DevOpsSchool

Course curriculum · November 2026

LEVEL 04 OF 04 · ADVANCED

Threat Modeling Advanced Training

Scale threat modeling across an organisation with risk-based triage, champions, metrics and coverage of AI and zero trust designs.

LIVE ONLINE **Max 8-10 hours**	CORPORATE (DAY-WISE) **5 days · Days 1-5**	SELF-PACED VIDEO **1-year LMS access**
BATCH SIZE **Max 10 learners**	NEXT BATCHES **1st of every month · weekends: first Saturday**	CERTIFICATE **Verifiable certificate of completion**

Foundation	Essential	Intermediate	Advanced
1 day · Included	2 days · Included	3 days · Included	5 days · This curriculum

INSIDE THIS CURRICULUM

What you will achieve	Outcomes and level focus
Who should attend	Audience and prerequisites
Agenda	45 topics · Foundation to Advanced
Hands-on labs	4 labs
Formats and fees	Live, 1:1, self-paced, corporate
Trainer and reviews	Rajesh Kumar
Enrolment	Batches, payment, contacts

WHY DEVOPSSCHOOL

- Rated 4.6 on Google
- 1,500+ verifiable certificates issued in the public registry
- Trainer Rajesh Kumar: 20 years in industry
- Small batches: max 10 learners, every session recorded

Course page: www.devopsschool.com/courses/threatmodeling/threatmodeling-and-advance-training.html
Talk to us: WhatsApp +91 99057 40781 · +1 (469) 756-6329 · contact@DevOpsSchool.com · reply within 1 hour

OUTCOMES

What you will achieve

By the end of the Threat Modeling course path, you will be able to:

1

Find design flaws early

Use data flow diagrams, STRIDE, attack trees and PASTA to find threats before code is written.

2

Turn threats into action

Rate risks and turn mitigations into tracked backlog work, security tests and pipeline checks.

3

Scale threat modeling

Run a sustainable programme with champions, threat modeling as code, metrics and governance.

WHAT THE ADVANCED LEVEL ADDS

Enterprise programmes, AI systems and governance

Hands-on: Capstone: enterprise threat model and roadmap. Threat model a cloud platform that includes an LLM feature, rate and map threats to ATT&CK and ATLAS, and present a prioritised mitigation roadmap with residual risk.

WHO SHOULD ATTEND

- Experienced Threat Modeling practitioners responsible for quality, security and scale.
- Senior engineers, architects and leads who design and troubleshoot Threat Modeling solutions.
- Teams making Threat Modeling an organisation-wide standard.

BEFORE YOU START

- The Intermediate level, or equivalent hands-on experience.
- You can already: Model cloud, container and API architectures, store models as code and connect threat modeling to CI and security testing.
- Basic computer skills and a laptop with a stable internet connection for the live sessions and labs.
- This curriculum includes every earlier level, so it is complete on its own.

AGENDA · FOUNDATION TO ADVANCED

Threat Modeling Advanced Training agenda

45 topics. Each level builds on the one before it, so this curriculum lists every earlier level in full. Days are for corporate (day-wise) delivery; live online batches cover the same agenda in max 8-10 hours.

DAY 1 — Foundation: Threat modeling concepts, STRIDE and data flows

Included from Foundation

1. Why threat model: finding design flaws before code, shift-left security and the cost of late fixes
2. The four questions: what are we working on, what can go wrong, what will we do about it, did we do a good job
3. Core vocabulary: assets, threats, vulnerabilities, attack surface, trust boundaries and mitigations
4. Data flow diagrams: external entities, processes, data stores, data flows and trust boundaries
5. STRIDE: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege
6. Security properties: mapping STRIDE to authentication, integrity, non-repudiation, confidentiality, availability and authorization
7. Threat Modeling Manifesto: the values and principles behind practical, repeatable threat modeling
8. Tool setup: OWASP Threat Dragon, Microsoft Threat Modeling Tool and draw.io for diagrams
9. First model: diagramming a web application with login, API, database and a third-party payment service
10. Recording threats: clear threat statements, affected element, impact and proposed mitigation
11. Responding to threats: eliminate, mitigate, transfer or accept, with common controls for each STRIDE category

DAY 2 — Essential: Systematic analysis, risk rating and team workflow

Included from Essential

12. Scoping: system decomposition, choosing diagram depth and deciding what is in and out of scope
13. STRIDE per element and per interaction: applying STRIDE systematically across a diagram
14. Attack trees: attacker goals, AND and OR nodes and estimating attacker effort and cost
15. Attack knowledge bases: CAPEC attack patterns, CWE weaknesses, OWASP Top 10 and OWASP API Security Top 10
16. Privacy threats: LINDDUN categories such as linkability, identifiability and disclosure of information
17. Risk rating: OWASP Risk Rating Methodology, CVSS for severity, likelihood and impact matrices and DREAD limits
18. Prioritisation: ranking threats against business impact and deciding what must be fixed before release
19. Workshops: running sessions with developers, architects, testers and product owners in 60 to 90 minutes
20. Tool-based modeling: Microsoft Threat Modeling Tool stencils, auto-generated threats and reports
21. Mitigations to backlog: security user stories, acceptance criteria and linked tickets in Jira or Azure Boards
22. Elevation of Privilege card game: gamified threat discovery to engage development teams
23. Validating the model: review checklists, ownership and keeping models current as the design changes

DAY 3 — Intermediate: Threat modeling as code, cloud and pipelines

Included from Intermediate

24. Threat modeling as code: pytm and Threagile models kept in Git next to the application
25. Pipeline integration: generating diagrams and risk reports in CI and flagging unmitigated high risks
26. Cloud architectures: shared responsibility, IAM misconfiguration, metadata service and storage exposure on AWS and Azure
27. Microservices and APIs: service-to-service authentication, mTLS, API gateways and broken object level authorization

28. Containers and Kubernetes: RBAC, admission control, secrets, network policies and the Kubernetes threat matrix
29. PASTA: the seven-stage risk-centric process aligned to business objectives
30. MITRE ATT&CK: mapping modelled threats to adversary tactics and techniques for detection coverage
31. Software supply chain: dependency confusion, build system compromise and SLSA build levels
32. From model to tests: deriving security test cases, DAST scope and penetration test objectives
33. Agile cadence: lightweight per-feature threat modeling, change triggers and definition of done
34. Common pitfalls: over-scoped diagrams, stale models, missing owners and unactionable findings

DAYS 4-5 **Advanced: Enterprise programmes, AI systems and governance** **New at this level**

35. Programme design: risk-based triage that decides which systems need a full, light or no threat model
36. Metrics: model coverage, mitigation closure time and threats found before versus after release
37. Governance: aligning with Microsoft SDL, NIST SSDF SP 800-218 and ISO/IEC 27001 audit evidence
38. AI and LLM systems: OWASP Top 10 for LLM Applications, prompt injection, data poisoning and MITRE ATLAS
39. Zero trust architecture: modelling identity-centric controls using NIST SP 800-207 principles
40. Mobile and IoT: device trust, firmware updates, physical access and insecure local storage
41. Threat intelligence: refreshing models with incident data, threat intel and red team findings
42. Security champions: training champions, review boards and scaling beyond the security team
43. Reusable knowledge: threat libraries, secure design patterns and architecture decision records
44. Communicating risk: executive summaries, residual risk acceptance and formal sign-off
45. Capstone: an end-to-end threat model and mitigation roadmap for a cloud-native AI-enabled platform

PRACTICE

Hands-on labs

You build these yourself during the course, guided by the trainer.

FOUNDATION **Threat model a simple web application**
Draw a data flow diagram for a login, API and database system in OWASP Threat Dragon and record at least one STRIDE threat and mitigation per trust boundary.

ESSENTIAL **Run a team threat modeling workshop**
Facilitate a STRIDE session on a microservice design, build an attack tree for the top risk and convert the agreed mitigations into prioritised backlog items.

INTERMEDIATE **Model a Kubernetes service as code**
Describe a containerised API on Kubernetes in pytm or Threagile, commit it to Git and generate the diagram and risk report from a CI job.

ADVANCED **Capstone: enterprise threat model and roadmap**
Threat model a cloud platform that includes an LLM feature, rate and map threats to ATT&CK and ATLAS, and present a prioritised mitigation roadmap with residual risk.

HOW YOU CAN LEARN

Formats and fees

The same agenda in four formats. Fees are in Indian rupees as of November 2026; the course page shows them in your currency.

FORMAT	DURATION	WHAT YOU GET	FEE
Live & interactive (online)	Max 8-10 hours	Instructor-led public batch of max 10 learners with demos, labs, Q&A and assignment review. Weekday batches start on the 1st of every month, weekend batches on the first Saturday of every month.	**INR 34,999**
1:1 live training (online)	Max 8-10 hours, one-to-one	The same agenda, taught one-to-one by the trainer. Starts immediately, without waiting for the next batch; sessions planned around your working hours, at your pace.	**INR 99,999**
Self-paced video	1-year LMS access	All four Threat Modeling levels, plus 20+ more courses and 50+ tools, at your own pace.	**INR 833/month** billed yearly at INR 9,996
Corporate (day-wise)	5 days for this level	A private batch for your team, on demand. Foundation 1 day, Essential 2, Intermediate 3, Advanced 5 (cumulative).	**Quote on request**

ASSESSMENT AND CERTIFICATE

Your progress is checked through hands-on labs and assignments at every level. On completion you receive a DevOpsSchool certificate of completion with a unique credential ID that anyone can verify at devopsschool.com/certificates.

INCLUDED WITH EVERY LIVE BATCH

- Every live session is recorded and stays in your LMS for a year.
- Can't attend your batch? Move to next month's batch.
- Free demo class before you pay.
- Free 10-15 minute call with an advisor or the trainer to check the course fits you.

YOUR TRAINER

Learn from Rajesh Kumar

Principal Architect, trainer and mentor in DevOps, SRE, DevSecOps and platform engineering, with 20 years across 8+ software MNCs, including Staff DevOps/SRE Engineer for a leading Japanese mobile-payment platform and Principal DevOps Architect and Manager in Europe.

Profile: www.rajeshkumar.xyz · Videos: youtube.com/@TheDevOpsSchool

20 years in industry	**200+** corporate trainings
10,000+ engineers mentored	**70+** organisations coached

REVIEWS

What learners say

Rated 4.6 on Google · more reviews at devopsschool.com/testimonials and in our video testimonials.

> “Rajesh is very good trainer. Rajesh was able to resolve our queries and question effectively. We really liked the hands-on examples covered during this training program.”
>
> Indrayani, India

> “The training was very useful and interactive. Rajesh helped develop the confidence of all.”
>
> Abhinav Gupta, Pune

START YOUR THREAT MODELING TRAINING

Join the next batch

Weekday batches start on the 1st of every month and weekend batches on the first Saturday of every month, with max 10 learners each. 1:1 training can start immediately; corporate batches run on demand. We reply within 1 hour.

Pay by UPI, credit and debit cards, net banking or PayPal. Before you pay, read our refund policy. All levels of this course: www.devopsschool.com/courses/threatmodeling/

ENROL OR RESERVE A SEAT **Threat Modeling Advanced Training**	WHATSAPP · INDIA **+91 99057 40781**
WHATSAPP · USA **+1 (469) 756-6329**	EMAIL **contact@DevOpsSchool.com**