



# ASCEND

## The Complete Tech Career Transformation Program 2026

From Any Background · Any Experience · .NET Full Stack + Cloud + AI + Cyber Security — 4 Months

■ Fresh Graduate	■ Working Professional	■ Non-IT → IT Switcher	■ Software Engineer Seeking Growth
------------------	------------------------	------------------------	------------------------------------

.NET+ Full Stack	AWS Cloud	DevOps +K8s	AI/ML +GenAI	Data Science	Agentic AI+LLMs	Cyber Security	Cloud Security
------------------	-----------	-------------	--------------	--------------	-----------------	----------------	----------------

5500+ Placements	16 Weeks	12 Projects	500+ Hours	9 Tracks	■22 LPA Highest Pkg
------------------	----------	-------------	------------	----------	---------------------

ALL 9 TRACKS START FROM DAY 1 — PARALLEL LEARNING MODEL

Expected Salary: ■4 LPA – ■22 LPA | \$65K – \$150K (Global)

■ 9666019191 | ■ www.cloudsoftsol.com | ■ Hyderabad | ■ 2026 Batch  
Cloud Soft Solutions — Hyderabad's #1 Tech Training Institute | 5500+ Successful Placements

# WHO IS ASCEND FOR?

■ <b>Fresh Graduates</b>	B.Tech/BCA/MCA/BSc or any stream. Zero experience needed. Build 12 projects, get placed.	No prior tech needed · Java from zero · Full placement support till offer
	Engineers, analysts, managers wanting to upskill or move to higher-paying tech/security roles. Weekend batches.	Fast-track for partial knowledge · Add AI/Cloud/DevOps/Security · Target ■5–10 LPA salary hike
■ <b>Non-IT Career Switchers</b>	Finance, HR, Marketing, Healthcare, Teaching entering tech. 1200+ of our 5500+ alumni are career switchers.	No engineering background required · IT fundamentals in Week 1–2 · Real-world industry curriculum
■ <b>Software Engineers</b>	Developers stuck in same role 2+ years wanting AI/ML, Cloud Arch, Security specialization or senior positions.	Skip basics — fast-track advanced · Add AI, LLMs, Security, Cloud Arch · Target lead/architect roles

■ 5500+ Placements — across India's top product companies, unicorns, MNCs & global remote firms. Founded by veterans from Google, Amazon & TCS.

■ 200+ Hiring Partners — direct referrals to companies in Hyderabad, Bangalore, Pune, Chennai & international. Curriculum built from 50,000+ JD analysis.

■ Flexible Batches — Weekday morning, evening & weekend options. Dedicated career team schedules interviews and provides placement support till offer.

## 9-TRACK PARALLEL MODEL — ALL TRACKS FROM DAY 1

All 9 domains run simultaneously from Week 1 — mirroring how senior engineers work at top companies: writing Java AND deploying to AWS AND securing systems AND using AI every single week. Depth increases each month as foundations compound.

TRACK	MONTH 1 Wks 1–4	MONTH 2 Wks 5–8	MONTH 3 Wks 9–12	MONTH 4 Wks 13–16
■ <b>C# .NET</b>	Core+OOP+LINQ+async	ASP.NET Core+EF Core	Microservices+Azure	Semantic Kernel+LLM
■ <b>Full Stack</b>	HTML/CSS+JS+ASP.NET MVC	React+ASP.NET REST	Ocelot+Polly+Next.js	Secure SaaS+AI UI
■ <b>Azure+AWS</b>	Entra ID+VM+Blob Wk1	Functions+ACI+AKS	Azure ML+Data Factory	Azure OpenAI+Multi-cloud
■ <b>DevOps</b>	Git+Docker+Linux	K8s+CI/CD+EKS	Terraform+ArgoCD	Full GitOps+LLMOps
■ <b>AI/ML</b>	scikit-learn+GPT-4o Wk1	XGBoost+MLflow+NLP	PyTorch+CV+Transformers	Fine-tuning+VLLM
■ <b>Data Sci</b>	Pandas+EDA+Plotly	Stats+Time Series	PySpark+Airflow+dbt	BigQuery ML
■ <b>Agentic AI</b>	Prompts+LangChain	RAG+Vector DBs	LangGraph+CrewAI	Multi-Agent+MCP
■ <b>Cyber Sec</b>	Linux Sec+OWASP	VAPT+Pentest Labs	SOC+SIEM+MITRE	Full Pentest+Report
■ <b>Cloud Sec</b>	IAM Sec+WAF+GD	DevSecOps+Vault	Zero Trust+CSPM	SOC2+ISO27001+Audit

### Daily Schedule — 10 Hours/Day

■ <b>6–7 AM</b>	DSA — 1 LeetCode problem daily · Easy→Medium progression over 16 weeks
■ <b>9 AM–12 PM</b>	PRIMARY track — Java/Spring Boot focused deep-dive (rotating each week)
■ <b>1–3 PM</b>	PARALLEL: AWS + AI/ML — both run every afternoon from Week 1
■ <b>3–5 PM</b>	Project building — integrate morning+afternoon learnings into deployable code
■ <b>6–7 PM</b>	Data Science + Cyber Security + Agentic AI — daily 1-hour exercises
■ <b>8–9 PM</b>	GitHub commit · LinkedIn post · Notes · Next-day prep

■ C# .NET

- OOP: Classes, Interfaces, Abstract, Sealed, Records
- Collections: List, Dictionary, IEnumerable, LINQ queries
- C# 12: async/await, Nullable refs, Pattern matching, Tuples
- Exception handling, File I/O, System.Text.Json, Generics

■ Full Stack

- HTML5/CSS3/Tailwind + JavaScript ES6+
- ASP.NET Core: Controllers, Minimal APIs, Middleware
- Entity Framework Core: DbContext, Migrations, LINQ
- Deploy ASP.NET Core on Azure App Service + Nginx

■ Azure+AWS

- Entra ID: users, roles, app registrations, MFA
- Azure VM + SSH + NSG + public IP
- Blob Storage + versioning + static website
- Azure SQL Database + Monitor + DNS Zones

■ DevOps

- Linux bash, filesystem, permissions
- Git branching, PRs, Git Flow
- Docker Dockerfile + Compose
- GitHub Actions first CI workflow

■ AI/ML

- scikit-learn: LR, RF, Decision Trees
- Cross-validation, evaluation metrics
- OpenAI GPT-4o API from Week 1
- Prompt engineering: CoT, ReAct, JSON

■ Data Sci

- NumPy, Pandas DataFrames, GroupBy
- Matplotlib, Seaborn, Plotly charts
- EDA on Kaggle + Streamlit app
- ydata-profiling automated EDA

■ Agentic

- LLM tokens, temperature, context
- LangChain LLMChain, PromptTemplate
- First RAG prototype with Chroma
- LangSmith tracing + Q&A; chatbot

■ Cyber

- CIA triad, OWASP Top 10 walkthrough
- Burp Suite install + first intercept
- Nmap network scanning + Wireshark
- Secure coding practices Python+Django

■ Cloud Sec

- Entra ID least privilege + RBAC audit
- NSG vs Azure Firewall lab
- Azure WAF rules + Activity Log setup
- Microsoft Defender for Cloud + Azure Policy

Week-by-Week Plan — Month 1

Week 1	C# Core (OOP, Collections, LINQ, Generics) · AZURE: Entra ID+VM+Blob Storage labs · AI: scikit-learn+GPT-4o first API calls+prompts · DATA: Pandas EDA · CYBER: OWASP Top10+Burp Suite · CLOUD SEC: Entra ID audit+Microsoft Defender enable · DevOps: Git+GitHub · DSA: 8 Easy
Week 2	C# Advanced (ASP.NET Core basics, NuGet, xUnit+Moq, FluentAssertions) · FULL STACK: HTML/CSS/Tailwind+JS · AZURE: Blob+Monitor+Azure SQL · AI: Random Forest+metrics · DATA: Plotly chart · CYBER: Nmap scanning · CLOUD SEC: WAF+Activity Log · AGENTIC: LangChain · DSA: 6 Easy
Week 3	ASP.NET Core: Web API controllers, EF Core entities, repositories, ASP.NET Core Identity · AWS: VPC+security groups · DevOps: Docker+Compose · AI: Decision Tree+SHAP · DATA: Streamlit on EC2 · CYBER: DVWA web app labs · CLOUD SEC: Config rules · AGENTIC: First RAG+Chroma · DSA: 6 Easy
Week 4	PROJECT SPRINT: Build Projects 1 & 2 · AWS EC2+RDS+S3+WAF deploy · GitHub Actions CI · CYBER: OWASP audit on own project · AI: ML recommendations+GPT-4o chatbot · Total LeetCode: 26 Easy

MONTH 1 — PROJECTS

PRJ 01	Secure E-Commerce + AI Recommendations	■ ASP.NET Core,React,SQL Server,EF Core,ML.NET,Azure OpenAI,Azure App Service+Azure SQL+Blob+WAF+Defender,Docker,GitHub Actions
Desc	Full-stack e-commerce: ASP.NET Core 8 Web API + React frontend, SQL Server on Azure SQL via EF Core, ML.NET collaborative filtering recommendation engine, Azure OpenAI GPT-4o shopping assistant, ASP.NET Core Identity+JWT auth, OWASP .NET hardening, Azure WAF+Microsoft Defender for Cloud, GitHub Actions CI.	
Deliverables	✓ ASP.NET Core 8 REST API ✓ EF Core+SQL Server ✓ React frontend ✓ Azure App Service+Azure SQL+Blob+WAF ✓ ML.NET recommendations ✓ Azure OpenAI chatbot ✓ OWASP checklist ✓ Defender for Cloud ✓ CI pipeline	
Roles	.NET Full Stack Dev   ASP.NET Core Developer   Cloud Engineer   AI-enabled Developer	
PRJ 02	Hospital Management System + Security Audit	■ ASP.NET Core,React,SQL Server,EF Core,RDLC/FastReport,Plotly,Streamlit,Azure OpenAI,Azure,Twilio,Burp Suite
Desc	Complete HMS: ASP.NET Core multi-role auth (Identity+JWT), appointment booking, RDLC PDF reports, Twilio SMS alerts, Azure OpenAI GPT-4o symptom checker, Plotly/Streamlit analytics, SignalR real-time notifications. PLUS full OWASP .NET security audit and Burp Suite pentest findings.	
Deliverables	✓ ASP.NET Core Identity+JWT ✓ RDLC PDF reports ✓ SignalR real-time ✓ Twilio SMS ✓ Azure OpenAI chatbot ✓ Plotly dashboard ✓ VAPT report ✓ Burp Suite findings ✓ Azure deploy	
Roles	.NET Full Stack Dev   Healthcare Tech   ASP.NET Core Developer   AI-enabled Developer	

**■ C# .NET**

- ASP.NET Core Identity: JWT, OAuth2, OpenID Connect
- NuGet package management + dotnet CLI mastery
- Design Patterns: Repository, CQRS, Mediator (MediatR)
- AutoMapper, FluentValidation, Options pattern, DI

**■ Full Stack**

- ASP.NET Core Web API: Controllers, DTOs, ActionResult
- Hangfire + IHostedService background jobs
- React Redux Toolkit + React Query + Axios
- SignalR: real-time WebSockets in ASP.NET Core

**■ Azure+AWS**

- Azure VMSS + Application Gateway load balancing
- Azure Functions triggers, Durable Functions
- ACI + ACR container registry
- Azure Service Bus + Azure Cache for Redis

**■ DevOps**

- K8s: pods, deployments, ingress, HPA
- Helm charts + EKS cluster setup
- GitHub Actions full CI pipeline
- SonarQube + Trivy security gates

**■ AI/ML**

- XGBoost, LightGBM, CatBoost+Optuna
- SMOTE imbalanced datasets
- MLflow experiment tracking+registry
- FastAPI model serving endpoint

**■ Data Sci**

- Statistics: A/B tests, hypothesis testing
- Time series: ARIMA + Prophet
- dbt SQL transformations + BigQuery
- Power BI / Tableau dashboards

**■ Agentic**

- LangChain LCEL + Memory types
- Vector DBs: Pinecone, Qdrant, pgvector
- Hybrid search BM25+dense+RRF
- RAGAS RAG evaluation framework

**■ Cyber**

- Nessus VAPT + OpenVAS scanning
- Burp Suite: SQLi, XSS, SSRF labs
- Metasploit exploitation basics
- Professional pentest report writing

**■ Cloud Sec**

- DevSecOps: Security Code Scan+DAST+SCA in CI
- Azure Key Vault secrets + certificate management
- OWASP ZAP automated security tests
- Microsoft Defender for Cloud + Vulnerability Assessment

**Week-by-Week Plan — Month 2**

<b>Week 5</b>	PRIMARY: ASP.NET Core REST+JWT+Hangfire background jobs+SignalR WebSockets · AWS: Lambda+API Gateway+SQS · DevOps: K8s basics+minikube · AI: XGBoost+MLflow · DATA: Stats+A/B+dbt · CYBER: Nessus VAPT+DVWA SQLi · CLOUD SEC: DevSecOps Snyk+Bandit in CI · AGENTIC: LangChain LCEL+Pinecone · DSA: 8 Easy+4 Medium
<b>Week 6</b>	PRIMARY: React Redux+React Query+hooks + ASP.NET Core Identity+OAuth2+Blazor intro · AWS: ASG+ALB+CloudFront+ElastiCache · DevOps: Helm+EKS+CI(Trivy+SonarQube+Docker+ECR) · AI: Hugging Face BERT · DATA: ARIMA+Prophet · CYBER: Burp Suite XSS+SSRF · CLOUD SEC: HashiCorp Vault+OWASP ZAP DAST · AGENTIC: Hybrid RAG+RAGAS · DSA: 5 Easy+6 Medium
<b>Week 7</b>	PRIMARY: ASP.NET Core performance: IMemoryCache, Redis, EF Core query optimization, Dapper · AWS: ECS Fargate+Secrets Manager · DevOps: Prometheus+Grafana on K8s · AI: FastAPI model serving · DATA: BigQuery+dbt+Tableau · CYBER: Metasploit exploitation lab · CLOUD SEC: Security Hub+Inspector · AGENTIC: Llamaindex+advanced RAG · DSA: 4 Easy+5 Medium
<b>Week 8</b>	PROJECT SPRINT: Build Projects 3, 4 & 5 · Full DevSecOps CI (SAST+DAST+Trivy) · Pentest report for project · MLflow endpoint · LangChain RAG chatbot integrated · LeetCode: 60 Easy+22 Medium

**MONTH 2 — PROJECTS**

<b>PRJ 03</b>	<b>Secure DevOps Pipeline — DevSecOps on EKS</b>	■ GitHub Actions,Docker,ACR,AKS,Helm,SonarQube,Trivy,OWASP ZAP,Snyk,Prometheus,Grafana,Terraform,dotnet CLI
<b>Desc</b>	DevSecOps pipeline for ASP.NET Core app: GitHub Actions → dotnet build+xUnit tests+Security Code Scan SAST+SonarQube+Snyk+Trivy+OWASP ZAP → Docker → ACR push → Helm deploy to AKS → Prometheus+Grafana monitoring. Security gate blocks on critical vulnerabilities. Full pentest report.	
<b>Deliverables</b>	✓ dotnet CLI+GitHub Actions pipeline ✓ Security Code Scan+SonarQube SAST ✓ OWASP ZAP DAST ✓ AKS+Helm deploy ✓ Prometheus+Grafana ✓ Security report ✓ Terraform IaC	
<b>Roles</b>	DevSecOps Engineer   Platform Engineer   Cloud Security Engineer   SRE	
<b>PRJ 04</b>	<b>Serverless API + Secure RAG Chatbot on AWS</b>	■ Azure Functions,API Management,Cosmos DB,Azure Synapse,Pinecone,LangChain,Azure OpenAI,Entra ID+MFA,Azure WAF,Defender for Cloud,Terraform
<b>Desc</b>	Serverless URL shortener + analytics RAG chatbot using Azure Functions (C#). Azure Cosmos DB for URL mappings, Azure Synapse for analytics. RAG chatbot: LangChain + Pinecone + Azure OpenAI GPT-4o. SECURITY: Azure WAF + API Management rate limiting, Entra ID+MFA, Defender for Cloud, Azure Monitor Activity Log. Full Terraform IaC.	
<b>Deliverables</b>	✓ Azure Functions C# ✓ API Management+WAF ✓ Cosmos DB ✓ Pinecone RAG ✓ Entra ID+MFA ✓ Defender for Cloud ✓ Terraform IaC ✓ Cost+security report	
<b>Roles</b>	Azure Cloud Engineer   Cloud Security Engineer   Serverless Developer   AI Engineer	

<b>PRJ 05</b>	<b>Fraud Detection ML + MLOps + Vault Secrets</b>	■ ML.NET,XGBoost,SMOTE,SHAP,MLflow,ASP.NET Core REST,Evidently,Airflow,Azure ML,ACI,GitHub Actions,Azure Key Vault
<b>Desc</b>	Credit card fraud detection (AUC-ROC 0.98+). XGBoost+SMOTE, SHAP explainability, MLflow registry. Spring Boot REST API wraps model with Vault secret management + Spring Security. Evidently drift monitoring, Airflow retraining DAG, SageMaker endpoint, DevSecOps CI pipeline.	
<b>Deliverables</b>	✓ ML.NET+XGBoost+20 MLflow runs ✓ SHAP report ✓ ASP.NET Core API+Azure Key Vault ✓ Evidently drift ✓ Airflow DAG ✓ Azure ML endpoint	
<b>Roles</b>	<b>ML Engineer   MLOps Engineer   Data Scientist   FinTech Security Developer</b>	

**MONTH 3 ALL 9 TRACKS — Advanced Engineering**      PyTorch+CV+NLP · Azure ML · Terraform+ArgoCD · PySpark · LangGraph · SOC+SIEM · Zero Trust      Weeks 9–12 | 2026

<b>■ C# .NET</b> <ul style="list-style-type: none"> <li>■ Ocelot API Gateway + Steeltoe service discovery</li> <li>■ Polly: retry, circuit breaker, bulkhead, timeout</li> <li>■ MassTransit + RabbitMQ/Azure Service Bus messaging</li> <li>■ xUnit, Moq, FluentAssertions, WebApplicationFactory</li> </ul>	<b>■ Full Stack</b> <ul style="list-style-type: none"> <li>■ Microservices with ASP.NET Core + Docker Compose</li> <li>■ GraphQL with Hot Chocolate (.NET)</li> <li>■ Next.js SSR/SSG/ISR + App Router</li> <li>■ Stripe.net integration + webhook handlers</li> </ul>	<b>■ Azure+AWS</b> <ul style="list-style-type: none"> <li>■ AKS managed node pools + workload identity</li> <li>■ Azure ML training jobs + model registry</li> <li>■ Azure Data Factory ETL + Event Hubs</li> <li>■ Azure Cognitive Search + Cost Management</li> </ul>
<b>■ DevOps</b> <ul style="list-style-type: none"> <li>■ ArgoCD GitOps continuous delivery</li> <li>■ Terraform modules + remote state</li> <li>■ Istio service mesh + mTLS</li> <li>■ ELK Stack + Jaeger + OpenTelemetry</li> </ul>	<b>■ AI/ML</b> <ul style="list-style-type: none"> <li>■ PyTorch CNN + ResNet50 transfer learning</li> <li>■ YOLOv8 custom object detection</li> <li>■ BERT fine-tuning + sentence-transformers</li> <li>■ Grad-CAM explainability + ONNX export</li> </ul>	<b>■ Data Sci</b> <ul style="list-style-type: none"> <li>■ PySpark DataFrames + MLlib</li> <li>■ Apache Airflow DAGs + sensors</li> <li>■ dbt models + Delta Lake</li> <li>■ Kafka + Flink stream processing</li> </ul>
<b>■ Agentic</b> <ul style="list-style-type: none"> <li>■ LangGraph stateful graphs + cycles</li> <li>■ HITL interrupts + checkpointing</li> <li>■ CrewAI role-based multi-agent</li> <li>■ Agentic RAG — agent decides retrieval</li> </ul>	<b>■ Cyber</b> <ul style="list-style-type: none"> <li>■ Splunk SIEM + log dashboards</li> <li>■ MITRE ATT&amp;CK; framework mapping</li> <li>■ Incident response simulation</li> <li>■ Memory forensics + malware analysis</li> </ul>	<b>■ Cloud Sec</b> <ul style="list-style-type: none"> <li>■ Zero Trust Architecture + Entra ID Conditional Access</li> <li>■ CSPM: Prisma Cloud / Wiz CNAPP</li> <li>■ Azure Key Vault + TLS + Managed Identity</li> <li>■ Microsoft Purview + Compliance Manager</li> </ul>

**Week-by-Week Plan — Month 3**

<b>Week 9</b>	PRIMARY: PyTorch CNN+transfer learning (Python ML stays parallel) · AZURE: Azure ML training+model registry · DevOps: ArgoCD+Terraform modules · DATA: PySpark+Databricks+Airflow · CYBER: Splunk SIEM setup+log dashboards · CLOUD SEC: Zero Trust lab+Okta SSO · AGENTIC: LangGraph stateful workflow · DSA: 7 Medium+1 Hard
<b>Week 10</b>	PRIMARY: BERT fine-tuning + Semantic Kernel integration · AZURE: Azure Data Factory+Event Hubs+Azure Search · DevOps: Istio+ELK+Jaeger · DATA: dbt+Delta Lake · CYBER: MITRE ATT&CK;+IR simulation · CLOUD SEC: Prisma CSPM+KMS encryption · AGENTIC: CrewAI multi-agent+HITL · DSA: 5 Medium+2 Hard
<b>Week 11</b>	PRIMARY: YOLOv8+ONNX Runtime + ASP.NET Core REST wrapper · AZURE: multi-region+cost audit · DevOps: LitmusChaos+Falco · DATA: Kafka streaming+Feast · CYBER: Memory forensics+malware analysis+blue team · CLOUD SEC: Audit Manager+Wiz CNAPP demo · AGENTIC: Agentic RAG+tool use · DSA: System design (Uber, Twitter)
<b>Week 12</b>	PROJECT SPRINT: Build Projects 6 & 7 · SageMaker model serving · ArgoCD GitOps deploy · LangGraph analyst agent · SIEM monitoring integrated · Cloud security validated · LeetCode: 80 Easy+36 Medium+3 Hard

**MONTH 3 — PROJECTS**

<b>PRJ 06</b>	<b>Medical AI — HIPAA-aware Platform with SIEM</b>	■ PyTorch,ResNet50,YOLOv8,ONNX Runtime,ASP.NET Core,React,Azure ML,Airflow,MLflow,Splunk SIEM,Azure WAF,Azure Key Vault,ArgoCD,AKS
<b>Desc</b>	Chest X-ray multi-disease classifier (14 classes) with YOLOv8 lesion detection, Grad-CAM explainability, ONNX Runtime inference. ASP.NET Core REST API + React diagnosis UI. SECURITY: Azure Key Vault encryption, Azure WAF, Splunk SIEM anomaly alerts, Entra ID least-privilege, VNet private subnets. Azure ML pipeline, MLflow registry, Airflow DAG, ArgoCD AKS deploy.	
<b>Deliverables</b>	✓ PyTorch+YOLOv8+ONNX Runtime ✓ Azure ML pipeline ✓ Azure Key Vault+WAF+Splunk SIEM ✓ HIPAA checklist ✓ Grad-CAM UI ✓ ASP.NET Core API ✓ ArgoCD AKS deploy	
<b>Roles</b>	<b>ML Engineer   Healthcare AI Developer   Cloud Security Engineer   MLOps Engineer</b>	

<b>PRJ 07</b>	<b>Retail Analytics + LangGraph Agent + SOC Monitoring</b>	■ PySpark,Kafka,Airflow,dbt,Azure Synapse,Power BI,Streamlit,LangGraph,Azure OpenAI,Elastic SIEM,Microsoft Defender,Wiz CSPM
---------------	------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------

<b>Desc</b>	End-to-end retail analytics: PySpark ETL→Delta Lake→dbt→Azure Synapse→Power BI + Streamlit dashboard (revenue, cohort, forecast Prophet+LSTM). LangGraph analyst agent emails weekly PDF reports. Elastic SIEM monitors pipeline components, Microsoft Defender alerts on anomalous data access, Wiz CSPM cloud posture report.
<b>Deliverables</b>	✓ PySpark+Kafka pipeline ✓ dbt+Azure Synapse ✓ Power BI+Streamlit ✓ LangGraph agent ✓ Elastic SIEM ✓ Microsoft Defender ✓ Wiz CSPM report
<b>Roles</b>	<b>Data Engineer   Analytics Engineer   Security Analyst   AI Developer</b>

**MONTH 4 ALL 9 TRACKS — Production + Capstone** Fine-tuning · Multi-Agent · Azure+AWS Multi-cloud · GitOps · Full Pentest · SOC2/ISO27001 + Capstone **Weeks 13–16 | 2026**

<b>■ C# .NET</b> <ul style="list-style-type: none"> <li>■ Semantic Kernel: LLM integration in C# apps</li> <li>■ ASP.NET Core SSE streaming for LLM token output</li> <li>■ .NET agent loops with async/await + Channel</li> <li>■ Security code review: OWASP .NET cheat sheet, Roslyn analyzers</li> </ul>	<b>■ Full Stack</b> <ul style="list-style-type: none"> <li>■ Multi-tenant ASP.NET Core SaaS with schema isolation</li> <li>■ Stripe.net billing + webhook signature validation</li> <li>■ SSE streaming for real-time LLM token output to React</li> <li>■ CSP headers, CORS config + OWASP .NET secure coding</li> </ul>	<b>■ Azure+Multi</b> <ul style="list-style-type: none"> <li>■ Azure OpenAI: GPT-4o, Phi-3, Llama 3 managed</li> <li>■ Azure AI Search managed RAG + vector store</li> <li>■ GCP Vertex AI + AWS Bedrock (multi-cloud)</li> <li>■ Azure Cost Management + Management Groups + Policy</li> </ul>
<b>■ DevOps</b> <ul style="list-style-type: none"> <li>■ ArgoCD ApplicationSets + GitOps</li> <li>■ Karpenter node autoscaling on EKS</li> <li>■ Falco runtime K8s security</li> <li>■ LLM CI/CD: prompt regression tests</li> </ul>	<b>■ AI/ML</b> <ul style="list-style-type: none"> <li>■ QLoRA fine-tuning + Unsloth (2x)</li> <li>■ HuggingFace TRL: SFTTrainer+DPO</li> <li>■ VLLM high-throughput inference server</li> <li>■ Guardrails: NeMo + Llama Guard 3</li> </ul>	<b>■ Data Sci</b> <ul style="list-style-type: none"> <li>■ BigQuery ML: train+serve in SQL</li> <li>■ Vertex AI end-to-end ML pipelines</li> <li>■ LLM pipelines: entity extraction at scale</li> <li>■ Privacy-preserving ML: differential privacy</li> </ul>
<b>■ Agentic</b> <ul style="list-style-type: none"> <li>■ Production agent: error, retry, fallback</li> <li>■ LangFuse LLM cost+quality observability</li> <li>■ Portkey: routing, caching, budgets</li> <li>■ Custom MCP server: expose DB+APIs</li> </ul>	<b>■ Cyber</b> <ul style="list-style-type: none"> <li>■ Full pentest: scope→recon→exploit→report</li> <li>■ API + cloud misconfiguration pentesting</li> <li>■ Bug bounty: HackerOne/Bugcrowd workflow</li> <li>■ CompTIA Security+ / CEH exam prep</li> </ul>	<b>■ Cloud Sec</b> <ul style="list-style-type: none"> <li>■ SOC2 Type II + Azure Compliance Center evidence</li> <li>■ ISO27001 + Microsoft Cloud ISMS documentation</li> <li>■ PCI-DSS Azure compliance mapping</li> <li>■ Azure Sentinel SOAR: automated incident response</li> </ul>

**Week-by-Week Plan — Month 4**

<b>Week 13</b>	PRIMARY: Semantic Kernel fine-tuned model integration, VLLM via REST, Guardrails · AZURE: Azure OpenAI RAG+GCP Vertex AI · DevOps: Karpenter+Falco+LLM CI · DATA: BigQuery ML+LLM pipelines · CYBER: API pentesting+cloud misconfig exploits · CLOUD SEC: SOC2 evidence+GDPR mapping · AGENTIC: Production LangGraph+LangFuse · DSA: Mock OA x2
<b>Week 14</b>	PRIMARY: Semantic Kernel MCP + voice agent + .NET OWASP secure coding review · FULL STACK: Stripe+SSE+Next.js+CSP headers · AZURE: Azure OpenAI+multi-cloud security · DevOps: ApplicationSets+Falco+SBOM · CYBER: Full pentest on capstone system+report · CLOUD SEC: ISO27001 mapping+IR playbooks · AGENTIC: CrewAI+Portkey+secure agents · DSA: Mock OA x2
<b>Week 15</b>	CAPSTONE Sprint Wk1: Architect + build Project 12 · Terraform all infra · Full DevSecOps CI/CD · Fine-tuned model on VLLM · RAG chatbot+Pinecone · Multi-agent backend · WAF+SIEM+CSPM+SOC2 controls
<b>Week 16</b>	CAPSTONE Sprint Wk2+PORTFOLIO: Polish+deploy all 12 projects · READMEs · Loom demos · GitHub+LinkedIn+Resume update · 5 mock technical+3 system design+2 HR interviews · Red team vs Blue team final exercise · LeetCode: 90 Easy+45 Medium+5 Hard DONE

**MONTH 4 — PROJECTS**

<b>PRJ 08</b>	<b>Autonomous Security-Aware Software Agent</b>	■ LangGraph,CrewAI,Claude Sonnet 4,Azure OpenAI GPT-4o,GitHub API,xUnit+MSBuild,VLLM,Security Code Scan SAST,LangFuse,AKS,Falco
<b>Desc</b>	Multi-agent system resolving GitHub .NET project issues. LangGraph: Read→RAG codebase→Plan→Generate C# code→MSBuild+xUnit tests→Security Code Scan SAST (blocks HIGH severity)→Code Review Agent→PR. Semantic Kernel for code generation. Falco runtime security on AKS. VLLM fine-tuned model. Evaluated on 25 real issues (60%+ success).	
<b>Deliverables</b>	✓ LangGraph workflow ✓ CrewAI agents ✓ GitHub API ✓ MSBuild+xUnit runner ✓ Security Code Scan SAST gate ✓ VLLM ✓ Falco alerts ✓ LangFuse traces ✓ AKS+ArgoCD ✓ 25-issue evaluation	
<b>Roles</b>	<b>AI Engineer   DevSecOps Engineer   Agentic AI Developer   Security Automation Engineer</b>	
<b>PRJ 09</b>	<b>Enterprise Secure RAG — Multi-tenant Knowledge Assistant</b>	■ LangChain,Semantic Kernel,Azure OpenAI GPT-4o,Azure Cognitive Search,ASP.NET Core SSE,React,RAGAS,LangSmith,entra ID+MFA,Azure WAF,Azure Key Vault,ACI,Terraform
<b>Desc</b>	Multi-tenant RAG chatbot built with ASP.NET Core + Semantic Kernel. Hybrid search: Azure Cognitive Search (vector+keyword) + BM25 + RRF fusion. Azure OpenAI GPT-4o with OpenAI fallback. SSE streaming to React. SECURITY: tenant namespace isolation, Entra ID+MFA, Azure WAF+Key Vault, Monitor Activity Log, Defender for Cloud. Redis cache 60% cost saving. RAGAS evaluation (faithfulness >0.85).	

<b>Deliverables</b>	✓ Azure Cognitive Search hybrid RAG ✓ Semantic Kernel integration ✓ Entra ID+MFA+WAF+Key Vault ✓ Tenant isolation ✓ RAGAS benchmark ✓ LangSmith traces ✓ Terraform ACI ✓ Security architecture doc
<b>Roles</b>	<b>AI Engineer   Cloud Security Engineer   LLM Engineer   Full Stack AI Developer</b>
<b>PRJ 10 Professional Cloud Penetration Testing Report</b>	■ Kali Linux, Metasploit, Burp Suite, Nmap, Nessus, Pacu, ScoutSuite, CloudSploit, OWASP ZAP, Splunk
<b>Desc</b>	Pentest of simulated AWS environment: web apps, APIs, EC2, S3 misconfigs, IAM flaws, Lambda. Tools: Pacu (AWS exploitation), ScoutSuite, Burp Suite, Metasploit. Deliverables: executive summary + technical findings + risk ratings + remediation.
<b>Deliverables</b>	✓ Scoping document ✓ Reconnaissance report ✓ Exploitation evidence ✓ Cloud misconfiguration findings ✓ Executive summary ✓ Technical report ✓ Remediation roadmap
<b>Roles</b>	<b>Penetration Tester   Cloud Security Engineer   Security Analyst   VAPT Specialist</b>
<b>PRJ 11 Cloud Compliance &amp; Security Architecture</b>	■ Security Hub, Audit Manager, Prisma Cloud, Terraform, Wiz, SOC2, ISO27001, PCI-DSS
<b>Desc</b>	Cloud security architecture for a fintech startup: SOC2 Type II controls, ISO27001 gap analysis, PCI-DSS mapping, Terraform baseline (GuardDuty, WAF, KMS, VPC flow logs), Prisma CSPM, IR playbooks.
<b>Deliverables</b>	✓ Architecture diagram ✓ SOC2 controls ✓ ISO27001 gap analysis ✓ Terraform baseline ✓ Prisma CSPM ✓ IR playbooks
<b>Roles</b>	<b>Cloud Security Architect   Compliance Engineer   GRC Analyst   Security Engineer</b>

## CAPSTONE — PROJECT 12: ALL 9 TRACKS INTEGRATED

<b>PROJECT 12 AI-Powered Secure SaaS Platform — Complete Production System</b>	■ CAPSTONE — 9 Tracks · 4 Months · Production-Ready		
■ Python+FS	ASP.NET Core 8+Next.js+Blazor+SQL Server+Redis+Hangfire	■ AWS+GCP	AKS+Azure ML+Blob Storage+Azure SQL+Azure OpenAI+Azure Synapse
■ DevOps	GitHub Actions+Terraform+ArgoCD+Prometheus+ELK+Karpenter+Falco (AKS)	■ AI+■	PyTorch+MLflow+LangGraph+CrewAI+Azure Cognitive Search+VLLM+LangFuse
■ Cyber	Pentest Report+Splunk SIEM+Bandit SAST+IR Playbook	■ Cloud Sec	WAF+KMS+Cognito+Security Hub+Prisma CSPM+SOC2+ISO27001
<b>What it is</b>	AI content creation SaaS — multi-tenant, Stripe-billed, GPT-4o streaming, brand RAG chatbot, fine-tuned LLM on VLLM, multi-agent pipeline, voice interface, analytics, AND enterprise security posture.		
<b>Core Features</b>	Multi-tenant ASP.NET Core 8+Next.js+Stripe.net billing (Free/Pro/Enterprise) · Azure OpenAI SSE streaming via Semantic Kernel · RAG brand chatbot (Azure Cognitive Search+hybrid search+Cohere Rerank) · Fine-tuned Llama 3.2 (QLoRA) on VLLM · CrewAI: Researcher→Writer→Editor→SEO · Whisper STT+ElevenLabs TTS · PySpark+Azure Synapse analytics · LangFuse LLM observability		
<b>Security Layer</b>	Azure WAF+Entra ID+MFA on all endpoints · Azure Key Vault encryption at rest+transit · Splunk SIEM event monitoring · Defender for Cloud+Microsoft Sentinel threat detection · Full pentest report of platform (exec+technical) · SOC2 Type II+ISO27001 controls mapping · DevSecOps CI: SAST+DAST+SCA+container scan gates · Falco runtime anomaly detection		
<b>DevOps &amp; Infra</b>	Terraform all Azure (VNet, AKS, Azure SQL, Blob, CDN, Redis Cache, WAF, Defender for Cloud) · GitHub Actions: dotnet build+xUnit+Security Code Scan+SonarQube+Snyk+Trivy+ZAP→ACR→ArgoCD→AKS (zero-downtime) · Prometheus+Grafana+LangFuse+ELK · Karpenter+Falco		
<b>Deliverables</b>	✓ Live app URL ✓ GitHub repo+CI badges ✓ Terraform Azure IaC ✓ Fine-tuned HuggingFace model ✓ 90%+ test coverage (xUnit) ✓ Swagger/OpenAPI docs ✓ Pentest report ✓ SOC2+ISO27001 docs ✓ Grafana+LangFuse dashboards ✓ Architecture diagram ✓ 3-min Loom demo		
<b>Target Roles</b>	.NET Full Stack Developer · AI/ML Engineer · Cloud Security Engineer · DevSecOps · LLM Engineer · SaaS Developer · Azure Cloud Architect · Penetration Tester		

## POST-PROGRAM PLACEMENT SUPPORT

<b>5500+ Placements</b>	<b>200+ Hiring Partners</b>	<b>98% Placement Rate</b>	<b>22 LPA Highest Pkg</b>	<b>60 Days Avg to Offer</b>
Students Placed	Active Partners	Of Completers	2025 Record	First Offer

# 5-PHASE PLACEMENT GUARANTEE PROGRAM

<b>PHASE 1 Wk 13-14</b>	<b>Portfolio &amp; Personal Brand</b>	ATS-optimized resume by career team · GitHub profile review (repos, READMEs, CI badges) · LinkedIn All-Star optimization + content strategy · Loom demos for all 12 projects · Tailored resume per role (Dev, ML, Security, Cloud)
<b>PHASE 2 Wk 15-16</b>	<b>Interview Preparation</b>	10 mock interviews: 5 DSA + 3 system design + 2 behavioral HR · STAR method coaching · System design templates for 7 popular questions · Domain Q&A; banks: Python, AWS, DevOps, ML, Security, AI · Salary negotiation scripts + offer evaluation framework
<b>PHASE 3 Post Wk16</b>	<b>Job Application Support</b>	Direct referrals to 200+ hiring partners · Weekly job alert digest for your tech stack · Naukri, LinkedIn, AngelList, Wellfound profile optimization · LinkedIn cold outreach templates to HRs and EMs · Application tracking support for 90 days
<b>PHASE 4 Ongoing</b>	<b>Interview Scheduling</b>	Placement team schedules all interviews on your behalf · Pre-interview company-specific briefing (culture, tech stack, rounds) · Post-interview debrief and targeted re-preparation if unsuccessful · 'Interview War Room' Slack channel — daily tips from placed alumni
<b>PHASE 5 Offer Stage</b>	<b>Offer Negotiation</b>	Market salary benchmarking by role, company and location · Counter-offer strategy without losing the offer · Offer letter review: joining bonus, variable pay, ESOPs, non-compete · Multiple offer comparison: growth vs compensation · Joining date + background verification support

## Companies Where ASCEND Alumni Work

<b>PRODUCT GIANTS</b>	Google, Microsoft, Amazon, Meta, Adobe, Salesforce, Uber, Stripe, Anthropic, OpenAI
<b>INDIAN UNICORNS</b>	Flipkart, Razorpay, Swiggy, Zomato, CRED, PhonePe, Meesho, Zepto, Groww, Paytm
<b>SECURITY FIRMS</b>	Palo Alto Networks, CrowdStrike, Qualys, Rapid7, Secureworks, HackerOne, BugCrowd
<b>GLOBAL MNCs</b>	TCS, Infosys, Wipro, HCL, Capgemini, Accenture, Cognizant, IBM, Deloitte, LTIMindtree
<b>AI STARTUPS</b>	Sarvam AI, Krutrim, Yellow.ai, Haptik, Darwinbox, Unacademy, Postman, LeadSquared
<b>GLOBAL REMOTE</b>	Toptal, Turing, Arc.dev, X-Team, Crossover + 60+ US/UK/Canada/Australia remote startups

## CAREER OUTCOMES & 2026 SALARY GUIDE

JOB ROLE	KEY SKILLS	INDIA 2026	GLOBAL
.NET / C# Developer	C#, ASP.NET Core, REST APIs, EF Core, SQL Server	■ 4-10 LPA	\$70-105K
.NET Full Stack Developer	React+Next.js, ASP.NET Core, Identity+JWT, SQL Server	■ 5-14 LPA	\$80-125K
Cloud/AWS Engineer	AWS, Terraform, Linux, Docker, K8s, CI/CD	■ 6-16 LPA	\$85-140K
DevOps / SRE Engineer	K8s, GitHub Actions, Prometheus, ELK, GitOps	■ 7-18 LPA	\$90-148K
DevSecOps Engineer	DevOps + SAST/DAST/SCA + Security in CI/CD	■ 8-20 LPA	\$95-155K
Cyber Security Analyst	VAPT, SOC, SIEM, Incident Response, Pentesting	■ 5-14 LPA	\$75-120K
Cloud Security Engineer	AWS Security, Zero Trust, CSPM, SOC2, Compliance	■ 7-20 LPA	\$90-150K
Penetration Tester	Metasploit, Burp Suite, Kali, Web+Cloud Pentesting	■ 6-18 LPA	\$80-140K
Data Engineer	PySpark, Airflow, dbt, BigQuery, Kafka, Delta Lake	■ 6-16 LPA	\$85-140K
ML / AI Engineer	PyTorch, ML.NET, MLflow, Semantic Kernel, Azure ML	■ 8-22 LPA	\$100-160K
LLM / GenAI Engineer	LangChain, Semantic Kernel, RAG, Fine-tuning, Agents	■ 12-20 LPA	\$120-180K
Agentic AI Developer	LangGraph, CrewAI, MCP, Multi-Agent, VLLM	■ 12-32 LPA	\$130-200K

# DSA + CERTIFICATIONS + SUCCESS CHECKLIST

## DSA + System Design Progress (Throughout 16 Weeks)

<b>Weeks 1–4</b>	Arrays, Strings, Linked Lists, Stacks, Queues — 26 Easy problems
<b>Weeks 5–8</b>	Binary Trees, Heaps, Graphs BFS/DFS — 20 Easy + 22 Medium problems
<b>Weeks 9–12</b>	DP (1D, 2D, knapsack), Greedy, Tries — 14 Easy + 14 Medium + 3 Hard
<b>Weeks 13–16</b>	Advanced DP, Bit Manipulation, Mock OA x 4 — 10 Medium + 2 Hard
<b>System Design</b>	URL Shortener · Twitter · Uber · Netflix · WhatsApp · Fraud Detection · AI Chatbot at Scale
<b>TOTAL</b>	<b>90 Easy + 45 Medium + 5 Hard = 140 LeetCode   7 System Designs   20 Behavioral Answers Prepared</b>

## Certifications Aligned to ASCEND

CERTIFICATION	PROVIDER	PRIORITY / BEST FOR
AWS Certified Solutions Architect – Associate (SAA-C03)	AWS	■■■■ Very High — Cloud roles
CompTIA Security+ (SY0-701)	CompTIA	■■■■ Very High — Cyber Security entry
Certified Kubernetes Administrator (CKA)	CNCF	■■■■ Very High — DevOps roles
AWS Certified Security – Specialty	AWS	■■■■ High — Cloud Security
Offensive Security OSCP	Offensive Security	■■■■ Premium — Senior Pentester
Certified Ethical Hacker (CEH)	EC-Council	■■■ High — Pentesting roles
Google Professional Cloud Architect	GCP	■■■ High — Cloud Architect
TensorFlow Developer Certificate	Google	■■■ High — ML Engineer
AZ-900: Azure Fundamentals	Microsoft	■■■■ High — Azure entry level
AZ-204: Azure Developer Associate	Microsoft	■■■■ Very High — .NET Azure roles

## Week 16 Success Checklist

■ <b>12 Projects Live</b>	All deployed with URLs, GitHub repos, clean READMEs, CI/CD badges, Loom demos
■ <b>GitHub Profile</b>	100+ commits/month, all 12 pinned, consistent green contribution graph throughout
■ <b>LinkedIn All-Star</b>	All 9 tracks listed, 5 project posts with demos, 300+ connections, open to work
■ <b>Personal Portfolio</b>	Next.js on Vercel — projects, resume download, contact, tech blog
■ <b>HuggingFace Hub</b>	Fine-tuned model with model card + interactive Gradio demo Space
■ <b>ATS Resume</b>	1-page PDF, quantified metrics, tailored per role, keywords from 50+ real JDs
■ <b>Pentest Report</b>	Professional VAPT: executive summary + technical findings + remediation
■ <b>Security Portfolio</b>	Cloud security architecture doc + compliance mapping + CSPM report
■ <b>Certifications</b>	AWS Cloud Practitioner + CompTIA Security+ — both passed by Week 16
■ <b>Mock Interviews</b>	10 done: 5 DSA + 3 system design + 2 behavioral HR sessions completed
■ <b>Demo Videos</b>	12 Loom walkthroughs (2–3 min each) linked in resume + LinkedIn
■ <b>Technical Blog</b>	3+ articles on Dev.to/Hashnode — what you built + lessons learned

# 8 RULES FOR GETTING HIRED IN 2026

1	<b>Code Every Day</b>	2–3 hours hands-on building minimum. Theory without practice = zero retention and zero interviews.
2	<b>Build in Public</b>	Post your projects on LinkedIn weekly. Share what you built. Recruiters follow active builders.
3	<b>Hack Ethically from Week 1</b>	Use DVWA and cloud labs. Document every vulnerability. Security skills double your interview value.
4	<b>Security-First Mindset</b>	Every project: OWASP checklist, WAF, IAM audit. Shows senior-level thinking to interviewers.
5	<b>Network Intentionally</b>	Connect with 5 developers/HRs/security pros on LinkedIn daily. 70% of jobs come via referral.
6	<b>Specialize by Month 4</b>	One primary role: Developer OR Security OR AI/ML. Specialists get hired faster than generalists.
7	<b>Stay Current</b>	AI+Security changes weekly. Read: Krebs on Security, The Pragmatic Engineer, TLDR AI, CloudSecList.
8	<b>DSA Non-Negotiable</b>	1 LeetCode every day from Day 1. No exceptions. 140 problems by Week 16 = FAANG-ready.



## ASCEND 2026

.NET Full Stack · 9 Tracks · 16 Weeks · 12 Projects · 5500+ Placements · 98% Placement Rate

■ 9666019191

■ [www.cloudsoftsol.com](http://www.cloudsoftsol.com)

■ Hyderabad

■ 2026 Batch — Enroll Now

Cloud Soft Solutions — Hyderabad's #1 Tech Career Transformation Institute  
.NET · C# · ASP.NET Core · Azure · DevOps · AI/ML · Data Science · Agentic AI · Cyber Security · Cloud Security

"Your career doesn't care where you started. It only cares where you decide to go." ■