**Cloud Security Automation**

Objective:

To automate and optimize cloud security operations by building fine-tuned detections, reducing false positives, and enabling automated alert enrichment and remediation.

Phase 1 (Week 1): Discovery and Environment Understanding

Goal: Understand the current AWS/GCP environment and Wiz setup.

Deliverables:

* Inventory of all AWS/GCP accounts.
* Wiz integration verification and alert mapping.
* Documentation of existing alert flow (where alerts go and who handles them).

Phase 2 (Week 2): Alert Analysis and Fine-Tuning

Goal: Reduce false positives and prioritize relevant alerts.

Deliverables:

* Export and categorize Wiz alerts (High/Medium/Low).
* Identify top recurring alerts.
* Fine-tuning plan for non-relevant or noisy alerts.
* Updated alert policy baseline.

Phase 3 (Week 3): Automation Planning

Goal: Design automation workflows and integration points.

Deliverables:

* Select top 2–3 use cases (e.g., Public S3 bucket, old IAM key, MFA missing).
* Workflow diagram (Wiz → Python → AWS → Slack/Jira/ServiceNow).
* Automation design document (inputs, triggers, expected actions).

Phase 4 (Week 4): Initial Automation Build and Testing

Goal: Build and test the first automation workflows.

Deliverables:

* Python-based alert handling and remediation script.
* Test report from staging account.
* Notification integration (Slack/Jira/ServiceNow).
* Demo of end-to-end automation flow.

“In the first week, I’ll focus on understanding your AWS/GCP environment and Wiz integration.

In the second week, I’ll analyze and fine-tune alerts to reduce false positives.

In the third week, I’ll design automation workflows and integrations.

And by the fourth week, I’ll deliver and demo the first automation use case in your environment.”