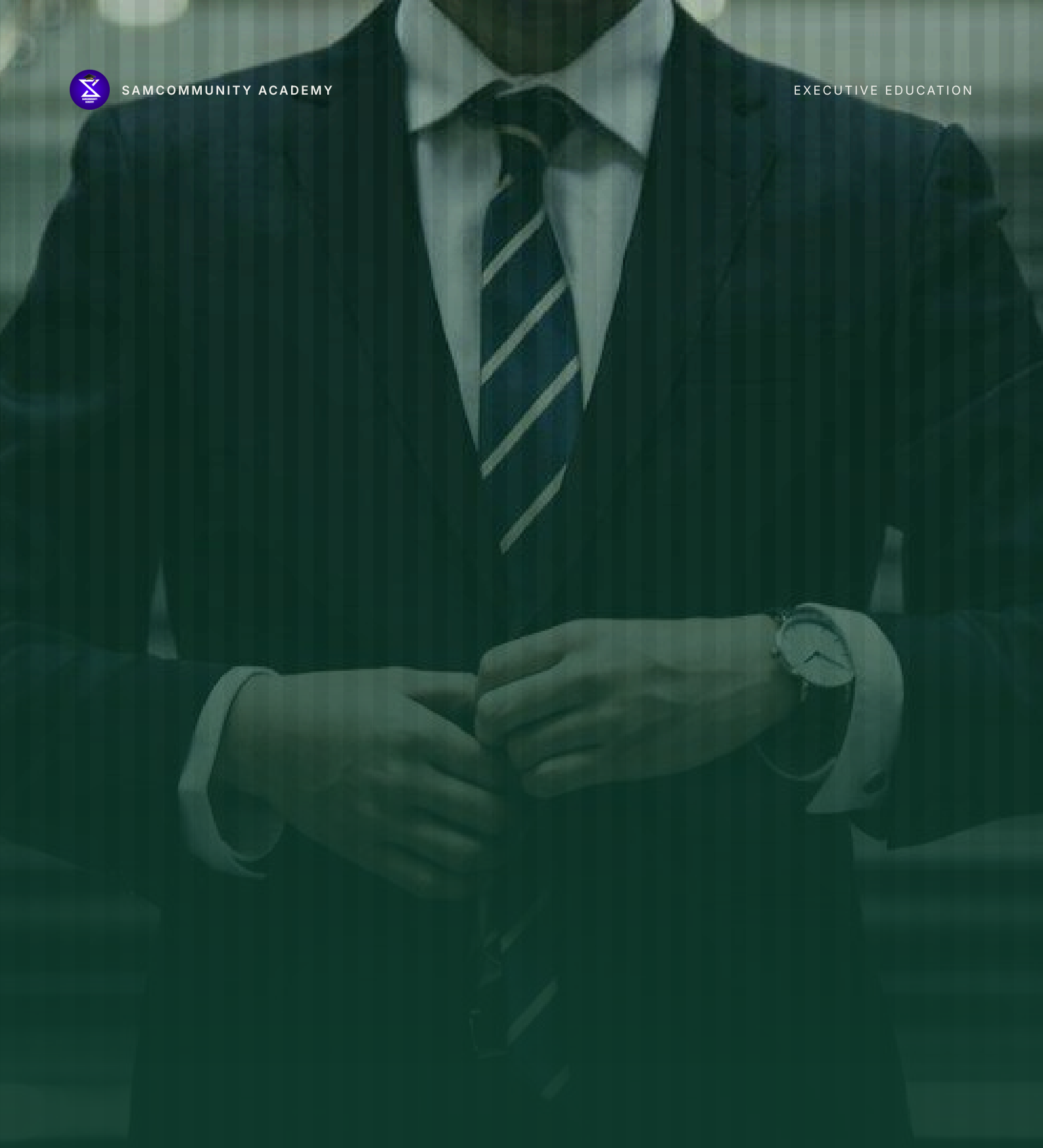


EXECUTIVE EDUCATION PROGRAMS · EXECUTIVE

National Security & Cyber Policy

Cyber in national security.

Contents

Why this program 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

Frameworks & tools 09

Projects & capstone 10

Certification & method 11

Learning path 12

FAQs 13



LEVEL	Executive
DURATION	24 Hours
MODULES	6
CERTIFICATE	SAM-NSCPG

Why this program

Cyber policy, strategy and national security for senior government leaders.

Cyberspace is now a central domain of national security, affecting critical infrastructure, elections, economic stability and public trust. Senior government leaders must understand evolving threats and shape coordinated policy responses. This program examines the cyber threat landscape, national cyber strategy and institutions, critical infrastructure protection, international norms, and inter-agency coordination for effective cyber policymaking.



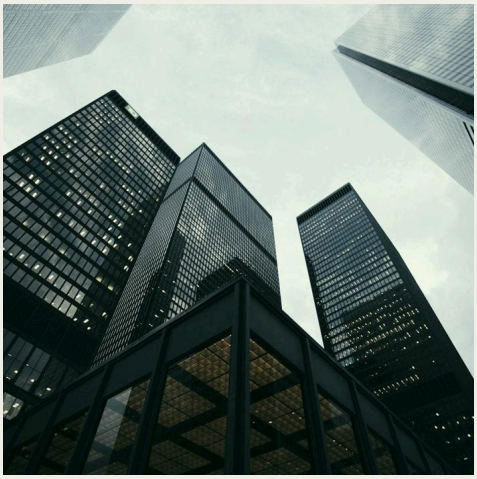
24 hours of compact, practical sessions

6 focused modules, built around real work

3 projects plus a capstone presentation



Who this program is for



01

Board members & directors

AI and technology risk governance

02

CXOs

AI strategy, data-driven leadership

03

CISOs & CIOs

CISO leadership program

04

Senior government officials

National security & cyber policy

PREREQUISITES

- Senior role in government or public sector
- Experience in policy, security or administration
- No technical background required

DESIGNED FOR

- Senior Civil Servant
- Policy Advisor (Cyber or Security)
- Defence and Law Enforcement Officer
- Regulator or PSU Leader
- Critical Infrastructure Executive

What you'll be able to do.

01 Analyse state-sponsored, criminal and hacktivist cyber threats

02 Examine national cyber strategies, institutions and legal frameworks

03 Evaluate critical information infrastructure protection approaches

04 Coordinate cyber incident response across agencies and sectors

05 Assess international cyber norms, diplomacy and cooperation

06 Develop practical cyber policy recommendations for government

How the program works

The Cyber Threat Landscape

State-sponsored threat actors, Cybercrime and ransomware ecosystems, Hacktivism and influence operations, Supply chain and espionage threats.

National Cyber Strategy and Institutions

Elements of national cyber strategy, India's cyber institutions: CERT-In, NCIIPC, IT Act and DPDP Act, Comparative national strategies.

Critical Infrastructure Protection

Critical information infrastructure sectors, OT and industrial control risks, Sector regulators and standards, Resilience and continuity planning.

Cyber Incident Coordination

National incident response frameworks, Inter-agency coordination models, Information sharing mechanisms, Crisis communication.

01 · The Cyber Threat Landscape	4 hrs
02 · National Cyber Strategy and Institutions	4 hrs
03 · Critical Infrastructure Protection	4 hrs
04 · Cyber Incident Coordination	4 hrs
05 · International Cyber Policy	4 hrs
06 · Shaping Cyber Policy	4 hrs
★ Capstone · National Cyber Policy Proposal	



The curriculum

MODULES 01–03

01 The Cyber Threat Landscape

4 HOURS

Practical: Analyse a public threat report and brief on implications for government.

- State-sponsored threat actors
- Cybercrime and ransomware ecosystems
- Hacktivism and influence operations
- Supply chain and espionage threats
- AI-enabled threats and deepfakes

02 National Cyber Strategy and Institutions

4 HOURS

Practical: Compare two national cyber strategies and identify lessons for policymakers.

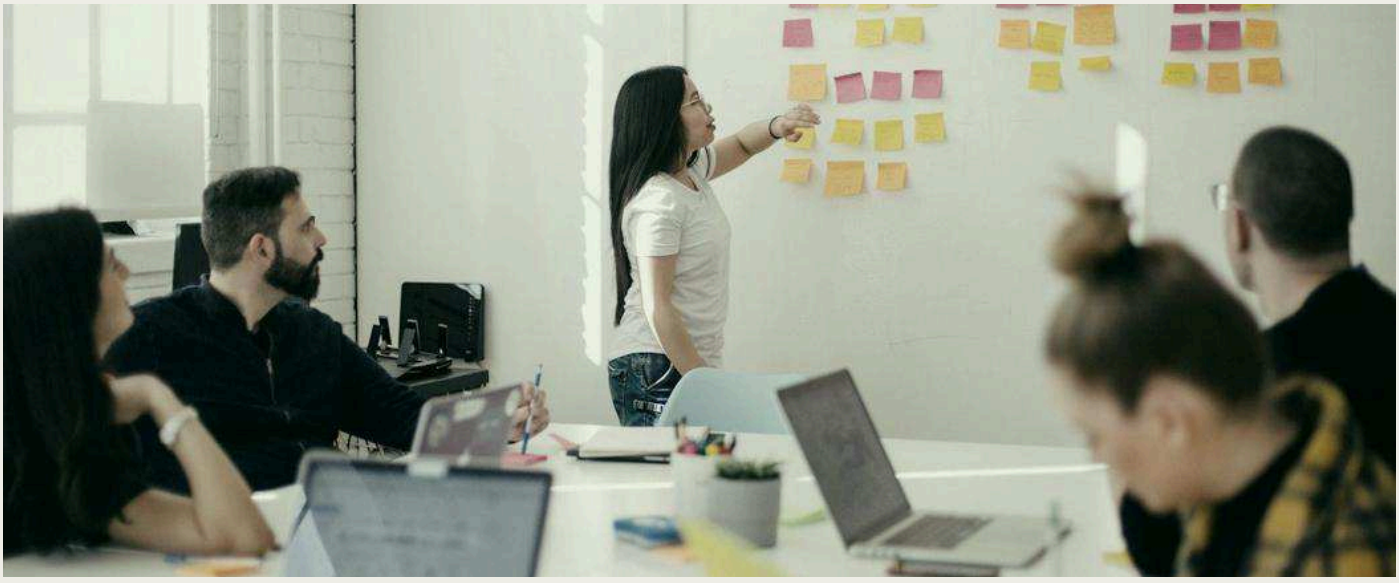
- Elements of national cyber strategy
- India's cyber institutions: CERT-In, NCIIPC
- IT Act and DPDP Act
- Comparative national strategies
- Public-private partnerships

03 Critical Infrastructure Protection

4 HOURS

Practical: Assess cyber risk to a critical sector and propose protective measures.

- Critical information infrastructure sectors
- OT and industrial control risks
- Sector regulators and standards
- Resilience and continuity planning
- Supply chain security policy



Curriculum, continued

MODULES 04–06

04 Cyber Incident Coordination

4 HOURS

Practical: Coordinate a multi-agency response in a national-scale cyber incident simulation.

- National incident response frameworks
- Inter-agency coordination models
- Information sharing mechanisms
- Crisis communication
- Attribution and response options

05 International Cyber Policy

4 HOURS

Practical: Prepare a negotiating position on a proposed international cyber norm.

- International law in cyberspace
- UN processes on cyber norms
- Cyber diplomacy and alliances
- Cross-border cybercrime cooperation
- Technology and export controls

06 Shaping Cyber Policy

4 HOURS

Practical: Draft a short policy brief recommending a cyber capacity-building initiative.

- Policy design and evaluation
- Cyber workforce and capacity building
- Emerging technology policy: AI, quantum
- Balancing security, privacy and rights
- Measuring policy effectiveness



What you'll focus on.

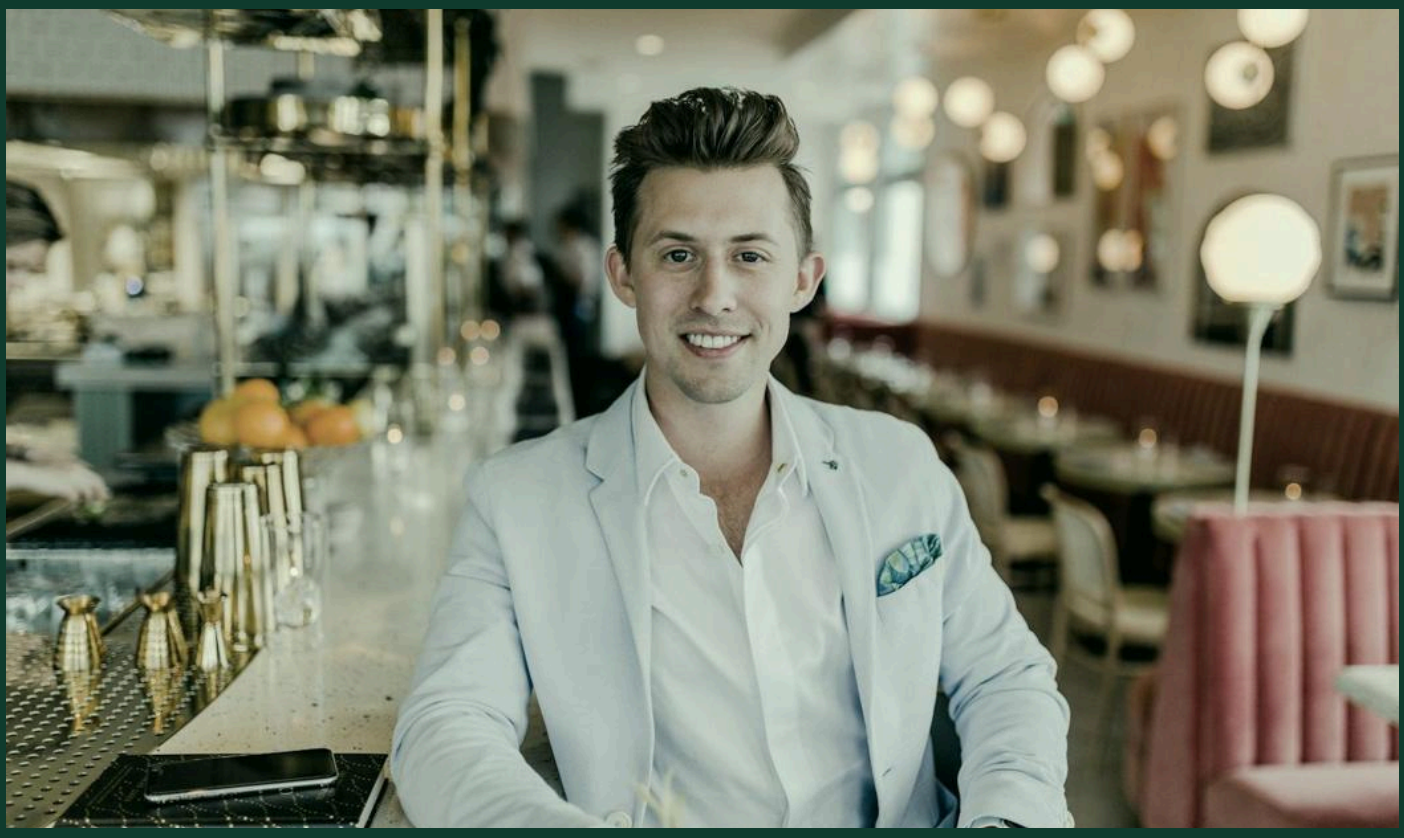
DPDP Act 01

CERT-In 02

The Cyber Threat Landscape 03

National Cyber Strategy and Institutions 04

Critical Infrastructure Protection 05



Projects & capstone

01

Threat Assessment Brief

Produce a concise threat assessment for a government department, highlighting priority actors, risks and implications.

02

Strategy Comparison Paper

Compare national cyber strategies across several countries and recommend practices that are relevant to the Indian context.

03

Incident Coordination Plan

Design a coordination plan defining agency roles, information flows and escalation for a major cyber incident.



CAPSTONE

National Cyber Policy Proposal

Develop a policy proposal addressing a national cyber challenge, covering threat analysis, institutional roles, legal considerations, international dimensions and implementation steps, and present it to a mock senior policy committee.

CERTIFICATION

SAM-NSCPG

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™

01 Scenario

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

02 Apply

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

03 Master

Assessment, peer review and certification prep.

04 Mentor

Post-program career guidance and support.



Delivery: Instructor-Led (ILT) · Virtual Instructor-Led · Self-Paced Online · E-Learning Licensing · Blended Learning · Corporate Onsite

Where this program fits

Executive

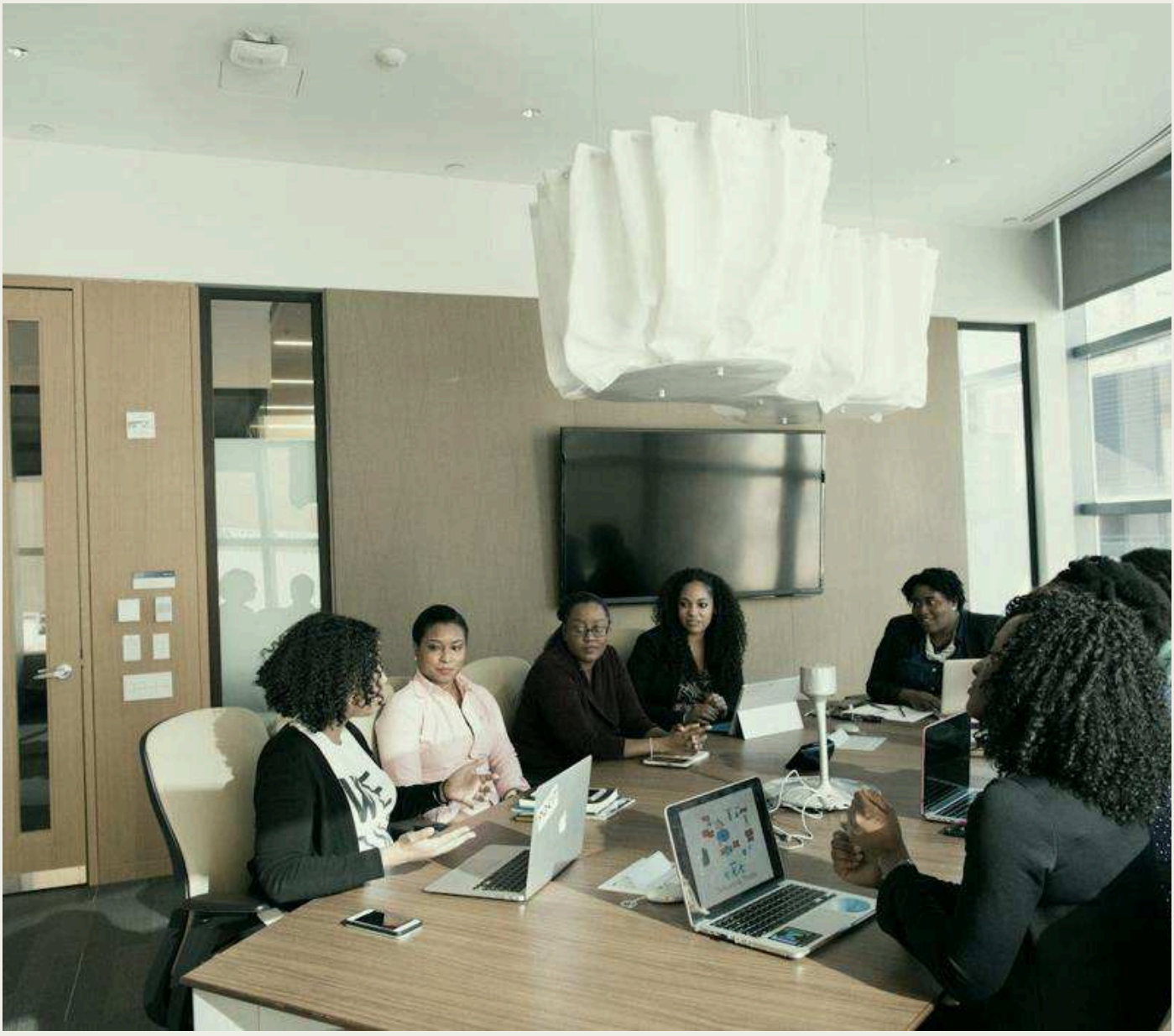
You are here

BEFORE THIS

A starting point — no prerequisite program needed.

UP NEXT

The top of this pathway — explore related programs.



Questions, answered

Do I need prior experience to join?

No technical background is required. The program is designed for senior government and public-sector leaders, focusing on policy, strategy and coordination rather than technical security operations.

How is the program delivered and scheduled?

Delivery is instructor-led, live virtual or blended, and can be arranged as a dedicated cohort for government departments. Schedules are confirmed in advance, and content uses publicly available, unclassified information and case studies.

What certification will I receive?

Learners who attend the sessions and pass the required assessments receive the Samcommunity Academy SAM-NSCPG certificate of completion. It recognises the skills demonstrated in the program and is not a third-party vendor credential.

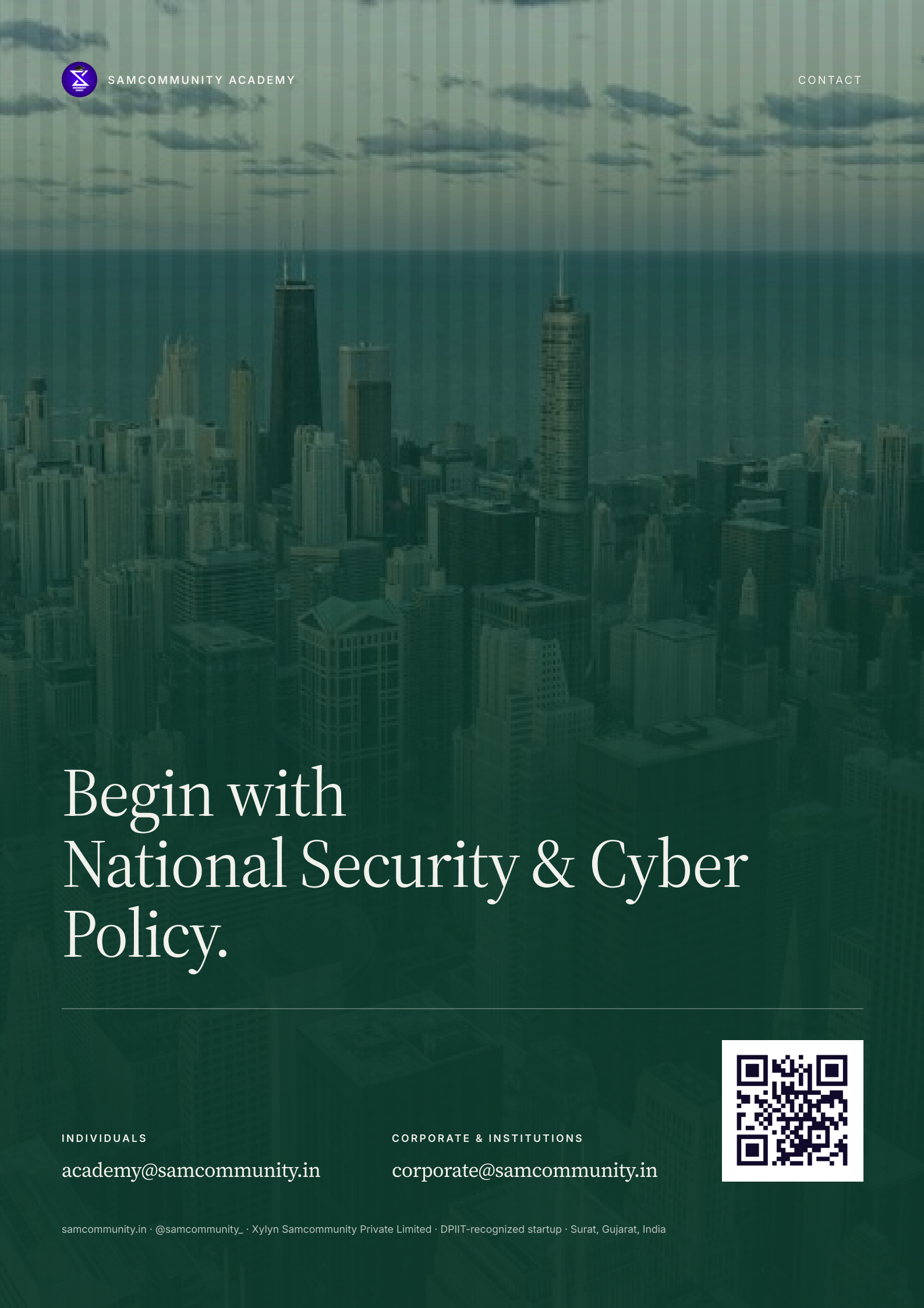
Will I get access to labs, tools and materials?

Yes. Sessions use realistic case studies, board-style simulations, discussion exercises and decision templates. Participants receive briefing materials and reusable frameworks; no technical software or hands-on configuration is required.

Is career support included?

Learners receive guidance on applying the skills at work, including mentor discussions and, where relevant, resume or portfolio feedback. Samcommunity Academy does not guarantee jobs, promotions or salaries; outcomes depend on individual effort.





SAMCOMMUNITY ACADEMY

CONTACT

Begin with National Security & Cyber Policy.

INDIVIDUALS

academy@samcommunity.in

CORPORATE & INSTITUTIONS

corporate@samcommunity.in