DATAMARCOS

LIVE ONLINE · MENTOR-LED PROGRAM

AI Security & SecOps

8 weeks · 6–8 hours a week · Part-time, live online

An 8-week, part-time live program for people who already have some IT, security or application background and want an advanced, lab-heavy path: securing AI and LLM applications, and using AI carefully inside security operations. You will threat-model and red-team chat, RAG and agent features, design guardrails and basic governance, then practise AI-assisted detection, triage and incident-response automation with a human approval step. Same length as our Cybersecurity with AI introduction, but built around labs, a scoped red-team and a SOAR-style playbook — not a first-pass survey.

Fees and EMI options shared on a counsellor call.

Program guide · Curriculum, projects and format. No prices are listed in this brochure.

Noida One, 303-304, Rasoolpur Nawada, Industrial Area, Sector 62, Noida, Uttar Pradesh 201309, India

www.datamarcos.com · hello@datamarcos.com · +91 88519 30644

About this program

Who it is for

- Security analysts, SOC, detection and incident-response professionals who want a lab-heavy path into AI-powered SecOps
- Software, platform and security engineers who ship chat, RAG or agent features and need to secure them in depth
- IT and security leads who need both LLM-application security labs and a practical SIEM/SOAR automation exercise with AI
- Learners who can commit 6–8 hours a week for 8 weeks, joining live from anywhere, and who already have some IT or security context

Who it is not for

- People looking for an official CompTIA, SANS, GIAC, (ISC)² or government certificate. This program issues a Datamarcos certificate of completion
- Complete beginners who need a first course in cybersecurity fundamentals
- People who want a first introduction to AI in security. Our 8-week Cybersecurity with AI course is the lighter starting point
- People seeking placement or salary guarantees — we do not offer those

Starting point

- Some exposure to IT, networks, application logs, security operations or application development is expected
- No prior machine-learning or LLM-engineering experience is required
- You should be willing to inspect logs, prompts or playbooks and write down what you actually tested
- If you are new to both cybersecurity and AI applications, start with the 8-week Cybersecurity with AI introduction

What you will be able to do

These are skills and work products from the program — not placement, salary or promotion promises.

- 1. Produce a written threat model of a chat, RAG or agent feature mapped to the OWASP Top 10 for LLM applications
- 2. Run a scoped, documented red-team pass, including prompt injection and data-leakage tests, and record residual risk
- 3. Recommend and sketch guardrails: input and output review, least privilege for tools, fallbacks and a human approval step
- 4. Draft basic AI-governance artefacts: an acceptable-use note, a logging and review plan, and when to involve legal or compliance review
- 5. Design an AI-assisted detection or triage workflow in a SIEM-style setting, with every model claim verified against source evidence
- 6. Build a SOAR-style response playbook with approvals, least privilege, verification and a kill switch — not unsighted automation
- 7. Leave with a capstone pack: an LLM security assessment and a SecOps playbook, not a vendor or professional pentest certification

Projects

Project 1: LLM application threat model and red-team note

A written threat model mapped to the OWASP Top 10 for LLM applications, plus a scoped, documented red-team pass with residual risk.

Project 2: Guardrails and governance pack

Input and output review, least-privilege tool use, a logging and review plan, and a short acceptable-use note. Not a legal or official compliance certificate.

Project 3: Capstone: AI-assisted SecOps playbook

A verified triage or detection workflow and a SOAR-style response playbook with approvals, verification and a kill switch, presented with the LLM security assessment.

DATAMARCOS

Curriculum · 8 weeks

6–8 hours a week, live and mentor-led. Open each week in the live sessions for labs and feedback.

Week 1: Attack surface, OWASP LLM Top 10 and a first-pass threat model

- How chat, retrieval and tool-using agents change the attack surface
- Walking the OWASP Top 10 for LLM applications as a working checklist, not as a certificate
- A lightweight threat-model method: assets, threats, existing controls, residual risk
- Picking one chat, RAG or agent feature you will carry through the labs

Lab: Sketch the system, score it against the OWASP list, and draft a first-pass threat model.
You ship: A system sketch, an OWASP-LLM worksheet and a first-pass threat model.

Week 2: Prompt injection labs

- Direct and indirect prompt injection, including documents and tool output
- Jailbreak-style attempts used only on a practice application you are authorised to test
- Recording steps so an engineer can reproduce a finding
- What a single successful injection does and does not prove

Lab: Run an authorised injection test plan on a practice app and log results.
You ship: An injection findings log.

Week 3: Red-teaming, leakage, tool misuse and guardrails

- Sensitive data in prompts, context windows, logs and retrieved documents
- Tool and agent misuse: unexpected actions and over-broad permissions
- Guardrails you can actually run: input and output review, least privilege, fallbacks and a human step
- A scoped red-team pass: rules of engagement, residual risk, and findings an engineer can act on
- This is structured coursework, not a professional penetration-testing or official red-team certification

Lab: Execute a short test plan, tighten a small set of guardrails, and re-test an earlier finding.
You ship: A red-team report with recommended guardrails and residual risk.

Week 4: Governance, logging and an incident note for AI systems

- Acceptable use, ownership and residual-risk language that does not over-claim
- Public frameworks such as the NIST AI Risk Management Framework used as a map, not as a certificate
- What to log (prompts, retrieval, tool calls) and what must be redacted
- When to involve legal, privacy or compliance review, and a sample incident note

Lab: Draft an acceptable-use note, a logging and review plan, and a sample incident note for your feature.
You ship: A short governance and monitoring pack.

Week 5: AI-assisted detection and log analysis, verified

- What a SIEM-style workflow is for, and where AI may and may not sit
- Writing precise questions over logs or alerts so answers can be checked
- Drafting or translating detection logic with an assistant, then testing it
- Verifying indicators, timestamps and asset names against the source
- You will practise in a SIEM or SOAR-style workflow you can access, or in a practice environment — Datamarcos is not a vendor for those products

Lab: Run an assisted analysis on a sample log or alert set and tick off every claim.
You ship: A verified detection or log-analysis note.

Curriculum (continued)

Week 6: Alert triage and enrichment

- Enrichment, clustering and a first-pass severity suggestion
- True-positive and false-positive discipline
- Writing a triage brief another analyst can pick up
- What not to paste into a public assistant

Lab: Triage a small alert batch with AI assistance and a review checklist.
You ship: A triage pack with enrichment notes and review points.

Week 7: SOAR-style incident response with a kill switch

- Turning a playbook into a SOAR-style workflow: triggers, conditions, actions
- Approvals, least privilege, verification and recovery
- Kill switches and rollback when automation is wrong
- Testing the playbook against a case where the obvious action would be wrong
- Auto-isolation and similar actions only with a clear approval path

Lab: Design a playbook for one incident type, including approval and stop conditions, then failure-test the gates.
You ship: A SOAR-style playbook with human gates and a short automation-risk note.

Week 8: Capstone: assessment, playbook and walk-through

- Assembling the threat model, red-team note, guardrails and governance artefacts
- Assembling the verified SecOps workflow and the SOAR-style playbook
- Live presentations and mentor feedback
- Honest scope: coursework, not an official pentest, GIAC, SANS or vendor certificate

Lab: Present the capstone pack and the checks you ran.

Format, fees and refunds

Part-time and live online, in a small mentor-led cohort. Weekend-morning batches are offered for learners in the US. Evening batches (India time) are offered for learners in the Gulf and Africa. Europe-oriented groups typically meet after work and on Saturdays. Recordings are shared if you miss a live session. Exact days, times and the next cohort date are confirmed on a counsellor call.

Join live from anywhere. Weekend-morning batches are offered for learners in the US; evening batches (India time) for the Gulf and Africa; Europe-oriented groups typically meet after work and on Saturdays.

A Datamarcos certificate of completion is awarded when you finish the program work. Cohort start dates are shared on a counsellor call — we do not publish a date until then.

Fees and EMI options shared on a counsellor call.

7-day refund policy: if the program is not right for you, ask within 7 days of enrollment.

Mentor

Live sessions are mentor-led by Deepesh Mishra, founder of Datamarcos, a BITS Pilani alumnus, and a solution architect and corporate trainer in data and AI who has trained teams at 200+ organizations.

DATAMARCOS

Questions, answered

How is this different from Cybersecurity with AI?

Both programs are 8 weeks and part-time. Cybersecurity with AI is the introduction: a first pass at AI in security operations and at securing LLM applications. AI Security & SecOps is the advanced, lab-heavy course. You spend more time in labs — prompt injection tests, a scoped red-team, guardrails you re-test, basic AI-governance artefacts, and a SIEM/SOAR-style detection, triage and incident-response playbook with approvals and a kill switch. If you want a first course, start with Cybersecurity with AI.

Is this an official CompTIA, SANS, GIAC or government certificate?

No. Completing the program leads to a Datamarcos certificate of completion. We use public frameworks such as the OWASP Top 10 for LLM applications, and we refer to maps such as the NIST AI Risk Management Framework, as working checklists. We do not award, and do not prepare you for, a third-party certification exam.

How long is the program and how much time does it take?

Eight weeks, part-time and live online, at about 6–8 hours a week including the live session and lab work.

Who is it for?

Security, SOC, detection and incident-response professionals, and engineers who ship LLM or agent features and need to secure them in depth. Some IT, logging or security exposure is expected. It is not a first course in cybersecurity fundamentals, and it is not the lighter introduction — that is Cybersecurity with AI.

Are the sessions live?

Yes. Sessions are live and mentor-led, with recordings if you miss a class. Weekend-morning batches are offered for learners in the US, with other regional times available. Exact times are confirmed on a counsellor call.

Will you teach a specific SIEM or SOAR product?

You will practise SIEM- and SOAR-style workflows — detection, triage, enrichment and playbooks with human gates — in a tool you can access or in a practice environment. Datamarcos is not a vendor for those products, and the program is not a vendor certification.

What about fees?

Fees and EMI options shared on a counsellor call.

Is there a refund policy?

Yes. Datamarcos has a 7-day refund policy. If the program is not right for you, ask within 7 days of enrollment.

DATAMARCOS

Talk to a counsellor

Share a few details on datamarcos.com and a counsellor will talk through program fit, the next cohort, fees and enrollment.

Fees and EMI options shared on a counsellor call.

7-day refund policy: if the program is not right for you, ask within 7 days of enrollment.

Noida One, 303-304, Rasoolpur Nawada, Industrial Area, Sector 62, Noida, Uttar Pradesh 201309, India

www.datamarcos.com · hello@datamarcos.com · +91 88519 30644

This brochure does not promise placement, salary or promotion outcomes. It is not legal, immigration or official-government certification advice.