**Session 1: Monitoring Resources & Custom Metrics**

**1. Design a monitoring strategy using CloudWatch Alarms for EC2 fleet**

For a critical banking application:

* **High CPU Utilization:** Create a CloudWatch alarm on CPUUtilization metric with a threshold (e.g., >80% for 5 minutes).
* **Unusual Network Traffic:** Monitor NetworkIn and NetworkOut metrics for spikes beyond normal patterns.
* **Low Disk Space:** Use custom metric for disk usage via CloudWatch Agent. **Automation:** Integrate alarms with **SNS** to send notifications and trigger **Lambda** functions for remediation (e.g., scale out EC2, clean temp files, or block suspicious IPs).

**2. Compare default AWS metrics vs custom CloudWatch metrics**

* **Default Metrics:** Provided by AWS services automatically (e.g., EC2 CPU, S3 bucket size).
* **Custom Metrics:** User-defined metrics for application-level data (e.g., transaction latency, queue depth). **Example:** A banking app needs to monitor failed payment transactions—this requires custom metrics since AWS does not provide app-specific KPIs.

**Session 2: Monitoring Integration with Key Services**

**3. End-to-end monitoring plan for serverless app (Lambda, API Gateway, DynamoDB)**

* **Lambda:** Monitor Duration, Errors, and Throttles.
* **API Gateway:** Track 4XX and 5XX error rates.
* **DynamoDB:** Monitor ConsumedReadCapacityUnits and ThrottledRequests. Integrate all metrics into **CloudWatch Dashboards** and set anomaly detection alarms for unusual patterns. Use **CloudWatch Logs Insights** for query-based troubleshooting.

**4. How CloudWatch integrates with AWS X-Ray and CloudTrail**

* **CloudWatch:** Provides metrics and logs.
* **X-Ray:** Traces requests across microservices for performance bottlenecks.
* **CloudTrail:** Logs API calls for auditing. **Scenario:** A payment API shows high latency. CloudWatch detects anomalies, X-Ray pinpoints slow Lambda execution, and CloudTrail verifies no unauthorized changes. Together, they improve troubleshooting and compliance.

**Compliance & Standards**

**5. Choose two compliance standards and explain AWS support**

* **PCI DSS:** AWS offers PCI-compliant services, encryption (KMS), and logging (CloudTrail).
* **HIPAA:** Provides HIPAA-eligible services, BAA agreements, and secure storage (S3 with SSE-KMS). AWS ensures infrastructure compliance, while customers configure workloads securely.

**6. PCI DSS audit checklist using AWS services**

* **CloudTrail:** Enable logging for all API calls.
* **AWS Config:** Track resource compliance.
* **Security Hub:** Centralize security findings.
* **KMS:** Encrypt sensitive data.
* **IAM Policies + MFA:** Enforce least privilege. This checklist ensures visibility, encryption, and governance for PCI DSS readiness.