Government Capacity Building

Program Brochure · 2026

DEFENCE CYBER OPERATIONS TRAINING

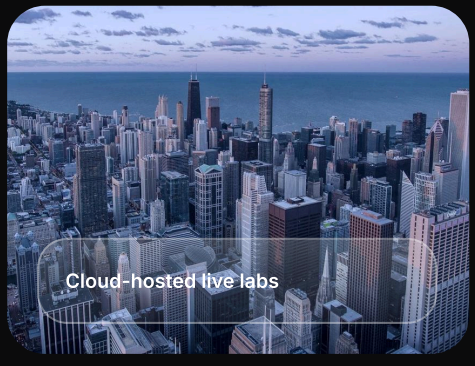
Cyber skills for defence.

Advanced ↗ 72 Hours ↗ SAM-DCO ↗

Government Capacity Building

Capable institutions. Secure nation.

20 programs in this track



8

modules · hands-on labs · capstone project

Inside this brochure

Contents

Program overview 03

Who it's for 04

Learning outcomes 05

Program runway 06

Detailed curriculum 07

Tools & frameworks 10

Projects & capstone 11

Certification & method 12

Learning path 13

FAQs 14



AT A GLANCE

Level	**Advanced**
Duration	**72 Hours**
Modules	**8**
Certificate	**SAM-DCO**

Program overview

Cyber skills for defence.

Specialised cyber operations training for defence and paramilitary personnel.

Cyberspace is now an operational domain alongside land, sea, air and space, and defence networks face persistent, well-resourced adversaries. This program builds specialised defensive cyber skills for defence and paramilitary personnel, covering network defence, threat and adversary analysis, monitoring and detection, vulnerability management, incident response, operational security and coordinated response, practised in isolated training ranges under legal and ethical frameworks.

DELIVERY

Instructor-led · Live virtual · Blended



WHAT YOU'LL PRACTISE

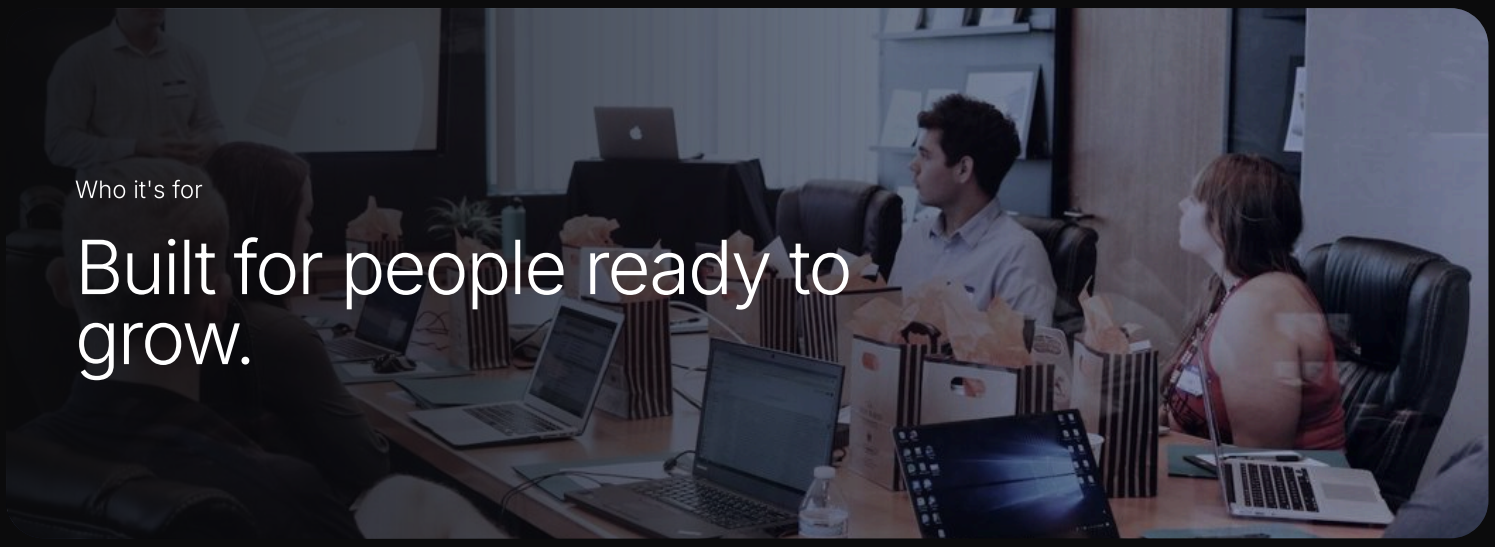
- Understand cyber operations
- Defend military networks
- Analyse threats and adversaries
- Coordinate cyber response

LEVEL
Advanced

DURATION
72 Hours

CERTIFICATION
SAM-DCO

TRACK
Government Capacity Building



Who it's for

Built for people ready to grow.

01

Government officials

Cyber awareness, AI for public service, e-governance

02

Senior IAS / IPS officers

Technology leadership and AI policy

03

PSU workforce

IT security, OT/ICS/SCADA, digital skills

04

Law enforcement & defence

Cyber forensics, CERT ops, defence cyber

PREREQUISITES

Service experience in defence, paramilitary or signals roles	01
Working knowledge of networking and Linux	02
Appropriate security clearance as required	03

ROLES THIS PREPARES YOU FOR

- Cyber defence analysts ↗
- Network security operators ↗
- Threat intelligence analysts ↗
- Incident response team members ↗
- Cyber unit planners and coordinators ↗

Learning outcomes

What you'll be able to do.



01	Explain cyberspace as an operational domain and its legal frameworks
02	Analyse network traffic to identify anomalous or hostile activity
03	Profile adversaries and map their techniques to MITRE ATT&CK
04	Develop and test detection rules for defence network monitoring
05	Respond to simulated breaches while preserving mission assurance
06	Coordinate joint cyber defence response through structured exercises

Program runway

Module by module.

8
modules · 72 hours

01	**Cyber Domain Fundamentals** Cyberspace as an operational domain, Defence network architecture concepts, Cyber operations terminology	9 hrs
02	**Network Defence Foundations** Linux administration for defenders, TCP/IP and protocol analysis, Traffic analysis with Wireshark	9 hrs
03	**Threat Analysis and Adversaries** Threat actor profiling, Adversary techniques with MITRE ATT&CK, Threat intelligence sources	9 hrs
04	**Security Monitoring and Detection** Defensive monitoring architecture, Log analysis and correlation, Intrusion detection concepts	9 hrs
05	**Vulnerability and Exposure Management** Vulnerability assessment processes, Authorised security testing concepts, Risk-based remediation	9 hrs
06	**Incident Response for Defence** Defence incident response lifecycle, Containment in mission environments, Digital evidence handling	9 hrs
07	**Information Operations Awareness** Influence operations and disinformation, Social media threat awareness, Operational security practices	9 hrs
08	**Coordinated Cyber Response** Joint and inter-agency coordination, Command and reporting structures, Cyber exercises and wargaming	9 hrs
★	**Capstone · Defensive Cyber Range Exercise** Assessment, capstone review and certification	

The syllabus.

Modules 01–03

Module 01

Cyber Domain Fundamentals

9 hours

Hands-on lab
Map assets and trust boundaries for a sample defence network

TOPICS COVERED

- Cyberspace as an operational domain
- Defence network architecture concepts
- Cyber operations terminology
- Legal and ethical frameworks
- Rules of engagement concepts

Module 02

Network Defence Foundations

9 hours

Hands-on lab
Analyse captured traffic to identify anomalous communications on a training network

TOPICS COVERED

- Linux administration for defenders
- TCP/IP and protocol analysis
- Traffic analysis with Wireshark
- Secure network configuration
- Hardening military endpoints

Wireshark Linux

Module 03

Threat Analysis and Adversaries

9 hours

Hands-on lab
Map a public threat report to MITRE ATT&CK techniques and defences

TOPICS COVERED

- Threat actor profiling
- Adversary techniques with MITRE ATT&CK
- Threat intelligence sources
- Campaign analysis
- Intelligence reporting formats



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 04–06

Module 04

Security Monitoring and Detection

9 hours

Hands-on lab
Develop and test detection rules against a simulated intrusion dataset

TOPICS COVERED

- Defensive monitoring architecture
- Log analysis and correlation
- Intrusion detection concepts
- Detection engineering basics
- Threat hunting hypotheses

Module 05

Vulnerability and Exposure Management

9 hours

Hands-on lab
Conduct an authorised vulnerability assessment of an isolated lab range

TOPICS COVERED

- Vulnerability assessment processes
- Authorised security testing concepts
- Risk-based remediation
- Configuration auditing
- Secure supply chain

Module 06

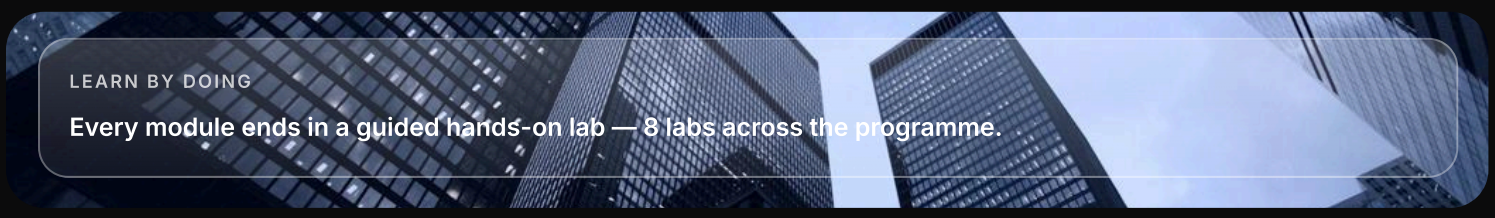
Incident Response for Defence

9 hours

Hands-on lab
Respond to a simulated breach within an isolated defence training range

TOPICS COVERED

- Defence incident response lifecycle
- Containment in mission environments
- Digital evidence handling
- Malware triage concepts
- Recovery and mission assurance



LEARN BY DOING

Every module ends in a guided hands-on lab — 8 labs across the programme.

Syllabus, continued.

Modules 07–08

Module 07

Information Operations Awareness

9 hours

Hands-on lab
Assess an operational security scenario and recommend personnel safeguards

TOPICS COVERED

- Influence operations and disinformation
- Social media threat awareness
- Operational security practices
- Protecting personnel information
- Countering deception

Module 08

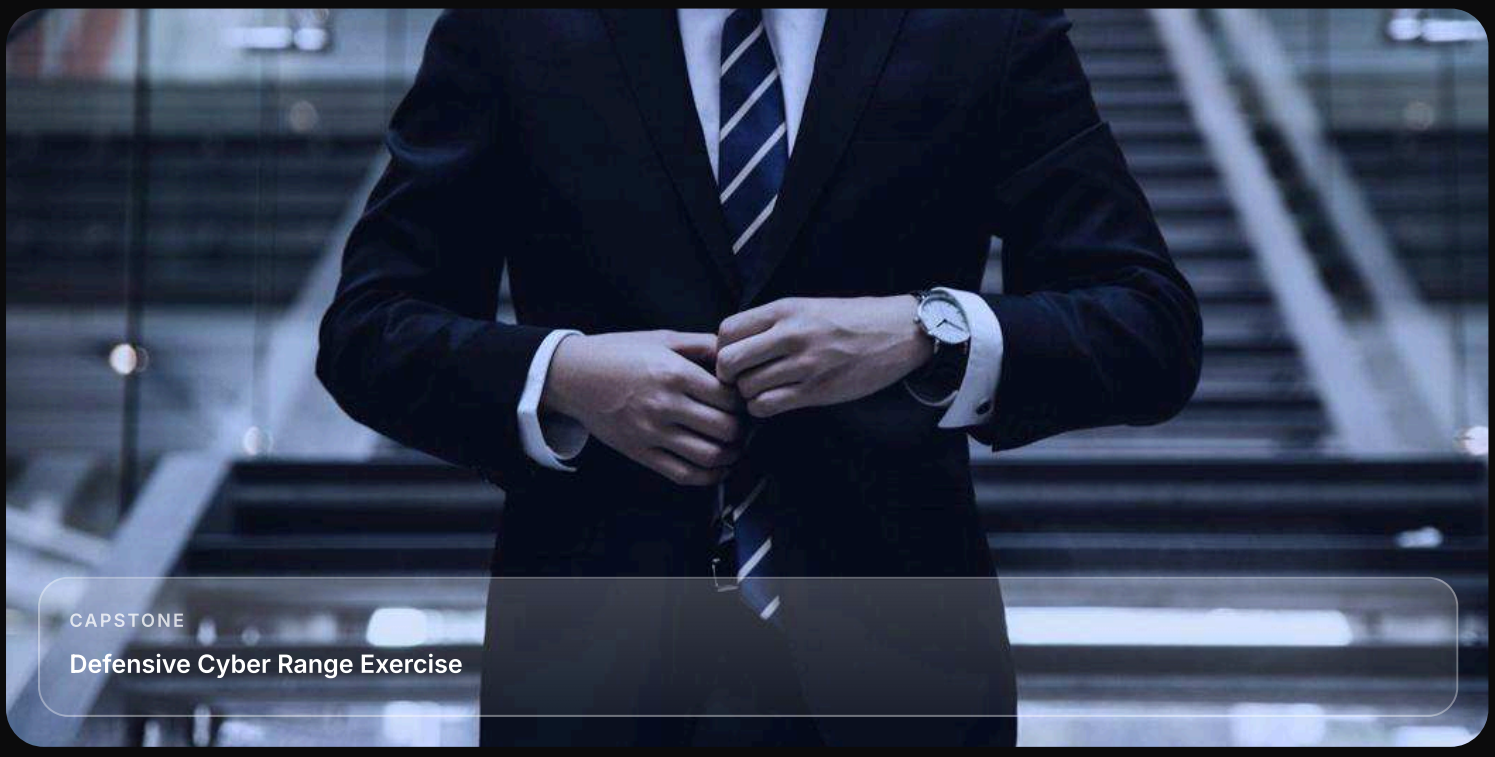
Coordinated Cyber Response

9 hours

Hands-on lab
Participate in a team-based cyber defence exercise with after-action review

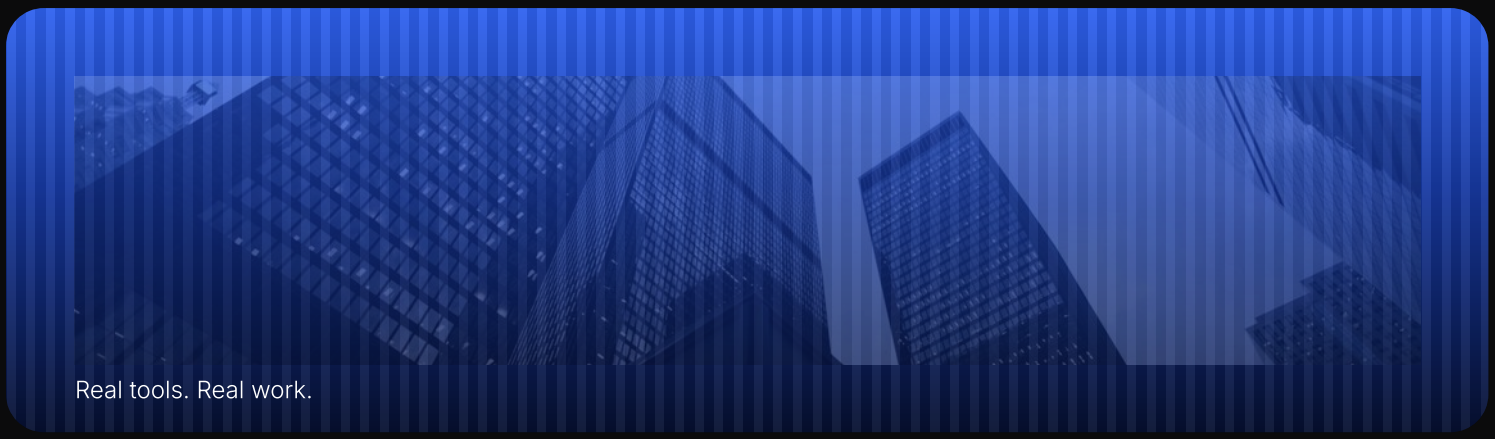
TOPICS COVERED

- Joint and inter-agency coordination
- Command and reporting structures
- Cyber exercises and wargaming
- After-action reviews
- Building cyber readiness



CAPSTONE

Defensive Cyber Range Exercise



Kali Linux
Security testing distribution

Wireshark
Packet capture & traffic analysis

Linux
Server & CLI fundamentals

Frameworks & standards

MITRE ATT&CK

FOCUS AREAS

- Understand cyber operations 01
- Defend military networks 02
- Analyse threats and adversaries 03
- Coordinate cyber response 04



LAB ACCESS

24×7 cloud labs for the length of the program

01

Adversary Technique Mapping

Analyse a public threat report, map adversary behaviour to MITRE ATT&CK and recommend detection and hardening measures for each technique.

02

Detection Rule Pack

Develop, test and document a set of detection rules for common intrusion behaviours using a simulated defence network dataset.

03

OPSEC Risk Assessment

Assess operational security risks in a unit's digital footprint scenario and recommend personnel and procedural safeguards.



Capstone project

Defensive Cyber Range Exercise

Operate as a defensive cyber team in an isolated training range, monitoring the network, detecting and analysing simulated intrusions, containing and recovering affected systems, coordinating reporting through command structures and delivering a structured after-action review.

Real-world scenario ↗ Mentor review ↗ Portfolio ready ↗

Certification

SAM-DCO

Awarded on successful completion of the program assessments.

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



The SAM Learning Framework™

Scenario · Apply · Master · Mentor

Phase 01

Scenario

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

Phase 02

Apply

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

Phase 03

Master

Assessment, peer review and certification prep.

Phase 04

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

Learning path · Government Capacity Building

Where this program fits.

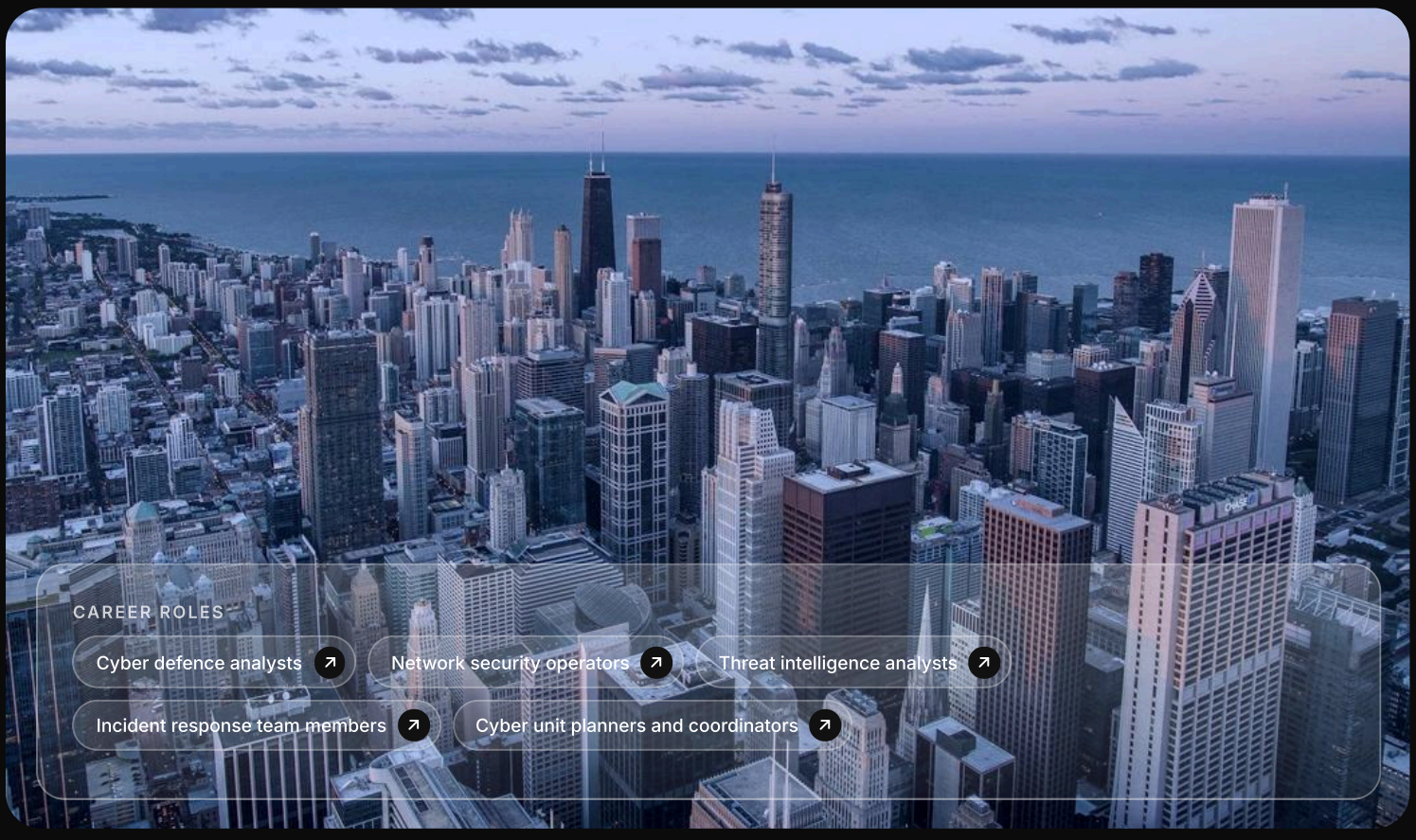
Foundation	Intermediate	Advanced	Expert	Executive
4 programs	5 programs	You are here	1 programs	2 programs

Before this

Digital Governance & e-Governance Platforms	32 Hours
Cybersecurity for Critical Infrastructure	40 Hours
AI Policy & Technology Regulation Workshop	24 Hours
OT/ICS/SCADA Security for Industrial PSUs	48 Hours

Up next

PSU Digital Transformation Advisory	Custom



Questions, answered.

Q01

Do I need prior experience to join?

Yes. This is an advanced-level program that assumes prior experience in networking, Linux and defence IT or signals environments. It moves quickly into frameworks, case studies and hands-on work, so participants should meet the listed prerequisites before enrolling.

Q02

How is the program delivered and scheduled?

The 72 hours program is instructor-led and can be delivered live virtual, in person at your institution, or in a blended format. Session timings and batch sizes are planned with the sponsoring organisation to fit official working schedules.

Q03

Will I receive a certificate?

Yes. Participants who meet attendance requirements and successfully complete the assessments receive the Samcommunity Academy SAM-DCO certificate. Assessments may include quizzes, practical exercises and a final capstone review, depending on the program format.

Q04

Will I get access to labs and tools?

Yes. Hands-on work uses a prepared lab environment with tools such as Kali Linux, Wireshark, Linux. Access details are shared before the program starts, and all exercises run in isolated, authorised environments rather than live production systems.

Q05

Is career or post-program support included?

The program is designed for capacity building of working professionals rather than placement. Participants receive learning resources, templates and guidance on further learning paths. Samcommunity Academy does not guarantee promotions, postings, jobs or salary outcomes.



Let's talk

START DEFENCE CYBER OPERATIONS TRAINING.

academy@samcommunity.in

corporate@samcommunity.in

samcommunity.in

@samcommunity_

Learn practical skills. Grow with mentors.

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