**Phase 2: Technical Implementation**

**Project: AWS Cloud Security Automation  
Prepared by: Vinay Kumar  
Date: October 2025  
Version: 1.0**

**1. Objective**

**Implement the automated AWS cloud security monitoring system designed in Phase 1. The system will:**

* **Aggregate security findings from AWS Config, GuardDuty, and Inspector.**
* **Trigger automated analysis and remediation using Python scripts via Lambda.**
* **Provide centralized visibility and notifications for security events.**

**2. Scope**

**In Scope:**

* **AWS-native services setup: Config, GuardDuty, Inspector, Security Hub, EventBridge, Lambda, SNS, S3.**
* **Python automation for alerting, remediation, and reporting.**
* **Optional dashboard visualization using Streamlit.**

**Out of Scope:**

* **Non-AWS third-party integrations.**
* **Production-scale data or multi-cloud setups.**

**3. AWS Services and Tools**

| **Category** | **Service / Tool** | **Purpose** |
| --- | --- | --- |
| **Configuration Management** | **AWS Config** | **Detect configuration changes and evaluate compliance** |
| **Threat Detection** | **Amazon GuardDuty** | **Identify malicious or suspicious activity** |
| **Posture Management** | **AWS Security Hub** | **Aggregate and normalize findings** |
| **Vulnerability Scanning** | **Amazon Inspector** | **Scan workloads for vulnerabilities** |
| **Automation** | **AWS Lambda** | **Execute Python scripts for analysis and remediation** |
| **Event Trigger** | **Amazon EventBridge** | **Trigger Lambda on Security Hub findings** |
| **Storage** | **Amazon S3** | **Store raw findings and processed reports** |
| **Notifications** | **SNS / Email / Slack** | **Alert security teams** |
| **Visualization** | **Python + Streamlit (optional)** | **Display findings and metrics on a**  **Dashboard** |
| **Monitoring & Logging** | **AWS CloudWatch** | **Capture Lambda logs, metrics, alarms, and support dashboards** |

**4. Technical Workflow**

1. **AWS resources generate configuration, activity, and event data.**
2. **CloudTrail logs feed into GuardDuty for threat detection.**
3. **AWS Config evaluates resource configurations against compliance rules.**
4. **Amazon Inspector performs vulnerability scanning of workloads.**
5. **Security Hub aggregates all findings from Config, GuardDuty, and Inspector.**
6. **EventBridge monitors Security Hub and triggers Lambda on new findings.**
7. **Lambda (Python) automates:**
   * **Analysis of findings**
   * **Remediation (optional)**
   * **Notifications via SNS/Email/Slack**
   * **Storing reports in S3**
   * **Logging execution, metrics, and errors to CloudWatch**
8. **Optional visualization of findings using Streamlit dashboard.**

**5. Data Flow Diagram**

