Certified DevSecOps Engineer (ECDE) – Course Outline

🔰 Module 01: Introduction to DevSecOps

• Evolution: Waterfall → Agile → DevOps → DevSecOps
• Key principles: “Shift Left” Security, CI/CD/CS (Continuous Security)
• DevSecOps culture, mindset, and organizational roles
• Mapping DevSecOps into SDLC

⚙️ Module 02: DevSecOps Toolchain & Pipeline Automation

• Building secure CI/CD pipelines
• DevSecOps tooling categories:
    - Code: GitHub, GitLab
    - Build: Jenkins, GitHub Actions, GitLab CI, CodeBuild
    - Artifact: Nexus, Artifactory
    - Deploy: ArgoCD, Helm, Terraform
• Toolchain integration strategies

📦 Module 03: Secure Software Development Lifecycle (SSDLC)

• Security integration into each SDLC phase
• Threat modeling frameworks: STRIDE, DREAD, PASTA
• Secure coding principles
• Vulnerability management lifecycle
• OWASP Top 10 & SANS Top 25 risks mapping

🧪 Module 04: Application Security Testing

• SAST (Static Analysis): SonarQube, Semgrep, SonarLint
• DAST (Dynamic Analysis): OWASP ZAP, Nikto, Burp Suite
• SCA (Software Composition Analysis): OWASP Dependency Check, Snyk, Trivy

• Secrets scanning: Gitleaks, GitGraber
• CI/CD integration of AppSec tools

☸️ Module 05: Container Security

• Docker image security best practices
• Scanning tools: Trivy, Clair, Grype
• Image hardening and minimal base images (e.g., Alpine, Distroless)
• Secrets management and image signing

🚢 Module 06: Implementing Security Policies

• What is Admission Controller?
• Why Admission Controller in DevSecOps?
• Admission Controller Workflows
• Types of admission controllers:
    - Built-in Admission Controllers
    - Custom/Dynamic Admission Controllers (Webhook)
• Enforce security policies with Kyverno (Hands-on demo)

🏗️ Module 07: Infrastructure as Code (IaC) Security

• IaC tools: Terraform, AWS CloudFormation
• Risks: hardcoded secrets, misconfiguration, privilege escalation
• Scanners: Checkov, TFSec, KICS, Terrascan
• CI/CD IaC security integration