NEXTGEN DEVSECOPS AI

AI-Powered DevSecOps

Professional Training Curriculum & Learning Roadmap

Learn • Build • Secure • Innovate

6–8 WEEKS	LIVE + LABS	PORTFOLIO
Instructor-led	Guided practice	Capstone projects

AI-ENHANCED DEVSECOPS	SECURE GENAI	AI OPERATIONS
AI-assisted CI/CD, scan triage and remediation workflows	LLM, RAG, prompt-injection and data-protection risks	Agent security, observability and human approval

Format: Concepts, live demonstrations, guided labs, assignments and capstone.

Prerequisites: DevSecOps/AppSec fundamentals and basic CI/CD familiarity. Basic Python is helpful.

Program fit: An advanced transition from traditional DevSecOps and Application Security into AI-assisted security engineering and secure GenAI applications.

01 Course Overview

Extend existing software delivery and security skills into AI-assisted security workflows, LLM application defence and secure AI operations.

02 Learning Roadmap

Stage	Learning path	Learner gains
1	AI foundations for DevSecOps	LLM concepts, prompts and responsible use
2	AI-enhanced DevSecOps pipelines	AI-supported triage and human-approved gates
3	AI-assisted application security	Secure code review and threat modelling
4	GenAI & LLM application security	Prompt-injection and RAG security awareness
5	AI agents & LLMOps security	Least privilege, tracing and auditability
6	Capstone & portfolio	End-to-end security engineering project

03 Program Outcomes

- Apply AI-assisted analysis to security findings and validate the results.
- Integrate LLM-supported triage into controlled CI/CD workflows.
- Assess common LLM application and AI agent risks.
- Demonstrate security decisions with evidence, logging and human approval.

04 Training Approach

Concept clarity → live demonstrations → guided hands-on labs → assignments → integrated capstone. AI supports the workflow; security validation and human oversight remain essential.

05 Curriculum Modules — Foundations & Delivery

MODULE 1 AI Foundations for DevSecOps Engineers

WEEK 1 · BRIDGE MODULE

Focus: Understand LLMs without requiring deep machine-learning prerequisites.

- LLM basics: tokens, context windows, embeddings and limitations.
- Prompt engineering for engineering and security tasks.
- Using local LLMs with Ollama.
- Responsible AI use, sensitive-data risks and human review.
- Lab: evaluate model responses and identify limitations.

MODULE 2 AI-Enhanced DevSecOps Pipelines

WEEK 2 · PIPELINE AUTOMATION

Focus: Integrate AI assistance into existing secure software delivery practices.

- Integrating AI into CI/CD workflows.
- Interpreting SAST, SCA, DAST and secrets-scan findings with an LLM.
- Vulnerability triage, prioritisation and remediation suggestions.
- Human-approved security gates and auditable decisions.
- Lab: create a controlled scan-summary workflow.

MODULE 3 AI-Assisted Application Security

WEEK 3 · SECURE CODING AND APPSEC

Focus: Use AI as a review assistant, not a replacement for security validation.

- AI-assisted secure code review.
- OWASP Top 10 vulnerability analysis and remediation.
- Threat modelling with STRIDE and security requirements.
- Validate AI-generated code and avoid false positives.
- Lab: review a sample application and verify findings.

06 Curriculum Modules — Secure AI

MODULE 4 GenAI & LLM Application Security

WEEK 4 · AI THREAT DEFENCE

Focus: Identify common security risks in LLM-enabled applications.

- OWASP Top 10 for LLM Applications.
- Prompt injection, sensitive information disclosure and insecure output handling.
- RAG security, embedding risks and vector-database access control.
- Model and dataset supply-chain risks, guardrails and security testing.
- Lab: test a sample LLM/RAG application against representative risks.

MODULE 5 AI Agents & LLMOps Security

WEEK 5 · SECURE AI OPERATIONS

Focus: Secure agent workflows and operational controls around AI-enabled systems.

- Agent tools, permissions and least-privilege access.
- Threat modelling AI agents and tool-calling workflows.
- Model evaluation, observability, tracing and audit logs.
- Secure model deployments, secrets and runtime configuration.
- Lab: map agent permissions and audit tool actions.

07 Capstone Project

Build an AI-assisted security engineering workflow connecting automated scans, LLM-supported analysis and secure GenAI testing.

BUILD CI/CD with automated security scans	**ANALYSE** LLM-supported triage and prioritisation	**SECURE** Guardrails, access controls and human review

- Combine automated security scanning with LLM summaries and human approval.
- Test a sample LLM/RAG application and capture security evidence.
- Document remediation, logs, decisions and the final demonstration.

08 Hands-on Lab Journey

Lab	Theme	Practical outcome
1	LLM and prompt foundations	Understand model limits and responsible use
2	AI-assisted CI/CD	Summarise scan findings with approval checkpoints
3	AI-assisted AppSec	Review and validate code findings
4	LLM application security	Explore prompt injection and data exposure
5	RAG and embedding security	Review retrieval access and data boundaries
6	AI agent security	Map permissions, tool calls and audit trails
Capstone	AI-powered security workflow	Integrated project with evidence and human review

09 Prerequisites & Learning Outcomes

Recommended prerequisites

- Familiarity with Git, CI/CD concepts and basic application-security scanning.
- Basic Python is helpful for AI labs; local LLM use may need additional CPU/RAM.
- A laptop and access to required lab tools. Optional third-party services may incur charges.

By the end of the program, learners should be able to:

- Integrate AI-assisted analysis into secure CI/CD workflows.
- Apply secure coding and threat-modelling practices with AI-assisted review.
- Identify common LLM application risks, including prompt injection and data exposure.
- Apply least privilege, logging and human approval to AI agent workflows.
- Deliver portfolio evidence through practical security projects.

Program notes

This is practical training, not a certification or job-placement guarantee. AI-generated findings must be validated. Tools and lab scope may vary by environment and licensing.

NEXTGEN DEVSECOPS AI • Learn • Build • Secure • Innovate