Executive Summary — WCDN Vibranium Cloud Defense Range

This project established a cloud-based cyber training range within AWS designed to simulate realistic attack-and-defense scenarios while strengthening both offensive and defensive cloud security capabilities.

The environment was deployed inside a custom AWS Virtual Private Cloud (VPC) spanning two Availability Zones, segmented into public and private subnets to enforce secure network boundaries and proper traffic flow control. This architecture allowed safe isolation of attack instances, victim instances, and monitoring tools.

The Red Team launched attacks from a designated attacker EC2 instance, performing network reconnaissance with Nmap, privilege escalation using metadata service abuse, and data exfiltration to S3 buckets.

The Blue Team monitored these events using AWS native security services: GuardDuty for threat detection, CloudTrail for API-level audit logs, VPC Flow Logs for network-level traffic analysis, and CloudWatch for detection correlation and alerts.

To enforce governance and compliance, the environment integrated AWS Config to detect and remediate insecure configurations, AWS Systems Manager for automation and patching, and CloudFormation to generate a reusable infrastructure blueprint.

VPC Flow Logs were configured to capture traffic metadata for forensic review, and logs were streamed to CloudWatch using a custom IAM role and log group. CloudTrail was configured to track API activity across the account, providing visibility into user actions and administrative changes.

During the build, the team faced challenges with VPC routing, NAT Gateway configuration, Internet Gateway attachment, and public/private subnet misconfigurations. These issues reinforced the importance of CIDR planning, subnet isolation, correct route table mapping, and methodical validation at each step.

Ultimately, the Vibranium Cloud Defense Range provided a comprehensive, hands-on environment combining offensive penetration testing, defensive monitoring, and compliance alignment. It demonstrated practical experience in secure cloud architecture, incident detection, remediation workflows, and governance-driven security design.