWS Overview](https://aws.amazon.com/compliance/iso-27001-faqs/)

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

ISO 27001 Standard (Annex A Controls Overview) - <https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained>

AWS Whitepaper: Navigating Compliance for ISO 27001 - <https://medium.com/@AlexanderObregon/aws-compliance-and-governance-for-beginners-985bd92f52b9>

**🎯End-of-Day Goal / Outcomes**

Participants should be able to:

Configure and manage cloud-native logging and monitoring using CloudTrail, Config, CloudWatch, and GuardDuty

Design monitoring architectures aligned with security and compliance requirements

Understand ISO 27001 requirements for monitoring, logging, and incident management

Map AWS service configurations to specific ISO 27001 Annex A controls

Build an auditable and alert-driven security monitoring pipeline