Cloud Security & DevSecOps

Secure Cloud Identities, Delivery Pipelines, and Detection Workflows

This advanced course is built for learners who already have core security foundations and now need stronger cloud-security judgment. The focus is not only on cloud attack paths. It is on building safer IAM boundaries, using logs and controls well, validating findings carefully, and connecting security work to real delivery systems.

You will work through cloud hardening, controlled attack-path review, identity and federation security, DevSecOps checks, and reporting in a way that rewards discipline over drama.

Why This Course?

The Market Reality

Global Context: Cloud adoption keeps increasing the need for stronger identities, hardened pipelines, detection workflows, and safer defaults. Teams need engineers who can make security part of delivery instead of treating it as a last-step audit.

Nepal Context: As banking, fintech, government platforms, and product teams continue using cloud infrastructure, the need for secure IAM, logging, incident response readiness, and pipeline security keeps growing. The gap is often in engineers who can connect architecture, detection, and remediation in one flow.

Your Opportunity: This course positions you for **cloud security, DevSecOps, and security-platform roles** that reward clearer IAM judgment, practical detection habits, and more usable security automation.

Nepal-Relevant Reality	Opportunity
FinTech, government, and product teams keep expanding cloud usage	Cloud-security judgment becomes more valuable every quarter
Identity and access mistakes still create major cloud risk	Strong IAM and federation habits stand out quickly
Teams want security inside delivery, not only after release	DevSecOps and guardrail design become practical career proof

Nepal-Relevant Reality	Opportunity
Logs and detections often exist without good triage	Better validation and reporting create trust with engineering teams

Course Snapshot

Parameter	Details
Course Code	TR-11
Title	Cloud Security & DevSecOps (Cybersecurity - Advanced)
Duration	2.5 Months (10 Weeks)
Schedule	Monday to Friday (Mon–Fri, 5 Days/Week), 2 Hours/Day
Total Hours	100 Hours of Live Training
Batch Size	Maximum 10 Students
Course Fee	NPR 35,000
Prerequisites	Completion of Ethical Hacking & Network Security (TR-04) or equivalent is required. You should already be comfortable with Burp Suite, Nmap, Linux logs and services, and core OWASP Top 10 thinking. Prior AWS or Azure exposure is strongly helpful. Before Day 1, review IAM basics, HTTP request flow, and Linux access-control concepts, then complete the advanced readiness review. Saarathi Gate Assessment before Day 1. This is not a zero-beginner entry course.
Self-Study	Minimum 2 hours/day outside class (mandatory)
Outcome	Cloud Security Engineer / DevSecOps Engineer

Your Learning Week

Day	Activity
Mon–Fri	2-hour live class session (hands-on, classroom-based)
Mon–Fri	Minimum 2 hours self-study & classroom practice (mandatory)
Saturday	No classes - flexible self-study, peer collaboration, classroom work

Day	Activity
Sunday	Whole day self-learn time. Classrooms remain fully open for you to come in, study, collaborate with peers, and build projects.

> *This is an advanced security track. The classroom builds the workflow, but repeated review, notes, and lab practice are what make the judgment stick.*

Week-by-Week Curriculum

Phase 1: Cloud Security Foundations (Weeks 1–2, 2 Weeks, 20 Hours)

Week	Focus Area	What You'll Master
Week 1	Shared Responsibility, IAM & Guardrails	Shared responsibility, IAM foundations, boundary design, cloud logging goals, and advanced-course expectations
Week 2	Logging, Secrets & Security Services	CloudTrail, GuardDuty, Security Hub, secrets management, KMS, Config rules, and practical cloud-hardening review

Phase 2: Cloud Attack Paths & Response (Weeks 3–4, 2 Weeks, 20 Hours)

Week	Focus Area	What You'll Master
Week 3	Misconfiguration, Metadata & Privilege Paths	Cloud attack surface, metadata risk, IAM privilege paths, S3 exposure, serverless misuse, and controlled attack-path reasoning
Week 4	Detection, Incident Response & Forensics	Detection engineering, incident-response playbooks, log-first forensics, hardening baselines, and response automation awareness

Phase 3: Identity & Access Security (Weeks 5–6, 2 Weeks, 20 Hours)

Week	Focus Area	What You'll Master
Week 5	Identity Architecture & Federation	AD and Entra ID awareness, trust boundaries, federation basics, service identities, and enterprise IAM architecture

Week	Focus Area	What You'll Master
Week 6	OAuth, SAML, Governance & Zero Trust	OAuth and OIDC review, SAML risk awareness, identity governance, access review, and Zero Trust design fundamentals

Phase 4: DevSecOps, Capstone & Career (Weeks 7–10, 4 Weeks, 40 Hours)

Week	Focus Area	What You'll Master
Week 7	Pipeline Security Foundations	Shift-left security, SAST, dependency scanning, secret scanning, and usable security gates
Week 8	Runtime, Container & IaC Security	DAST automation, container review, IaC scanning, Falco runtime monitoring, and API security inside delivery workflows
Week 9	SecureRetail Capstone & Reporting	Cloud-security architecture review, detection and pipeline integration, remediation planning, and professional reporting
Week 10	Portfolio, Interviews & Career Launch	Resume, GitHub and LinkedIn polish, architecture discussion, mock interviews, and job-search planning

Skills You'll Gain

Security Engineering Tools

Tool/Technique	Proficiency Level
AWS IAM	Identity boundary design
CloudTrail & GuardDuty	Logging and detection workflows
Semgrep	Pipeline code scanning
Trivy	Dependency and container review
Checkov	IaC review
Falco	Runtime monitoring awareness

Security Frameworks

Framework	Application
Shared Responsibility	Cloud control boundaries
Zero Trust	Identity-first security design
DevSecOps Methodology	Shift-left security automation
Incident Response Playbooks	Detection and containment workflows

Topic Depth and Awareness

Section	Guidance
Purpose	This course intentionally separates what you need to master in depth from what you only need to understand with working awareness.
Depth	Cloud hardening, IAM review, logging and triage, DevSecOps checks, runtime review, and remediation-focused reporting practiced repeatedly in class
Awareness	Deeper AD or Entra specialization, broader SOAR ecosystems, and more advanced forensics paths introduced as comparison context
How to use this syllabus	Spend most of your self-study time strengthening the depth topics first. Use awareness topics to broaden judgment, not to split your focus too early.

Project Pool

> *All options below are **intermediate-level final projects**. Each student chooses **one** final project from this pool. Trainers may run smaller guided exercises during the course, but public phase-wise project sections are intentionally removed so the completion standard stays clear and consistent.*

#	Final Project Choice	What You Will Build	Core Stack / Tools
1	AWS IAM Hardening Pack	Audit and improve identity, access boundaries, and account hygiene inside a realistic AWS setup.	AWS IAM, least privilege, CloudTrail, policy review

#	Final Project Choice	What You Will Build	Core Stack / Tools
2	Cloud Logging & Detection Stack	Build a detection-oriented logging setup with alerts, evidence trails, and response notes.	CloudTrail, GuardDuty, alerting, log analysis
3	Secure CI/CD Gate Pipeline	Add security gates for secrets, images, dependencies, and infrastructure before deployment.	GitHub Actions, Trivy, gitleaks, policy checks
4	Container & IaC Security Review	Audit container images and infrastructure-as-code for common security weaknesses and remediation steps.	Docker security, tfsec / checkov awareness, IaC review, hardening
5	Incident Response Automation Pack	Build a small cloud-security response workflow with alert triage, playbook steps, and evidence handling.	AWS, response playbooks, security automation, incident workflow

Career Paths & Trajectory

Role Path	Focus and Proof	Stage and Timeline	What Actually Matters
Cloud Security Analyst	Review IAM, logging, detection, and hardening findings across a cloud environment. Proof you leave with: GuardDuty and CloudTrail review habits, IAM evidence, and stronger triage judgment	Entry role - first 0–12 months	Accurate triage, least-privilege thinking, and documentation that engineers can actually use.
Cloud Security Engineer	Harden AWS environments, improve identity boundaries, and build guardrails into delivery workflows. Proof you leave with: IAM hardening, secure pipeline proof, and stronger cloud-security reasoning	Growth role - 1–3 years	Strong IAM judgment, better guardrails, and security that fits engineering flow instead of fighting it.
DevSecOps / Security Platform Engineer	Own reusable security checks, container and IaC scanning, and response automation across teams. Proof you leave with: SAST, DAST, IaC automation, and playbook design	Senior individual contributor - 3–5 years	Practical automation, good defaults, and knowing when to alert, block, or escalate.

Role Path	Focus and Proof	Stage and Timeline	What Actually Matters
Senior Cloud Security Engineer / Security Architect	Guide cloud guardrails, detection strategy, and design reviews for larger systems. Proof you leave with: Reference architectures, response workflows, and platform guidance	Senior design path - 5+ years	Trade-off judgment, cross-team influence, and building guardrails teams will actually adopt.

Saarathi Gate & Completion Review

Before You Start: Saarathi Gate Assessment

All students complete the **Saarathi Gate Assessment** before Day 1. It is a short diagnostic review of aptitude, learning behaviour, and thinking style. It has **no pass/fail** and is used only to tailor support from the start.

After Course Completion: Saarathi Completion Review

The **Saarathi Academy Certificate** is issued after the selected final project is completed, documented, and reviewed by the trainer. There is **no separate certification exam** for this course.

Completion Requirements:

1. **Attendance:** Minimum 80% attendance
2. **Weekly Work:** Core deliverables, revision work, and practice tasks completed
3. **Final Project:** One intermediate-level project selected from the project pool and completed to trainer-approved quality
4. **Portfolio Proof:** Screenshots, documentation, case-study notes, or equivalent proof assets updated
5. **Trainer Review:** Practical execution, consistency, communication, and overall growth signed off by the trainer

Enrollment & Next Steps

Next Batch: Starting soon (contact for exact dates) **Offline Location:** Old Baneshwor Chowk, Kathmandu, Nepal **Mode:** Online + Offline **Contact (Call/WhatsApp):** 9761095364, 9744442469

» **[ENROLL NOW]** - Limited to 10 seats per batch

Cloud security is clearer when IAM, detection, response, and delivery all make sense together.

Last Updated: Mar 30, 2026