Syntho Quest

CLOUD VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prepared By (CTO) SYNTHOQUEST

45 Days Duration

Duration: 45 days × 2 hrs/day = 90 hrs

Goal: Teach safe, authorized cloud security testing across IaaS/PaaS/SaaS + containers & serverless: discovery → misconfiguration hunting → privilege escalation → lateral movement (identity/data plane) → reporting & remediation.

Core cloud risk areas (compact)

- IAM misconfigurations & privilege escalation (over-privileged roles, role chaining)
- Public storage/exposed buckets & object permissions (S3/GCS/Azure Blob)
- Insecure or leaked secrets (secrets in code, env, metadata)
- Misconfigured networking (public subnets, exposed management endpoints)
- Excessive service permissions / lateral movement via APIs
- Insecure CI/CD & IaC (Terraform/CloudFormation mistakes, secrets in pipelines)
- Serverless risks (insecure functions, excessive permissions)
- Container & Kubernetes weaknesses (privileged pods, RBAC misconfig)
- Insufficient logging/monitoring & detection gaps (no alerts, missing trails)
- Supply chain & third-party integrations (managed services, APIs)

Business Associate: vivek
Email: contact@synthoquest.com
Mobile: +91-8333801638 (whats app)