samcommunity.in

✦ EMERGING TECHNOLOGIES · INTERMEDIATE

IoT Security & Architecture

Secure the connected world.



48	7	SAM-IOTSEC
HOURS	MODULES	CERTIFICATION

✦ 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	Intermediate
Duration	48 Hours
Modules	7
Certificate	SAM-IOTSEC

✦ PROGRAM OVERVIEW

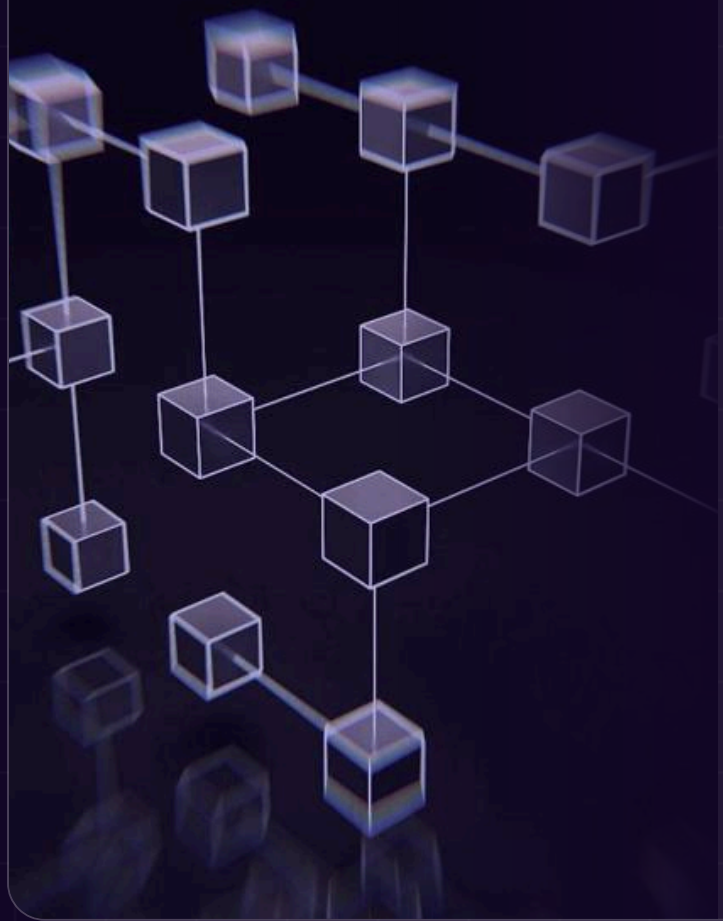
Secure the connected world.



Secure IoT devices, networks and platforms end to end.

Connected devices often ship with weak credentials, outdated firmware and insecure communications, making them attractive targets. As IoT spreads across homes, industry and healthcare, secure design is essential. This intermediate program teaches IoT threat modelling, device and firmware security, secure communications, cloud platform protection and monitoring, aligned with OWASP IoT guidance and recognised standards.

LEVEL	DURATION	CERTIFICATION	DELIVERY
Intermediate	48 Hours	SAM-IOTSEC	Instructor-led · Live virtual · Blended



✦ WHAT YOU'LL PRACTISE

Threat-model IoT systems	01
Secure devices and firmware	02
Protect IoT communications	03
Monitor IoT environments	04

✦ WHO IT'S FOR

Built for people ready to grow.

01

Curious professionals

Quantum, blockchain, IoT and AR/VR fundamentals

02

Developers

Solidity, XR development, edge AI / TinyML

03

Security teams

Quantum-safe crypto, IoT and 5G security

04

Innovation teams

Digital twins and emerging-tech strategy

PREREQUISITES

Networking fundamentals including TCP/IP	01
Basic Linux command-line skills	02
Familiarity with IoT concepts or devices	03

ROLES YOU CAN TARGET

- IoT Security Engineer ↗
- Embedded Security Analyst ↗
- OT/IoT Security Specialist ↗
- Security Architect (IoT) ↗
- Penetration Tester (IoT) ↗

✦ LEARNING OUTCOMES

What you'll be able to do.

01 Threat-model IoT systems using STRIDE and OWASP IoT guidance

02 Analyse firmware for hardcoded secrets and vulnerabilities

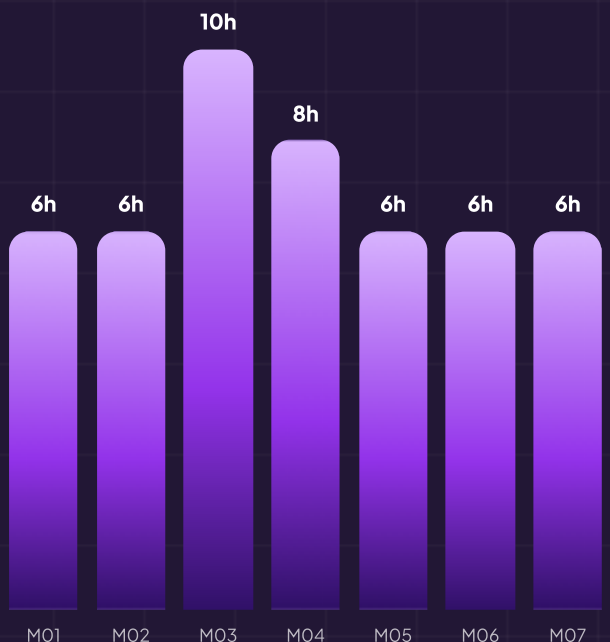
03 Secure device boot, updates and identity management

04 Protect MQTT and wireless communications with TLS and authentication

05 Harden IoT cloud platforms and APIs

06 Monitor IoT networks to detect anomalous device behaviour

HOURS PER MODULE



✦ PROGRAM RUNWAY

Your journey, module by module.

7
MODULES · 48 HRS

01	**IoT Architecture and Attack Surface** IoT reference architectures, Device, network, cloud attack surfaces, OWASP IoT Top 10	6 hrs
02	**Threat Modelling IoT Systems** STRIDE methodology, Data flow diagrams for IoT, Risk rating and prioritisation	6 hrs
03	**Device and Firmware Security** Hardware interfaces: UART and JTAG, Firmware extraction techniques, Firmware analysis with binwalk	10 hrs
04	**Securing IoT Communications** MQTT security and authentication, TLS and certificate-based device identity, Bluetooth LE security	8 hrs
05	**Cloud and API Security** IoT cloud platform security models, Device provisioning and identity, API authentication and authorisation	6 hrs
06	**Monitoring and Incident Response** Network segmentation for IoT, Device inventory and discovery, Anomaly detection for devices	6 hrs
07	**Standards, Compliance and Secure Design** ETSI EN 303 645, IEC 62443 for industrial IoT, NIST IR 8259 baseline	6 hrs
★	**Capstone · Secure IoT Solution Design** Assessment, capstone review and certification	

✦ DETAILED CURRICULUM

The syllabus.

Modules 01–03

MODULE 01

IoT Architecture and Attack Surface

6 hours

Hands-on lab
Map the attack surface of a sample smart home system.

TOPICS COVERED

- IoT reference architectures
- Device, network, cloud attack surfaces
- OWASP IoT Top 10
- Notable IoT attacks such as Mirai
- IoT security standards overview

OWASP

MODULE 02

Threat Modelling IoT Systems

6 hours

Hands-on lab
Build a STRIDE threat model for an industrial sensor network.

TOPICS COVERED

- STRIDE methodology
- Data flow diagrams for IoT
- Risk rating and prioritisation
- Security requirements definition
- Attack trees for connected devices

MODULE 03

Device and Firmware Security

10 hours

Hands-on lab
Extract and analyse firmware to find hardcoded credentials.

TOPICS COVERED

- Hardware interfaces: UART and JTAG
- Firmware extraction techniques
- Firmware analysis with binwalk
- Secure boot and root of trust
- Secure OTA updates

LEARN BY DOING

7 guided labs, one in every module.



✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 04–05

MODULE 04

Securing IoT Communications

8 hours

Hands-on lab
Capture insecure MQTT traffic, then secure it with TLS.

TOPICS COVERED

- MQTT security and authentication
- TLS and certificate-based device identity
- Bluetooth LE security
- Zigbee and LoRaWAN security
- Traffic analysis with Wireshark

Wireshark

MODULE 05

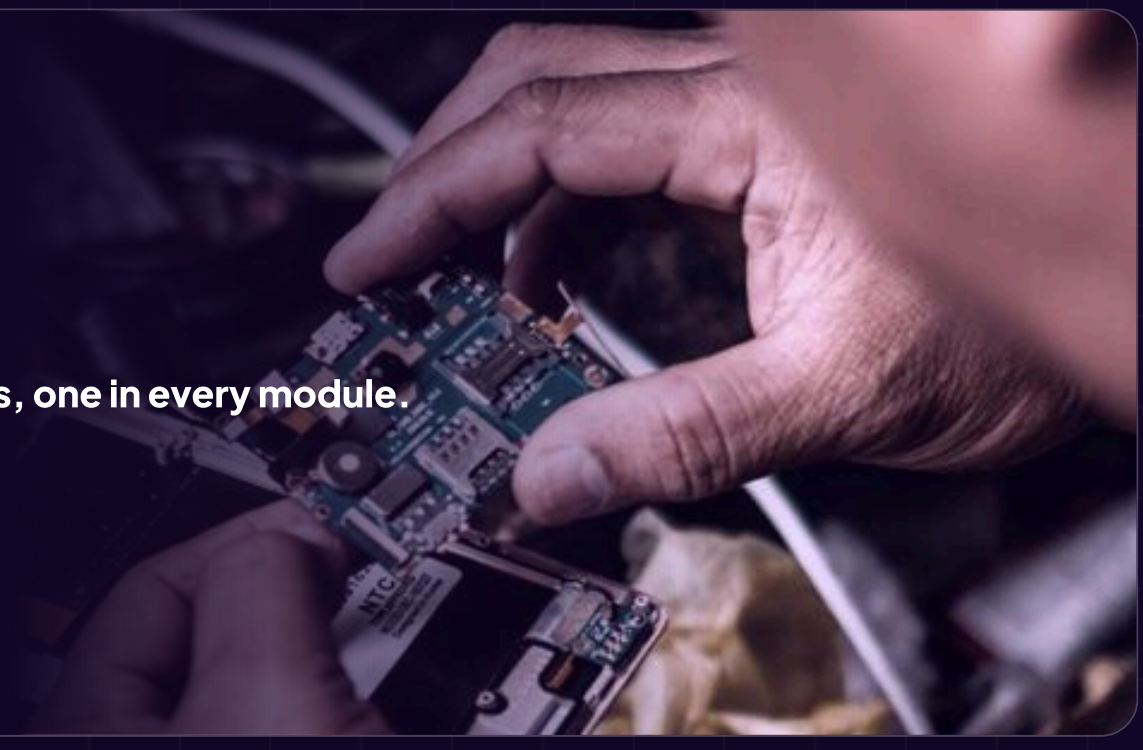
Cloud and API Security

6 hours

Hands-on lab
Audit an IoT cloud API for authentication and access weaknesses.

TOPICS COVERED

- IoT cloud platform security models
- Device provisioning and identity
- API authentication and authorisation
- Data protection at rest and in transit
- Mobile companion app risks



LEARN BY DOING

7 guided labs, one in every module.

✦ DETAILED CURRICULUM

Syllabus, continued.

Modules 06–07

MODULE 06

Monitoring and Incident Response

6 hours

Hands-on lab
Detect anomalous device behaviour using Zeek and network baselines.

TOPICS COVERED

- Network segmentation for IoT
- Device inventory and discovery
- Anomaly detection for devices
- IoT incident response playbooks
- Vulnerability disclosure and patching

MODULE 07

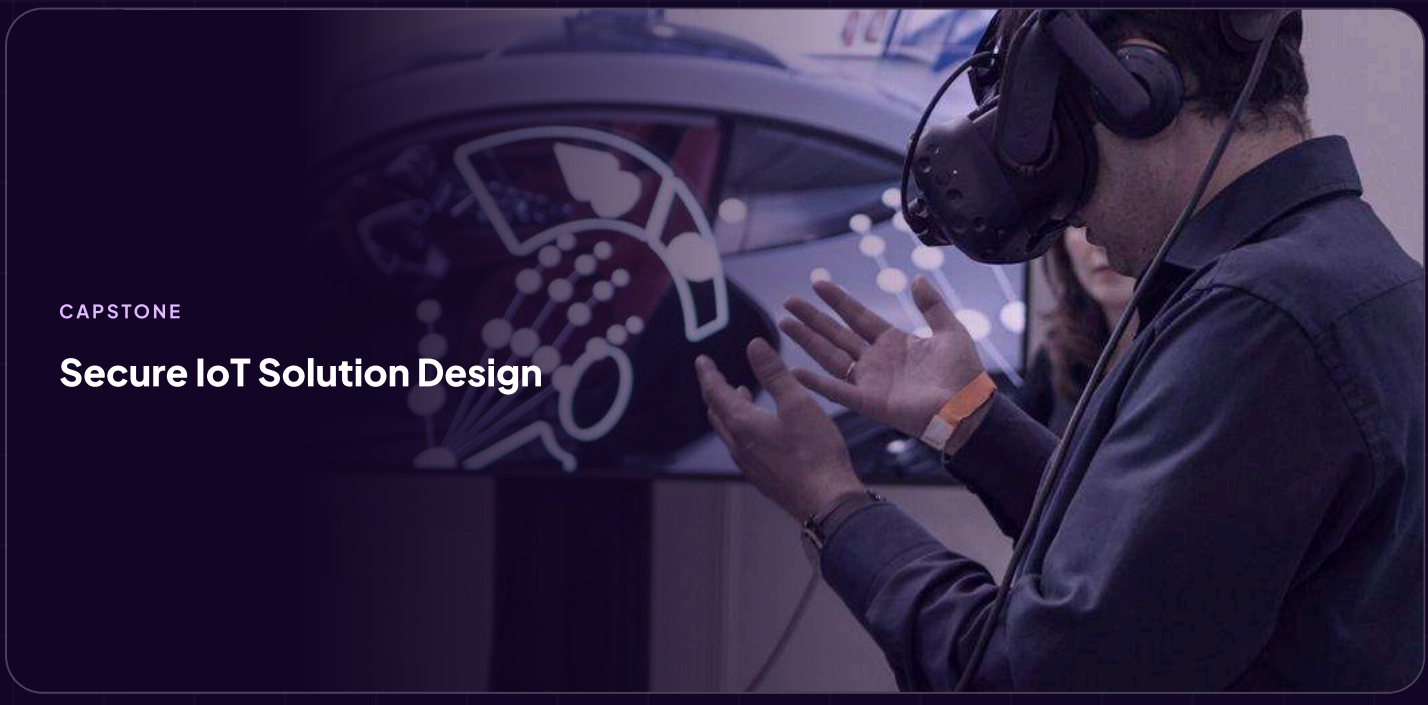
Standards, Compliance and Secure Design

6 hours

Hands-on lab
Assess a device against ETSI EN 303 645 provisions.

TOPICS COVERED

- ETSI EN 303 645
- IEC 62443 for industrial IoT
- NIST IR 8259 baseline
- Secure-by-design development lifecycle
- EU Cyber Resilience Act overview



CAPSTONE

Secure IoT Solution Design

✦ YOUR STACK

Tools you'll build with.

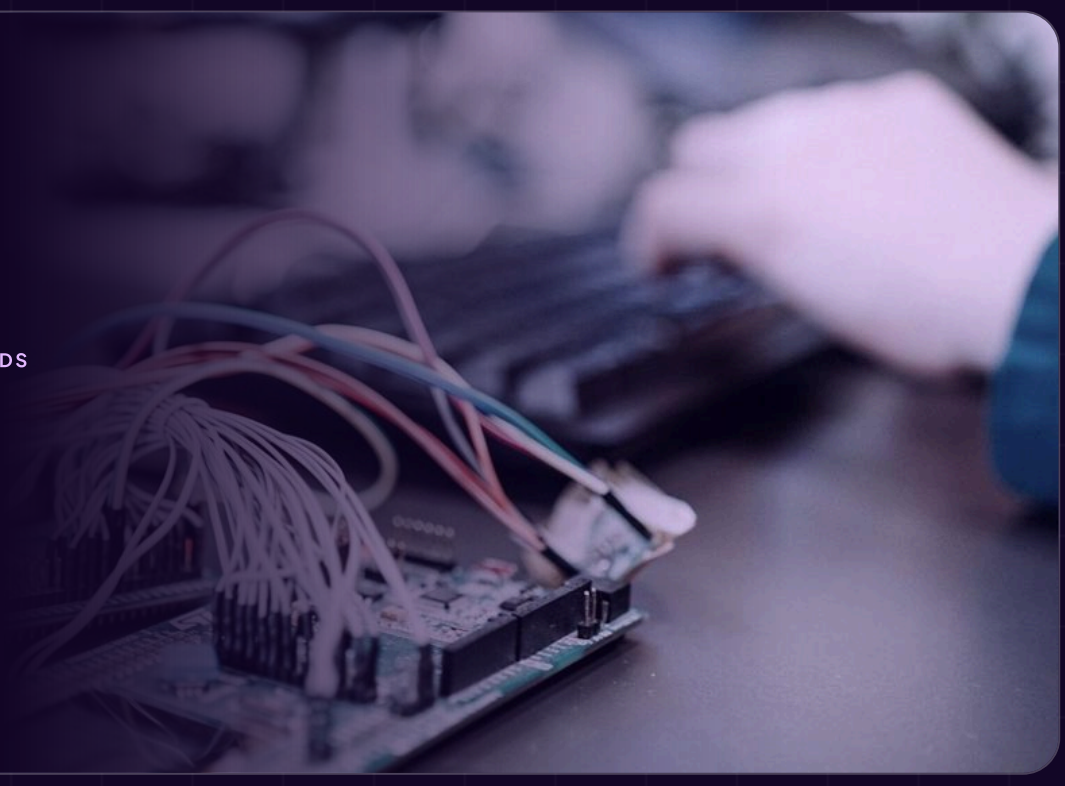
Real platforms and frameworks — the same stack modern teams ship with, practised in cloud-hosted labs.

Raspberry Pi
Edge computing board

Wireshark
Packet capture & traffic analysis

Linux
Server & CLI fundamentals

OWASP
Top 10 & testing standards



FRAMEWORKS & STANDARDS

OWASP

✦ HANDS-ON WORK

Projects that prove you can do it.

01

IoT Threat Model

Create a complete STRIDE threat model with data flows, risks and mitigations for a connected product.

02

Firmware Security Analysis

Analyse a sample firmware image for hardcoded secrets, outdated components and insecure services, then document weaknesses and practical remediation steps.

03

Secure MQTT Deployment

Deploy an MQTT broker with TLS, authentication and access control lists, then verify protection with packet captures.

CAPSTONE PROJECT

Secure IoT Solution Design

Design and build a secured IoT prototype on Raspberry Pi, covering threat modelling, hardened firmware and device identity, encrypted communications, segmented networking and monitoring, then demonstrate defences against simulated attacks.

Real-world scenario | Mentor review | Portfolio ready



CERTIFICATION

SAM-IOTSEC

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 · EMERGING TECHNOLOGIES

Where this program fits.

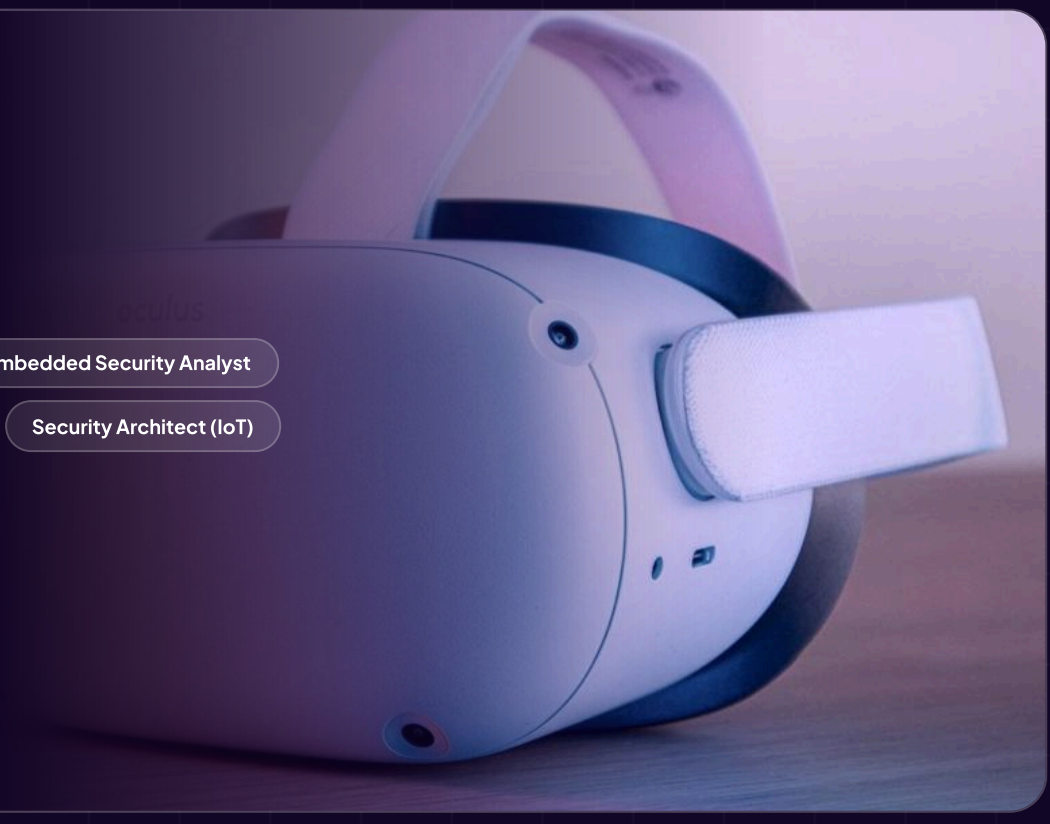
Foundation	Intermediate	Advanced
4 programs	You are here	4 programs

BEFORE THIS

Quantum Computing Fundamentals	32 Hours
Blockchain & Web3 Fundamentals	32 Hours
IoT & Edge Computing Fundamentals	32 Hours
AR/VR & Immersive Technologies	24 Hours

UP NEXT

Smart Contract Auditing	48 Hours
Edge AI & TinyML	48 Hours
Digital Twin Technology	40 Hours
Extended Reality (XR) Development	56 Hours



CAREER ROLES

- IoT Security Engineer
- Embedded Security Analyst
- OT/IoT Security Specialist
- Security Architect (IoT)
- Penetration Tester (IoT)

✦ FAQS

Questions, answered.

Q01

Do I need prior experience to join?

You should understand networking basics and be comfortable with the Linux command line. Some exposure to IoT devices or security concepts helps. Electronics expertise is not required, as hardware interfaces are demonstrated step by step.

Q02

How is the program delivered and scheduled?

The 48 hours program is instructor-led and delivered live virtual or blended, combining concept sessions, demonstrations and guided hands-on work. Batch timings and session frequency are confirmed with the academy team at enrollment.

Q03

Will I receive a certificate?

Yes. Participants who attend the required sessions and pass the program assessments, including practical tasks and a capstone review, receive the Samcommunity Academy SAM-IOTSEC certificate for IoT Security & Architecture.

Q04

What labs and tools will I have access to?

Labs use Raspberry Pi, Linux, Wireshark, Mosquitto, binwalk and Zeek, with sample firmware images in virtual environments. Hardware kit arrangements and setup guidance are shared at enrollment.

Q05

Is career support provided?

Yes. You receive guidance on building a portfolio from your projects, presenting skills on your resume and preparing for interviews. Career support helps you present yourself well, but job placement, interviews and salaries are not guaranteed.



✦ LET'S TALK

Start IoT Security & Architecture 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