samcommunity.in

✦ ARTIFICIAL INTELLIGENCE · ADVANCED

AI for Cybersecurity

AI-powered defence for modern SOCs.



48	8	SAM-AISOCC
HOURS	MODULES	CERTIFICATION

SAMCOMMUNITY ACADEMY

academy@samcommunity.in

samcommunity.in

✦ INSIDE THIS BROCHURE

Contents

Program overview 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

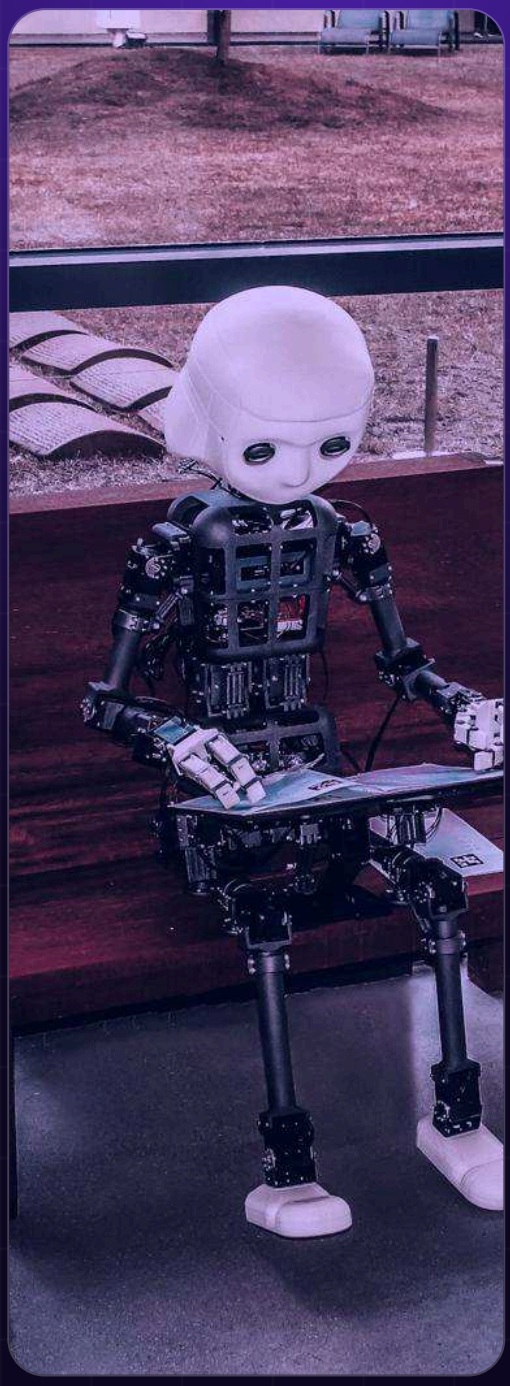
Tools & platforms 10

Projects & capstone 11

Certification & method 12

Learning path 13

FAQs 14



AT A GLANCE

Level	Advanced
Duration	48 Hours
Modules	8
Certificate	SAM-AISOCC

✦ PROGRAM OVERVIEW

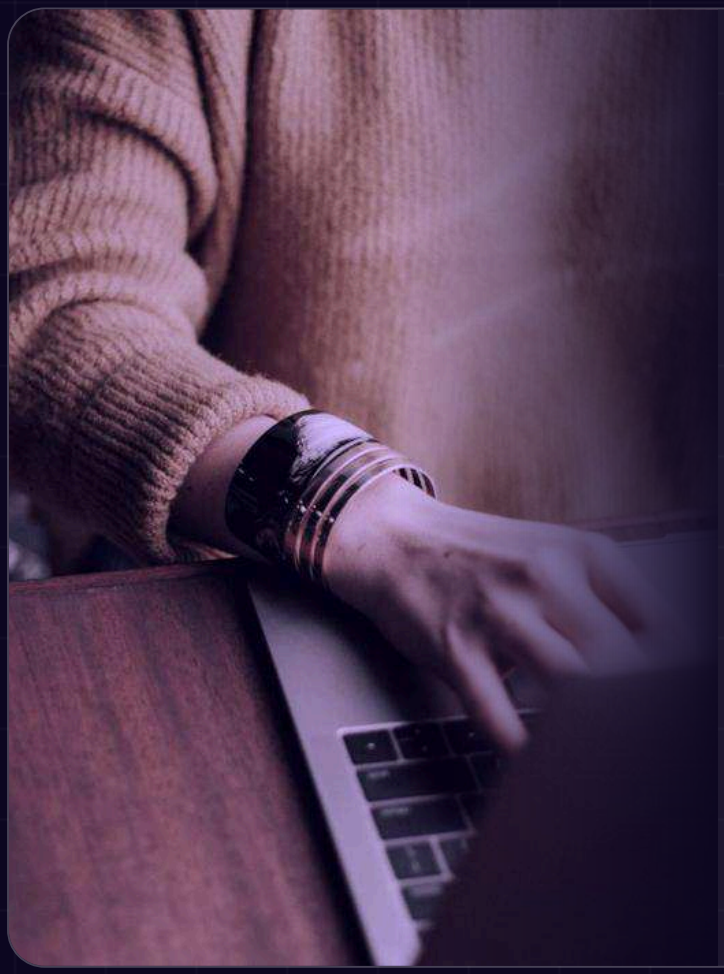
AI-powered defence for modern SOCs.



AI-powered alert triage, LLM-assisted threat hunting and automated playbooks for security operations teams.

Security operations teams face more alerts, data and threats than analysts can manually review. AI and large language models can help triage alerts, enrich context, summarise incidents, assist threat hunting and automate playbooks, when applied carefully with human oversight. This advanced program teaches practical AI-augmented SOC workflows using SIEM, SOAR and LLM tooling, plus how to evaluate AI security tools critically.

LEVEL	DURATION	CERTIFICATION	DELIVERY
Advanced	48 Hours	SAM-AISOCC	Instructor-led · Live virtual · Blended



✦ WHAT YOU'LL PRACTISE

Use AI to triage and prioritise alerts	01
Hunt threats with LLM assistance	02
Automate SOC playbooks	03
Evaluate AI security tools	04

✦ WHO IT'S FOR

Built for people ready to grow.

01

Every professional

AI Fundamentals, ChatGPT, Copilot, Gemini, Claude

02

Developers & data teams

ML, deep learning, NLP, computer vision, MLOps

03

AI engineers

LLM fine-tuning, RAG, vector DBs, AI agents

04

Leaders & public sector

AI for C-suite, government and governance

PREREQUISITES

SOC, SIEM or incident response experience	01
Basic Python scripting	02
Understanding of MITRE ATT&CK and common attack techniques	03

ROLES YOU CAN TARGET

- AI-Augmented SOC Analyst ↗
- Threat Hunter ↗
- Detection Engineer ↗
- Security Automation (SOAR) Engineer ↗
- Incident Responder ↗

✦ LEARNING OUTCOMES

What you'll be able to do.

01 Apply machine learning and LLMs to SOC alert triage

02 Build anomaly detection models on security log data

03 Hunt threats using LLM-assisted queries and analysis

04 Automate enrichment and response playbooks with SOAR and LLMs

05 Generate and validate detection rules with AI assistance

06 Evaluate AI security tools for accuracy, risk and value

HOURS PER MODULE



✦ PROGRAM RUNWAY

Your journey, module by module.

8
MODULES · 48 HRS

01	**AI in Security Operations** SOC workflows and pain points, ML, LLM and agent use cases, Human-in-the-loop principles	4 hrs
02	**Security Data and ML Basics** Log sources and normalisation, Feature engineering for logs, Supervised versus unsupervised detection	6 hrs
03	**Anomaly Detection and UEBA** Isolation Forest and clustering, User and entity behaviour analytics, Baselining normal activity	8 hrs
04	**LLM-Assisted Alert Triage** Alert summarisation with LLMs, Context enrichment pipelines, Prioritisation and scoring	8 hrs
05	**Threat Hunting with AI** Hypothesis-driven hunting, Natural language to SPL and KQL, MITRE ATT&CK mapping	8 hrs
06	**Detection Engineering with AI** Sigma rule generation, Rule testing and validation, Detection-as-code workflows	4 hrs
07	**Automated Playbooks and Agents** SOAR concepts and platforms, Shuffle and n8n playbooks, LLM steps in response workflows	6 hrs
08	**Evaluating and Securing AI Tools** Measuring precision and recall, Vendor AI tool evaluation, Prompt injection in security tools	4 hrs
★	**Capstone · AI-Augmented SOC Workflow** Assessment, capstone review and certification	

✦ DETAILED CURRICULUM

The syllabus.

Modules 01–03

MODULE 01

AI in Security Operations

4 hours

Hands-on lab
Map a SOC workflow and identify safe AI augmentation points.

TOPICS COVERED

- SOC workflows and pain points
- ML, LLM and agent use cases
- Human-in-the-loop principles
- AI risks in the SOC
- Copilot-style security assistants

MODULE 02

Security Data and ML Basics

6 hours

Hands-on lab
Prepare authentication logs and engineer features for analysis in Python.

TOPICS COVERED

- Log sources and normalisation
- Feature engineering for logs
- Supervised versus unsupervised detection
- Python with pandas and scikit-learn
- Elastic Common Schema

Elastic · Python · pandas · scikit-learn

MODULE 03

Anomaly Detection and UEBA

8 hours

Hands-on lab
Detect anomalous logins with Isolation Forest and Elastic ML jobs.

TOPICS COVERED

- Isolation Forest and clustering
- User and entity behaviour analytics
- Baselining normal activity
- Reducing false positives
- Splunk MLTK and Elastic ML

Splunk · Elastic



LEARN BY DOING

8 guided labs, one in every module.

✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 04–06

MODULE 04

LLM-Assisted Alert Triage

8 hours

Hands-on lab
Build an LLM triage assistant that summarises and scores SIEM alerts.

TOPICS COVERED

- Alert summarisation with LLMs
- Context enrichment pipelines
- Prioritisation and scoring
- Structured triage outputs
- Handling sensitive data safely

MODULE 05

Threat Hunting with AI

8 hours

Hands-on lab
Hunt for lateral movement using LLM-generated and analyst-validated queries.

TOPICS COVERED

- Hypothesis-driven hunting
- Natural language to SPL and KQL
- MITRE ATT&CK mapping
- Threat intelligence summarisation
- RAG over threat reports

MODULE 06

Detection Engineering with AI

4 hours

Hands-on lab
Generate Sigma rules with AI and validate them against test data.

TOPICS COVERED

- Sigma rule generation
- Rule testing and validation
- Detection-as-code workflows
- Atomic Red Team testing
- Avoiding AI-generated rule errors

LEARN BY DOING

8 guided labs, one in every module.



✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 07–08

MODULE 07

Automated Playbooks and Agents

6 hours

Hands-on lab
Build a phishing response playbook with LLM analysis and human approval.

TOPICS COVERED

- SOAR concepts and platforms
- Shuffle and n8n playbooks
- LLM steps in response workflows
- Agentic investigation assistants
- Approval gates for actions

n8n

MODULE 08

Evaluating and Securing AI Tools

4 hours

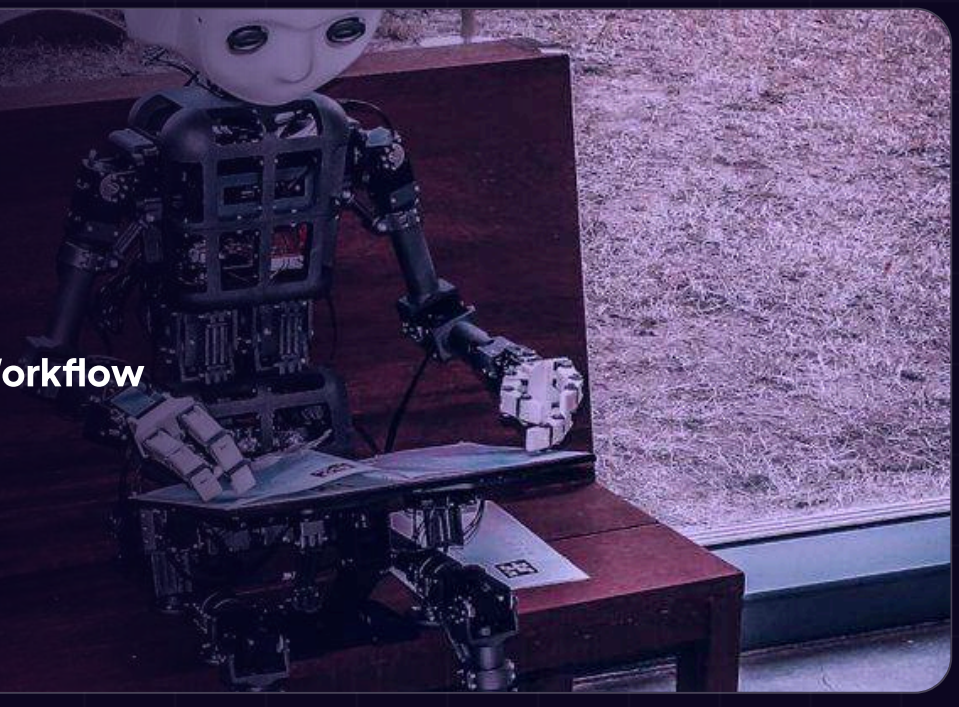
Hands-on lab
Score an AI triage assistant's accuracy against labelled alerts.

TOPICS COVERED

- Measuring precision and recall
- Vendor AI tool evaluation
- Prompt injection in security tools
- Data privacy and governance
- Building an AI SOC roadmap

CAPSTONE

AI-Augmented SOC Workflow



✦ YOUR STACK

Tools you'll build with.

Real platforms and frameworks — the same stack modern teams ship with, practised in cloud-hosted labs.

Splunk
SIEM search, dashboards & alerting

Elastic
ELK / Elastic SIEM analytics

Python
Automation & scripting

OpenAI
GPT models & APIs

pandas
Data wrangling

scikit-learn
Classic machine learning

n8n
Workflow automation



FRAMEWORKS & STANDARDS

MITRE ATT&CK

✦ HANDS-ON WORK

Projects that prove you can do it.

01

Anomalous Login Detector

Train and tune an anomaly detection model on authentication logs and integrate results into SIEM dashboards.

02

LLM Alert Triage Assistant

Build an assistant that enriches, summarises and prioritises alerts with structured output and analyst feedback.

03

AI Phishing Playbook

Automate phishing email analysis with LLM classification, IOC extraction, enrichment and approval-gated response actions in SOAR.

CAPSTONE PROJECT

AI-Augmented SOC Workflow

Design and build an end-to-end AI-augmented SOC workflow combining log analytics, anomaly detection, LLM triage, AI-assisted hunting and automated playbooks with human approval, then evaluate accuracy and present operational and risk findings.

Real-world scenario | Mentor review | Portfolio ready



CERTIFICATION

SAM-AISOCC

Awarded on successful completion of the program assessments.

- MCQ assessments
- Practical lab evaluation
- Project & capstone review
- Final presentation



✦ HOW YOU LEARN

The SAM Learning Framework™

PHASE 01

S

Scenario

Real-world attack and use-case scenarios open every module.

PHASE 02

A

Apply

Hands-on lab work, CTF challenges and live projects.

PHASE 03

M

Master

Assessment, peer review and certification prep.

PHASE 04

M

Mentor

Post-program career guidance and support.

DELIVERY MODELS

- Instructor-Led (ILT)
- Virtual Instructor-Led
- Self-Paced Online
- E-Learning Licensing
- Blended Learning
- Corporate Onsite
- Bootcamp Intensive
- Hackathon / CTF
- Mentorship

✦ LEARNING PATH · AI AUTOMATION & ENTERPRISE INTEGRATION

Where this program fits.

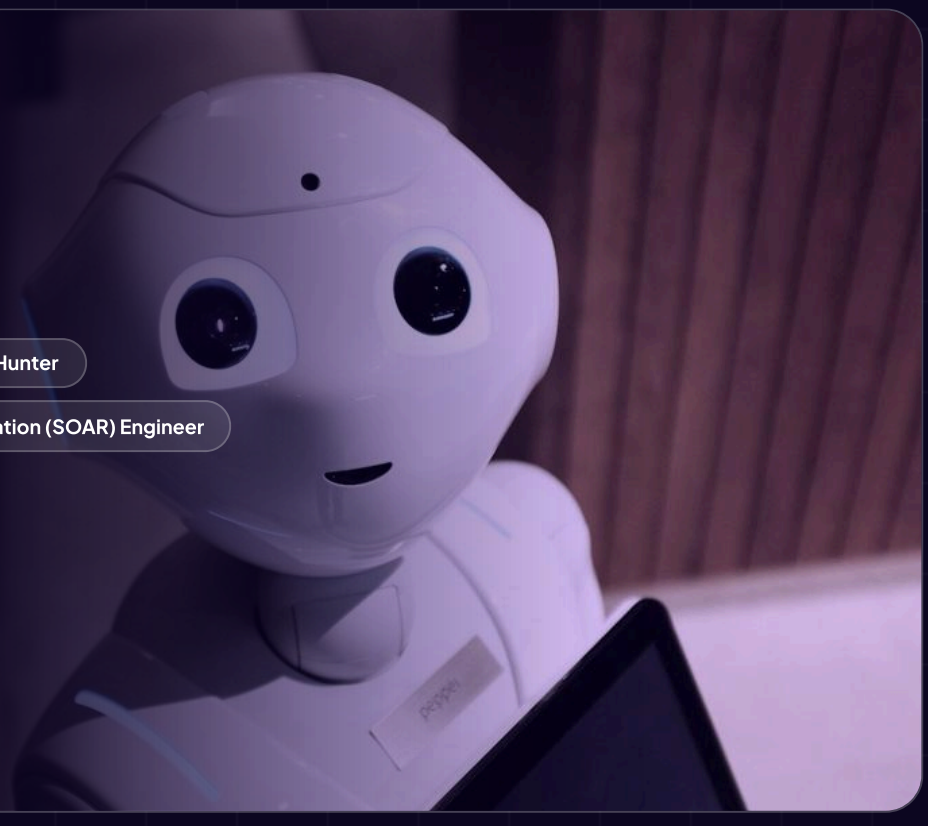
Intermediate	Advanced
2 programs	You are here

BEFORE THIS

AI Automation with n8n / Make / Zapier	32 Hours
Microsoft Power Platform + Copilot Studio	40 Hours

UP NEXT

The top of this pathway — explore related tracks.



CAREER ROLES

- AI-Augmented SOC Analyst
- Threat Hunter
- Detection Engineer
- Security Automation (SOAR) Engineer
- Incident Responder

✦ FAQS

Questions, answered.

Q01

Do I need prior experience to join?

Yes. You should have SOC, SIEM or incident response experience, basic Python skills and familiarity with MITRE ATT&CK. This advanced program builds on security operations knowledge rather than teaching SOC fundamentals.

Q02

How is the program delivered and scheduled?

The program is instructor-led and delivered as live virtual or blended sessions. Batch timings, weekday or weekend schedules and session lengths are shared at enrolment, and recordings or notes support revision between sessions.

Q03

What certification will I receive?

Learners who complete the sessions, labs and final assessments are awarded the Samcommunity Academy SAM-AISOCC certificate. It is issued after successful assessment, not on attendance alone, and reflects the practical skills covered in the program.

Q04

Will I get access to labs and tools?

Yes. Labs use Splunk free or trial editions, the Elastic Stack, Python with scikit-learn, Shuffle or n8n, and LLM APIs, with sample security datasets. All exercises run in isolated lab environments with guided setup.

Q05

Is there career support after the program?

Learners receive guidance on portfolio projects, resume positioning and interview preparation related to the skills covered. Career support is advisory; the program does not guarantee job placement, specific roles or salary outcomes.



✦ LET'S TALK

Start AI for Cybersecurity with Samcommunity.

INDIVIDUALS

academy@samcommunity.in

Batches, enrolment & career guidance

CORPORATE & INSTITUTIONS

corporate@samcommunity.in

Team batches & custom programs

Xylyn Samcommunity Private Limited · DPIIT-recognized startup · Surat, Gujarat, India